Premier Reference Source

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM

Regner Sabillon

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM

Regner Sabillon
Universitat Oberta de Catalunya, Spain

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Sabillon, Regner, 1967- author.
Title: Cyber security auditing, assurance, and awareness through CSAM and CATRAM : emerging research and opportunities / by Regner Sabillon.
Description: Hershey, PA : Information Science Reference, an imprint of IGI Global, [2021] | Includes bibliographical references and index. | Summary: “This book evaluates the implementation and validation of the Cyber Security Audit Model (CSAM), along with the delivery and inception of the Cybersecurity Awareness TRAining Model (CATRAM) to train personnel on cyber security awareness matter”-- Provided by publisher.
Identifiers: LCCN 2020009695 (print) | LCCN 2020009696 (ebook) | ISBN 9781799841623 (hardcover) | ISBN 9781799856092 (paperback) | ISBN 9781799841630 (ebook)
Subjects: LCSH: Computer security--Management. | Data protection--Management.
Classification: LCC HF5548.37 .S23 2021 (print) | LCC HF5548.37 (ebook) | DDC 658.4/78--dc23
LC record available at https://lccn.loc.gov/2020009695
LC ebook record available at https://lccn.loc.gov/2020009696

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

ISSN:2327-0381
EISSN:2327-0373

Editor-in-Chief: Bryan Christiansen, Global Research Society, LLC, USA
& Agnieszka Piekarz, Independent Researcher, Poland

MISSION

The digital revolution has allowed for greater global connectivity and has improved the way we share and present information. With this new ease of communication and access also come many new challenges and threats as cyber crime and digital perpetrators are constantly developing new ways to attack systems and gain access to private information.

The **Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series** seeks to publish the latest research in diverse fields pertaining to crime, warfare, terrorism and forensics in the digital sphere. By advancing research available in these fields, the **ADCFCT** aims to present researchers, academicians, and students with the most current available knowledge and assist security and law enforcement professionals with a better understanding of the current tools, applications, and methodologies being implemented and discussed in the field.

COVERAGE

- Global Threat Intelligence
- Encryption
- Digital Crime
- Identity Theft
- Watermarking
- Hacking
- Information Warfare
- Telecommunications Fraud
- Digital surveillance
- Cyber Terrorism

The Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series (ISSN 2327-0381) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit:
http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676

Critical Concepts, Standards, and Techniques in Cyber Forensics
Mohammad Shahid Husain (Ministry of Higher Education, Oman) and Mohammad Zunnun Khan (Integral Universit, India)
Information Science Reference • © 2020 • 292pp • H/C (ISBN: 9781799815587) • US $225.00

Utilization of New Technologies in Global Terror Emerging Research and Opportunities
Emily B. Stacey (Swansea University, UK)
Information Science Reference • © 2019 • 141pp • H/C (ISBN: 9781522588764) • US $135.00

Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism
Arif Sari (Girne American University Canterbury, UK)
Information Science Reference • © 2019 • 396pp • H/C (ISBN: 9781522589761) • US $195.00

Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems
S. Geetha (VIT Chennai, India) and Asnath Victy Phamila (VIT Chennai, India)
Information Science Reference • © 2019 • 334pp • H/C (ISBN: 9781522582410) • US $225.00

Mobile Network Forensics Emerging Research and Opportunities
Filipo Sharevski (DePaul University, USA)
Information Science Reference • © 2019 • 337pp • H/C (ISBN: 9781522558552) • US $185.00

Psychological and Behavioral Examinations in Cyber Security
John McAlaney (Bournemouth University, UK) Lara A. Frumkin (Open University, UK) and Vladlena Benson (University of West London, UK)
Information Science Reference • © 2018 • 334pp • H/C (ISBN: 9781522540533) • US $225.00

For an entire list of titles in this series, please visit:
http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676

701 East Chocolate Avenue, Hershey, PA 17033, USA
Tel: 717-533-8845 x100 • Fax: 717-533-8661
E-Mail: cust@igi-global.com • www.igi-global.com

Table of Contents

Foreword

In the current age of information and computing, cybersecurity is a still emerging field of knowledge and practice that has to be consolidated in the daily lives of people, companies and organizations in general. The digital transformation of the information processes where human activities carried out in general that has substantially modified the risks to which these processes are exposed.

The need to protect the value of information, as well as all those aspects related to computing, software, hardware, networks, etc. from malicious attacks or malicious use, it is a requirement that includes increasing complexity. The progress of technology and the sophistication of the media is accompanied by an increase in the sophistication of techniques to compromise standard defense systems as well.

The formidable work of Dr. Regner Sabillon, collected in this book, responds to this need for increasing complexity and provides a wealth of detail at all scales of action and in all areas of activity where information security is potentially vulnerable and requires systematic intervention. The virtue of the book that the reader has in his hands is precisely this triple character: systematicity, exhaustiveness and detail.

Thanks to the extensive review of cybersecurity systems that are being implemented worldwide in different organizations, developed by different corporations, the author proposes Audit and Awareness Training models that are extremely useful and have been successfully applied in several institutions with results that have radically improved the capacity of computer protection.

In this sense, the book provides an overview and detail that completes the deficits of numerous existing manuals that do not go down to concrete practice or propose a systematization of the measures to be implemented and a methodology of proven success in practice.

The exposition of the concepts developed in the book, from National Cybersecurity Strategies to key concepts such as Electronic Discovery

(e-Discovery), Incident Handling and Incident Management, are highly didactic and allows readers from different backgrounds a friendly access to the subjects - Cybersecurity and Cybercrime.

The inclusion of chapters dedicated to the Digital Forensic Analysis of Cybercrimes or the Use of Cyberforensics Tools to Obtain Digital Evidence is an especially interesting aspect to know the expert practice of professionals in the field.

The chapters on The CyberSecurity Audit Model (CSAM) and the Cybersecurity Awareness TRAining Model (CATRAM), represent an exceptional peak in the field of knowledge and a courageous commitment to the definition of a model that multidimensionally evaluates the preparation and implementation phases of cybersecurity systems.

Furthermore, the chapter dedicated to Cyber Warfare and the Challenges that Exist in the Cyber Domain, provides a vision of the challenges faced by cybersecurity that allows experts to have a vision of the main obstacles that still exist. It has to win in the context of globality and global competitiveness.

Undoubtedly, this book is a must-read for advanced specialists or for those who want to get started in the discipline and be able to know the latest on cybersecurity and cybercrime from an expert.

Victor Cavaller
Open University of Catalonia, Spain

Victor Cavaller *is a faculty member in the Department of Information and Communication Sciences at the Open University of Catalonia (UOC).*

Preface

This book provides research models, methodologies, taxonomies and best practices related to different areas of cybersecurity. Cybersecurity involves a mix of science and art to deal with the everchanging cyberthreat landscape. On one hand, organizations must continuously implement, enforce, evaluate and re-adapt security controls to protect their most critical cyber assets to ensure normal operations. And on the other hand, organizations also are searching new ways to implement defensive and offensive cyber strategies to deal with constant cyberattacks from cybercriminals. Cybercriminals are always defining innovative Techniques, Tactics and Procedures (TTP) by adding complexity and increased sophistication to their cyberattacks and cyber target detection.

The most important contribution of our book is the design, research and validation of our two main models in alignment with cybersecurity audit, awareness and assurance:

1. The CyberSecurity Audit Model (CSAM)
2. Cybersecurity Awareness TRAining Model (CATRAM)

The CyberSecurity Audit Model (CSAM) is a comprehensive model that can be implemented by any organization or a team of cybersecurity auditors to conduct partial or complete cybersecurity audits classified by a specific domain, selected domains or the full audit of all domains within any organization. CSAM was designed to be functional for any type of organization, no matter the size nor the industry or sector where the organization is positioned. The CyberSecurity Audit Model (CSAM) is a new exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place. The CSAM

can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO). The aim of this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was envisioned as a seamless and integrated cybersecurity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment for the integration of a national cybersecurity policy, program or strategy at the country level.

The Cybersecurity Awareness TRAining Model (CATRAM) can represent a substantial foundation for the implementation of any organizational cybersecurity awareness program. CATRAM can also review any awareness training model that is steady and updated with the current cyberthreat landscape. The Cybersecurity Awareness TRAining Model (CATRAM) was created distinctively to deliver cybersecurity awareness training to specific groups within any organization. CATRAM was designed to deliver the awareness training for the members of the Board od Directors, Top Executives, Managers, IT (Information Technology) staff and of course, end-users. The Cybersecurity Awareness TRAining Model (CATRAM), is an innovative model that can be implemented at any organization to consolidate the awareness foundations of a corporate Cybersecurity Awareness Program or to start the implementation of an organizational Cybersecurity Awareness Training Program. The Cybersecurity Awareness TRAining Model (CATRAM) has been created to deliver the initial cybersecurity awareness training at any organization or to re-introduce a better awareness training approach to an existing cybersecurity or information security awareness training program.

CATRAM has been designed to provide specific cybersecurity awareness training for personnel:

1. Board of Directors and Executives: Members of this group are trained based on the organizational cybersecurity strategy, governance and program.
2. Managers: Department managers are trained to support and lead cybersecurity initiatives in their corporate environment.
3. End Users: This group gets awareness training to improve cybersecurity practices in the workplace and their personal lives.
4. IT Staff: Information Technology specialists are trained in the use of advanced cybersecurity techniques, methods, procedures and best practices to support the corporate awareness program and the cybersecurity program.

We also contributed to the global scientific community by creating some additional models and taxonomies that are in alignment with certain domains of cybersecurity:

1. Sabillon et al. (2016): Cybercrime Taxonomy
2. Sabillon et al. (2016): Common Types of Cyberattacks
3. Sabillon et al. (2016): National CyberSecurity Strategy Model (NCSSM)
4. Sabillon et al. (2016): Dual Cyber Warfare Model
5. Sabillon et al. (2017): Cyber Forensics Model in Digital Ecosystems (CFMDE)

These models and taxonomies are in alignment with Cybersecurity National Strategies, Digital Forensics, Cybercrime and Cyberattacks prevention, containment, resolution, management and lessons learned.

The material is suitable for information security/cybersecurity researchers, academics, information security/cybersecurity practitioners, IT/ information security/cybersecurity auditors, penetration testers and graduate students specializing in different domains of cybersecurity. This book can be an excellent resource for any library or technical repository for cybersecurity topics as well.

The first chapter presents a comprehensive review of the origin, typologies and developments of Cybercrime and Hacker subculture. This chapter confronts the issues, by describing and discussing different criteria of classification in the field and secondly, providing a broad list of definitions and an analysis of the cybercrime practices. A conceptual taxonomy of cybercrime is described as well. Common categories include where the digital device is the target to commit the crime, where the digital device is used as a tool to perpetrate the

felony, or where a digital device is an incidental condition to the execution of a crime. We complete our study by analyzing lessons learned and future actions that can be undertaken to tackle cybercrime and harden cybersecurity at all levels.

The second chapter introduces a systematic literature review on best practices regarding cybersecurity incident response handling and incident management. The study identifies the most incident handling models that are used worldwide when responding to any type of cybersecurity incident. We highlight the importance of understanding the current cyber threat landscape in any incident response team and their Standard Operations Procedures. The chapter provides guidelines for building a cybersecurity incident team in terms of incident categorization, capabilities, tasks, incident cost calculation and metrics.

The third chapter assesses the most relevant methodologies and best practices for conducting digital investigations, preserving digital forensic evidence and following Chain of Custody (CoC) of cybercrimes. Cybercriminals are assuming new strategies to launch their sophisticated cyberattacks within the ever changing digital ecosystems. We recommend that digital investigations must continually shift to tackle cybercrimes and prosecute cybercriminals, to increase international collaboration networks, to share prevention knowledge and to analyze lessons learned. We also establish a cyber forensics model for miscellaneous ecosystems called Cyber Forensics Model in Digital Ecosystems (CFMDE). This chapter also reviews the most important categories of tools to conduct digital investigations. Nevertheless, as the cybercrime sophistication keeps improving it is also necessary to harden technologies, techniques, methodologies and tools to acquire digital evidence in order to support and make cyber investigation cases stronger.

The fourth chapter reviews the concept of Electronic discovery (e-Discovery), paying special attention to the legally established procedures for consideration as digital evidence, to the computer tools developed for obtaining them, as well as to the historical background that frame its origin. We review techniques and functionalities associated with advanced information systems and describe the possibilities and limits for the evaluation and exploitation of electronic discoveries in the cloud, in social networks, as well as in Bring Your Own Device (BYOD), Big Data or Business Intelligence settings. It also includes a review of the reference frameworks, standards and resources associated with the EDRM Model (Electronic Discovery Reference Model).

The fifth chapter highlights the phases to unify our National CyberSecurity Strategy Model (NCSSM) in any Nation Cyber strategy that is either under

development or improvement stages. This methodology consists of developing international cybersecurity strategies, alliances and cooperation with different stakeholders at all possible levels. Our research evaluated the best practices of ten leading countries and five intergovernmental organizations in terms of developing effective cybersecurity strategies and policies. We also assessed a series of cybersecurity best practices that can be aligned with cyber governance and cyber law when countries wish to develop or enhance national cyber strategies. Furthermore, we propose guidelines to audit the national cyber strategies by utilizing our CyberSecurity Audit Model (CSAM). CSAM could be considered for conducting cybersecurity audits in any Nation State in pursuance of reviewing and measuring the cybersecurity assurance, maturity and cyber readiness and to detect the needs to increase cyber awareness to defend and protect critical cyber assets.

The sixth chapter examines the cyber warfare phenomenon in all its dimensions in order to provide a wide conceptualization of factors and elements, strategies, generations and theoretical models. On the second part of the chapter, a set of definitions is introduced in order to gain a common field of conceptual agreement for the explanation of the main theoretical models that have been developed for the Cyber domain. The third section presents the Dual Cyber Warfare Model applicable to military and corporate environments. We conclude that cyber Warfare is perhaps the most radical consequence of the Knowledge Era and must be systematically analyzed from both perspectives: empirical-practical and theoretical-conceptual.

The seventh chapter provides a comprehensive literature review of the most relevant approaches for conducting cybersecurity audits. The study includes auditing perspectives for specific scopes and the best practices that many leading organizations are providing for security and auditing professionals to follow. The chapter reviews relevant features for auditing approaches in the following order: ISO/IEC 27001:2013; ISO/IEC 27002:2013; Control Objectives for Information and Related Technology (COBIT) 2019; Information Technology Infrastructure Library (ITIL) 4, AICPA; ISACA; NIST SP 800-53; NIST CSF v1.1; IIA; PCI DSS; ITAF; COSO; ENISA; NERC CIP and CSAM.

The eighth chapter produces presents the outcome of two empirical research studies that assess the implementation and validation of the CyberSecurity Audit Model (CSAM), designed as a multiple-case study in two different Canadian higher education institution. CSAM can be applied for undertaking cybersecurity audits in any organization or Nation State in order to evaluate and measure the cybersecurity assurance, maturity and cyber readiness.

The architecture of CSAM is explained in central sections. CSAM has been examined, implemented and established under three research scenarios (1) Cybersecurity audit of all model domains (2) Cybersecurity audit of numerous domains and (3) a single cybersecurity domain audit. The chapter concludes showing how the implementation of the model permits to report relevant information for future decision making in order to correct cybersecurity weaknesses or to improve cybersecurity domains and controls, thus the model can be implemented and sufficiently tested at any organization.

The ninth chapter introduces the results of of one empirical research study that assess the implementation and validation of the Cybersecurity Awareness TRAining Model (CATRAM), designed as a multiple-case study in a Canadian higher education institution. Information security awareness programs have become unsuccessful to change people's attitude in recognizing, stopping or reporting cyberthreats within their corporate environment. Therefore, human errors and actions continue to demonstrate that we as humans are the weakest links in cybersecurity. The chapter studies the most recent cybersecurity awareness programs and its attributes. Furthermore, we compiled recent awareness methodologies, frameworks and approaches. The Cybersecurity Awareness TRAining Model (CATRAM) has been created to deliver training to different corporate audiences, each of these organizational units with peculiar content and detached objectives. We concluded our study, by addressing the necessity of future research to target new approaches to keep cybersecurity awareness focused on the everchanging cyberthreat landscape.

This publication is very relevant for any organization that is just starting implementing cybersecurity controls or any Company that has a mature Cybersecurity program wanting to continuously improve their cybersecurity function and practice. It is aimed for researchers but also for cybersecurity practitioners and auditors wishing to improve and audit cybersecurity at operational, tactical and strategic levels.

Chapter 1
Cybercrime and Cybercriminals

ABSTRACT

The rising expansion and diversification in the cybercrime arena have become difficult obstacles in order both to understand the extent of embedded risks and to define efficient policies of prevention for corporations, institutions, and agencies. The present study represents a comprehensive review of the origin, typologies, and developments of cybercrime and hacker subculture. This chapter confronts the issues by describing and discussing different criteria of classification in the field and by providing a broad list of definitions and an analysis of the cybercrime practices. A conceptual taxonomy of cybercrime is described as well. Common categories include the digital device is the target to commit the crime, the digital device is used as a tool to perpetrate the felony, or a digital device is an incidental condition to the execution of a crime. The authors complete their study by analyzing lessons learned and future actions that can be undertaken to tackle cybercrime and harden cybersecurity at all levels.

HISTORY

From the *Jargon file*, a globally recognised lexicon of hacker slang. The following entry refers to the "Hacker Culture":

DOI: 10.4018/978-1-7998-4162-3.ch001

The 'hacker culture' is actually a loosely networked collection of subcultures that is nevertheless conscious of some important shared experiences, shared roots, and shared values. It has its own myths, heroes, villains, folk epics, in-jokes, taboos, and dreams. Because hackers as a group are particularly creative people who define themselves partly by rejection of 'normal' values and working habits, it has unusually rich and conscious traditions for an intentional culture less than 50 years old.

The Hacking term has its roots at the Massachusetts Institute of Technology (MIT), when it was coined by MIT students to attribute the development of novel techniques to identify computer shortcuts or clever pranks; the term was also popularized in the film WarGames (1983) –and the hacker subculture exploded (Britz, 2009).

In the late 1950s, computing and programming developments took place in universities where the term hacker was coined at MIT, Cornell and Harvard where they developed elegant solutions to existing problems in slow-operating mainframes (Levy, 1984). Pioneer hackers helped by speeding up the processes used in developing techniques by removing lines of code in existing programs. These skills and their hacking tasks were recognized as a sign of respect (Furnell, 2002).

The hacker conception moved into the 1960s from universities into military operations. Many programmers were angry because of the overall existence of military applications, despite their work was mostly funded by the USA military and federal government (Thomas, 2002).

In the 1970s a shift occurred with the phone systems hacking known as "phone pheaking". This practice involved tampering with telephone systems and phone technology to make free calls to anyone worldwide by controlling telephone system switches (Landreth, 1984); these individuals were known as *phreaks*. Also during late seventies, the first computer Bulletin Board System (BBS) was created – allowing the online interaction and communication between hackers.

During the 1980s, the hacker ethic was challenged due to major technological inventions like personal computers and modems. The exploration of computer networks and online interaction outside university and business environments allowed the proliferation of online users and the participation of underground hackers (Furnell, 2002).

Hacker subculture became more divided when "The Hacker Manifesto" was published originally as "The Conscience of a Hacker" by a notorious member of the hacker group Legion of Doom called "The Mentor". This

created different beliefs within the hacker communities as was opposed to the Hacker's Code of Ethics of Levy (1984):

- Access to Computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust Authority - Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

By mid-to-late 1980s, several malicious hacker attacks took place and became the focus of law enforcement agencies. High profile hacker attacks happened during the 1990s. The technology progress provided user friendly systems, access to the Internet and the World Wide Web (WWW).

By mid 1990s, new generations were attracted to hacking with the release of a new film "Hackers" – in 1995 (Holt, 2005). The movie highlights that a young boy (age 11) a.k.a. Dade "Zero Cool" Murphy crashed 1,507 systems in one day and caused a single day operations drop of the New York Stock Exchange. The movie presents how this hacker and his group were able to hack and crash several government systems without finding enough evidence to prosecute them. This film helped to reinforce the notion that hackers are criminals.

Nowadays, the growth of the hacker subculture and latest advancements in Information and Communications Technology (ICT) have divided hackers even more as they all have different motivations, activities and affiliations. In addition to this, we can identify several sorts of hackers, each with their own agenda and propaganda.

HACKER SUBCULTURE

While the *"hacker"* term meaning has changed over the last decades, the conceptualization of the activities of this group is mostly seen as dark, evil, operating in underground environments and particularly with intentions to cause damage against society's information systems.

The main agents in cybercrime activities are hackers. Their motives can be from just having personal fun – like script kiddies defacing websites and breaking access passwords, to the satisfaction of being recognized as an elite hacker by breaking cybersecurity and stealing from Fortune 500 Companies.

The Hacker subculture is a global convoluted community that encircles multiple motivations, idealism and skill set. When analyzing digital crime can be possible to understand the hacking types and their behaviour motivation; thus predict future cybercrime activities. Like in a chess game, a good strategy is that the *best offense is a good defense* – then we can apply this strategy to defend our information systems and at the same time will provide us with an insight on how the criminal mind of hackers will react.

One of the best methods to understand the hacker mentality is to examine research based on the social psychology theory. This utilizes a broad range of specific theories for several social and cognitive phenomena. In addition, other fields apply psychological profiling to figure out common crimes. Further research is required to study the implications connecting psychological theory with cybercriminality – this can include some dominant factors like social learning in their hacking groups and justification of outlawed activity.

Hacker Profiles

Rogers (2001) compiled from different studies some profiles from hackers that have either been caught, come to the officials' attention or were volunteers to be interviewed. He clarifies that these individuals are a small portion of the overall hacker community and as such, the outcome of these studies cannot be considered generalized to the whole community. The current profile from these studies indicate that hackers are predominantly Caucasian, 12-28 years old, members of middle-class families, with limited social skills and are low academic achievers. While they show a strong aptitude with computer and electronic devices; these hackers are not career- oriented.

They come from families that are often dysfunctional, single parent, physically and emotionally abusive and in some cases sexually abusive. These hackers recurrently display compulsive behaviour, like staying online for days or end without sleep. They use computers as a method to gain control over a certain portion of their lives. Hacking is a solitary activity that allows individuals to be the master over the machine. As there is no face-to-face interaction on the Internet, they tend to claim whomever they wish to be, giving them the opportunity to be someone with power and prestige. This is

reflected in the use of nicknames taken form from science fiction or science fantasy.

These hackers appear unhappy with their surroundings and use the computer as a mean of escaping from reality. They are lonely people, yet they have a strong need to belong to a larger social group. This membership is mostly virtual in nature and hackers attend conventions and are subscribed to various hacker publications. Individuals engaged in hacking activities have a tendency to brag about their exploits; they desire to be admired by their hacking peers. Nevertheless, this attitude attracts the attention of law enforcement and consequently drags them to be arrested.

The documented attacks of hackers were malicious in nature, which suggests that these people have unsettled anger and need to strike out at something or someone. That is the reason why, they strike out at computers and networks, justifying that corporations are immoral and need to be taught a lesson. Hackers from these studies claimed that they were motivated by challenges, the excitement to succeed and a desire to learn for intellectual satisfaction. In spite of, some hackers showed vengeance, sabotage and fraud to be the motivating factors. The most common attack that they tend to target is the defacing of websites and is a type of virtual vandalism or virtual graffiti.

The *Jargon File* (2004) is a computer programmer slang document that describes the hacker subculture and the hacker lifestyle. *Appendix B. A Portrait of J. Random Hacker* highlights likes and dislikes of the hacker community members. This document provides overview of some topics like appearance, dress, reading habits, interests, education, food, politics, gender, religion, communication style and personality characteristics.

It is important to emphasize that hackers do not get to be the way they are by imitating each other. Hackerdom is an intentional subculture, as each individual must choose by action to join.

TYPES OF HACKERS

There are a lot of hacker categories; these categories include different terminology and iconography that create controversy over the computer attacker terms. The media and general public refer to people who are responsible for attacking and damaging computer systems as “hackers”. But using the term hacker to label a cybercriminal or computer vandal denigrates the term as well the historic concept. Most of hacker online activities are perfectly legal; the

difference between hackers, hackers who commit crimes and cybercriminals rest upon their attitudes when a hacker accepts the activity and the motives.

McQuade III (2006) compiled from different researchers the categorization of cybercriminals:

M.L. Lee (1991) identified hackers, crackers, phreakers and software pirates. Young (1995) argued that there were utopians- contributors to society by exposing security vulnerabilities; cyberpunks- malicious people that cause damage to websites and cyber assets; cyberspies- those who engage in surveillance of computing activities of several groups; and cyberterrorists- capable of disrupting critical information infrastructures to cause harm in order to advance their political agendas. Parker (1998) observed the following categories: pranksters- who perpetuate risks; hackers- who idealize the original hacker ethic; malicious hackers- who intend to cause harm; personal problem solvers- who often resort to crime by avoiding lawful practices; career criminals- who support themselves via cybercrimes; extreme advocates- known as cyberterrorists and malcontents, addicts, irrational and incompetent persons – a category for all other type of cybercriminals. Denning (1999) categorized cyberactivists- who legally use the Internet to protest and advocate for social and governmental reforms; hacktivists- who perform illegal activities against computer systems and cyberterrorists (meeting Young's description). Wall (2001) described four categories: cybertrespassers- offenders using hacking and cracking activities; cyber deceptionists and thieves- referring to online criminality actions; cyberpornographers- who are actively trading sexually explicit content and cyberviolents- those who are involved with online stalking and harassment. And, Castellano (2004) identified five discrete types of cybercriminals: hackers- who cause computer's system harm; harassers- who use computer to harass people; pirates- who are online thieves; academic cheats- who use computers or electronic devices to plagiarize or cheat in academic environments and data snoops- who gain unauthorized access solely to look at data and files.

Crume (2000) points out that hacker category can be organized in a pyramid. The novice hackers make up the largest segment of the hacker population, hackers in this group are sometimes are 'script kiddies' due to the fact that they mostly rely on computer scripts developed by more knowledgeable hackers to execute their attacks. Intermediate hackers have a better understanding of what they are doing when perpetrating computer attacks. And Elite hackers are capable of penetrating most systems and take advantage of computer exploits.

The SANS Institute (2004) based on previous researcher's work have determined various categories and subgroups of hackers:

Categories

White hats: These individuals work within the laws of the hacker ethic (to do no harm) or as security experts.

Gray hats: This term was coined by L0pht – one of the best known old school hacking groups. These hackers are reformed Black Hats now working as security consultants. They want to stand apart from corporate security analysts and also distance from the Notorious Black Hats.

Black Hats: These hackers are motivated by power, anger or hate. They do not have any qualms to steal or destroy network data that they penetrate.

Classes

These classes of hackers are under both Black Hat and White Hat categories:

Elite: They have the knowledge and skills of the highest level. This status can be gained by a particularly famous exploit, hack or longevity on the scene.

Script Kiddies: The most scorned subgroup within the larger hacker community. These tend to be the least skilled and youngest members using the tools created by elite hackers. Script kiddies have no particular motivation than to seek out easy targets.

Cyber-terrorists: They use stenography and cryptology for exchanging information and sharing plots online. These hackers are considered to become the most serious of computer criminals.

Disgruntled (ex) employees: one of the most dangerous, least publicized groups. These people believed they were owed special recognition for their corporate work and would take revenge for the lack of it.

Virus Writers: This group tends to exploit weaknesses found by hackers, then code methods to execute computer flaws.

Hacktivist: This name derives from combining the words 'activism' and 'hacking'. One of the fastest growing hacker subgroups, which are motivated to deface websites and launch Denial of Service (DOS) attacks to satisfy political, religious and social agendas.

The EC-Council (2014) has created a different taxonomy based on Hacker classes. They highlight the differences between regular hacking versus ethical hacking. This categorization includes eight different classes:

Black Hats: Hackers with excellent computing skills that are attracted to malicious activities. Their motives are to cause damage, steal information, destroy data and earn money.

White Hats: Individuals with hacking skills those act to protect networks in a defensive way. They work is corporate environments as security analysts.

Gray Hats: Hackers that work both offensively and defensively at different situations.

Suicide Hackers: Hackers that aim to bring down critical infrastructure for radical causes and are not afraid to go to jail. They are related to suicide bombers and are active member of cyber terrorism groups.

Script Kiddies: The most unskilled hackers that are not well versed in hacking techniques. They tend to focus in getting high quantities of attacks rather than performing quality attacks.

Spy Hackers: These hackers are on contract to penetrate and gain trade secrets of their employer's competitors.

Cyber Terrorists: These could be people or organized groups that are motivated by political or religious motives to cause harm by disrupting large scale computer networks.

State Sponsored Hackers: State sponsored hackers that are employed to damage other countries' networks and information systems.

Chiesa et al. (2009) have created a hacker categorization that was adopted by the UNICRI (United Nations Interregional Crime and Justice Research Institute, 2014):

Wannabe (Lamer): These individuals want to be hackers. Their modus operandi involves using "hacker toolkits" without knowing how the tools work. Their actions usually result in causing huge damages to some networks.

Script kiddie: The term means 'The boy from the scripts' – relaying on UNIX/Linux shell scripts written by elite hackers. They are not very technically skilled and lack sophistication on their attacks. The least capable are called "point-and-clickers".

Cracker: This term was created in the early 1990s, to identify malicious hackers and differentiate them from the hacker community. In general terms, they have good technical skills. They try to take control of systems and when in danger, they will erase files, logs and any kind of trace.

Ethical Hacker: These are white hat hackers that help the community, by digging with software and discovering flaws used in IT infrastructures.

QPS (Quiet, Paranoid, Skilled Hacker): These hackers break into systems mostly by curiosity, likely to get access to new application versions or technological tools. Their acts are very similar to ethical hackers.

Cyber-warrior/Mercenary: This category is product of the Internet's globalization and the "hacktivism" phenomenon. Russian mobs such the RBN- Russian Business Network hire these individuals to support unlawful operations.

Industrial Spy Hacker: This practice has its roots within industrial espionage. These hackers modernized their techniques using Information Technology to steal Intellectual Property, inventions and patents.

Government Agent Hacker: These individuals or groups can work for specific government purposes that can compromise national cybersecurity.

Military Hacker: This is a polemic category that was created by the HPP – *Hackers Profiling Project* in 2004. These hackers have association with state-sponsored attacks and cyberwarfare.

Warren and Leitch (2009) have created an additional hacker category that was not considered before. The researchers have identified a sub group of hackers called "Hacker Taggers". These hackers like to deface websites with the intention of leaving a 'hacker tag' or 'calling card' behind. This tag or card is updated to show hacker's individual scores. The website Zone-H (www.zone-h.org) contains an archive of website defacement history since 1999. This group of hackers are very competitive, hold a strong desire to succeed, cause minimal damage to websites, rely on media reports to cause embarrassment or political harm and work as individuals or as a group.

In terms of hacker categories and classes, our research concludes that there is not a globally accepted categorization of hacker groups nor classes. While many organizations have agreed on certain categories, that intend to group hackers by their motives and actions. We agree that the most common categories are black, grey and white hat hackers and any resulting sub-categorizations are based on specific motives, propaganda, hacktivism, political or religious reasons.

FAMOUS HACKERS

Kevin Mitnick

Even though, he trumpeted himself as a "Social Engineer" than a hacker, he preferred to use persuasion, influence and manipulation to obtain information from influential people and Companies. He broke into various systems, online databases, cellular phones networks, credit card repositories, secret project

data and personal information. He performed many hacks between 1987 and 1995 with an estimated damage of USD 1 million.

He was prosecuted twice and spent five years in jail in two different periods; 1988 and 1995 – He was not allowed to use the Internet for three years. His targets included Digital, SCO, NetCom, Motorola, California Department of Motor Vehicles, Fujitsu, Nokia, Sun microsystems and NEC. He is now a rehabilitated hacker working as a security consultant.

Kevin Poulsen

As a teenager, he discovered to whistle into payphone systems to get free calls. His most remarkable hack was when he took over a radio station's phone system (KIIS-FM) in Los Angeles to make sure he would be the 102nd caller to win a Porsche 944 S2. He earned the distinction of being the first hacker accused of espionage. His call sign was Dark Dante. Other hacks included the US Air Force and Pacific Bell. He was sentenced to fifty one months in jail; after he was released from prison, he gave up hacking and became a journalist- he is the Senior editor at Wired magazine. He designed and developed Secure Drop, an open-source application for secure communication between journalists and their sources.

Adrian Lamo

He gained notoriety in 2001 after hacking into internal networks of Excite@ Home, MCI WorldCom, Yahoo, Microsoft and Google. He contacted these companies to inform them about the security holes. He was known as "the homeless hacker" as he travelled the USA by Greyhound bus and stayed in abandoned buildings. He hacked into *The New York Times* – he avoided jail time by negotiating a plea bargain that included six months of house arrest. He was diagnosed with Asperger disorder, an autism category associated with individuals of high intellectual coefficient who have trouble to socialize. In recent years, Lamo reported Bradley Manning to the police. Manning funneled thousands of classified documents to the whistleblower organization WikiLeaks.

Leonard Rose

He was convicted in 1991 with two counts of wire fraud, stemming from publishing an article he wrote for *Phrack Magazine* about Trojan Horses. The incidents took place between May, 1988 and January, 1990. He spent twelve months and one day in jail. He was known as "Terminus"; Leonard was accused of being the leader of the Legion of Doom hacking group. This Unix group pioneered the hacking of AT&T telephone networks using brute-force dictionary attacks.

Julian Paul Assange

This Australian editor and publicist is famous for his founding role of WikiLeaks – a website that publishes worldwide secret information. WikiLeaks have broken stories about war, killings, torture, detention, governments, trade, suppression of free speech/press, diplomacy, spying, counter-intelligence, ecology, climate, nature sciences, corruption, finance, taxes, trading, censorship technology, Internet filtering, cults, religious organizations, abuse, violence and violations. As a teenager, he hacked the Pentagon, USDoD, MILNET, US Navy, NASA, Citibank, Lockheed Martin, Motorola, Panasonic and Xerox, and published US military documents. His pseudonym was "Mendax" and was a member of the International Subversives Group. He was charged in 1994 with thirty one counts of hacking. He pleaded guilty to twenty five charges and paid reparations of AU$ 2,100. He was released from jail on good behaviour bond.

Michael Calce

MafiaBoy was his cyberspace alias when he launched a series of Denial of Service (DoS) attacks to large commercial websites including Fifa, Amazon, Yahoo, Dell, ETrade, eBay and CNN. He initially denied the accusations but accepted his offenses later. He was a Quebec high school student when he performed all his hacks in 2000. He was discovered by the FBI and the Royal Canadian Mounted Police (R.C.M.P.) when he bragged about his attacks on IRC chatrooms. He was sentenced to eight months to open custody, one year of probation, restricted use of the Internet and a small fine.

Ehud Tenembaum

This Israeli cracker also known as *The Analyzer* was arrested for hacking NASA, The Pentagon, US Air Force, US Navy, Knesset, MIT and various American/ Israeli universities. Other hacks included terrorist groups based in Palestine and destroyed websites of the Islamist organization called Hamas. In 2001, he was sentenced to year and half, from he only served eight months and later pardoned by the Deri Law. After his prison time, he had other incidents involving credit card fraud in 2008. In 2009, he was extradited to the USA, trialed and convicted for more than a year. He was arrested again in 2013 for laundering millions of Israeli shekels.

Robert Morris

In 1988, while an undergraduate student at Cornell University, he wrote and launched the destructive Morris worm in an attempt to measure how big the Internet was at that time. The worm infected 6,000 Unix-based computers, which were 10% of the entire Internet. The estimated damage was US $ 97 million. He was the first person prosecuted under the 1986 Federal Computer Fraud and Abuse Act – Morris served three years probation, 400 hours of community service and paid $ 10,000 in fines. He is a rehabilitated hacker and is now a professor at MIT Computer Science and Artificial Intelligence Laboratory

HACKTIVISM

There is no doubt that *Anonymous* is the most powerful global hacking group, nevertheless there are a number of less popular hacker groups that fight for certain political, religious, warfare or espionage motives.

Here are some of the global active hacking groups:

- **Deadeye Jackal:** They are also known as the *Syrian Electronic Army (SEA)*. According to Crowdstrike (2013) this group formed in May 2011. This group's illegal activities include Facebook spamming, disruptive attacks, website defacements and to support Assad's regime by slanting messaging about the Syrian conflict. Deadeye Jackal have launched cyberattacks against *The Associated Press (AP), Truecaller.*

com, TangoME Inc., Viber Media Inc., Outbrain, Melbourne IT, The New York Times, The Washington Post, the Financial Times, NPR, twimg, Twitter feeds for Reuters, BBC Weather, SocialFlow, HootesSuite, the State of Qatar, Saudi Arabia's Ministry of Foreign Affairs, NBC, Tribune Company, U.S. GovDelivery and Vice.com.

- **Numbered Panda:** A Chinese hacktivism group that is focused on infiltrating U.S. Companies. They are orchestrating spear phishing campaigns by targeting current or upcoming global events like the G-20 Summit. This group have created malware like the *ShowNews* and *3001*. ShowNews conducts basic machine reconnaissance and record keystrokes typed by the victim. And *3001*, a Remote Access Trojan (RAT) that contains a complete command set including downloading, uploading, executing files, remote shell and self-deletion. This Trojan horse did not embrace persistent mechanisms; this allows having a low profile of the Trojan but it will need to be reinstalled after every computer reboot.
- **Magic Kitten:** This is an Iranian hacking group; its origin may have started in 2009. This group usually targets political motives and international technology sector corporations. Their vector include Windows executables, spear phishing, malicious Word documents and exploiting images files by using Right-to-Left Override (RLO) tricks. This exploits the Unicode encoding system, especially the RLO character (U+202E) to support languages written from right to left such the Arabic and Hebrew.

Their recent activity was between May and June 2013 by targeting Iranian political dissidents and people supporting Iran's political opposition.

- **Energetic Bear:** This is a cyberthreat group from the Russian Federation that specializes in intelligence collection operations and mining data within the global energy sector. They utilize two Remote Access Trojans called HAVEX and SYSMain. There have been discovered more than 25 versions of the HAVEX RAT; each version is installed as DLL with a name starting with "TMPprovider".
- **Emissary Panda:** This China based hacking group has been very active since the Q4 of 2013.They exploit vulnerabilities to gain access to web servers; their attacks included defense technology companies, US foreign embassies, political peace organizations. They have used

JQuery injection attacks. Some malware from this group are called HttpBrowser and PlugX.

Motivation

Describing a typical cybercriminal stereotype and its motives is almost impossible, mostly because cybercrime agents act based on one or several motives.Some motives entail curiosity, fun, satisfaction, publicity, manipulation, destruction, revenge, ego gratification, hacktivism, nationalism, radicalism, religion, politics, and financial benefit.

In fact, the SKRAM (Skills, Knowledge, Resources, Authority, Motivation) model can calculate the threat potential of cybercriminals using their skills, knowledge, resources, authority, intensity of motives and countervailing information assurance linked on technological and human factors. The formula is (S*K*R*A*M) / IA where these factors have impact on the amount and time under certain circumstances of the cybercriminal's capabilities.

CYBERATTACK CLASSIFICATION

We base our study on previous research work (*Table 1*) from practitioners, scholars and industry experts. Arief et al. previously studied cybercrime on two different perspectives: Part 1 from the attacker's side and Part 2 for defenders and victims. Chawki et al. focused on cybercrime and its management issues. Cardwell et al. studied theft of intellectual property,

Table 1. Previous studies on cybercrime and cyberattacks

Authors	Insight about their taxonomy
Arief, Adzmi and Gross (2015)	Taxonomy about stakeholder's involvement: attackers, defenders and victims
Chawki, Darwish, Khan and Tyagi (2015)	They studied the cybercrime fundamentals, computer systems a targets, computer systems as tools, content-related offences and cyberspace anonymity including privacy, security and crime control
Cardwell et al. (2007)	Comprises the 3 Ts: tools to commit crimes, targets of the victim and tangential material to the crime. They categorized cybercrime using insider and external attacks.
Britz (2013)	Typology included early hackers, theft of components, neotraditional cybercrime, identity theft/fraud, cyberterrorism and its links with the organized crime
McQuade, III (2006)	Categories of IT abusers and cybercriminals are negligent users, traditional criminals, fraudsters, hackers, malicious code writers, media pirates, harrasers, cybersex offenders, academic cheats, organized criminals, freelance spies and cyberterrorists

damage of corporate networks, financial fraud, hacker system penetration and execution of viruses and worms. Britz introduced traditional computer crime, contemporary computer crime, identity theft, identity fraud, cyberterrorism and technological organized crime. Mc Quade, III categorized cybercriminals based on the nature of their cybercrimes.

Our cyberattack and cybercrime taxonomies are established on current threats, vulnerabilities, hacker subculture, risks, impact, technology and human factors. With those principles in mind, our efforts must be oriented towards the safeguarding of the cybersecurity triad that encircles confidentiality, integrity and availability.

Nowadays, cyber vulnerabilities are exploited using simple, sophisticated or a combination of several cyberattacks. In this section, we present (Sabillon et al., 2016) the most common type of cyberattacks, we need to understand that as technology evolves new risks and threats will lead to more advanced Techniques, Tactics and Procedures (TTP) to system's hacking.

1. **Advanced Persistent Threats (APT):** The term Advanced Persistent Threat was coined in 2005 by an USAF security analyst. According to the US National Institute of Standards and Technology (NIST), an APT is an adversary that possesses sophisticated levels of expertise and significant resources to create opportunities to achieve its objectives using multiple attack vectors. It pursues objectives over an extended period of time; adapts to efforts of the defenders and maintains an adequate level of interaction aligned with its objectives. The attack cycle encircles target selection, target research, target penetration, command and control, target discovery, data exfiltration, intelligence dissemination and information exploitation.
2. **Arbitrary/remote code execution:** Attackers use techniques to install malware remotely in order to take partial or complete control of a system.
3. **ARP poisoning:** Address Resolution Protocol poisoning misleads interconnection devices about the real MAC of a machine. ARP contains only two types of messages: ARP request and ARP reply. Attackers create ARP reply packets using spoofed MAC addresses to poison ARP cache on any network system. VLAN segregation prevents this type of attack.
4. **Bluejacking:** It is the process of sending text messages using a private Bluetooth device without the owner's consent. In addition to text messaging, some Bluetooth devices can include sound. The best security strategy is to operate the device in a non-discovery mode.

5. **Bluesnarfing:** Unauthorized access to a Bluetooth device or data theft from any Bluetooth connection. This attack will take place as long the device is on and set to discovery mode. Linux users can launch this type of attack using hcitool and ObexFTP tools.
6. **Buffer overflow:** This usually happens whenever an application receives more input than it can handle. The result is a system memory error that exposes a vulnerability that later can be exploited to write malicious code. Normally the sequence attack is primarily causing the buffer overflow, then is sending a long NOOP (No Operation) command, inserting the malicious code and finally by triggering the code execution.
7. **Client-side attacks:** This type of attack can be launched using a client application aiming to access specific servers or databases. This can be avoided if proper input validation and stored procedures are in place. Client-side attacks are based on transitive trust access that allows forest trust relationships in all Active Directory domains.
8. **Cookies and attachments:** Cookies can store web browsing history and sensitive data including usernames, passwords and session IDs that are instrumental for additional attacks like session hijacking. Malicious attachments can trigger malware attacks like viruses, Trojans and worms.
9. **Cross-site Request Forgery (XSRF):** Attackers fool users by creating malicious HTML links and redirecting the victims to perform specific actions. A security measure is to create expiration cookies and to prevent automatic log on.
10. **Cross-site Scripting (XSS):** This attack redirects end users to malicious webpages, by encoding <or>, <img>, <and> tags and embedding HTML or JavaScript code into websites or emails. Once the link is open then the code will run on the user's computer. Local cookies can be read after the script is executed. Web developers must block HTML and JavaScript tags by hardening input validation on webpages.
11. **Denial-of-Service (DoS):** Attack that inhibits legitimate users from accessing computer services. Normally DoS target connectivity or network bandwidth by overflowing server traffic, resources, nodes or services. Some techniques to launch the DoS attacks include SYN flood, bandwidth, service request, ICMP, P2P, permanent DoS, smurf, app level and buffer overflow.
12. **Directory/command injection:** These attacks use commands to manipulate an application via the Operating System or the deletion of directories, subdirectories or files. A good security measure is to implement input validation.

13. **Distributed Denial-of-Service (DDoS):** DDoS are launched using several zombie computers (botnet- derived from roBOT NETwork) attacking a specific target. During a DDoS the target computer will sustain extreme network traffic, memory and processors usage. To detect outbound traffic, use the command line tool **netstat -a**
14. **DNS poisoning:** Domain Name System poisoning is an attack that modifies or corrupts cached DNS results. The major risks are the propagation of poisoned DNS information to the Internet Service Providers and be cached in their servers.
15. **Domain Name kiting**: This practice allows attackers to register domain names and delete them after the five-day free trial. During the free period, domain tasting will generate traffic and likewise generate revenue without paying for the domain registration.
16. **Evil twin:** Rogue access point attack that configures a WAP (Wireless Access Point) with the same SSID (Service Set Identifier) of a valid WAP. Attackers set these devices in public places with free Wi-Fi. Sensitive information is stolen from the users that connect to the evil twin.
17. **Flash cookies:** Because Adobe Flash cookies can be set to never expire; they represent a high risk to steal user's browsing history. Flash cookies are normally 5 MB in comparison to regular cookies that only store 1,024 bytes of information. Flash cookies are able to recreate deleted cookies.
18. **Fuzz Testing**: It is used to detect system vulnerabilities that can be later exploited. This attack transmits strings of data from scripting to specific applications.
19. **Hash injection:** It is an attack that injects an altered hash to authenticate into a local session in order to access network resources. Attackers will log onto the domain controller, accessing the Active Directory and manipulating domain accounts.
20. **Header manipulation:** Flags are modified within data packets granting legitimate rights to attackers. Dual authentication prevents manipulating user's data.
21. **ICMP flooding:** DoS attack that sends Internet Control Message Protocol (ICMP) packets with spoof source addresses so TCP/IP requests stop. Once the ICMP threshold is reached the router no longer accepts the ICMP echo requests.
22. **Information disclosure**: These attacks allow perpetrators to obtain valuable information about a system. Some examples include revealing passwords, shoulder-surfing, loss of thumb drives, laptop theft, message

insecurity over HTTP, sharing of confidential policies, data leakage and social engineering information disclosure.

23. **Integer overflow:** This attack is the result when an arithmetic operation exceeds the maximum value of an integer used for storage. This exploit can be used for buffer overflow, infinitive loops and data corruption.
24. **IV (Initialization Vector) attack:** This exploit takes place on Wi-Fi networks using the WEP (Wired Equivalent Privacy) security protocol. WEP has known vulnerabilities. The attackers use packet injection for cracking the small IV for keys and obtaining the encryption key.
25. **Jamming interference:** This attack can be part of a major Wireless Denial of Service (WDoS) attack. Attackers use malicious nodes to block access to the medium and likewise interfere with wireless or wired reception. Sophistication increases from continual transmission interference to exploiting protocol vulnerabilities.
26. **Keylogger attack:** This can be a hardware device or a small program that records user's keystrokes or screen content. If it is a physical device, the attacker must remove it in order to access the information. On the other hand, if the hidden program was installed on the victim's computer – its DLL (Dynamic Link Library) file will record all keystrokes.
27. **Lightweight Directory Application Protocol (LDAP) injection:** This attack targets Active Directory accounts so can be modified using LDAP commands.
28. **Malicious add-ons:** We have to be very careful about any additional add-ons that the browsers will install on our computers. There have been cases in the past that browser add-ons installed malware on the client computers. Some measures include running additional scans, do not download from compromised sites and keep system with the latest security patches.
29. **Malicious insider threat:** An insider attack using valid system access credentials can compromise data confidentiality. Motives include revenge, financial gain and industrial espionage. Insider threats are very difficult to detect but a mix of controls can be implemented like least privilege, proper segregation of duties, auditing, enforcement of legal and security policies, restricted access and critical data backup management.
30. **Malware attacks:** Malicious software that is installed through different devious ways. There are several categories of malware, the most common are viruses, worms and Trojan horses.

    30.1 Virus: Malicious code that replicates by itself and needs execution in order to cause damage.

30.2 Worm: Self-replicating malicious code that spreads across the network without intervention or execution.

30. **3 Trojan horse:** Trojans hide within a valid application that will get activated upon certain actions. These programs can even disable firewalls, create backdoors, activate botnets, generate fake traffic and delete system files.

30.4 Logic bomb: Malicious scripts that will activate for a particular event. Normally, they are programmed to destroy the operating system, deletion and formatting of all network drives.

30. **5 Rootkits:** Programs that hide other malware by modifying the operating system. Some rootkits are at the boot loader, library, hardware, application, firmware, kernel and hypervisor levels.

30.6 Spyware: This program gathers sensitive information about the user.

30.7 Rogueware: These programs are also named scareware, the malicious programs masquerade as a security application and send messages of malware infection. After a system scan or trial expiration, users get asked to pay for a full version.

30.8 Ransomware: Extortive malware that locks user's data in order to get payment for unlocking the data.

31. **Man-in-the middle (MITM):** This type of attack allows active interception of network traffic and sending malicious code to the client's machine. Kerberos prevent MITM attacks by enforcing authentication.
32. **Misconfiguration attacks**: These attacks take advantage of wrong, default or compromised configurations to access systems, networks, computers, servers, mobile devices or interconnection devices.
33. **Near field communication (NFC):** There are a few attacks under NFC including eavesdropping, data corruption and smartphone viruses. NFC devices can communicate if the separation is four centimeters or less. The biggest risk is card skimming due to the fact when mobile card readers are used to complete the online payments. NFC channels are also vulnerable to MITM attacks.
34. **Packet sniffing:** Attackers use protocol analyzer or sniffer programs like Wireshark, TCPDump and Sniff-O-Matic to capture and track network packets. Unencrypted data is the most vulnerable when using sniffers – captured packets can easily be read and analyzed data can also be used to plan further cyberattacks.
35. **Password attacks:** These attacks use different techniques to crack server, network device, systems or user passwords. Weak passwords

can be avoided if they use a long combination of capital/ small case letters, numbers and special characters. Cracking techniques include brute force, rule based, dictionary, hybrid and syllable attacks. Some password cracking tools are L0phtCrack, John the Ripper, Cain and Abel, Passscape and Aircrack.

36. **Pharming:** This type of attack aims DNS servers; it is particularly a DNS poisoning attack that redirects traffic to a fraudulent website. Cyber crooks can take advantage of this by stealing confidential information of users.
37. **Privilege escalation:** When hackers penetrate systems, they normally have limited access accounts and want to obtain full privilege accounts like super admin accounts. Elevated rights and permissions of attackers allow them to gain additional controls and remain unnoticed in the target system.
38. **Rainbow attack**: Attackers check the stolen password validity during this type of attack. By using cryptanalysis techniques, the time-memory trade off calculates memory information, inserting the password hash table, comparing and matching passwords until they are cracked.
39. **Replay attack:** Attackers replay data between communication sessions. Using the data, they can impersonate a user to obtain information. Kerberos block this type of attack using time-stamped tickets.
40. **Rogue access points:** Counterfeit WAPs are connected to networks to capture traffic. This rogue device will easily grant access to unauthorized users using wireless and wired networks of the victim.
41. **Session hijacking:** This process seizes an active network or application session. By intercepting and taking control of a user's session, the attacker inserts malicious code to target server afterwards. Packet interception happens at the network level and HTTP session takeover at the application level in OSI model. Some prevention measures against session hijacking include the use of Secure Shell (SSH), HTTPS, log-out functionality implementation and data encryption.
42. **Shrink wrap code attacks:** These attacks are aimed at applications immediately after its initial installation. The most common vulnerability is to exploit default code from libraries.
43. **Smurf attack:** A DoS attack that spoofs the source host to flood the target computer with ping replies.
44. **Social Engineering:** Hackers use social tactics to persuade people to reveal sensitive information that can be later used for malicious actions. Social engineering types include using human interaction, computers

or mobile devices. Attackers normally pose as legitimate users, VIP executives or technical support analyst to commit their attacks. Best anti-social engineering strategies are education, security awareness training and enforcement of IT security policies.

45. **Spear phishing:** This attack targets a specific user or a group of users. Normally uses an email that seems legitimate to ask for some wire transfer already approved by a top executive within a company.
46. **Spim:** Spam instant messaging targets instant messaging apps such Yahoo Messenger, WhatsApp and Line. The attackers need mobile number confirmation if the users click the link. Best way to deal with Spim is to ignore the messages and delete them.
47. **Spoofing:** Cyberattacks can use spoofing in many ways, from changing IP addresses to changing Media Access Control (MAC) addresses to email address by hiding the attacker identity.
48. **SQL injection:** These attacks are the highest web vulnerability impacts on the Internet. A flaw in the coding of a web application is exploited to allow additional data entry to generate unique SQL statements. Many relational databases are vulnerable to this attack including DB2, MySQL and SQL SRV. These attacks can avoid authentication, trigger code execution and affect data integrity.
49. **SYN flooding:** Common DoS attacks use SYN to flood servers. It is based on the Transmission Control Protocol (TCP) handshake process that overflows the normal three-way handshake using SYN and ACK packets between hosts. Attackers never send the ACK part and otherwise they keep sending multiple SYN packets to get several half-opened connections causing a system crash.
50. **Transitive access:** This access involves a trusted relationship within a network that can be exploited to attack core systems. Client-side attacks use transitive relationships whenever an attacker cannot aim a direct cyberattack.
51. **Typo squatting:** This is a form of cybersquatting that reroutes users to malicious websites. Active domain names with typographical errors are created, registered as valid URLs and then uploaded as alternate websites to infect users with malware.
52. **URL hijacking:** This attack is also known as Man-in-the-Browser attack. It triggers a Trojan to hijack the communication between the browser and the libraries. The extension files from the Trojan convert the Document Object Model (DOM) interface and modify the user values.

53. **Vishing:** This attack uses Voice over Internet Protocol (VoIP) or a phone system calls to trick users to give personal information in a similar way to phishing attacks. Attackers can spoof caller IDs to masquerade a phone call within a company. Personal information is at risk if the user provides the required information to validate some kind of financial transaction.
54. **War chalking:** This technique is used to place special symbols on sidewalks or walls indicating an open Wi-Fi network.
55. **War driving:** Attackers drive around to discover wireless networks for future exploits. Cantennas (Open-ended metal can antennae) are used to detect Wi-Fi networks.
56. **Watering hole:** This attack identifies an organization website, exploits web vulnerabilities and installs malware that attacks silently the users.
57. **WEP/WPA attacks:** These Wired Equivalent Privacy/ Wi-Fi Protected Access attacks use cracking tools to break 802.11 WEP secret keys. 40-bit to 512-bit keys can be cracked from captured data packets.
58. **Whaling:** Whaling is a spear phishing attack that aims upper management executives. This attack targets a top executive by name using some kind of legal subpoena or customer complaint.
59. **Wire sniffing:** This is a form of an active or passive wiretapping attack that monitors data traffic or alters data packets as required. Some vulnerable protocols to sniffing are HTTP, IMAP, Telnet, POP, FTP, SMTP and NNTP. Some measures to defend sniffing include physical restrictions, encryption, use of static IP addresses and IPv6 configuration.
60. **WPS attacks:** Wi-Fi Protected Setup use buttons to connect to wireless networks and a secure WPA link. This Pin attack sets up a brute force method to crack into a WPA wireless network. Some countermeasures include disabling WPS or updating the access point firmware.
61. **Xmas attack:** The Christmas tree attack is a port scan type used as a reconnaissance attack and the gathered information is crucial for further cyberattacks. The particular features are the inclusion of bit sets and flags in the TCP packet header that will trigger responses about open ports.
62. **XML injection:** eXtensible Markup Language injection attacks are similar to SQL injection attacks. Major vulnerabilities include code insertion to input or export database data. In addition, XPath the XML query language can be entered using query statements for retrieval or modification of data.

63. **Zero day:** This attack exploits undisclosed software vulnerability that the vendor has not yet created a security patch to fix it. Best action plan against zero-day vulnerabilities is to limit the amount of active protocols and services.

CYBERCRIME TAXONOMY

Some relevant previous studies from ITU and ENISA have categorized typologies of cybercrime. We present a comprehensive taxonomy that has classified cybercrimes in our cyber era (Sabillon et al., 2016).

1. **Child pornography**: Illegal online pornography involves the participation of minors in sex activities. Some illicit online activities include exposing children in pornographic productions, sex exhibition, cybersex, prostitution, sex slavery, image and video distribution, chats, dating sites, Webcam Child Sex Tourism (WCST), sex toys, phone sex services and sex shows. Pornographers use digital software to merge images involving minors – this is known as morphing. Terres de Hommes Netherlands fights children sexual exploitation; They created the 10-year old virtual Filipino girl called Sweetie- this project identified 1,000 predators from 71 countries using 19 chat rooms – These pedophiles were handed over to Interpol. 20,172 predators tried to engage with Sweetie. Sweetie 2.0 continues the fight against WCST.
2. **Cyber hate speech:** Any form of online hate expressions that affect social rights, liberties and freedom of expression. Online hatred can target races, religions, nationalism, ethnic groups, countries, individuals, groups, minorities, migrants, gender identity, disabilities, national origin, political parties, sport teams, sexual orientation, youth, old people, children and animals. Some international agencies are fighting against cyberhate and some countries have created laws as well.
3. **Cyber offenses against Intellectual Property:** Any cyber tort that infringes the protection of patents, trade secrets, trademarks and copyrights. More related to networks and computer security, the list will expand to software, databases, digital content, algorithms and raw data.
4. **Cyberbullying**: This involves the use of communication technologies to harass people. Cyber harassment mostly affects children and teenagers but can also target adults. Some forms include cyber extortion, distribution

of embarrassing pictures, delivery of threatening messages, cyberbashing to mock people and impersonating victims. Parents can document the cyberbullying evidence, report to schools and local police.

5. **Cyberespionage:** Acts that involve exfiltration, unauthorized access, interception and acquisition of data. Freelance spies utilize spyware, keyloggers, surveillance methods, data traffic interception, event recording and communication monitoring.
6. **Cyberextortion:** Attackers will harass victims in order to avoid cyber damage. Cybercriminals will demand money for financial gain to avoid computer-related threats. A typical attack takes place using ransomware and asking the victim for a Bitcoin payment.
7. **Cyberfraud:** Online fraud or forgery does exist in many possible ways. Victims are tricked using digital technologies. Some examples combine online auctions, stock fraud, credit card fraud, telemarketing fraud, false advertising schemes, false damage claims, insider trading, cybersmear campaigns, ad hoc fraud, computer hoaxes, click fraud, Ponzi/pyramid schemes, lottery/sweepstakes and contest scams, get-rich-quick schemes, Nigerian scam, ringtone scam, missed call scam, text message scam, SMS trivia scam, health scam, emergency scam, dating scam, job scam, small business scam and service scam.
8. **Cybergrooming:** This online conduct allows a pedophile to build a relationship with the victim in order to gradually engage in sexual molestation. Once the offender gains the victim's trust, he will escalate using texting and phone calls containing sexually explicit material.
9. **Cyberheist:** This cybercrime involves a largescale theft from banks or financial institutions. Malware, hacking or phishing techniques are normally part of the crime. The theft takes place using e-banking transactions, e-payments, inflating bank accounts and stealing cash from ATMs.
10. **Cybering**: This involves a series of online sex behaviors to stimulate children in a sexual way. The offenders exchange texting, images and video clips with their victims. Cyber child molesters access online communities, chat rooms, games and virtual worlds.
11. **Cyberlaundering:** Cybercrime that comprises financial transactions using funds from criminal activities. Cyberlaundering is based on e-payments, digital money and illegal hard cash that is converted to illegal e-money.
12. **Cyberstalking:** Online activities used by perpetrators to monitor people without their consent. This illegal activity involves online and

offline tasks to intimidate, blackmail or any unlawful motive against their victims. The best way to prosecute the attackers is gathering all evidence to support a police case.

13. **Cyberterrorism:** Cyberterrorists may carry terrorism activities exploiting computer vulnerabilities that will impact society in metropolitan or regional areas. Attackers are motivated by political, religion, hacktivism or personal matters.
14. **Cybertheft:** Cybercriminals seek financial profit by stealing and selling information in every possible way. The dark web is where most of the stolen information is for sale, the most common sold goods are credit card numbers, online auction credentials and bank account numbers.
15. **Cybervandalism:** Vandalism that takes place using computer technology. The most common attacks are website defacement, malware to delete data, DDoS and social media account hijacking.
16. **Cyberwarfare:** Attacks in cyberspace that are aligned with a specific military operation or a national cybersecurity strategy to attack another nation's cyberspace. These operations have a military connotation that are led by commanders and executed by government cyber warriors.
17. **Data breach:** Disclosure of data or information that breaks confidentiality that leads to the distribution in the public domain. The leakage can occur by insider agents or hacker attacks. Damages can affect or trigger corporate reputation, financial losses, lawsuits, share prices, fraud and physical assets.
18. **Disgruntled *employees* and former employees**: These people will take revenge by compromising their employer or former employer's information systems. Some actions include theft of intellectual property using steganographic applications, install malware or backdoor programs, obtain unauthorized access and damage critical data.
19. **Hacking:** Hacking becomes illegal once is used for unauthorized access to computer systems. Cybercrime is consummated once criminal hacking takes place. Illegal hacking activities are usually part of organized crime networks, specific motives and a high degree of sophistication.
20. **Identity theft:** This crime is the theft of someone's identity; the attacker pretends to be a different person to gain financial benefits. John Sileo- a successful entrepreneur was a victim of identity theft that caused his business bankruptcy and two years of his life to stay out of prison.

Identity theft leads to identity fraud that exploits additional crimes like financial identity theft, business identity theft, criminal identity theft and money laundering.

21. **Online gaming:** Online gaming and gambling are targets of cybercriminals. Hackers can steal user's personal information using malware, DDoS, phishing, black hat search engine optimization and webshell creation. Online gaming can also lead to cyberbullying of users. Factors like online casinos accessibility, 24/7 operations, minor's access and e-banking can easily lead to addictions, bankruptcy and cybercrime operations.
22. **Online Obscenity:** Online pornography may not be illegal on the Internet but it may twist the concept that some sexual relationships are acceptable by society. Youth audiences are more vulnerable to this phenomenon; online obscenity offends and affects the morality of the audiences. USA protects minors with laws like the PROTECT Act and the Child Online Protection Act.
23. **Phishing:** Fraudulent process that steals confidential information from end users. Phishing normally involves the use of fake websites. Phishers configure a universal man-in-the-middle phishing kit to activate a real time URL that interacts with a valid website.
24. **Racism and Xenophobia cyber offenses:** Distribution of online material to discriminate, insult or threaten against groups or individuals based on race, ethnicity, culture, minority, colour, national descent, country of origin and dislike of foreigners.
25. **Religion cyber offences:** Coming from one of the most dangerous forms of terrorism – the religious terrorism, religious cyber offences deliver hate speech against other religions and their followers. Adepts claim that they are empowered by their Gods and their actions are justified by the scriptures. The Cyber Jihads from the Islamic State (IS) are a radical group in charge of disseminating propaganda and censorship against other religions.
26. **Revenge porn:** This cyber felony is the act of distributing sexual material of a victim without their consent. This is very common between disgruntled former partners that seek revenge or hackers that are blackmailing their victims seeking profit. As a result, victim's lives can be ruined, losing their jobs or the inability to obtain a new one. Google will respond to victims of nonconsensual pornography (NCP) to remove the content from search engine results.

27. **Spam:** Unsolicited junk messages, images and advertisements are sent on every possible electronic way including email, blogs, search engines, instant messaging (IM) and smartphones. Spammers use botnets and virus infected networks to distribute spam.

CONCLUSION AND FUTURE RESEARCH

Cybercrime is a complex and vast phenomenon; the proliferation of mobile devices, Wi-Fi networks and the Internet openness has increased the expansion of cyberattacks, the cybercriminality and the cyber victimization.

Protection against cybercrime starts at taking personal measures for protection and then escalates to organizational, societal, corporate, national, military and international levels. Defense in depth of cybersecurity at all levels will minimize, prevent and decelerate cyberattacks. Technology by itself is not enough, the integration of other fields like training, awareness, social aspects, culture, laws, prosecution and international cooperation are needed to blend with technical solutions to tackle cybercrime. The creation of national governance to fight cybercrime, International cooperation to prosecute cybercriminals, the hardening of laws for prosecution, additional academia research and a participating cybersecurity industry are just some areas to be improved.

Research units are considering the growing need for governments to intrude on the privacy of individuals for the sake of national security. These researchers also focus on the tendency of people to preserve their anonymity and engage in forms of digital protest, as well as the thorough issue of regulatory compliance in data protection.

Further research is required to study the implications of connecting psychological theory with cybercriminality – this can include some dominant factors like social learning in their hacking groups and justification of outlawed activity.

Additional research must include in-depth analysis of how the notion of privacy is itself socially constructed. Failure to do so would commensurate to ignoring the explicit and tacit agreements where people choose to share or not to share data, based on their own personal assessments of the risks and benefits involved in the digital environment. Legal jurisdiction is one of the most challenging issues, and it requires immediate attention. Until we witness the creation of comprehensive and effective cybercrime laws at national and international levels, it is essential that mutual cooperation

continues between cross border entities such as Interpol, leading cybersecurity nations, intergovernmental agencies, private sector corporations, academia, national cybercrime units and law enforcement agencies.

REFERENCES

Arief, B., & Bin Adzmi, M. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2— Defenders and Victims. *IEEE Security and Privacy*, *13*(2), 84–88. doi:10.1109/MSP.2015.44

Arief, B., Bin Adzmi, M., & Gross, T. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1—Attackers. *IEEE Security and Privacy*, *13*(1), 71–76. doi:10.1109/MSP.2015.19

Britz, M. (2013). *Computer forensics and cybercrime: An introduction* (3rd ed.). Pearson.

Cano, J. (2016). Cinco lecciones por aprender en seguridad y control. Un marco de acción transdisciplinar desde la inevitabilidad de la falla. *IT-Insecurity blog*. Retrieved from http://insecurityit.blogspot.com.co/2016/01/cinco-lecciones-por-aprender-en.html

Chawki, M. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing. doi:10.1007/978-3-319-15150-2

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Auerbach Publications.

Cooper, T., Siu, J., & Wei, K. (2015). *Corporate digital responsability: Doing well by doing good*. Retrieved from https://www.accenture.com/t20150521T071950__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Outlook/Documents/2/Accenture-Corporate-Digital-Responsibility-Web-PDF-V2.pdf

Crume, J. (2000). *Inside Internet Security: What Hackers don't want you to know*. Addison Wesley.

European Network and Information Security Agency – ENISA. (2014). *ENISA Threat Landscape 2014*. Retrieved from https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

Fitch, C. (2004). *Crime and Punishment: The Psychology of Hacking in the New Millenium. GIAC Repository*. SANS Institute.

Gibson, D. (2011). CompTIA Security+: Get Certified get ahead. Charleston, SC: Academic Press.

Hamsi, J., Zeadally, S., & Nasir, Z. (2016, Jan.). *Interventions in cyberspace: status and trends. IEEE IT Professional*.

International Telecommunication Union (ITU). (2014). *Understanding cybercrime: phenomena, challenges and legal response.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Internet Society. (2015). *Global Internet Report 2015: Mobile Evolution and Development of the Internet*. Retrieved from https://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf

ISACA. (2013). *Advanced Persistent Threats: How to Manage the Risk to Your Business*. Rolling Meadows.

ISACA. (2016). *State of Cybersecurity: Implications for 2016. An ISACA and RSA Conference Survey*. Retrieved from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Kleinhempel, M. (2015). *Compliance challenges in emergent markets. IESE Insight*. IV Trim.

Landwehr, C. (2016, February). Privacy research directions. *Communications of the ACM*, *59*(2), 29–31. doi:10.1145/2856451

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday.

McAffee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies.* Retrieved from https://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

McQuade, S. III. (2006). *Understanding and managing cybercrime*. Pearson/Allyn and Bacon.

Micro, T. (2015*). Below the Surface: Exploring the Deep Web*. Forward-Looking Threat Research Team. TrendLabs. Retrieved from https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

Pagliery, J. (2014). The five cyberattacks keys against Sony Pictures. *CNN*. Retrieved from https://cnnespanol.cnn.com/2014/12/09/las-5-claves-del-ciberataque-contra-sony/

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security.*, *4*(6), 165–176.

Sabillon, R., Cavaller, V., Cano, J., & Serra, J. (2016). Cybercriminals, Cyberattacks and Cybercrime: Privacy, security and control. In *Proceedings of the 4th IEEE International Conference on Cybercrime and Computer Forensics (ICCCF)*. IEEE Xplore Digital Library. DOI: 10.1109/ICCCF.2016.7740434

Sileo, J. (2010). *Privacy means profit*. Wiley.

Terres des Hommes Netherlands. (2013). *Webcam Child Sex Tourism: Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism*. Retrieved from https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report.pdf

United Nations Office on Drugs and Crime - UNODC. (2013). *Comprehensive study on Cybercrime*. Retrieved from https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Cybercrime: Technological crimes or crimes committed to complement traditional crimes for financial gain.

Cybercriminals: Individuals or groups involved with all types of cybercrimes.

Hacker: Someone who is able the break the security of computer systems. The intention can go for enforcing penetration testing from the ethical hackers to launch powerful cyberattacks lead by black hat hackers.

Hacktivism: Hacking that is motivated for certain causes like politics, social expressions and social activism.

Chapter 2
Cybersecurity Incident Response and Management

ABSTRACT

This chapter presents a systematic literature review on best practices regarding cybersecurity incident response handling and incident management. The study identifies incident handling models that are used worldwide when responding to any type of cybersecurity incident. The authors highlight the importance of understanding the current cyber threat landscape in any incident response team and their standard operations procedures. The chapter provides guidelines for building a cybersecurity incident team in terms of incident categorization, capabilities, tasks, incident cost calculation, and metrics.

INTRODUCTION

Following the devastating Internet effects of the "Morris Worm" in 1988, the Defense Advanced Research Projects Agency (DARPA) assigned the Software Engineering Institute of the Carnegie Mellon University with the mission to set up a security center for emergencies – this center was lately named the CERT Coordination Center (CERT/CC). The CERT Division (Computer Emergency Response Team) of the Software Engineering Institute (SEI) has been a pioneer in providing resources to create and implement Computer Security Incident Response Teams (CSIRT) and Incident Management resources against global cybersecurity threats and vulnerabilities. According to the National Institute of Standards and Technology-NIST (2012), an event

DOI: 10.4018/978-1-7998-4162-3.ch002

is any observable occurrence in a system or network, an adverse event is a negative consequence and a computer security incident is a violation or imminent threat of violation of acceptable use policies, standard security practices or computer security policies.

A recent study from Hathaway et al. (2015) about Cyber Readiness Index (CRI) 2.0, the CRI 2.0 methodology evaluated the cyber readiness of 125 countries by assessing the national cybersecurity commitment and maturity. The analysis included more than seventy indicators across seven basic elements: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development (R&D), diplomacy and trade, and defense and crisis response.

The Cybersecurity incident response capability can be organized and achieved as a national agency (National Computer Security Incident Response Team - CSIRT) or a military unit, or through the development of an organizational team like the Computer Emergency Response Team (CERT).

INCIDENT HANDLING MODELS

According to ISACA (2012), Incident Management is the capability to effectively manage unexpected disruptive events with the objective of minimizing impact and maintaining or restoring normal operations within defined time limits. Subsequently, Incident response is considered as a subset of incident management as the operational capability of incident management that identifies, prepares, responds to incidents to controls to control and limit damage; provides forensic and investigative capabilities; maintaining, recovering and restoring normal operations based on the service level agreements (SLAs).

According to Oriyano et al. (2020), an incident is defined as any violation or impending of the security policy. Existing corporate security policies clearly define what events are considered cyber incidents, contain procedures and guidelines for responding to cyber incidents and define clear course of action to deal with detection and response to security incidents.

Table 1 shows the most relevant incident handling and management models:

While some incident handling models have similar phases, others combine certain elements in conjoined phases but in the end, any specific model must

Table 1. Cybersecurity incident handling and management models

Name of the model	Phases
Donaldson et al. (2015): Incident Response Process	Identify, investigate, collect, report, contain, repair, remediate, validate, report conclusions and resume normal IT operations
CREST (2014): Cyber security incident management capability	Prepare, respond and follow up
NIST (2012): The Incident Response Life Cycle	Preparation; detection & analysis, containment; eradication & recovery and post-incident activity
ISACA (2012): Incident Management Life Cycle	Planning and preparation; detection, triage and investigation; containment, analysis, tracking and recovery; postincident assessment and incident closure
SANS (2011): Incident handling step-by-step	Preparation, identification, containment, eradication, recovery and lessons learned
ISO/IEC 27035 (2011): Information Security Incident Management	Plan and prepare; detection and reporting; assessment and decision; responses and lessons learnt
ENISA (2010): Incident handling process	Report, registration, triage, incident resolution, incident closure and post-analysis
Kennedy (2008): Modified small business approach for incident handling	Develop a security policy, protect computer equipment, keep data safe, use Internet safely, protect the network, secure line of business applications and training
CERT/CC (2003) Incident handling life-cycle process	Report, analyze, obtain contact information, provide technical assistance, coordinate information & response and provide resolution

be able to mitigate and eradicate the cybersecurity incident in order to avoid additional cyber threats.

THE EVERCHANGING CYBERTHREAT LANDSCAPING

The cybersecurity threat landscape is always morphing and evolving due to the constant proliferation of new technologies. Furthermore, cybercriminals are continually launching cyberattacks that tend to grow in sophistication, by adopting new anti-forensics techniques and by using procedures to avoid cybercrime detection and tracing.

McAffee estimates that the cybercrime industry has an annual worldwide revenue of $ 400 billion, with a conservative estimate in global losses of $ 375 billion and a maximum reaching the $ 575 billion. The Internet economy can generate annually between $ 2 trillion and $ 3 trillion and cybercrime takes

15% and 20% of the Internet created value. Nevertheless, most cybercrimes are never reported to avoid further financial losses, damage to corporate reputation and credibility.

ISACA and RSA reported on its global cybersecurity survey that phishing, malware and social engineering were the three most frequently occurring cyberattacks in organizations during 2015. The same study highlighted the motivation behind the cyberattacks; financial gain was the top motivator for cybercriminals, followed by service disruption and data theft. Describing a typical cybercriminal stereotype and its motives is almost impossible, mostly because cybercrime agents act based on one or several motives. Some motives entail curiosity, fun, satisfaction, publicity, manipulation, destruction, revenge, ego gratification, hacktivism, nationalism, radicalism, religion, politics, and financial benefit.

According to ENISA Threat Landscape (2016), the top cyber threats that are increasing in comparison to the previous annual report are malware, web based attacks, web application attacks, Denial of Service (DoS), insider threats, exploit kits, information leakage, ransomware and cyber espionage. The emerging technologies that are considered in the latest report include cloud computing, mobile computing, Cyber Physical Systems (CPS), Internet of Things (IoT), Big Data, Network Virtualization and Software Defined Networks (SDN/5G).

Table 2. Functional, information and recoverability impact categorization of incidents

Functional Impact	Information Impact	Recoverability effort
None: No effect to business	None: No information was compromised	Regular: Time to recover is achievable with current resources
Low: Minimal effect	Privacy breach: Sensitive information was accessed or exfiltrated	Supplemented: Time to recover is achievable with extra resources
Medium: A critical service is not operating	Proprietary breach: Unclassified information was accessed or exfiltrated	Extended: Time to recover is not predictable; additional help is needed
High: Some critical services are not delivered	Integrity Loss: Sensitive or proprietary information was modified or deleted	Not Recoverable: Unable to recover from cyber incident

(NIST 800-61 Rev 2, 2012)

CYBER INCIDENT CATEGORIZATION

According to NIST (2012), the incident prioritization is one the most critical decision when it comes to handling incidents. There are relevant factors that will help prioritize how a cybersecurity incident is handled (Table 2):

Functional Impact: Business applications that are a target will normally impact organization's functionality; affecting at some point the user's productivity. Incident handlers also need to analyze what are the future consequences if the functional impact of the incident cannot be contained.

Information impact: This factor depends on how the confidentiality, integrity and availability of the information are being affected. Sensitive information leakage and data theft are some examples of privacy breach.

Recoverability: The number of hours and resources to recover from an incident will determine the recoverability level.

The government of Canada (2013) created the Cyber Incident Management Framework (CIMF) which intends to provide a national approach to the management and coordination of future or current cyber threats or cybersecurity incidents. The CIMF contains the Canadian Cyber Incident Response Centre (CCIRC) impact severity matrix to help categorize cyber incidents based on information disclosure, economic, well-being, health and safety, public confidence and essential services. The matrix severity levels range from very low to the catastrophic level which is very high.

BUILDING THE CYBERSECURITY INCIDENT RESPONSE TEAMS

Kaplan et al. (2015) argue that the main objective of an incident response plan is to manage a cybersecurity incident by limiting damage, increasing the confidence of external stakeholders, and reducing costs and recovering times. In order to achieve this objective, it is required to have a clear decision making, strong coordination and accountability skills and a superior collaboration with third-party agents.

ISACA (2013) highlights that a CSIRT should cover specific key capabilities and services:

- Security incident analysis
- Intelligence assessment

- Incident resolution
- Security investigations
- Forensic evidence collection
- Coordination tasks and collaboration with external stakeholders
- Conduct proactive advice including alerts, warnings, vulnerability assessments, training and user cybersecurity awareness

A CSIRT is a group comprised of staff with advanced cybersecurity skills that is formed to deal with incident handling. A CSIRT can be recognized by other names or acronyms like Cyber or Computer Incident Response Team (CIRT); Cyber or Computer Emergency Response Team (CERT); Cyber or Computer Incident Response Capability (CIRC); Cyber or Computer Emergency Response Capability (CERC); Security Incident Response Team (SIRT); Security Emergency Response Team (SERT); Security Incident Response Capability (SIRC); Security Emergency Response Capability (SERC); Incident Response Team (IRT); Emergency Response Team (ERT); Incident Response Capability (IRC) or Emergency Response Capability (ERC).

NIST (2012) recommends a series of key tasks in order to organize a cybersecurity incident handling capability:

- Establish a formal incident response (IR) capability: Organizations must be able to respond effectively when cybersecurity defenses are breached.
- Implement an incident response policy: Having the IR policy in place assures the basis of the incident response program.
- Develop an incident response plan according to the incident response policy: The IR plan presents a roadmap for the implementation of the IR program based on the IR policy. The plan should include short- and long-term goals and program metrics.
- Implement IR procedures: IR procedures sustain detailed steps for dealing with cybersecurity incidents.
- Create clear policies and procedures related to sharing information about incidents:
- Provide the required information about incidents to the appropriate organizations: The organization should share communication about specific incidents with the media, law enforcement and the required security agencies.

- Outweigh the necessary factors when choosing the IT team model: Evaluate advantages and disadvantages of the most convenient team structure model based on the organization's resources and needs.
- Recruit staff with the appropriate skills for the IR team: Critical technical, teamwork and communications skills are fundamental for any CERT or CSIRT.
- Identify internal groups that may support the IR capability: The expertise of other internal groups or units are required to rely on such groups to fulfill the IR mission
- Decide which IR services will be offered: The main focus is to offer IR services but, in some cases, additional services can be available like security awareness, training and cybersecurity advisory services.

CALCULATING A CYBER INCIDENT COST

Calculating the losses of cyberattacks implying a Dollar value is very difficult, there are direct losses affecting certain environments but there are also indirect financial losses like the downtime of end users not being productive due to certain consequences of the cybersecurity incident dealing with loss of network connectivity, unavailable servers, corrupted data, limited access to applications or inaccessible IT services.

Ditrich (2002) developed an effective incident cost analysis that involves answering several questions to calculate the security incident cost:

1. People involved responding to or investigating the incident?
2. Number of hours these people spent?
3. Number of people that did not work because of the incident?
4. How many hours of productive time they did lose?
5. What is the hourly rate of this staff?
6. What is the overhead percentage that the employer pays for the employees?

Another option is the Incident Cost Analysis Modeling Project (I-CAMP), that was introduced in 1997 and the second edition (I-CAMP II) that was updated in 2000 with a goal to design a cost analysis model for IT related incidents. For the initial I-CAMP study, 13 American universities did participate in this study and in the I-CAMP II, 5 additional universities joined the study. These universities were located in eastern, western and central US States which had a strong history of information technology development

and use. This model estimates time and cost with an average of 48 hours per incident and the cost depends of the staff involved in the investigation. To calculate the total cost per incident, it is required to add employee benefits, indirect costs and a median cost of +/- fifteen percent.

Bottom line is to create a proper cybersecurity incident cost model for your organization using the criteria listed above.

APPROACHES TO MEASURE AND AUDIT OF CSIRTs

As new cyber threats evolve on a daily basis, it becomes necessary the evaluation and measure of operations, growth and maturity of CSIRTs. At this time, there are not any specific standard set of benchmarks for the assessment of CSIRT operations.

Several organizations are working to develop CSIRT evaluation metrics and benchmarks (Table 3). Organizations like the Organisation for Economic Co-operation and Development (OECD), the European Network and Information Security Agency (ENISA), the CSIRT Metrics Special Interest Group, The CSIRT Development and Training team in the Carnegie Mellon University Software Engineering Institute's CERT Division, George Mason University, Hewlett-Packard, Dartmouth University, the Forum of Incident Response and Security Teams (FIRST) and the Center for Internet Security.

CONCLUSION AND FUTURE RESEARCH

Organizations of all sizes are mostly aware that the cyber threat landscape keeps growing and can target any size company at any time. Cybersecurity incidents can impact business financial, legal, regulatory, operation and reputational. It is vital for any organization to align the cybersecurity agenda with business priorities by implementing an incident management plan. A CSIRT must have a well-defined incident service catalog that separates reactive services, proactive services and cybersecurity quality management services.

Future research for incident management must target incidents in cloud computing, in industrial systems, IoT, and to develop new incident handling approaches against emerging cyber threats.

In addition, the standardization and benchmarks needs further research to assess the incident detection, containment, remediation, recovery and restoration phases. The effectiveness can be measured based on CSIRT

Table 3. CSIRT evaluation metrics and benchmarks initiatives

Organizations	CSIRT evaluation metrics and benchmarks initiatives	Key features
Organisation for Economic Co-operation and Development (OECD)	Guidance for improving the comparability of statistics produces by Computer Security Incident Response Teams (CSIRTs) – 2015	• Understanding CSIRT data, statistics and statistical indicators • Main uses of CSIRT statistics • Measuring CSIRT capacity • Improving cybersecurity incident statistics
European Network and Information Security Agency (ENISA)	Deployment of baseline capabilities of National Governmental CERTs (2012)	• Cybersecurity incident service portfolio • National and cross-border cooperation • n/g CERT maturity model and services
CSIRT Metrics Special Interest Group (SIG) - Forum of Incident Response and Security Teams (FIRST)	Metrics SIG (2016)	• Seeking approaches for benchmarking and/or improving the CSIRT processes and metrics to provide effective incident management quantification • Help to refine, align, and test metrics, as well as to suggest additional improvements for standardizing CSIRT practices within the community
CSIRT Development and Training team in the Carnegie Mellon University Software Engineering Institute's CERT Division	Incident Management Capability Metrics (2007)	• Protection phase metrics • Detect phase metrics • Respond phase metrics • Sustain phase metrics
George Mason University, Hewlett-Packard, Dartmouth University	Improving CSIRT Skills, Dynamics, and Effectiveness (2013)	• Conduct contextual performance analysis and cognitive task analysis • Provide measurement criteria for improvement
Center for Internet Security	The CIS Security Metrics (2010)	Incident management: • Cost of Incidents • Mean Cost of Incidents • Mean Incident Recovery Cost • Mean-Time to Incident Discovery • Number of Incidents • Mean-Time Between Security Incidents • Mean-Time to Incident Recovery
		Vulnerability management: • Vulnerability Scanning Coverage • Percent of Systems with No Known Severe Vulnerabilities • Mean-Time to Mitigate Vulnerabilities • Number of Known Vulnerability Instances • Mean Cost to Mitigate Vulnerabilities

processes, satisfaction, performance against goals, incident management and avoidance of incident re-occurrence.

REFERENCES

Big Ten Academic Alliance. (1997). Incident Cost Analysis and Modeling Project. *CIC Chief Information Officers*. Retrieved from https://www.btaa.org/docs/default-source/technology/icampreport1.pdf?sfvrsn=0

Big Ten Academic Alliance. (2000). Incident Cost Analysis and Modeling Project I-CAMP II. *CIC Chief Information Officers*. Retrieved from https://www.btaa.org/docs/default-source/reports/icampreport2.pdf?sfvrsn=0

Campbell, T. (2003). *An Introduction to the Computer Security Incident Response Team (CSIRT): Set-Up and Operational Considerations. Global Information Assurance Certification (GIAC) Paper*. SANS.

Center for Internet Security - CIS. (2010). *CIS Security Metrics v1.1.0*. Retrieved from https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-61 Revision 2. Gaithersburg: U.S. Department of Commerce.

CREST. (2014). Cyber Security Incident Response Guide. *CREST International*. Retrieved from https://crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

CSIRT Metrics Special Interest Group – SIG. (2016). Metrics SIG. *FIRST SIG*. Retrieved from https://www.first.org/global/sigs/metrics

Dittrich, D. (2010). Developing an Effective Incident Cost Analysis Mechanism. *Symantec Connect*. Retrieved from http://www.symantec.com/connect/articles/developing-effective-incident-cost-analysis-mechanism

Donaldson, S., Siegel, S., Williams, K., & Aslam, A. (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. Apress. doi:10.1007/978-1-4302-6083-7

Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). *Incident Management Capability Metrics.* SEI, Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14873.pdf

European Network and Information Security Agency - ENISA. (2010). *Good Practice for Incident Management*. ENISA.

European Network and Information Security Agency - ENISA. (2012). *Deployment of baseline capabilities of National Governmental CERTs.* ENISA.

European Network and Information Security Agency - ENISA. (2016). *ENISA Threat Landscape 2015*. ENISA.

Government of Canada. (2013). *Cyber Incident Management Framework for Canada*. Author.

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). *Cyber Readiness Index 2.0 – A plan for cyber readiness: a baseline and an index*. Potomac Institute for Policy Studies.

International Organization for Standardization - ISO. (2011). *ISO/IEC 27035 Information Technology – Security tecniques- Information security incident management". International Organization for Standardization*. ISO.

ISACA. (2012). *Incident Management and Response.* Rolling Meadows: ISACA White Paper.

ISACA. (2013). *Advanced Persistent Threats: How to manage the risk to your business.* Rolling Meadows: ISACA Cybersecurity Nexus.

ISACA. (2016). *State of Cybersecurity: Implications for 2016. An ISACA and RSA Conference Survey*. Retrieved from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting your digital business*. John Wiley & Sons. doi:10.1002/9781119055228

Kennedy, G. (2008). *Security Incident Handling in Small Organizations*. SANS Institute.

Killcrece, G. (2005). *Incident Management*. Software Engineering Institute, Carnegie Mellon University.

Kral, P. (2012). *Incident Handler's Handbook*. The SANS Institute.

McAffee. (2014). Net Losses: Estimating the Global Cost of Cybercrime. *Center for Strategic and International Studies.* Retrieved from https://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

Organisation for Economic Co-operation and Development – OECD. (2015). *Guidance for improving the comparability of statistics produces by Computer Security Incident Response Teams (CSIRTs).* Retrieved from https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINA&doclanguage=en

Oriyano, S., & Solomon, M. (2020). *Hacker Techniques, Tools, and Incident Handling* (3rd ed.). Jones & Bartlett Learning.

Pethia, R. (2013). *20+ Years of Cyber (in)Security*. SEI Webinar series. Retrieved from https://www.sei.cmu.edu/webinars/view_webinar.cfm?webinarid=59067

Pfleeger, S., Tetrick, L., Zaccaro, S., Dalal, R., & Horne, B. (2013). *Improving CSIRT Skills, Dynamics, and Effectiveness*. Cybersecurity Division, George Mason University – HP- Darmouth University. Retrieved from https://www.dhs.gov/sites/default/files/publications/csd-pi-meeting-2013-day-2-pfleeger-and-tetrick.pdf

Ruefle, R., Dorofee, A., Mundie, D., Householder, A., Murray, M. & Perl, S. (2014, Sept.). Computer Security Incident Response Team: Development and Evolution. *IEEE Security & Privacy*, 16-26.

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176.

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute, Carnegie Mellon University. doi:10.21236/ADA413778

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Cybersecurity Event: Things that happen in particular situation that affect cybersecurity areas.

Cybersecurity Incident: Critical events that compromise normal operations of cyber assets within any organization.

Chapter 3
Digital Forensics of Cybercrimes and the Use of Cyber Forensics Tools to Obtain Digital Evidence

ABSTRACT

This chapter evaluates the most relevant methodologies and best practices for conducting digital investigations, preserving digital forensic evidence and following chain of custody (CoC) of cybercrimes. Cybercriminals are assuming new strategies to launch their sophisticated cyberattacks within the ever-changing digital ecosystems. The authors recommend that digital investigations must continually shift to tackle cybercrimes and prosecute cybercriminals to increase international collaboration networks, to share prevention knowledge, and to analyze lessons learned. They also establish a cyber forensics model for miscellaneous ecosystems called cyber forensics model in digital ecosystems (CFMDE). This chapter also reviews the most important categories of tools to conduct digital investigations. Nevertheless, as the cybercrime sophistication keeps improving, it is also necessary to harden technologies, techniques, methodologies, and tools to acquire digital evidence in order to support and make cyber investigation cases stronger.

DOI: 10.4018/978-1-7998-4162-3.ch003

INTRODUCTION

The Information Age has led to humanity an accelerated acceptance of technology in modern societies. This era empowers us to access information freely and the ability to access knowledge almost instantly. We no longer depend on personal computers to achieve this purpose; the vast proliferation of digital devices has allowed us to depend on technology. From laptops to tablets, from landlines to smart phones, from private networks to public wireless networks – all these technologies keep improving in terms of processing power, miniaturization, portability, display resolution, battery lifespan, storage and connectivity (Sabillon et al., 2014).

This technology blast has also created a negative effect, with the creation of computer related crimes or the use of digital devices to commit common crimes. To investigate the cybercriminality in more in-depth analysis, it was required the inception of computer forensics methodologies that over the years have evolved into cyberforensics or digital forensics.

Digital forensics is define as the use of scientific methodologies to preserve, collect, validate, identify, analyze, interpret, document and present evidence from digital devices for civil purposes, to prove and prosecute cybercrimes.

These days, cybercrime continues to escalate due to global connectivity, the advancements of networks, information exchange and the proliferation of mobile technologies. Moreover, digital investigators and prosecutors need to understand how cybercriminals act in order to understand their modus operandi including Techniques, Tactics and Procedures (TTP) of criminal hacking.

Cyberattacks constantly increase its sophistication to avoid detection, monitoring, remediation and eradication. The proliferation of digital devices has attracted endless possibilities to commit cybercrimes or to utilize these devices to perpetrate common crimes. Cybercriminals are frequently launching cyberattacks that are conducive to grow in sophistication, the adoption of anti-forensics techniques and the use of procedures to avoid cybercrime detection and tracing.

McAffee (2014) determined that cybercrime costs $ 400 billion to the global economy on an annual basis, but this can easily reach a maximum of $ 575 billion. Stolen personal information could cost $ 160 billion per annum, G20 nations experience most financial losses due to cybercrime activities especially the USA, China, Japan and Germany. Developing countries are only experiencing small losses yet this tendency will likely change in the future as business use Internet for commercial purposes particularly mobile

platforms and network connectivity. Nevertheless, most cybercrime activities go unreported on the organizational level to avoid further impacts like harming business operations, customer relationships and company reputations. The cybercrime effect targeting end users is not distinctive when it comes to the theft of personal information.

For many years, digital forensics methodologies and practices have not been evolving at the same rate that cybercriminality exploits Information and Communication Technologies (ICT) vulnerabilities. In this chapter, we review existing methodologies and how is imperative to revisit cybercrime and digital investigations operations to cover a vast number of technological environments. Our Cyber Forensics Model combines the most relevant phases of digital investigations and targets multiple environments in digital ecosystems.

LITERATURE REVIEW

Arief et al. (2015) point out that cybercrime losses are normally presented using surveys, these surveys do not provide a representative sample of the losses. In addition, surveys can be distorted and it does not exist an authoritative source for calculating cybercrime losses as many incidents are never reported to not lose organizational reputation. They stress that the number of cybercrime losses is arguable but what is indisputable is the rising threat of cybercrime. In order to assess how cybercrime operates, we must comprehend the attackers, the defenders and the victim's environments.

Cybercriminals are continually launching cyberattacks that tend to grow in sophistication, the adoption of anti-forensics techniques and the use of procedures to avoid cybercrime detection and tracing.

In 2018, the Internet Crime Complaint Center (IC3) - FBI received over 351,936 complaints with a combined loss exceeding $ 2.7 billion; the IC3 dealt with 3,463,620 cybercrime complaints during a period of six years (2010-2015) and they estimate that only 15% of the cyber victims file a complaint. According to their Internet Crime Report (2018), the top 5 cyber victimization by country occurs in the USA, UK, Canada, Australia and Georgia mostly linked to non-delivery of products or payment, 419 schemes, identity theft, online auctions, personal data breach, cyber extortion, employment fraud, credit cards, phishing and cyber harassment. Since its inception in 2000, the IC3 received 4,415,870 complaints. The IC3 follows specific procedures to fight cybercrime including detection, victim complaint, mitigation, liaison

with industry/law enforcement, cybercrime analysis, deterrence, investigation, prosecution and prevention.

As reported by Cano (2016), cybercriminals modus operandi has been elevated from traditional cyber operations to cybercrime digital ecosystems where they take advantage of logic infrastructures, digital platforms and highly connected users. He describes a Criminal Digital Ecosystem (CDEco), as the group of relationships between local and global participants that interact to create a flexible network to engage in criminal activities by exploiting vulnerabilities of cyber victims; mainly, aiming at specific goals under full anonymity and leaving untraceable digital evidence when possible.

He claims that the intent of the cybercriminal's actions is set on five premises:

1. Maximum effectiveness with minimum effort.
2. Maximum anonymity, with the minimum possible evidence.
3. Maximum legal ambiguity, with minimal technological knowledge available.
4. The use of free digital platforms, assisted by specialized communities.
5. Using cryptocurrency as payment. Being Bitcoin, the digital currency mostly used for hacking communities and underground operations in the Deep Web.

Cyber investigators must adapt to the way cybercriminals operate, by developing new skill set based on data analytics, revisiting the search and collection phases of digital evidence and evaluate the hacking scenario design aimed to assimilate these new criminal digital ecosystems (Sabillon, 2016).

METHODOLOGIES FOR DIGITAL FORENSICS

Digital forensics (DF) is defined as the use of scientific methodologies to preserve, collect, validate, analyze, interpret, document and present evidence from digital devices for civil or criminal investigations, to prove and prosecute cybercrime.

Kruse and Heiser (2001) did present the basic computer investigation model in their book named *Computer Forensics: Incident Response Essentials*. This model included four phases: Assess, Acquire, Analyze and Report.

Citizens in modern societies are well connected with technology through their digital devices. Initiating a crime or cybercrime investigation will induce to access these digital devices that contain potential digital evidence.

According to Davidoff et al. (2012), digital evidence is any documentation that satisfies the requirements of "evidence" in a proceeding, but that exists in electronic digital form. NIST also consists of digital evidence in the form of information on computer, audio/video files and digital images but it helps to recognize people's faces, image/video analysis and to solve common crimes and cybercrimes as well.

In order to detect and gather digital evidence, cyber investigators ought to follow certain principles like keeping intact the cybercrime scene, always avoid irrelevant risks, record everything in a sequential order and follow the proper chain of custody.

The Scientific Working Group on Digital Evidence (SWGDE) contributes with best practices for computer forensics specifically for collecting, acquiring, analyzing and documenting digital evidence found in computer forensic examinations.

Considering the steps of a digital investigation, here it is stressed the importance of assessing and preserving data. This is known as the six-step model from Casey (2001) that emphasizes the importance of preserving data. The six steps are:

- Identification/assessment
- Collection/acquisition
- Preservation
- Examination
- Analysis
- Reporting

Ambhire and Meshram (2012) developed a similar model which includes a planning phase, the scene phases (Identification, Collection, and Preservation) and the Lab phases (Examination, Analysis and Report).

There are three types of digital investigations:

- Internal investigations: These ones are sponsored by organizations and are treated as corporate secrets.
- Civil investigations: These investigations are initiated when intellectual property is at risk. Possible attacks include intrusions, Denial-of-

service (DoS) attacks, malicious code, malicious communication and abuse of resources.

- Criminal investigations: Computer crimes cover the computer or the data in the computer as the objects, computer is the instrument or tool of the act or it is used to intimidate. Some cybercrimes comprise online auction fraud, child pornography, child endangerment, counterfeiting, cyberstalking, forgery, gambling, identity theft, intellectual property piracy, prostitution, securities fraud and theft of services.

The reporting phase encompasses a very important document that must be updated at all times. This is the chain of custody report, which applies to every physical unit of evidence in possession under a digital investigation.

We studied 26 models and frameworks related to digital forensics investigations for digital crime and cybercrime (Table 1,2 and 3). Starting from its inception with the Politt Process (1984) until one of the latest, the Digital Forensics Cybercrime Ontology developed by Talib et al. (2015).

Table 1 highlights an overview of digital forensic methodologies from 1984 until 2006.

While there are many options out there for cyber investigators to choose from and follow a specific framework or model, there isn't a globally accepted or an universal digital investigation methodology.

In Table 2, we present the DF methodologies in the 2007-2010 period.

With the adoption of new technologies, it is necessary to adapt Digital Forensics practices and we have to recognize that the cyber threat landscape will keep growing as well (Table 3).

By studying the aforementioned digital forensic methodologies, we were able to detect similar patterns when comparing all its different phases. In table 4, we compared the similarity of DF methodologies in the identification, investigation, collection, analysis and presentation phases.

TOOLS FOR DIGITAL FORENSIC INVESTIGATIONS

Hardware Tools

Some important hardware tools are required to succeed in any digital investigation:

Table 1. An overview of digital forensic methodologies (1984-2006)

Digital Forensic Methodologies	Phases
Politt (1984): Computer Forensic investigate process	Acquisition, identification, evaluation and admission
Kruse and Heiser (2001): Basic computer investigation model	Assess, acquire, analyze and report
Digital Forensic Research Workshop -DFRWS (2001): DFRWS Investigative model	Identification, preservation, collection, examination, analysis and presentation
Casey (2001): Six-step model	Identification/assessment, collection/acquisition, preservation, examination, analysis and reporting
Reith et al. (2002): Abstract Digital Forensics Model (ADFM)	Identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence
Carrier et al. (2003): Integrated Digital Investigation Process (IDIP)	Readiness, deployment, physical crime scene investigation/digital crime scene investigation phase. The digital crime scene investigation phases are preservation, survey, document, search for digital evidence, scene reconstruction and presentation
Ciardhuain (2004): Extended Model of Cybercrime investigations	Awareness, authorization, planning, notification, search, collection, transport, storage, examination, hypothesis, presentation, proof/defense and dissemination
Baryamureeba et al. (2004): Enhanced Digital Investigation Model (EIDIP)	Readiness, deployment, traceback, dynamite and review
Beebe et al. (2004): A Hierarchical, Objectives-Based Framework for the Digital Investigations Process	Preparation, incident response, data collection, data analysis, presentation and incident closure
Rogers et al. (2006): Computer Forensics Field Triage Process Model (CFFTPM)	Planning, triage, usage/user profiles, chronology/timeline, Internet and case specific evidence
Kohn et al. (2006): Framework for a Digital Investigation	Preparation, investigation and presentation
Kent et al. (2006): Four-Step Forensic Process	Collection, examination, analysis and reporting
Ieong (2006): FORZA- Digital Forensics Investigation Frame	8 layers: Contextual investigation, contextual, legal advisory, conceptual security, technical preparation, data acquisition, data analysis and legal presentation
Venter (2006): Process Flows for Cyber Forensics Training and Operations	Inspect & prepare scene, collect evidence & evidence information and debrief scene & record seizure information

IT technician standard toolkit: There might be cases where removing physical drives is part of the data acquisition phase. A complete kit should include the following tools:

§ Phillips screwdrivers (No. 0 and 1)
§ 1/8”,1/4” and 3/16” flat screwdrivers

Table 2. An overview of digital forensic methodologies (2007-2010)

Digital Forensic Methodologies	Phases
Freiling et al. (2007): The Common Process Model	Pre-incident preparation, detection of incidents, initial response, formulate response strategy, investigate the incident and reporting
Khatir et al. (2008): The Two-Dimensional Evidence Reliability Amplification Process Model	Five major phases (Initialization, evidence collection, evidence examination and analysis, presentation and case termination). Under two dimensions that include 16 sub-phases and umbrella activities (computer tools utilization, case management/ team setup, preservation/authenticity and documentation)
Selamat et al. (2008): Digital Forensic Investigation Framework	Preparation, collection and preservation, examination and analysis, presentation and reporting and disseminating the case
Perumal (2009): Digital Forensic Model on Malaysian Investigation Process	Planning, identification, reconnaissance, analysis, result, proof & defense and diffusion of information
Pilli et al. (2010): A Generic Framework for Network Forensics	Preparation and authorization, detection, incident response, collection, preservation and protection, examination, analysis, investigation and attribution, presentation & review

Table 3. An overview of digital forensic methodologies (2011-2016)

Digital Forensic Methodologies	Phases
Agarwal et al. (2011): Systematic Digital Forensic Investigation Model (SRDFIM)	Preparation, securing the scene, survey & recognition, documenting the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation and result & review
Ambhire and Meshram (2012): Phases model	Planning phase, scene phases (Identification, collection and preservation) and the lab phases (Examination, analysis and report)
U.S. Department of Justice (2014): Process model	Collection, examination, analysis and reporting
Prayudi et al. (2015): Digital Forensics Business Model	Identify purpose of digital investigation, identify principles for handling evidence, identify object involved in the digital forensics activity, recognize environment and how digital forensics activity works and construct a business model of digital forensics
Jain et al. (2015): Digital Forensic Framework	Plan, authenticate, gather evidence, categorize cybercrime, report and future update
Talib et al. (2015): Comprehensive Ontology Based-Investigation for Digital Forensics Cybercrime	180 classes, 179 subclasses and 84 instances related to digital forensics crime cases. Digital forensics phases are readiness, investigation, physical crime scene, digital crime scene, presentation and deployment
Jadhao et al. (2016): Digital Forensics Investigation Model for Social Networking Site	Check, analyze context, scan suspicious words, call heuristic method, call knowledge base rule, report to E-crime department and check connection

Table 4. Similar phases in Digital Forensics methodologies

<table>
<tr><th></th><th>Identification phase (6)</th><th>Investigation phase (5)</th><th>Collection phase (13)</th></tr>
<tr><td rowspan="3">Digital Forensic Methodologies</td><td>1) Pollit (1984)
2) DFRWS (2001)
3) Casey (2001)
4) Reith et al. (2002)
5) Perumal (2009)
6) Ambhire and Meshram (2012)</td><td>1) Carrier et al. (2003)
2) Kohn et al. (2006)
3) Freiling et al. (2007)
4) Pilli et al. (2010)
5) Talib et al (2015)</td><td rowspan="3">1) DRFWS (2001)
2) Casey (2001)
3) Reith et al. (2002)
4) Ciardhuain (2004)
5) Beebe et al. (2004)
6) Kent et al. (2006)
7) Venter (2006)
8) Khatir et al. (2008)
9) Selamat et al. (2008)
10) Pilli et al. (2010)
11) Agarwal et al. (2011)
12) Ambhire and Meshram (2012)
13) U.S. Department of Justice (2014)</td></tr>
<tr><td>Analysis phase (13)</td><td>Presentation phase (10)</td></tr>
<tr><td>1) DRFWS (2001)
2) Casey (2001)
3) Reith et al. (2002)
4) Beebe et al. (2004)
5) Kent et al. (2006)
6) Ieong (2006)
7) Selamat et al. (2008)
8) Perumal (2009)
9) Pilli et al. (2010)
10) Agarwal et al. (2011)
11) Ambhire and Meshram (2012)
12) U.S. Department of Justice (2014)
13) Jadhao et al. (2016)</td><td>1) DRFWS (2001)
2) Reith et al. (2002)
3) Carrier et al. (2003)
4) Ciardhuain (2004)
5) Beebe et al. (2004)
6) Kohn et al. (2006)
7) Ieong (2006)
8) Agarwal et al. (2011)
9) Talib et al. (2015)
10) Pilli et al. (2010)</td></tr>
</table>

§ 3/16” and 1/4” nut drivers
§ T7, T10 and T15 Torx screwdrivers
§ Tweezers
§ Reverse action tweezers
§ 3-claw part grip
§ 5” needle nose pliers
§ A plastic scribe

Write-protected interfaces: In many instances, you will need a copy of any device that is part of an ongoing digital investigation. In order to avoid any problem, digital forensics analyst must acquire any image that will be acceptable under any legal standpoint. Some vendors for this category include Advanced Test Products, Digital Intelligence, Forensic Computers, Inc., Forensic PC, Guidance Software, Intelligent Computer Systems and WiebeTech.

External storage units: A valid repository is required conducive to store the target image.

§ Several USB drives

§ DVD recorder
§ External hard drives

Forensics workstations: Analysts need to have powerful workstations either for field work or for conducting forensic lab operations. Some technical requirements consist of multiprocessor capabilities, extra RAM memory, enough disk capacity, hot-swappable hard disk drive bays, external SATA connectors, external SCSI connectors, memory card capability, built-in write protect devices and several monitors.

Software Tools

According to Graves (2014), software tools can be organized into two important categories:

§ Basic categorization
§ Functional categorization

These categories are organized in more detail as follows:
Basic categorization

1. Operating System utilities
2. Open-source applications
3. Commercial applications and suites

Functional categorization

1. Physical media capture and analysis
2. Memory capture and examination
3. Application analysis
4. Network capture and analysis

Data abstraction layers are the different steps that every single file will go through from electrical charge, reading the binary code and get the results in ASCII (American Standard Code for Information Interchange) characters. These layers are applied to data stream to convert it to another type of format. So depending on the data stream format, we will need to select a tool that can allow us to access and analyze the data.

Basic Categorization

Operating System utilities: The most common operating systems are Windows, Linux and Macintosh OSX.

Windows: The most prevailing ones are Regedit, Event viewer and SysInternals. Regedit is the registry editor that includes a set of configuration files. Event viewer is mostly used for network forensics and SysInternals is a suite of utilities with very powerful tools including Autoruns, EFSDump, PendMoves, PSFile, PSList, PSService, RootkitRevealer, Streams and Strings.

Linux: Many Linux utilities can work on Windows and Macintosh environments. Some utilities are included in Linux distributions but there may be cases where is necessary to download and install them separately. Some of these utilities include Disk Dump (DD), GREP, Linux Disk Editor (LDE) and PhotoRec.

Macintosh OSX: This operating system is based on Unix. Like Linux, the Mac file system is based on journal entries and self-maintained. Some utilities are GREP, HEAD, Finder and Spotlight.

Open-source applications:

While open source tools are free to use forever, shareware tools on the other hand are valid for a trial period and you are required to buy a license after the expiration date.

If you are using freeware or shareware tools, consider to get expertise on your tools as you may encounter some issues from courts, lawyers and judges in order to validate credibility, functions, reliability and acceptance of your digital evidence conclusions. Some tools include Safecopy, Metaviewer, Hash, Filematch, Disk Explorer for NTFS, Disk explorer for FAT, DriveImageXL, Captain Nemo, DriveLook, Disk Investigator, Directory Snoop and Winhex.

If you are unsure if your tool is accepted in the industry, you can always check the Computer Forensics Tool Testing website (www.cftt.nist.gov). This project is sponsored by the National Institute of Standards and Technology (NIST) and it was created to help toolmakers to improve quality, for users to share knowledge and interested parties to understand tools capabilities. It features the Computer Forensics Tool Catalog that allows searching, accessing the tool taxonomy and a vendor access to keep updating the information about their tools. This site provides the testing methodologies of different forensic tools. The development process starts once a tool is selected by steering committee and testing environment will be defined for the selected forensic tool. Then, the next phase is the tool test process where the tool will

be acquired, the documentation will be reviewed, test cases will be created, a test strategy will be designed, tests will be executed, test reports will be produced the steering committee evaluates the report, assigned vendor will then review the test report and the last steps will include posting support software and test report to NIST and the Department of Homeland Security (DHS) websites.

CFTT information is provided in different tool categories including disk imaging, forensic media preparation, write block for software, write block for hardware, deleted file recovery, mobile devices, forensic file carving, string search, Windows registry tools and to download raw test files generated in the the testing cases. In addition, NIST maintains the Computer Forensic Reference Data Sets (CFReDS) site for digital evidence, digital investigators can find sets of simulated digital evidence for examination, validating their own software tools, training, equipment check outs and proficiency testing of digital investigators. And finally, NIST also provides another site that maintains a catalog for computer forensic tools and techniques where searches can be performed by forensic tool functionalities including the following:

- Cloud Services
- Data Analytics
- Database Forensics
- Deleted File Recovery
- Disk Cataloging
- Disk Imaging
- Drone Forensics
- Email Parsing
- File Carving
- Forensics Boot Environment
- Forensic File Copy
- Forensic Tool Suite (Mac Investigations)
- Forensic Tool Suite (Windows Investigations)
- GPS Forensics
- Hardware Write Block
- Hash Analysis
- Image Analysis (Video & Graphics Files)
- Incident Response Forensic Tracking & Reporting
- Infotainment & Vehicle Forensics
- Instant Messenger
- Live Response

- Media Sanitization/Drive Re-use
- Memory Capture and Analysis
- Mobile Device Acquisition, Analysis and Triage
- P2P Analysis
- Password Recovery
- Remote Capabilities / Remote Forensics
- Social Media
- Software Write Block
- Steganalysis
- String Search
- Video Analytics
- Video Format Conversion
- VoIP Forensics
- Web Browser Forensics
- WiFi Forensics
- Windows Registry Analysis

Commercial applications and suites:

Individual applications are used for specific purposes. The following utilities are organized by vendors:

AccessData: EDiscovery and SilentRunner

Guidance Software: Encase Forensics and Neutrino

Paraben: P2 Commander, Forensic Replicator, Decryption Collection and Lockdown

Pinpoint Labs: SafeCopy, Metadiscover and PG Pinpoint

X-Ways: WinHex, Capture and Trace

A digital forensic suite is a group of utilities with a wide variety of functions. Most of these suites include forensic imaging, data search, recovery functions, a hash generator and reporting capabilities.

Some commercial suites are:

Windows: AccessData, Guidance Software, Paraben and X-Ways Forensics/ Investigator

Linux: The Sleuth Kit, Forensic or Rescue Kit (FoRK) and FCCU Forensic Boot CD

Mobile Device Forensics (MF) is an interdisciplinary field that involves smartphones and satellite navigation systems. These devices include operating systems like Android, Blackberry, iOS, Maemo, Symbian, WebOS and Windows Mobile. While traditional application and suite tools are mostly

used to retrieve data from this kind of mobiles devices, other tools are also required from time to time.

Finally, it is the selection of forensics tools for cloud computing environments. While some of the existing tools can be used for certain tasks; there are many challenges that require more research like acquisition of remote data, large data volumes, distributed and elastic data, data ownership and chain of custody.

Cano (2011) highlights that digital investigations in cloud computing environments, are completely different than traditional cyberforensics scenarios. Data analysis is fairly complex, virtualization and traditional tools must be suitable to cloud cyberforensics investigations. As this is a new technological ecosystem for cyberforensics investigations.

Other Tools

Some additional devices are needed to do the job of any cybersecurity analyst or investigator. The non- technical tools are:

- A laptop computer
- A digital camera with video recording capacity
- A digital audio recorder
- Antistatic bags
- A Faraday shield
- Presslock bags
- Adhesive labels
- Felt-tip pen

Anti-Forensics (AF)Tools

Anti-Forensics (AF) is the process of utilizing tools and techniques that infringe forensic scientific methodologies, investigations and the work of digital investigators. Harris (2007) defines anti-forensics as any attempts to compromise the availability or usefulness of evidence to the forensics process.

Several AF categories have been defined by academics and practitioners (Table 5):

Hilley (2007): Use of metasploit exploits, stenography, data wiping and encryption

Rogers (2007): Datahiding, artifact wiping, trial obfuscation and attacks against the cyberforensics process/tool. Table 1 provides more details about Roger's taxonomy.

De Lucia (2013): Datahiding, obfuscation and encryption, data forgery, data deletion and physical destruction, analysis prevention and online anonymity

The most prevailing AF techniques are to overwrite or destroy data. Some overwriting tools include disk sanitizers (Microsoft remove hidden data, cipher and ccleaner) and timestamp eliminators (timestomp).

Table 5. Anti-Forensic categories – Rogers (2007)

Anti-Forensic categories	
Datahiding	· Rootkits · Encryption · Steganography
Artifact wiping	· Disk cleaner · Free space and memory cleaners · Prophylactic
Trial obfuscation	· Log cleaners · Spoofing · Misinformation · Zombied accounts · Trojan commands
Attacks against the Cyberforensic process/ tools	· File signature altering · Hash fooling · Nested directories

The use of cryptography and steganography tools like EFS, TrueCrypt, Onion routing, Burneye, rootkits, Slacker, FragFS, RuneFS, KY FS and Data Mule FS.

Tools, techniques and utilities to minimize the footprint like memory injection, buffer overflow exploits, Userland Execve, Syscall proxying. The use of CDs, bootable USB tokens and virtual machines to run code without leaving digital traces.

Online storage and anonymous activities include using anonymous e-mail accounts, attacker's data that can be stored anywhere and the use of BGP (Border Gateway Protocol) to create spoof IP addresses to launch cyberattacks.

And the use of techniques to attack cyberforensic investigators, exploit cyberforensic tool bugs and even to implicate them. Some of these attacks exploit buffer-overflow bugs in programs like tcpdump, snort and ethereal. By

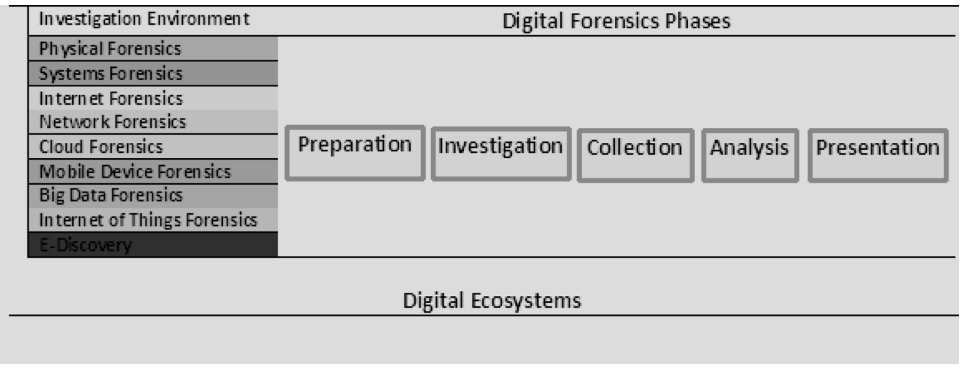
launching Denial-of-Service (DoS) attacks that use techniques like creating millions of files, overwhelming the logs and using zip bombs (42.zip).

Furthermore, The Software Engineering Institute (SEI) from the Carnegie Mellon University has developed the Digital Intelligence and Investigation Tools (DIID) with restricted access tools exclusively for law enforcement agencies (Live View LE, CCFinder, CryptHunter and ADIA) and unrestricted free access tools (AfterLife, Live View, DINO, LATK and CERT Linux Forensics Tools Repository). SEI also offers a wide range of methods and tools in the areas of acquisition support, cybersecurity engineering, cyber risk and resilience management, digital intelligence and investigation, insider threat, measurement & analysis, network situational awareness, performance & dependability, risk management, secure coding, smart grid, software architecture, software product lines, system of systems and vulnerability analysis.

THE CYBER FORENSICS MODEL IN DIGITAL ECOSYSTEMS (CFMDE)

We introduced the "Cyber Forensics Model in Digital Ecosystems" in our previous research (Sabillon et al., 2017). The model combines the traditional cyber forensics phases with all the diverse digital environments that create digital ecosystems. The main phases of the model (Figure 1) are preparation, investigation, collection, analysis and presentation that can run on a specific investigation or combined with several forensic environments.

Figure 1. Cyber Forensics Model in Digital Ecosystems (CFMDE)



The model consists of the following phases that are applicable to any or multiple investigation environments:

Preparation: This initial phase involves all the required planning for a specific environment or in multiple environments.

Investigation: This phase deploys the response plan to the incident

Collection: Relevant data is collected based on the approved methods and techniques

Analysis: Significant digital evidence is selected and the drawing of conclusions

Presentation: The findings of the digital investigation are presented

The investigation environments are suitable for physical forensics, systems forensics, Internet forensics, network forensics, cloud forensics, mobile device forensics, big data forensics. IoT forensics and e-discovery.

This model in comparison with the studied DF methodologies focuses on:

- Defining emergent environments for digital investigations
- Identifying all data sources and digital evidence acquisition
- Determining the digital evidence requirements and chain of custody management
- Integrating DF practices in digital ecosystem environments

The main objectives of this model are to consider emergent technological trends in cybercrime investigations and to align digital forensic investigations within digital ecosystems.

CONCLUSION AND FUTURE RESEARCH

Digital investigations can be time sensitive in order to identify, collect, preserve, assess, analyze and present digital forensic evidence. Digital investigations and forensics analysis are conducted on systems or digital devices suspected of storing digital evidence linked to a cyberincident or crime. Cyber forensic investigators must have expertise in the tools, techniques and procedures that they operate when conducting cyber investigations and build their cases. Each tool does have weaknesses and strengths that require a substantial use in either corporate, lab or field environments. Digital Forensics tools are available for all phases of an investigation including acquisition, validation, verification, extraction, reconstruction and reporting.

Nelson et al. (2019) highlight that digital forensics investigators must be aware that tools are encompassed in lifecycles where these tools are following procedures and standards for developing, updating, patching, reviewing and decommissioning. Provisoning of Digital Forensics (DF) tools are available as open source, commercial and suite packgages, further consideration for acquiring these tools must be decided based on specific criteria, new features and improvements.

The challenges will remain to expand over the coming years but cyber investigators have to attain common technical and legal standards; in order to create a strong model for the use of cyberforensic tools and the fight against anti-forensics practices.

Cybercrime is global issue that generates many financial losses and jurisdictional and political issues as well. Cyberattacks and further consequences can affect people's privacy, corporate reputation and in many cases are never ever reported for a follow up action or investigation.

In this chapter, we stress the importance of aiming digital investigations towards criminal digital ecosystems. One way or another, the Digital Forensics methodologies in the last three decades are not being effective in dealing with the international magnification of cybercriminality.

The Digital Forensics community demands new approaches to investigate and prosecute cybercriminals. Traditional digital forensics phases need to be redesigned to keep up with vast amount of new technologies and to counterattack new and diverse Techniques, Tactics and Procedures (TTP) of cybercrime.

Digital forensics methodologies, phases, tools, techniques, digital investigations, digital evidence collection and cyber investigators must constantly adapt to new technologies, environments, scenarios, best practices and regulations. The functionalities of DF tools need global frameworks and standards in order to conduct better cyber investigations and especially, international cooperation and collaboration ought to improve to start fighting cybercrime more aggressively.

DFRWS (2016) has classified future digital forensics challenges like forensic analysis for the Invisible Internet (I2P), evidence in the cloud, Windows 10, Internet of Things (IoT), unmanned aerial vehicles (drones), abstraction of digital evidence, malware, pattern searching, graph queries of digital evidence, visual analytics techniques and automation of forensic artifacts. Future research of these new DF challenges must aim at creating new tools, methodologies and technologies to improve early detection, investigation, containment and eradication of cyberattacks.

The spread of new digital devices will continue to grow at accelerated rates, likewise more advanced and sophisticated technologies will emerge in the years to come. Digital Forensics must evolve with new holistic approaches and paradigms to face these coming challenges.

REFERENCES

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security*, *5*(1), 118–131.

Amshire, V., & Meshram, B. (2012). Digital Forensic Tools. *IOSR Journal of Engineering*, *2*(3), 392–398. doi:10.9790/3021-0203392398

Arief, B., Bin Adzmi, M., & Gross, T. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1—Attackers. *IEEE Security and Privacy*, *13*(1), 71–76. doi:10.1109/MSP.2015.19

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013, December). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349. doi:10.1016/j.diin.2013.10.003

Batyamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *Proceedings of the Digital Forensic Research Conference (DFRWS 2004)*, 1-9.

Beebe, N., & Clark, J. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigation*, *2*(2), 146–166. doi:10.1016/j.diin.2005.04.002

Cano, J. (2016). *Cinco premisas de la delincuencia digital en un mundo digitalmente modificado*. Retrieved from https://www.linkedin.com/pulse/cinco-premisas-de-la-delincuencia-digital-en-un-mundo-jeimy

Cano, J. (2016). *Ecosistemas Digitales Criminales: La nueva frontera de los investigadores forenses informáticos*. Retrieved from http://insecurityit.blogspot.ca/2016/03/ecosistemas-digitales-criminales-la.html

Cano, J., & Cifuentes, J. (2012, April). Analysis and Implementation of Anti-Forensics Techniques on ZFS. *IEEE Latin America Transactions*, *10*(3), 1757–1766. doi:10.1109/TLA.2012.6222582

Carnegie Mellon University. (2016a). *Digital Intelligence and Investigation Tools*. CERT, Software Engineering Institute. Retrieved from https://www.cert.org/digital-intelligence/tools/

Carnegie Mellon University. (2016b). *Tools & Methods Developed at the SEI*. CERT, Software Engineering Institute. Retrieved from https://www.sei.cmu.edu/tools/

Casey, E. (2004). *Digital evidence and computer crime*. Elsevier Academic Press.

Ciardhuain, S. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, *3*(1), 1–22.

Cisar, P., Maravic, C., & Bosnjak, S. (2014). *Cybercrime and Digital Forensics – Technologies and Approaches. DAAAM International Scientific Book*. DAAAM International.

Davidoff, S., & Ham, J. (2012). *Network Forensics: Tracking Hackers through Cyberspace*. Prentice Hall.

De Lucia, E. (2013). *Anti-forensics – Part 1*. Retrieved from https://resources.infosecinstitute.com/anti-forensics-part-1/

Department of Homeland Security -DHS. (2020). *Computer Forensic Tool Testing (CFTT) Reports*. Retrieved from https://www.dhs.gov/science-and-technology/nist-cftt-reports

Digital Forensic Research Workshop – DFRWS. (2016). *Roadmap*. Retrieved from http://www.dfrws.org/roadmap

Dykstra, J., & Sherman, A. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation, 9*, S90-S98.

Federal Bureau of Investigation - FBI. (2015). 2015 Internet Crime Report. Internet Crime Complaint Center (IC3), U.S. Department of Justice.

Federal Bureau of Investigation - FBI. (2018). 2015 Internet Crime Report. Internet Crime Complaint Center (IC3), U.S. Department of Justice.

Freiling, F., & Schwittay, B. (2007). A Common Process Model for Incident Response. *Proceedings of the IT Incident Management and IT Forensics Conference*, 19-40.

Garfinkel, S. L. (2007). Anti-Forensics: Techniques, Detection and Countermeasures. *ICIW 2007*. Retrieved from http://simson.net/ref/2007/slides-ICIW.pdf

Graves, M. (2014). *Digital Archaeology: The Art and Science of Digital Forensics*. Addison-Wesley.

Hilley, S. (2007, March). Anti-forensics with a small army of exploits. *Digital Investigation*, *4*(1), 13–15. doi:10.1016/j.diin.2007.01.005

Ieong, R. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3S*, S29–S36. doi:10.1016/j.diin.2006.06.004

ISACA (2013). *Transforming Cybersecurity*. Rolling Meadows: ISACA Cybersecurity Nexus.

Jadhao, A., & Agrawal, A. (2016). A Digital Forensics Investigation Model for Social Networking Site. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS 16)*. New York: ACM. 10.1145/2905055.2905346

Jain, N., & Kalbande, D. (2015). Digital Forensic Framework using feedback and case history keeper. *Proceedings of the 2015 International Conference on Communication, Information & Computing Technology (ICCICT),* 1-6. 10.1109/ICCICT.2015.7045670

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology.

Khatir, M., Hejazi, S., & Sneiders, E. (2008). Two-Dimensional Evidence Reliability Amplification Model for Digital Forensics. *Proceedings of the Third International Annual Workshop on Digital Forensics and Incident Analysis*, 21-29. 10.1109/WDFIA.2008.11

Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forensic Investigation. *Proceedings of Information Security South Africa (ISSA) from Insight to Foresight Conference*, 1-7.

Kruse, I. I. W., & Heiser, J. (2002). *Computer Forensics: Incident Response Essentials*. Addison-Wesley.

Marcella, A. J., & Menendez, D. (2008). *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes* (2nd ed.). Auerbach Publications.

McAffee. (2014). Net Losses: Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II. Center for Strategic and International Studies. Santa Clara: Intel Security.

National Institute of Standards and Technology – NIST. (2016). *Digital Evidence*. Retrieved from https://www.nist.gov/property-fieldsection/digital-evidence

National Institute of Standards and Technology – NIST. (2020). *Computer Forensics Tool Catalog*. Retrieved from https://toolcatalog.nist.gov/

National Institute of Standards and Technology – NIST. (2020). *Information Technology Laboratory: Computer Forensics Tool Testing Program*. Retrieved from http://www.cftt.nist.gov/

National Institute of Standards and Technology – NIST. (2020). *The Computer Forensic Reference Data Sets (CFReDS)*. Retrieved from https://www.cfreds.nist.gov/

Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations (6th ed.). Boston, MA: Cengage Learning, Inc.

Palmer, G. (2001). DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research. *Proceedings of The Digital Forensics Workshop (DFRWS 2001)*, 1-42.

Perumal, S. (2009). Digital Forensis Model based on Malaysian Investigation Process. *International Journal of Computer Science and Network Security*, *9*(8), 38–44.

Pilli, E., Joshi, R., & Niyogi, R. (2010). A Generic Framework for Network Forensics. *International Journal of Computers and Applications*, *1*(11), 1–6. doi:10.5120/251-408

Politt, M. (1995). Computer Forensics: An Approach to Evidence in Cyberspace. *Proceedings of the National Information Systems Security Conference*, *2*, 487-491.

Prayudi, Y., Ashari, A., & Priyambodo, T. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*, *7*(11), 1–8. doi:10.5815/ijcnis.2015.11.01

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics. Security and Law*, *1*(2), 19–37.

Sabillon, R. (2016). Digital Forensic Analysis of Cyber crimes: Best Practices and Methodologies. In *Proceedings of the 2nd International Conference on Cyber Security (ICCS) 2016*. Rajasthan Technical University.

Sabillon, R., Cano, J., & Cavaller, V. (2014). Digital Evidence Acquisition Using Cyberforensic Tools. *ISSA Journal*, *12*(7), 22–27.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. & Cano, J. (2017). Digital Forensic Analysis of Cyber crimes: Best Practices and Methodologies. *International Journal of Information Security and Privacy, Special Issue: Cyber Security and Privacy in Communication Networks, 11*(2), Article 3.

Scientific Working Group on Digital Evidence – SWGDE. (2014). SWGDE Best Practices for Computer Forensics. *Version*, *3*(1), 1–12.

Selamat, S., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *International Journal of Computer Science and Network Security*, *8*(10), 163–169.

Sindhu, K., & Meshram, B. (2012). Digital Forensics and Cyber Crime Datamining. *Journal of Information Security*, *3*(3), 196–201. doi:10.4236/jis.2012.33024

Software Engineering Institute -SEI. (2020). *Software and Tools*. Carnegie Mellon University. Retrieved from https://www.sei.cmu.edu/publications/software-tools/index.cfm

Tahiri, S. (2016). *Digital Forensics Models*. Infosec Institute. Retrieved from https://resources.infosecinstitute.com/digital-forensics-models/

Talib, A., & Alomary, F. (2015). Towards a Comprehensive Ontology Based-Investigation for Digital Forensics Cybercrime. *International Journal on Communications Antenna and Propagation*, *5*(5), 263–268. doi:10.15866/irecap.v5i5.6112

Venter, J. (2006). *Process Flows for Cyber Forensics Training and Operations*. Retrieved from http://researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter_2006.pdf

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics. *International Journal of Computer Science & Information Technology*, *3*(3), 17–31. doi:10.5121/ijcsit.2011.3302

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Anti-Forensics Tools: Tools, procedures, and techniques use to counteract the forensics methodologies.

Classes of Cyber Forensics: These classes involve physical, systems, internet, network, cloud, mobile, big data, and internet of things (IoT) forensics.

Cyber Forensics: Methodologies and techniques used to preserve, collect, validate, analyze, interpret, document, and present evidence from digital devices for civil or criminal investigations, to prove and prosecute cybercrime.

Cyber Forensics Tools: Any tool including hardware and software that can be used in digital investigations to obtain, process, analysis, and document electronic evidence.

Cyberattack: Attack that is launched against one or more specific cyber assets in order to cause disruption or damage.

Chapter 4
Electronic Discovery (E-Discovery)

ABSTRACT

The objective of this chapter is to review the concept of electronic discovery(e-discovery) paying special attention to the legally established procedures for consideration as digital evidence, to the computer tools developed for obtaining them, as well as to the historical background that frame its origin. The authors review techniques and functionalities associated with advanced information systems and describe the possibilities and limits for the evaluation and exploitation of electronic discoveries in the cloud, in social networks, as well as in bring your own device (BYOD), big data, or business intelligence settings. It also includes a review of the reference frameworks, standards, and resources associated with the EDRM model (electronic discovery reference model).

INTRODUCTION

Electronic discovery (E-discovery) is the set of traditional legal procedures in a digital framework in order to obtain evidence to be presented in civil and criminal litigation, digital evidence is based on information stored in digital media. Electronic discovery is also considered as data mining, a method that allows obtaining information about clients, suppliers and also to support judicial investigations. Digital evidence can be acquired from various static devices, as well as mobile devices. Data and metadata can be obtained from

DOI: 10.4018/978-1-7998-4162-3.ch004

any electronic means of a user, an organization or that are hosted in the cloud. There are some perspectives on this, when producing digital evidence based on those who obtain it. In the first instance, electronic discovery experts are more legal oriented and usually tend to hire forensic cyber experts to obtain what is required by being technical specialists. In contrast, forensic cyber experts do not consider electronic discovery as part of their work. In the case of police units, data extraction and copying are executed directly.

Initially, it is necessary to define the scope of the electronic discovery to be executed, this includes establishing the types of data to be collected in certain places or provided by certain system administrators.

A larger scale scope will include the increase of the established budget due to tasks of storage, search and evaluation of data that could not be relevant in digital research. Nevertheless, we must clarify what types of computer tools will be used to perform the necessary data filtering. Finally, how the digital evidence obtained will be transferred, converted and presented in a court of law.

HISTORY AND FRAMEWORKS

Although the English term ‘e-discovery’ is quite new, the field as such has already existed for several decades. For example, legal demands in the 70s and 80s did not have the support of today’s digital evidence, the evidence at that time was based on huge paper-printed listings.

The history of electronic discovery is mostly related to historical events that occurred when passing laws, regulations and events (Table 1) in North America.

Table 1. Historic events related to Electronic Discovery (e-Discovery)

	Year	Events
When?	1986	Computer Fraud and Abuse Act (CFAA)
	1996	Health Insurance Portability and Accountability Act (HIPAA)
	1997	Introduction of the “e-discovery” term
	2001	U.S. PATRIOT Act
	2002	Sarbanes-Oxley Act
	2006	Use of electronic discovery in the legal field
	2007	Sedona framework

In 1970, federal laws of the USA were modified with a view to clarifying the processes of electronic discovery. It was in 2005, that new reforms were proposed to adapt electronic documentation according to changing technology. Finally, the US Supreme Court approved all modifications to the laws of electronic discovery in 2006. The Computer Fraud and Abuse Act (CFAA) was created in order to counteract crime and electronic fraud. The regulations listed in Table 1 have been constantly evaluated and subjected to the updating of these laws, primarily aligned with electronic discovery, knowing that Information and Communication Technologies (ICT) are constantly being improved and updated. The aforementioned to justify that electronic discovery is becoming burdensome, takes a long time and it is necessary to evaluate vast amounts of data in electronic format. It should be noted that many laws and regulations in the global context are totally outdated with the electronic communications and information technologies of our time.

Since 2005, EDRM (Electronic Discovery Reference Model) is the de facto global entity in the electronic discovery industry. EDRM is at the forefront constantly proposing standards, best practices, tools, guides and test data to improve electronic discovery management and information governance. EDRM includes 276 organizations of which 179 are software providers, 69 law firms, an academic institution, 3 corporate groups and 24 corporations linked to electronic discovery and information governance.

EDRM has created a series of frameworks, standards and resources:

Frameworks:

1. Reference model of electronic discovery
2. Reference model of computer-assisted evaluation
3. Reference model of information governance
4. EDRM metrics model
5. Security and privacy risk reduction model

Standards:

1. EDRM phases
2. Model of EDRM code of conduct
3. Extensible Markup Language (XML) EDRM
4. Uniform Task-Based Management System (UTBMS) test data set for electronic discovery. UTBMS is a management system based on uniform tasks designed to facilitate the analysis of legal and cost tasks.

Resources:

1. Guides
2. Data set
3. Metrics
4. Technical documentation

EDRM FRAMEWORKS

1. Reference model of electronic discovery

This model is currently used globally in relation to electronic discovery. EDRM proposes that you can follow all the steps or some of them; even by following the steps in a different order from the one proposed. It begins with the governance of information for the creation of ESI, then the identification, preservation, collection, processing, review, analysis, production and presentation of the results found.

2. Reference model of computer-assisted evaluation

This model serves to expedite the process of classification of electronic documents using computer programs based on expert review. The goals are defined, the protocols are established, documents are codified, results are predicted, the results are tested, the results are evaluated and the goals are finally met.

3. Reference model of information governance

The Information Governance Reference Model (IGRM) is related to the governance of information between various agents to obtain an efficient and effective administration of it. The IGRM as a reference framework complements EDRM, can also be oriented to information management, regulation and IT Infrastructure.

4. EDRM metrics model

This model provides a frame of reference between electronic discovery issues and their projects. Specifically, between electronic discovery processes and how measurements can be made regarding information, activities and

results. Central variables such as volume, cost and time are identified and then evaluated against the seven nodes that correspond to the most important aspects in the development of electronic discovery. The nodes include custodians, systems, devices, status, formats, activities and quality assurance in all phases of EDRM life cycle.

5. Security and privacy risk reduction model

This model includes a series of steps to reduce the volume of private, protected and risky data. The model is used before producing or exporting private data, and then being separated from the rest of the information found.

Additionally, EDRM has created a matrix of responsibilities associated with the roles in electronic discovery.

Wortzman (2017) proposes to follow the 12 principles of Sedona Canada from the Second Edition (2015), the provincial rules, common law jurisdiction rules, federal court rules, the Ontario e-Discovery implementation committee model documents and the Uniform Law Conference of Canada (ULCC) to assist clients, counsel and judiciary in terms of e-Discovery needs. According to The Sedona Conference (2017), the latest Sedona edition (Third edition, October 2017) contains 14 practical principles for addressing electronic document production.

TECHNIQUES AND TOOLS FOR E-DISCOVERY

Boolean searches constitute the de facto solution for almost everything in electronic discovery. There are two methods that experts use in their searches; the first is to perform searches without categorizing the documentation to be used, obtaining irrelevant results and the second based on holistic reviews to find meaningful words, so that none of these methods usually have fully automated solutions.

To this end, searches can be improved using Boolean and Machine Learning searches. The Boolean operators that are basically used are “AND”, “OR” and “NOT” while the more advanced Boolean searches include searches for terms with some separation from others. Additionally, to expand searches, you can search for concepts and use fuzzy logic.

Machine learning or predictive programming is ideal when using tools that search large collections of documentation. This type of tools learns from user preferences, documents are first reviewed for preliminary results, then

the process will be repeated until better predictions are generated. In the next phase, the system separates the documentation into relevant, irrelevant and for further review and finally the lawyers complete the process by reviewing the separate documents.

Some tools in this area include:

- WordSmith: Program whose objective is to find word patterns
- AntConc: Program for concordance and text analysis
- Grep: Windows utility that prints a found pattern of words
- N-Grams: Attributes used in data mining and natural language processing tasks
- ANSI / ASQ Z1.4: It is a standard for the definition of samples and inspection of attributes in tables
- Sample categorization: Searching in other types of categories and subcategories

Business Intelligence (BI) is composed of a series of applications and technologies with multiple uses to improve organizational decisions. There are a good number of vendors that offer BI solutions such as IBM, Information Builder, Oracle, SAS, Microsoft, SAP and Microstrategy.

Organizational data resides in a structured or unstructured manner, whether online or offline, and can be hosted on databases, servers, storage devices, computers, mobile devices or in the cloud. Structured data is usually in databases, web servers and transactional systems such as ERP (Enterprise Resource Planning), Electronic Commerce (EC), CRM (Customer Relationship Management), SCM (Supply Change Management) and some other specialized applications in the areas of finance, human resources, accounting and engineering.

On the other hand, there is unstructured data found in many parts of an organization such as electronic documents, presentations, worksheets, emails, instant messaging, multimedia files and the list can continue to grow. Normally, electronic discovery has focused on unstructured data since the information found is easier to interpret by judicial investigators. In addition, structured data is discarded because of the complexity of the databases in which they reside and without due support of analytical tools they become very difficult to interpret. However, this type of data can be very useful to solve cases of electronic discovery.

In this context, there are very important considerations when trying to perform BI searches such as redundant data, data quality and movement.

Other relevant aspects include the migration, integration and ownership of the data. This leads us to the confluence of all the information that could be obtained to solve a digital investigation and consequently the integration of BI with electronic discovery tools.

In many corporate environments, Microsoft Exchange email servers are used and users receive their emails through the Outlook client application. Employees and consultants involved in illegal transactions can use email to commit crimes. There are some functionalities and tools that can be configured at the server level to preserve digital evidence in case of a legal electronic discovery.

As a measure to restore emails deleted by users, it is necessary to have an information backup policy. The absence of the above exposes an organization to potential legal sanctions, lawsuits and fines for lack of implementation of electronic discovery procedures and retention of digital and physical documentation.

Exchange includes features related to messaging and compliance policies:

1. On-site backup: System administrators are able to take control of data in personal mailboxes therefore eliminating the creation of .PST (Personal Storage Table) files
2. On-site and Litigation Retention: In Compliance Management status, emails and other components remain on hold while on-site searches are conducted and emails are maintained based on previously established query criteria. Under these conditions no component can be deleted, modified or manipulated considering that preservation can be indefinite or temporary.
3. On-site electronic discovery: Allows you to search mailboxes and then copy to an electronic discovery account or export the content to a PST file
4. Administrator audit logs: These logs show the operations performed by the administrators to the servers and the system configuration
5. Mailbox audit records: It is necessary to clearly authorize personnel with access to personal mailboxes because they may contain personal and confidential information. In this case, a court order will be necessary to proceed legally.
6. Data loss prevention (DLP): In the version of Exchange 2016, 80 different types of information taxonomy are presented
7. Transport rules: These rules are used to configure certain accounts and define certain actions

This new functionality in Exchange 2016 allows unlimited searches in all mailboxes simultaneously, as administrator you must have access permissions in mailbox search management or be a member of the electronic discovery management group.

To perform compliance searches, a series of commands can be used using the Exchange Management Shell:

- Get-ComplianceSearch
- New-ComplianceSearch
- Remove-ComplianceSearch
- Set-ComplianceSearch
- Start-ComplianceSearch
- Stop-ComplianceSearch

The New-ComplianceSearch command is functional in Exchange 2016 servers and also in the services hosted in the Cloud. At least one object is required and mailboxes, distribution groups or all mailboxes in the organization can be included.

Additional parameters such as:

ContentMatchQuery: Exclusively to add a search filter using a text string or a query under the KQL (Keyword Query Language) format

AllowNotFoundExchangeLocationsEnabled: To include inactive mailboxes in the search

PublicFolderLocation: Used to specify the inclusion of public folders

Once the search is done, it must be verified if the criteria were found in the mailboxes. It is recommended that the search results be exported to another mailbox or that the objects found are placed in a hold state to perform the corresponding analysis. Other Microsoft applications such as SharePoint and Lync 2010/2013 have integrated electronic discovery features. You can export electronic discovery data in SharePoint using the Export function. Once you have made a query, then customize the results and save an external device.

For each exported file, an EDRM (Electronic Discovery Reference Model) XML manifest is included that includes metadata. Each file exported from SharePoint, Exchange and Lync 2013 includes:

- In Exchange, including Lync content in PST files
- In SharePoint, pages are exported in MHT format, listings as CSV files and documentation stored in their original format.

The new versions of Microsoft Exchange, SharePoint and Lync now called Skype for Business, include new electronic discovery features to support the regulations in force in any civil or criminal investigation.

A tool used in Linux environments is rsync, it serves to copy files locally, between servers or between remote machines. Rsync is used to copy links, devices, owners, groups and permissions. It does not require super user privileges; it is ideal for copying images and you can use a remote shell transparently either ssh or rsh.

ELECTRONICALLY STORED INFORMATION (ESI)

According to Wiles et al. (2007), the ultimate goal of e-discovery is to provide Electronically Stored Information (ESI) to any requesting party like the government, lawyers or any other third-party vendor. When identifying the locations of ESI, we need to consider inventories for on-site and off-site locations. Some approaches in identifying ESI include interviewing key individuals, performing network inventories using automated tools, completing physical inventories on on-site and off-site records, indexing archived backup tapes that are on-site and off-site, determining the level of accesibility of existing records and information and sample data restoration including collection techniques.ESI consists of type of files for processing and potential metadata within each type of file.

Common metadata fields are file name, file path, the unique identifier of file, document type, email, parent file, child file, duplicate, date accessed, date modified, date created, extracted text from file, author and character count. Personnel involved with e-discovery functions should be responsible in identifying all sources of Enterprise Content Management (ECM) like the lifecycle for information management, records and information management, email/Instant Messaging management, backup management, proprietary system management, network management, desktop/laptop management, Help Desk procedures, software development and web development. All these components will be later used to link Enterprise Content Management (ECM) with e-Discovery. ESI and e-Discovery have specific phases for preservation, collection, processing, indexing, searching, culling, extracting, reviewing and production of data and information.

DATA RECOVERY IS SOME SPECIFIC ENVIRONMENTS

e-Discovery in the Cloud

The electronic discovery of cloud computing does not yet have sufficient confidence in the procedures that providers could use to ensure a secure chain of custody. Organizations that store data in the cloud must negotiate properly with their suppliers, how the processes of electronic discovery would be managed before any legal request. The primary dilemma between cloud technologies and electronic discovery has to do with the geographic location of the data owner and where the evidence is stored. Therefore, it would prove to know under what jurisdiction the laws would apply to the evidence found in electronic discovery.

Transactional data hosted in the ASP (Application Service Provider) cloud is hardly available for electronic discovery, to achieve this the cloud data should be moved using a procedure called ETL (Process used in data storage to Extract, Transform and load the data.

e-Discovery for Social Networks

Social networks are undoubtedly an inexorable source for obtaining digital evidence in litigation, fraud, criminal investigations and compliance audits. Facebook reported in May 2013, that 4.75 billion objects of digital content were shared daily. Compared to 2012, there was a 94% increase based on 2.45 billion digital content and Twitter reports that 135,000 new users register daily. Although organizations have privacy policies, they are commonly violated by users when posting content that exposes the privacy of individuals and organizations.

With the increase of responsibility and also of the electronic discovery in social networks, it is necessary for organizations to implement appropriate policies in this regard, including plans for training the behavior in social networks of their employees. The greatest risks in this area entail the increase in information filtering and the discovery of electronically stored information (ESI) as well as the dissemination of private information.

Social networks can generate evidence for electronic discovery such as:

- User profile
- Wall posts

- Videos and photos
- User friend list
- Notes
- Event history
- Additional comments
- IP Addresses
- Session history
- Pending friend requests
- Account Logs
- Cell number
- City of residence and origin
- Family names
- Information about personal relationships
- Languages
- History of changes to the user's account

e-Discovery for BYOD

BYOD (Bring Your Own Device) programs allow employees and consultants to use personal equipment to do their job. These personal devices may include tablets, laptops, cell phones, external storage disks and USB drives among others. The study of trends in electronic discovery of Kroll Ontrack 2014 reports that 58% of legal offices and corporations experienced situations related to the electronic discovery of data in personal equipment. 26% of respondents participated in cases of which three or more issues of electronic discovery included data extracted from personal devices.

BYOD in cases for electronic discovery requires that digitally hosted information be accessible and equally relevant or proportional to the claims of the accusers or the defense. With the inevitable growth in the use of technology, companies, lawyers and judicial courts must include in their plans how to organize and evaluate electronic discovery in BYOD programs.

e-Discovery for Big Data

Massive data simply increases security risks in litigation. Forrester Research emphasizes that massive data has four characteristics that are volume, speed, variety and variability. In addition, it is not the amount of data to be explored

but the way they are manipulated by making use of techniques and technologies that become burdensome.

In the era of Big Data, it would be impossible to collect, search and review digitally stored data without adequate technological tools. These technological platforms allow sophisticated analyzes, robust searches and workflows to corporations and their teams of lawyers.

CONCLUSION

Electronic discovery researchers must remain flexible to obtain results by using predictive codes, social networks, BYOD, Internet of things and in Big Data. Additionally, they should prepare in the future to interact with best practices in information governance, custody chains, use of analytical tools in mass data, increase in the adoption of predictive codes, future regulations and modifications to current laws and regulations. Alignment of cybersecurity practices with electronic discovery and as technological advances continue, it is necessary to adapt the techniques, methods and processes to obtain digital evidence in cases of electronic discovery.

REFERENCES

Ambrogi, B. (2013). *Information Governance and E-Discovery in the age of Big Data*. ARMA International.

AntLab. (2020). Retrieved from: http://www.laurenceanthony.net/software.html

ASQ. (2016). *ANSI / ASQ Z1.4 and Z1.9*. Retrieved from: http://asq.org/knowledge-center/Z14.Z19/index.html

Brannon, N. (2010). Business Intelligence and E-Discovery. *Intelectual Property & Technology Law Journal*, *22*(7), 1–5.

Christensen, Q. (2012). Intro to eDiscovery in SharePoint, Exchange, and Lync 2013. *SharePoint Team, Microsoft*. Retrieved from: https://blogs.office.com/2012/11/08/intro-to-ediscovery-in-sharepoint-exchange-and-lync-2013/

EDRM LLC. (2016). Retrieved from: https://www.edrm.net/

Garrie, D., & Armstrong, M. (2004). *Electronic Discovery and the Challenge posed by the Sarbanes-Oxley- Act*. Legalthinktank.

Grep for Windows. (2020). Retrieved from: http://gnuwin32.sourceforge.net/packages/grep.htm

Hietala, J. (2014). *Linguistic Key Words in E-Discovery*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394254

Kroll Ontrack. (2014). *EDiscoveryTrends: Industry survey results*. Author.

Mota, N. (2016a). *Improvements to Compliance in Exchange 2016 (Part 1).* Retrieved from: http://www.msexchange.org/articles-tutorials/exchange-2016-articles/compliance-policies-archiving/improvements-compliance-exchange-2016-part1.html

Mota, N. (2016b). *Improvements to Compliance in Exchange 2016 (Part 2).* Retrieved from: http://www.msexchange.org/articles-tutorials/exchange-2016-articles/compliance-policies-archiving/improvements-compliance-exchange-2016-part2.html

Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2014). E-discovery: An Introduction to Digital Evidence. Boston: Cengage Learning.

Pramas, T., Berres, A., & Bjorklund, S., & Ellison. (2014). Using Technology to facilitate production of E-discovery. *William Mitchell Law Review*, *40*(20), 8.

Rsync webpages. (2020). Retrieved from: https://rsync.samba.org/

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2016). Descubrimiento Electrónico: Retos y Tendencias. *Proceedings of XVI Jornada de Seguridad Informática ACIS*.

Sipior, J., Ward, B., Volonino, L., & MacGabhann, L. (2013). A framework for the E-Discovery of Social Media Content in the United States. *Information Systems Management*, *30*(4), 352–358. doi:10.1080/10580530.2013.832965

Text Mining & Analytics. (2015). *Text Mining, Analytics & More*. Retrieved from: http://www.text-analytics101.com/2014/11/what-are-n-grams.html

The Sedona Conference. (2017). *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (3rd ed.). Retrieved from https://thesedonaconference.org/publication/The_Sedona_Principles

Wiles, J. (2007). *Techno Security's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook for Investigators, Examiners, IT Security Managers, Lawyers, and Academia*. Syngress Publishing, Inc.

Windows software for finding word patterns. (2020). Retrieved from: https://lexically.net/wordsmith/

Wortzman, S. (2017). *E-Discovery in Canada* (3rd ed.). LexisNexis Canada Inc.

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Electronically Stored Information (ESI): Designated electronically information that can be collected and processed as electronic evidence in e-discovery investigations.

Sedona Principles: Electronically stored information authoritative guidelines provided the Canadian Sedona Conference.

APPENDIX 1

The Sedona Principles, Third Edition. Published on the Sedona Conference website at https://thesedonaconference.org/publication/The_Sedona_Principles

Table 2. The Sedona Principles for Electronic Discovery (e-Discovery). Third Edition

Principles	Content
Principle 1	Electronically stored information is generally subject to the same preservation and discovery requirements as other relevant information.
Principle 2	When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(1) and its state equivalents, which requires consideration of the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.
Principle 3	As soon as practicable, parties should confer and seek to reach agreement regarding the preservation and production of electronically stored information.
Principle 4	Discovery requests for electronically stored information should be as specific as possible; responses and objections to discovery should disclose the scope and limits of the production.
Principle 5	The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that is expected to be relevant to claims or defenses in reasonably anticipated or pending litigation. However, it is unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve each instance of relevant electronically stored information.
Principle 6	Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.
Principle 7	The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.
Principle 8	The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional.
Principle 9	Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.
Principle 10	Parties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions.
Principle 11	A responding party may satisfy its good faith obligations to preserve and produce relevant electronically stored information by using technology and processes, such as sampling, searching, or the use of selection criteria.
Principle 12	The production of electronically stored information should be made in the form or forms in which it is ordinarily maintained or that is reasonably usable given the nature of the electronically stored information and the proportional needs of the case.
Principle 13	The costs of preserving and producing relevant and proportionate electronically stored information ordinarily should be borne by the responding party.
Principle 14	The breach of a duty to preserve electronically stored information may be addressed by remedial measures, sanctions, or both: remedial measures are appropriate to cure prejudice; sanctions are appropriate only if a party acted with intent to deprive another party of the use of relevant electronically stored information.

Chapter 5
National Cybersecurity Strategies

ABSTRACT

This chapter studies the phases to unify our national cybersecurity strategy model (NCSSM) in any nation cyber strategy that is either under development or improvement stages. This methodology consists of developing international cybersecurity strategies, alliances, and cooperation with different stakeholders at all possible levels. The research evaluated the best practices of 10 leading countries and five intergovernmental organizations in terms of developing effective cybersecurity strategies and policies. The authors also assessed a series of cybersecurity best practices that can be aligned with cyber governance and cyber law when countries wish to develop or enhance national cyber strategies. Furthermore, they propose guidelines to audit the national cyber strategies by utilizing their cybersecurity audit model (CSAM). CSAM could be considered for conducting cybersecurity audits in any nation state in pursuance of reviewing and measuring the cybersecurity assurance, maturity, and cyber readiness and to detect the needs to increase cyber awareness to defend and protect critical cyber assets.

INTRODUCTION

A study from Luiijf et al. (2013) was conducted to research about the the structure, sections and elements of nineteen National Cybersecurity Strategies (NCSS) from these countries [Australia, Canada, Czech Republic, Estonia,

DOI: 10.4018/978-1-7998-4162-3.ch005

France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, New Zealand, South Africa, Spain, Uganda, The United Kingdom - UK (2009 and 2011) and The United States of America (USA)]. Most NCSS in this research, embraced a holistic approach for cyberspace, and all nations have considered international threats and risks in cyberspace. Most NCSS are focusing on societies, more specifically citizens, businesses, public sector and government. Subsequently, the authors proposed a structure for developing NCSS that encompasses an executive summary, an introduction, a strategic national vision on cybersecurituy, existing NCSS' relationships with other strategies at the national and international level and legal frameworks, any guidance principles, the definition of cybersecurity objectives, an inventory of tactical actions and a glossary.

As reported by NATO (2013), cyber operations indicate the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace, and under international laws States may be responsible for the conduction of cyber operations by their organs including non-state actors.

For several years, there have been four notorious domains in warfare: Air, Sea, Space and Land. With the information era booming, a new domain was added which is now Cyberspace. Lemieux (2015) reserached several events that led to the consolidation of cyber domains as part of modern warfare studies. Network-Centric Warfare (NCW) was conducive during the US military dominance during the 1991 Gulf War, commanders took advantage of NCW to maintain their forces informed at all times regarding situational awareness, troop movement and always outmaneuvering enemy forces. Henceforth, these battlefield experiences were observed and explored by Russia and China for further acceptance into their own military operations.

The US Department of Defense - DOD (DOD, 1991) published the *Joint Publication 3-0: Operations* which included 'Information' as the fifth warfighting domain to join the existing Air, Sea, Space and Land domains. The DOD (1996) declassified the *National Military Strategy for Cyberspace Operations (NMS-CO)* where information was escalated to the cyberspace domain.

Many nations are straighten out their cyber capabilities in cyberspace by proposing, creating, implementing and continuously updating a National Cybersecurity Strategy, policy or programme. Sabillon et al. (2016) described a cybersecurity policy as the instrument developed by nations to communicate

and express those aspects that want a state to protect in cyberspace. North Atlantic Treaty Organization - NATO (2019) introduced a repository with NCSS and legal documents for 81 countries [13 for Africa, 11 for Americas and The Caribbean, 19 for Asia and Oceania and 38 for Europe] and The European Union Agency for Cybersecurity (ENISA, 2019) maintains the ENISA NCSS map for the 28 member states of the European Union (EU) and for the 4 member states of the European Free Trade Association (EFTA) that lists the implementation date and the number of objectives of each NCSS . International Telecommunication Union (ITU) (2016) highlights that 72 out 193 member states have published a National Cybersecurity Strategy but the majority of countries now have a NCSS (ITU, 2019). According to the Global Cybersecurity Index GCI 2018 v3 (ITU, 2019), 58% of the United Nations members have a NCSS in place with Europe and countries from the Commonwealth of Independent States (CIS) with the highest numbers of nations with NCSS, while the Africa region has the lowest indicator (14 out of 44 countries with a NCSS).

NATIONAL CYBERSECURITY STRATEGIES (NCSS)

A cybersecurity policy is an instrument designed by nations to communicate and express selected aspects that want a state to protect cyberspace. It is a statement which embodies the stance of a nation to bind strongly to citizens, their rights and duties; now in a stage of the widespread reality of society where instant information, mobility and social networks are the norm of its operation. This perceptibility of cyberspace requires a renewed understanding of the relationships with others and with the nations. Given the background, cybersecurity in a state policy formalizes a decision that a country now declares as a digital territory – and it has extended where similarly will exercise sovereignty, knowing that virtual space is shared with other nations and possess a national synergy (Sabillon et al., 2016).

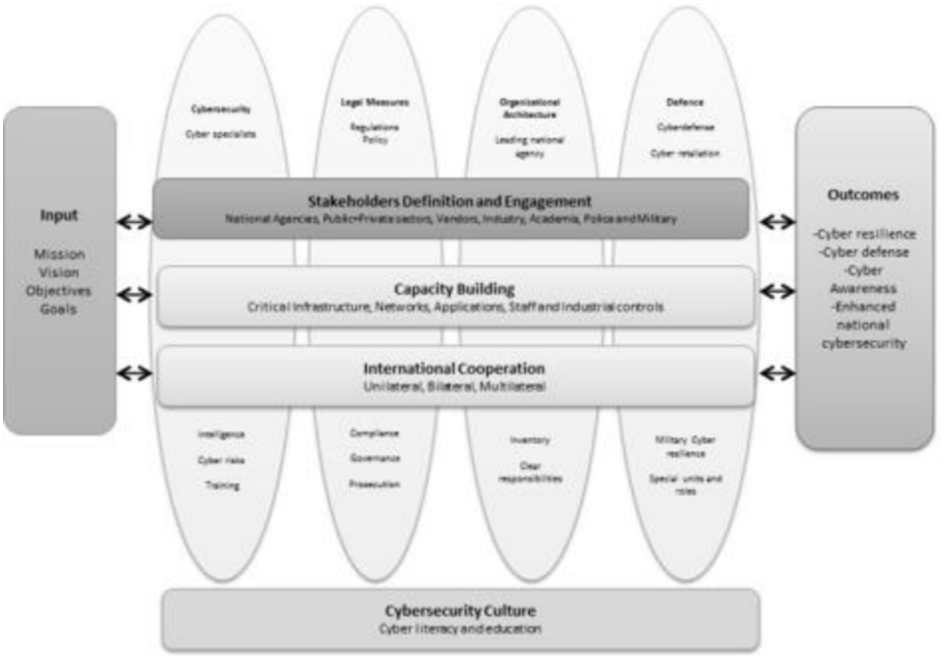
Our primary research was aimed to study national security strategies in ten countries from five different continents, study policy-making considerations from five global intergovernmental organizations and describe the most current cybersecurity frameworks. The fundamental research had five parts. Part I reviewed the main features of national cybersecurity strategies in Australia, Canada, Israel, Japan, Malaysia, Norway, South Africa, The Netherlands, The United Kingdom and The United States of America. Part II examined the national security strategy perspectives from intergovernmental organizations

like United Nations (UN), International Telecommunication Union (ITU), European Union (EU), the Organisation for Economic Co-operation and Development (OECD) and the North Atlantic Treaty Organization (NATO). Part III highlighted eleven cybersecurity frameworks that are in use globally. Part IV introduced a proposal of the National Cybersecurity Strategy Model (NCSSM) and all its components. And in Part V, we reviewed the international cooperation and knowledge transfer of the existing national strategies (Sabillon et al., 2016).

THE NATIONAL CYBERSECURITY STRATEGY MODEL (NCSSM)

We introduce a National CyberSecurity Strategy Model (NCSSM) that is based on our previous research (Sabillon et al., 2016). The NCSSM (Figure 1) contains eight pillars that are in constant interaction and it includes certain input features to become effective. Therefore, specific outcomes are in need to be assessed continually due to the changing nature of cyberspace. According

Figure 1. The National CyberSecurity Strategy Model (NCSSM)



to Greiman (2015), including the comparison of national cybersecurity strategies, and then our research is based on main components of any national strategy, goals, action plans, involved agencies and future developments to consolidate and expand the strategies

Our Model was designed on the recommendations that the ITU, NATO, OECD and EU introduced to include key aspects, stakeholders, components and pillars of any NCSS.

Input

This section requires a clear definition of the scope of the national cybersecurity strategy. Ideally, a clear understanding in terms of protecting critical information infrastructure must be achieved.

Mission, Vision, Objectives and Goals of the national cybersecurity strategy are identifiable at this stage.

The Pillars

Pillar 1: Cybersecurity Culture is the main pillar that supports the other pillars. How citizens and society apply the use of cyber security measures

Pillar 2: Stakeholders definition and engagement: A national agency will be in charge of the NCSS creation and implementation. All stakeholders must be identified with clear roles and responsibilities.

Pillar 3: Capacity Building: All necessary measures must be taken to ensure protection from cyber threats, risks and vulnerabilities. Baseline security requirements for each sector must be defined including a minimum set of cyber security measures. Specific cybersecurity standards and frameworks are selected. A cadre of cybersecurity professionals must be recruited.

Pillar 4: International Cooperation: Countries need to be involved with the cybersecurity policy making leaders including developed nations and intergovernmental organizations due to the international nature of cyber threats.

Pillar 5: Cybersecurity: This pillar helps to achieve a strong cybersecurity framework and work in harmony with all different stakeholders to ensure jurisdiction. Procedural measures include accountability, risk management, security policing, compliance and assurance. Lastly, the technical measures are aligned with core systems and networks in terms of administration, identifying cyber threats, inspections, IT health monitoring and audits.

Pillar 6: Legal Measures: Countries must engage in creating modern laws, policies to fight and prosecute cybercrime. Develop cyberlaw capacity including police, private sector, judicial and legislative branches.

Pillar 7: Organizational Architecture: This pillar is fundamental to define the NCCS coordinator and the different agencies that participate at the national level. Participating agencies are responsible to lead cybersecurity activities in all industries and sectors. A National CERT is defined

Pillar 8: Defense: Military forces and national security agencies are prepared to develop some kind of military cyber capability in protecting defense networks, cyber warfare activities, enabling network centric warfare or manage cyber warfare strategies.

Outcomes

Valid outcomes of NCSS must be continually evaluated using key performance indicators and objective performance metrics.

Cyber defense, Awareness, Cyber resilience and Enhancement of national cybersecurity output are the main components in this final phase.

In defance of, many nations have already implemented or are planning to implement a national cybersecurity strategy, very little efforts are targeted towards the contribution of international cybersecurity standardization, defining jurisdiction in international cyberspace or the contribution from developed nations to help developing countries to establish an initial cybersecurity programme, policy or strategy. There are just a few exceptions that can initiate the knowledge transfer, international cooperation and lessons learn sharing in these areas.

Consequently, existing national cybersecurity strategies include very little details for international cooperation in cybersecurity matters but in most cases this topic is inexistent or country leaders in cybersecurity topics are not interested in this kind of international cooperation. A consistent approach must be taken to defining a broader international cooperation to fight cybercrime, coordinate cybersecurity efforts and initiate a more aggressive approach for cyber governance and cybersecurity policy-making.

Nations like the USA, the UK and the Netherlands have a more consistent approach to international cooperation in cybersecurity matters.

The United States of America developed the *International Strategy for Cyberspace* that consists of core principles to support cyberspace operations like fundamentals freedoms, respect for property, safeguard privacy, protection

from cybercrime and the right of cyber self-defense[1]. The strategy intends to provide knowledge transfer to build cybersecurity capacity, to continually develop and share cybersecurity best practices, to enhance the ability to fight cyber criminality and to develop relationships with policy makers.[2]

The United Kingdom promoted an international dialogue at the London Conference on Cyberspace for the sake of developing international norms in cyberspace and The Netherlands through their national Cyber Security Council wish to collaborate with other countries to strengthen its international orientation. The Dutch Cyber Security Council wishes to expand the international network collaboration to develop national views.

THE CYBERSECURITY AUDIT MODEL (CSAM)

The CyberSecurity Audit Model (CSAM) is a comprehensive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place. The aim of this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS).

Guideline Assessment

The guideline assessment only applies to the Nation States domain. The guidelines are evaluated for cybersecurity culture, National Cybersecurity Strategy (NCS), cyber operations, critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy.

Evaluation Scorecard

The control, guideline and sub-control evaluation is calculated after the audit has been completed. The evaluation consists in assigning scores and ratings for each control, guideline and sub-control.

We calculate the final cybersecurity maturity rating of the Nation States domain by using the following criteria. The score can be mapped to a specific maturity level:

Immature (I): 0-30

The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy (NCS) or Policy is inexistent.

Developing (D): 31-70

The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace.

Mature (M): 71-90

While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters.

Table 1. Cybersecurity Maturity Rating of the Nation States Domain

Cybersecurity Audit Model (CSAM)					
Domain	**1-Nation States**				
Sub-Domain: 1.1 Cyberspace	**Ratings**				**Score**
	I	**D**	**M**	**A**	
1.1.1 Cybersecurity Culture	☐	☐	☐	☐	
1.1.2 National Cybersecurity Strategy	☐	☐	☐	☐	
1.1.3 Cyber Operations	☐	☐	☐	☐	
1.1.4 Critical Infrastructure	☐	☐	☐	☐	
1.1.5 Cyber Intelligence	☐	☐	☐	☐	
1.1.6 Cyber Warfare	☐	☐	☐	☐	
1.1.7 Cybercrime	☐	☐	☐	☐	
1.1.8 Cyber Diplomacy	☐	☐	☐	☐	
Final Cybersecurity Maturity Rating	☐	☐	☐	☐	

Auditing a National Cybersecurity Strategy using the CSAM

The CSAM has a specific domain "Nation States" and a sub-domain "Cyberspace" to audit the Cyber function at a national, state, province or territory level.

The Cyberspace sub-domain verifies controls in the cyber culture, National Cybersecurity Strategy, Cyber operations, critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy areas in Table 1.

Overall Nation State CyberSecurity Readiness (NSCSR)

The CyberSecurity Readiness rating can be classified for any Nation State as follows:

Immature (I): 0-30

The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy or Policy is inexistent. The Cybersecurity readiness is inexistent at this level.

Developing (D): 31-70

The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace. The Cybersecurity readiness is developing at this stage.

Mature (M): 71-90

While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses. The Cybersecurity readiness is at a mature level.

Advanced (A): 91-100

Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters. The Cybersecurity readiness is at an advanced level, but the Nation State must continually update its cybersecurity strategy at all times.

One of the most comprehensive guidelines (ITU, 2018) to develop a NCSS was recently designed for global cybersecurity leaders including the Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Deloitte, the Geneva Centre for Security Policy (GCSP), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the International Telecommunication

Union (ITU), Microsoft, the NATO Cooperative Cyber Defence Centre Of Excellence (NATO CCD COE), the Potomac Institute for Policy Studies, RAND Europe, The World Bank and the United Nations Conference on Trade and Development (UNCTAD). And the guide also focuses on seven areas for good practice: Governance, Risk management in national cybersecurity, Preparedness and resilience, Critical infrastructure services and essential services, Capability and capacity building and awareness raising, Legislation and regulation and Internal cooperation.

We strongly recommend that Domain 1 from our CyberSecurity Audit Model (CSAM) could be considered to plan and conduct partial or comprehensive cybersecurity audits of any NCSS in development, implementation, monitoring and evaluation phases.

CONCLUSION AND FUTURE RESEARCH

This chapter has fixated on analyzing our research regarding the creation, policy making, structure, implementation, sustaining and auditing national cybersecurity strategies and the cyber domain for nations.

The substance of the national strategies varies widely and each country structures the strategy based on their needs related to fight cybercrime, critical infrastructure protection, stakeholders engagement, cybersecurity awareness, cyber resilience, cyber intelligence gathering, cyber attacks alertness and eradication, cyber incident response, cybersecurity research and development, cyber police organization, communication, military involvement, law and judiciary collaboration, cyber governance and international cooperation.

As a result of our research, we present 'The National CyberSecurity Strategy Model (NCSSM)' that contains eight pillars: Cybersecurity Culture, Stakeholders definition and engagement; Capacity Building; International Cooperation; Cybersecurity; Legal Measures; Organizational Architecture; and Defense. The Model involves specific input features and the outcome is measured in terms of cyber defense, cyber awareness, cyber resilience and national cybersecurity.

We also included Domain 1: Nation States of our CyberSecurity Audit Model (CSAM) that evaluates cybersecurity culture, NCCS, cyber operations, cyber critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy. Some countries have a higher level of maturity than others when dealing with cyberspace, cybersecurity and national cybersecurity strategy policy-making. These leading countries have to recognize the importance

of international cooperation, alliance development to fight cybercrime, rule cyberspace and knowledge transfer of cybersecurity strategy matters.

The impediments of our study is that Domain 1: Nation States and Subdomain 1.1: Cyberspace from our CyberSecurity Audit Model (CSAM) have not been validated in a single Nation or State. Hereinafter, future testing will enhance the model architecture by engaging potential Nation States that may be interested in auditing their national cyberspace and strategy. Future studies will require to focus on the development of international standards and regulations to tackle cybercrime, to expand international cooperation in cybersecurity and national strategies. The challenges to overcome are to secure nations, keep peace in cyberspace while creating dynamic cybersecurity strategies.

REFERENCES

Australian Government. (2013). *Defence white paper 2013*. Canberra: Department of Defence, Commonwealth of Australia. Retrieved from http://www.defence.gov.au/whitepaper/2013/docs/wp_2013_web.pdf>

Australian Government. (2016). *Australia's Cyber Security Strategy*. Canberra: Department of the Prime Minister and Cabinet, Commonwealth of Australia. Retrieved from https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf

Benoliel, D. (2015). Towards a Cyber Security Policy Model: Israel National Cyber Bureau Case Study. *North Carolina Journal of Law & Technology*, 435–486. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https://www.google.ca/&httpsredir=1&article=1283&context=ncjolt

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010). *Cyber Security Governance, MITRE*. Retrieved from https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

Boyce, R. (2001). *Vulnerability Assessment: The Pro-Active Steps to Secure your Organization, SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453

Canadian Government. (2010). *Canada's Cybersecurity Strategy for a Stronger and More Prosperous Canada*. Ottawa: Her Majesty the Queen in Right of Canada. Retrieved from http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

Canadian Government. (2013). *Action Plan 2010-2015 for Canada's Cybersecurity Strategy*. Ottawa: Her Majesty the Queen in Right of Canada. Retrieved from https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf

CERT Division. (2017). *CSIRT Frequently Asked Questions, Carnegie Mellon University*. Retrieved from https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

Department of Defense. (2015). *Resilient Military Systems and the Advanced Cyber Threat. Defense Science Board*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Department of Homeland Security. (2012). *Vulnerability Assessment and Management, NICSS*. Retrieved from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/vulnerability-assessment-and-management

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*. Apress. doi:10.1007/978-1-4302-6083-7

Elran, M., & Siboni, G. (2015). Establishing an IDF Cyber Command. *The Institute for National Security Studies Insight, 719*, 1-3. Retrieved from https://www.inss.org.il/uploadImages/systemFiles/No.719-MeirandGabiforweb.pdf

European Network and Information Security Agency. (2012). *National Cyber Security Strategies: Practical Guide on Development and Execution.* Heraklion: ENISA. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

European Union. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission. Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Union Agency for Cybersecurity – ENISA. (2019). *National Cyber Security Strategies (NCSSs) Map.* Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Financial Executives International – FEI. (2014). *Financial Executives, Cyber Security & Business Continuity, Canadian Executives Research Foundation (CFERF).* Retrieved from https://www.feicanada.org/enews/file/CFERF%20studies/2013-2014/IBM%20Cyber%20Security%20final3%202014.pdf

Financial Industry Regulatory Authority – FINRA. (2015). *Report on Cybersecurity Practices*. Retrieved from https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Foresite. (2016). *Quick guide to common Cybersecurity Frameworks*. Retrieved from https://www.foresite.com/blog/quick-guide-to-common-cybersecurity-frameworks/

Greiman, V. (2015). Cyber Security and Global Governance. In *Proceedings of the 14th European Conference on Cyber Warfare & Security*. Hattfield: University of Hertfordshire.

International Telecommunication Union (ITU). (2012). *National Cybersecurity Strategy Guide.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

International Telecommunication Union (ITU). (2018). *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity.* Geneva: International Telecommunication Union ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

International Telecommunication Union (ITU). (2019). *Global Cybersecurity Index (GCI) 2018.* Geneva: International Telecommunication Union ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ISACA. (2013). *Transforming Cybersecurity.* Rolling Meadows: ISACA.

ISACA. (2014). *Implementing the NIST Cybersecurity Framework*. Rolling Meadows: ISACA.

ISACA. (2015). *Cybersecurity Fundamentals*. Rolling Meadows: ISACA.

Japanese Government. (2013). *Japan's Cybersecurity Strategy: Towards a World Leading, Resilient and Vigorous Cyberspace*. Tokyo: Information Security Policy Council. Retrieved from https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf

Kaspersky Lab. (2015). *Top 10 Tips for Educating Employees about Cybersecurity, AO Kaspersky Lab*. Retrieved from http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf

Lee, R. (2015). *The Sliding Scale of Cybersecurity, SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Lemieux, F. (2015). Current and emerging trends in cyber operations: Policy, Strategy and Practice. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity. New York: Palgrave Macmillan. doi:10.1057/9781137455550

Lindsay, J. (2013). Stuxnet and the limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. doi:10.1080/09636412.2013.816122

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*(1/2), 3–31. doi:10.1504/IJCIS.2013.051608

Malaysia Government. (2006). National Cyber Security. Purtrajaya: Minister of Science, Technology and Innovation. *ICT Policy Division*. Retrieved from http://www.cybersecurity.my/data/content_files/46/1235.pdf?diff=1392970989

Ministry of Economic Affairs and Communication. (2017). *2014-2017 Estonia Cybersecurity Strategy, ENISA*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

National Cyber Security Alliance. (2017). *Stay Safe Online, NCS*. Retrieved from https://staysafeonline.org/ncsam/

National Institute of Standards and Technology - NIST (2017). *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*. NIST.

National Institute of Standards and Technology – NIST. (2017). *NIST Special Publications SP*. Retrieved from https://csrc.nist.gov/publications/PubsSPs.html

NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE. (2019). *Cyber Security Strategy Documents*. Retrieved from https://ccdcoe.org/library/strategy-and-governance/

Netherlands Government. (2014). *National Cyber Security Strategy (NCSS)2: From awareness to capability. Den Haag: National Coordinator for Security and Counterterrorism, Minister of Security and Justice*. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

North American Electric Relaibility Corporation – NERC. (2010). *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, NERC*. Retrieved from <www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf

North Atlantic Treaty Organization. (2012). *National Cybersecurity framework manual*. Retrieved from https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

North Atlantic Treaty Organization. (2013). *The Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Norway Government. (2013). *Cyber Security Strategy for Norway*. Oslo: The Ministry of Government Administration, Reform and Church Affairs. Retrieved from https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf

Organisation for Economic Co-Operation and Development – OECD. (2012). *Cybersecurity Policy Making at a Turning Point, OECD*. Retrieved from http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

PCI Security Standards Council. (2014). *Best Practices for implementing a Security Awareness Program, PCI DSS*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Pricewaterhouse Coopers - PwC. (2016). *PwC's Board Cybersecurity Governance Framework, PwC*. Retrieved from https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf

Proaño, R., Saguay, C., Jacome, S., & Sandoval, F. (2017). Knowledge based systems as an aid in information systems audit. *Enfoque UTE, 8*(S1), 148-159. doi:10.29019/enfoqueute.v8n1.122

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, *9*(1), 127–137. doi:10.29019/enfoqueute.v9n1.214

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering, 5*, 67-81.

Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2016). Cyber Warfare: Challenges within the Cyber Domain. *European Journal of Public Order and National Security.*, *3*(4), 7–16.

Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *2nd International Conference on Information Systems and Computer Science (INCISCOS 2017),* 253-259. 10.1109/INCISCOS.2017.20

Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39. doi:10.4018/JCIT.2019070102

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *2017 Second International Conference on Information Systems and Computer Science (INCISCOS)*, Quito, Ecuador. 10.1109/INCISCOS.2017.20

SANS Institute. (2017). *SANS Forensics Whitepapers, SANS Institute*. Retrieved from https://digital-forensics.sans.org/community/whitepapers

Shackleford, D. (2015). *Who's using Cyberthreat Intelligence and how?* SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

South Africa Government. (2012). *South Africa National Cyber Security Policy Framework*. Pretoria: Minister of State Security. Retrieved from http://www.cyanre.co.za/national-cybersecurity-policy.pdf

The Organisation for Economic Co-operation and Development. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. Paris: OECD Publishing. Retrieved from http://www.oecd.org/sti/ieconomy/cybersecurity policy making.pdf

Trusted Computing Group. (2013). *Architect's Guide: Cybersecurity*. Retrieved from https://www.trustedcomputinggroup.org/wp-content/uploads/Architects-Guide-Cybersecurity.pdf

UN Institute for Disarmament Research. (2013). *The Cyber Index: International Security Trends and Realities*. Geneva: UNIDIR 2013. Retrieved from https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

UN Institute for Disarmament Research. (2017). *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. Geneva: UNIDIR. Retrieved from https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

United Kingdom Cabinet Office. (2011). *The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world.* London: UK Cabinet Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

United Kingdom Cabinet Office. (2014). *The UK Cyber Security Strategy - Report on progress and forward plans.* London: UK Cabinet Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

United States Computer Emergency Readiness Team - US-CERT. (2017). *Cybersecurity Framework, US-CERT*. Retrieved from https://www.us-cert.gov/ccubedvp/cybersecurity-framework

United States of America Government. (2003). *The National Strategy to Secure Cyberspace*. Washington, DC: The White House. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

United States of America Government. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington DC: The White House. Retrieved from https://www.hsdl.org/?view&did=5665

United States of America Government. (2017). The President's National Infrastructure Advisory Council (NIAC). In *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

U.S. Department of Energy. (2007). *IT Security Architecture*. Retrieved from https://energy.gov/sites/prod/files/cioprod/documents/DOE_Security_Architecture.pdf

U.S. Department of Homeland Security. (2016). *Cybersecurity*. Retrieved from https://www.dhs.gov/topic/cybersecurity

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Critical Infrastructure: The most important infrastructure or related services to provide basic sustenance to citizens like water, utilities, electricity, and internet connection.

Cybersecurity Culture: Manifestations of cybersecurity matters for any nation-state.

National Cybersecurity Policy: National instrument designed by nations-states to communicate and express selected aspects that want a state to protect cyberspace.

ENDNOTES

1 United States of America Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington D.C: The White House 2011), Ch. 1, 5.

2 United States of America Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 10-15.

Chapter 6
Cyber Warfare and the Challenges That Exist in the Cyber Domain

ABSTRACT

This chapter studies the cyber warfare phenomenon in all its dimensions in order to provide a wide conceptualization of factors and elements, strategies, generations, and theoretical models. On the second part of the chapter, a set of definitions is introduced in order to gain a common field of conceptual agreement for the explanation of the main theoretical models that have been developed for the cyber domain. The third section presents the dual cyber warfare model applicable to military and corporate environments. The authors conclude that cyber warfare is perhaps the most radical consequence of the knowledge era and must be systematically analyzed from both perspectives: empirical-practical and theoretical-conceptual.

INTRODUCTION

Studying cyber warfare in the cyberspace era can rapidly evolve into a matter of detecting cyber strengths and weaknesses in any national critical infrastructure, and we are not necessarily focusing on military protection. The US Department of Homeland Security (DHS) has identified key areas that are applicable to any nation: Defense, transportation, public health, energy, dams, defensive industrial base, banking, nuclear reactors, communications,

DOI: 10.4018/978-1-7998-4162-3.ch006

agriculture and food, chemical, emergency services, commercial facilities, government, information technology and postal system. Andress & Winterfeld (2014) established areas that are more directly connected with cyber warfare like communications, transportation, defense and defensive industrial base.

CYBER WARFARE

In order to understand cyber warfare in the digital age, we require to review how information warfare has transformed over time. Changes have been taking place in the technological, organizational and environmental areas.

Ryan et al. (2015) introduced three information warfare generations (IW 1.0, IW 2.0 and IW 3.0) that started with the use of information until our days with the growth of cyber warfare capabilities.

1. First generation (IW 1.0): Information in warfare started from the beginning of sentience to around the 1940s. Information was used as a leverage function. Some strategists like Sun Tzu, Napoleon Bonaparte and Carl von Clausewitz did concentrate in using information instead of engaging in combat. Main features of this time included the protection of information to reinforce and enhance conventional warfare.
2. Second generation (IW 2.0): Information as warfare emerged from World War II to roughly the 1980s. Important contributions like operations research development to leverage information in the engineering, information systems and the military fields. Information sophistication was instrumental to develop new ways to manage strategic operations. Some milestones that revolutionized this generation were the transistor era, electronic databases, packet-based networks, consumer electronics and the Internet commercialization.
3. Third generation (IW 3.0): Information as a warfighting domain is the period that we are currently living. Nowadays, information warfare is considered the warfare fifth domain similar to land, air, sea and space. Information warfare is something new and many stakeholders do not really know how to approach this concept. Scholars suggested that information warfare must include Electronic Countermeasures (ECM), Electronic Counter-Countermeasures (ECCM) and influence operations. New terms were added to our current generation including Computer Network Attack (CNA), Information Operations (IO), Computer Network Defense (CND) and Computer Network Exploitation (CNE).

These warfare generations are very differently from each other in terms of used artifacts and its effects, older information warfare generations are meaningful to perceive the current cyber warfare and cyberspace architecture. Countries will continue to create or update its national cybersecurity strategies, policies or programmes and ideally a section to address the protection, defense and cyber retaliation of national cyber assets and critical infrastructure must be included.

TERMINOLOGY

We intent to provide some previous definitions of cyber warfare components, although universal acceptance of these concepts has not been reached yet. We need to clarify nine critical components in our study, while global clearness may represent a great disadvantage for standardization of these terms. The following definitions are still under debate globally:

1. Cyberspace: The new arena for cyber related issues and challenges takes place in cyberspace- But what is cyberspace?

According to Kuehl (2009), his definition involves an operational space, a natural domain, it is based on information and between interconnected networks:

A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies.

McQuade (2006) defines it as "that amorphous realm through which the exchange of digitized information takes place."

2. Cybersecurity: Over the last decades, we have seen many changes to security operations and management. Many terms have been in use to highlight the protection of information assets: IT security, computer security, cybersecurity, information security and network security. All these concepts have been often utilized interchangeably.

ISACA (2015) defines cybersecurity as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

Kaplan et al. (2015) stated that cybersecurity is a delivery function that includes managing both technologies such firewalls, intrusion detection, malware detection, and identify and access management, and also activities that are focused primarily on protecting information assets and online processes such as compiling and analyzing threat intelligence and conducting forensic analysis.

3. Information warfare: Libicki (1995) studied the term by smaller parts that involved command and control, intelligence based, electronic, psychological, hacker, economic information and cyber. Kopp (2000) stated that the aim of information warfare is to corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity and availability of one's own information.

Robinson et al. (2015) summarized that the term can be used to describe a wide range of activities beyond the cyber domain and is unclear if cyber warfare is a form of information warfare.

4. Cyber warfare: Green et al. (2015) adapted a definition based on Shakarian and Clausewitz:

Cyberwarfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived).

According to Applegate (2015), Cyber warfare is the use of armed attacks in or through cyberspace as an extension of one nation-state's politics to impose its political will onto another nation-state. Moreover, he argues that probably two additional conditions will create a cyber warfare scenario:

– That multiples nation-states were involved
– And an armed attack or use of force has been deployed

5. Cyberattack: Donaldson et al. (2015) define it as an attack conducted using computers and information systems to compromise the confidentiality, integrity, or availability of the target's information and information system.

NATO (2013) on its Tallinn Manual provides a definition of cyberattack – Rule 30, that definition applies to international and non-international armed conflict:

A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction objects

6. Cyberwar: Robinson et al. (2015) presented a definition of cyberwar, it occurs when a nation state declares war, and where only cyber warfare is used to fight that war.

Brose (2015) studied the definitions that Arquilla and Ronfeld provided for "Cyberwar" and "Netwar". These researchers focused on cyberwar and netwar as two emergent warfare forms for potential research. Brose stated that cyberwar targets information systems and supports combat in the physical domain. While netwar targets societal self and world perceptions-it includes collective, personal, or machine- generated speech or action, economic choices, or other legally protected activities, in addition to acts of information conveyance, distortion, or denial that may or may not violate laws or sovereignty.

7. Cyberdeterrence: Liles (2013) defines cyberdeterrence as the ability of institutions and organizations to deny, protect and retaliate against cyberattacks.

Rivera (2015) defines it as the mechanism through which nation-states can communicate proportionate, reciprocal, and credible military power effects through cyberspace that strategically affect their adversary's decision-making calculus and the aim is to deter an adversary from conducting hostile actions through cyberspace and broader.

8. Cyberespionage: ISACA (2015) stated that cyberespionage are activities conducted in the name of security, business, politics or technology to find information that ought to remain secret and it is not inherently to the military.

Furthermore, cyberespionage is the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization (Oxford English Dictionary, 2016).

9. Cyberterrorism: Applegate (2015) defines it as the use of the information systems to conduct or threaten to conduct violent criminal acts in order to induce a state of terror in the general public, in the furtherance of a political, ideological, or religious agenda.

According to Clifford (2006), it consists of using computer technology to carry out terrorist acts that are intended to advance a political or social agenda.

Cyberspace Operations

According to NATO (2013), cyber operations refer to the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace, and under international laws States may be responsible for the conduction of cyber operations by their organs including non-state actors.

Traditionally, there have been four known domains in warfare: Air, Sea, Space and Land. With the booming of the information era, a new domain was added which is now Cyberspace. Lemieux (2015) summarized several events that led to the consolidation of cyber domains as part of modern warfare studies. Network-Centric Warfare (NCW) was instrumental during the US military dominance during the 1991 Gulf War, commanders took advantage of NCW to maintain their forces informed at all times regarding situational awareness, troop movement and always outmaneuvering enemy forces. Later on, these battlefield experiences were observed and explored by Russia and China for further acceptance into their own military operations.

The US Department of Defense (DOD -1991) published the *Joint Publication 3-0: Operations* which included 'Information' as the fifth warfighting domain to join the existing Air, Sea, Space and Land domains. The DOD (1996) declassified the *National Military Strategy for Cyberspace Operations (NMS-CO)* where information was escalated to the cyberspace domain.

But cyberspace is far beyond information and networking technologies, human interaction is also part of the 'Cyber' domain. According to Applegate (2015), cyberspace is structured in three different layers:

1. A physical layer: This layer consists of multiple physical interconnection devices like switches, routers, gateways; thus cables, wires, computers, information systems, servers, telecommunication channels and any physical device that connect private networks with the Internet. Special consideration must be taken seriously as these physical devices are located within any sovereign nation and proper jurisdiction rules are applicable.
2. A logical layer: It provides the transparent communication between nodes that are represented by Internet Protocol (IP) addresses. The numerous technologies that use dissimilar platforms to communicate with each other are not an inconvenience to end users.
3. A cognitive or social layer: The interactions that encircle information and human beings, this layer includes stored, transmitted and processed information on any Internet protocol. Moreover, from raw data to big data to sophisticated processed information of any kind.

Cyber Resilience

Axelos (2015) defines Cyber resilience as the ability to prevent, detect and correct any impact that incidents have on the information required to do business. We must stress that cyber resilience is not only applicable to the military but it also applies to corporate and organizational environments. A good cyber resilience strategy includes controls to prevent, detect and recover from cybersecurity breaches and cyberattacks. Bodeau et al. (2011:6) view cyber resilience as part of a national cybersecurity level based on improving the resilience to cyber incidents, to reduce cyber threats and can be viewed as integral to cyber operations or computer network defense as well.

Suarez et al. (2014) studied several frameworks and standards in the areas of cyber resilience and cybersecurity; the first part of the study compared ISO 22301, NIST-SP 800-30, Octave Allegro, ISO/IEC 27001, CRAMM, Magerit/ENS, ISO 27032 and SANS Critical Security Controls. The analysis included key indicators like governance, risk analysis, corporate environments, critical infrastructure, cyber incident reports, new cyber threats and metrics. Furthermore, the next part of the study analyzed cybersecurity metric management on standards like NIST-SP800-53, ISO 27004, CIS Security

Metrics, ENISA, CCN-STIC-815 and CYSPA. The conclusions stated that even tough that several cybersecurity standards exist, they lack a governance framework to lead organizations in terms of cyber resiliency neither to follow a metric approach to assess the maturity level of cyber resilience, information exchange, new cyber threats in cyberspace and incident management.

Cyberdeterrence

Ghionis (2015) summarizes that deterrence's aim is to conceive disincentives to avoid further hostile actions. The target threatens to counterattack but clearly states that repercussions will be avoided only if the attacks are called off. The strategy involves a defending state by deterring any cyber aggressor's malicious cyber activity in order to avoid engaging in destructive escalation of cyber attacks. Cyberdeterrence can be activated either as the cyber attackers turning back due to the target's cyber defenses in place or restraining further actions for fear of cyber retaliation.

Bendiek et al. (2015) identified deterrence-by-resistance and deterrence-by-resilience approaches; both approaches aim to reduce the cyberattacks by using cyber defense positions or by ensuring immediate recovery after a cyberattack. Wei (2015) presented the cyber deterrence components that in the cyber realm have three pillars: a credible defence, the ability to retaliate and the will to retaliate. The cyber defence of any country should be sufficient to stop cyberattacks, the ability to cyber retaliate will translate to identify the cyber attackers and to launch retaliatory actions that will cause greater damages than the inflicted by attackers and the will to retaliate will stop or dissuade the cyber attackers from launching further attacks.

Cyber Threat Landscape

The main obstacle comparing kinetic war and cyber warfare is separating activities from geography. The cyber domain includes the Internet as the new battlespace that can be used either as a resource and as an attack vector, reconnaissance can be done from anywhere, attackers and victims will utilize networking and information technologies to attack and defend their positions in cyberspace.

In our physical world, countries are separated by boundaries which is no longer the case in cyberspace but in cyber operations, a cyber battlespace will

comprise physical infrastructure, networks, computers, hardware, software, interconnection devices, communication channels and people.

Most active cyber threat actors are all categories of hackers – from script kiddies to elite hackers, organize crime agents, hacktivism, insiders, political attackers, religious attackers, cyberterrorism and cyberespionage.

Strategic Cyber Intelligence

Like in any military or police investigation, intelligence and counter intelligence tasks are vital for preparation and support of their operations. Moreover, the same principles ought to be adapted to cyber operations.

Andress et al. (2014) point out that Intelligence Preparation of the Battlefield (IPB) has transformed into Intelligence Preparation of the Operational Environment (IPOE) for modern warfare. On the other hand, it is now necessary to add the intelligence feed to cyberspace that support communication, influence operation and terrain.

Cyber IPOE is crucial to be fully involved inside the Observe/Orient/Decide/Act loop for cyber intelligence (OODA) loop, cyber intelligence must be timely, accurate, usable and complete.

Cyberspace Battlefield

The Cyber domain is applicable throughout all other domains: Air, Space, Land and Sea. This new domain is crucial to military commanders because it is a global domain that encircles information technology networks, the Internet, telecommunication networks, computers and embedded circuits. The Air and Space domains are very comparable to the cyber domains.

Cyber Doctrine

While Doctrine exists in all worldwide military forces, it is not clear if the countries exercising sovereignty in cyberspace have defined their own national cyber doctrine. Many nations are already defining or updating their national cybersecurity strategies, a section to clarify cyber doctrines is more than necessary to focus on military and civilian directives related to cyber warfare. The cyber doctrine definition must include agents from all members of society in order to defend, attack, deter and counterattack in cyberspace.

Cyber Weapons

Nowadays, current challenges exist to classify, differentiate, control and predict cyber weapons against traditional weapons used in kinetic wars.

The US Air Force designated six different cyber capabilities as weapons:

1. Air Force cyberspace defense
2. Cyberspace defense analysis
3. Cyberspace vulnerability assessment
4. Cyber command and control mission system
5. Air Force Intranet control
6. Cybersecurity and Control system

Cyber Warriors

A cyber warrior is someone that participates in cyber warfare operations either in the military or the technology fields, they can be part of cyber defensive or cyberattack operations. Many countries recruit young o veteran individuals to join national cybersecurity groups or cyber military units.

Cyber Wargames

Traditional kinetic wargames have been running for decades to prepare the military for real wars, but with the new cyber threats in cyberspace it is also necessary to conduct cyber wargames. Cyber wargaming can be conducted in military and corporate environments and can be set up around a specific scenario to simulate a significant cyber reality. According to Jajodia et al. (2015), cyber wargaming objectives are training, to test the utility of a new network defense, to assess the efficacy of recent modifications to the network sensor infrastructure, to test the skills of the organization's cyber intelligence analysts and to evaluate learning and testing strategies to rehearsals of critical operations.

Cisco (2015) developed their Cisco Security Posture Assessment specializing in corporate cyber war games. This role play framework evaluates any organization's blue team capabilities in terms of identification, defense, response and recovery from a cyberattack. The Cisco red team launches a prolonged and persistent attack while the organization's blue team deals with the cyber aggression. The assessment phases include alerting and detection

capabilities, first response, situational awareness, escalation management, effectiveness analysis and recommendations.

Cyber wargaming includes three teams: Red, White and Blue. The red team represents the cyber attackers, the white team monitors red and blue teams and the access to "real assets" and the blue team are defenders of the organization, military unit or state.

Cyber Red Team

Brangetoo et al. (2015) define a cyber red team as an element that conducts vulnerability assessments in a realistic threat environment and with an adversarial point of view, on specified information systems, in order to enhance an organization's level of security.

Cyber Red teaming includes functions like cyber intelligence gathering, threat/risk/vulnerability assessment, penetration testing, cyber security experiments and exercises, cyber training, document cyber activities, implement cyber security controls and promote cybersecurity awareness. Their activities follow a cycle composed by planning, reconnaissance gathering, execution and debriefing analysis phases.

Cyber Red teams can operate in an actual operation environment or in a specialized environment called 'Cyber Ranges', The DoD considers 'Cyber Ranges' environments necessary to test and evaluate cyberspace concept, policies and technologies.

Cyber White Team

The white team is in charge of defining the rules of engagement during the cyber games, thus providing full game control. This team continually monitors the actions of the red and blue teams so they keep moving forward towards their goals. The white team also enforces the team roles and can readapt the cyber environment as required. Overall, the white team can role play a high authority agency of both teams (Red and blue) and that cyber games are not seen as real world cyber threats.

Cyber Blue Team

The blue team has a defending role in the cyber war games. The blue team represents friendly members in an organization and they execute defensive

cyber operations. A blue team is responsible to identify and defend high priority targets, mitigate cyber risks, use cyber intelligence to dissect cyberattacks and validate the integration of technology, people and processes.

Cyber Warfare Ethics

Taddeo (2012) argues that in order to understand the cyber warfare ethics is required to put forward three 'Just Cyber War' principles:

1.Cyber war ought to be waged only against those entities that endanger or disrupt the wellbeing of the Infosphere.

2. Cyber war ought to be waged to preserve the well-being of the Infosphere.
3. Cyber war ought not to be waged to promote the well-being of the Infosphere.

Lin et al. (2012) took a more practical approach by considering some key ethical aspects like aggression, discrimination, proportionality and attribution.

Nowadays, there aren't guidelines for cyber warfare ethics as many questions exists before launching a cyber warfare attack, not to mention what could possibly happen in a declared cyber war between nations.

Some warfare laws may be applicable to cyberspace but again the lack of cyber warfare clarity, ownership and applicability are arguable.

Bellum Iustum (Just war theory): This theory provides a framework for ethics in warfare and cyber warfare. The framework includes conducts organized by phases: Beginning a war (Jus ad Bellum), during a war (Jus in Bello) and ending the war (Jus Post Bellum).

Jus ad Bellum (The right to wage war): It discusses the right to engage in war, including the right authority, right intention, success probability, last resort and proportionality principles.

Jus in Bello (Proper conduct in war): This specifies state behavior during war time. Its two main principles are distinction and proportionality of targets without causing extreme collateral damages.

Jus Post Bellum (Justice after war): This includes the justice after war, its principles are to seek a lasting peace after war, find accountable guilty people and initiate reparations.

Some dilemmas persist like moral and legal rights to declare cyber war, identify attackers in cyberspace and likewise targeting our responses

to cyberattacks. Simply by the fact that computer networks might be geographically disperse and any cyber operations can cause vast collateral damage.

CYBER WARFARE MODELS

Grant et al. (2012) studied seven offensive cyber operations process models summarized in Table 1. The selected models include target system penetration, few produce attack planning, target selection and Denial of Service (DoS) attacks and none of these models show a group coordination to launch a cyberattack.

Table 1. Offensive cyber operations process models (Grant et al., 2012)

Model's authors	Context	Basis	Type of attacker
Van Heerden & Burke (2012)	Cybercrime and warfare	Case studies	Lone or Group
Dreijer (2011)	Warfare	Previous models and case studies	Group
Croom (2010)	Cybercrime	Case studies	Group
Owens et al. (2009)	Warfare	Literature	Group
Damballa (2008)	Cybercrime	Case studies	Lone
Colarik & Janczewski (2008)	Terrorism	Analogy to cybercrime	Group
Grant et al. (2007)	Cybercrime	Hacker's documentation	Lone

Actor and Intent Definition Model

Robinson et al. (2015: 74-77) introduced this model that highlights a methodical process where events in cyberspace can occurred. The model is applicable to cyber warfare, cyber war, cyber terrorism, cyber bullying, cyber activism, cybercrime or any cyber related situation.

The main components are actor, intent, cyber event and cyberattack. The initial process is to identify the actor and the implicit intent, then analyzing the cyber situation that can cause harm.

Politically Motivated Cyberattack Model

Moran proposed a five stage model that mix technical and political awareness to develop an early warning system (Robinson et al., 2015).

While the first two steps show some a weakness due to the fact that are not required stages for the model.

Moran asserts that the most powerful cyberattacks will follow all phases while less sophisticated cyberattacks will pursue the last three stages of the model.

Cyberwarfare Conduct Model

Parks and Duggan created the cyber warfare model (Robinson et al., 2015) that is based on the kinetic warfare principles of the US Department of Defense:

1. Lack of physical limitations: A cyber warfare attack can be launched from anywhere with the same impact that army and navy troops can achieve. The authors point out that cyber weapons can be replicated cheaply and quickly.
2. Kinetic effects: The cyber warfare aim is to cause kinetic effects any type of attack that does not cause real world damage is not a cyber warfare attack.
3. Stealth: The stealth principle in cyberspace is to hide within valid traffic. Although, it is arguable that the stealth principle has similar effects in both kinetic war and cyber warfare.
4. Mutability and inconsistency: Activities in cyberspace are unpredictable but brings doubtfulness into the theory that cyber warfare is mutable and inconsistent.
5. Identity and privileges: In cyberwarfare, a cyber attacker with elevated accounts and system privileges will cause harm.
6. Dual use: All cyber warfare tools can use for war and peaceful purposes.
7. Infrastructure control: Infrastructure control is a significant component in cyberwarfare, having control over infrastructure will give advantages to both defenders and attackers.
8. Information as operational environment: In cyberwarfare, the operating environment is already information. In certain cases, physical requirement ought to be converted to information.

Schmitt Cyberattack Analysis

NATO (2013) described an approach based on the Michael Schmitt's analysis about computer network and the use of force in international law. NATO's model is focused on the level of harm inflicted by cyberattacks and certain qualitative elements of cyber operations.

The factors that influence states to assess the use of force include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. NATO emphasizes that these factors are not formal legal criteria. While the list is not exhaustive, States may look for additional factors like political environment, the use of cyber operations with military force, attacker's identity, attacker's cyber operations record and target nature.

Tibbs' Cyber Game Board

Tibbs presented a model (Robinson et al., 2015) that is seeing cyber warfare as a game, with players that only need an Internet connection but States exert the most power.

The game board includes the following situations:

- Connection, computation and cognition
- Cooperation, co-option and coercion
- Information hardware, information software and information wetware
- Positive social reciprocity power, balanced social reciprocity power and negative social reciprocity power

Cyber Warfare Communications Effect Model

Wihl et al. (2010) introduced a synthetic cyber warfare model that is based on Network-Centric Warfare (NCW), Computer Network Operations (CNO) Computer Network Attack (CNA), cyber warfare communications and a Commercial-Off-The-Shelf (COTS) Computer Generated Forces (CGF) system.

The cyber warfare communications effect model must provide following features Wihl et al. (2010):

– Data communication at packet level and network security (for eavesdropping)
– Model information such as location, movement, roles (eavesdropping)
– Protocol stack operations (DoS), including routing (routing misconfiguration) and wireless (wireless specific)
– Emulation with real hardware and software (malicious agents and code exploits)
– Human-in-the-loop (human errors)
– Wireless detailed physical layer models and routing models

Lockheed Martin Cyber Kill Chain

This framework is part of the Intelligence Driven Defense model for dealing with cyber intrusion activity. The Cyber Kill Chain consists of seven phases:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. C2 (Command & Control)
7. Actions on Objectives

The phases are combined with a series of processes in a course of action matrix. The course of action matrix presents available countermeasures where the phase and the process intersect. The processes for every phase are: detect, deny, disrupt, degrade and deceive.

Cyber Warfare Laws

The most comprehensive cyber warfare legal reference is provided by the Tallinn manual (NATO, 2013). An international group of experts participated in the creation of this manual; Lawyers, scholars and technical experts including observers from the NATO's Allied Command Transformation, the US Cyber Command and the International Committee of the Red Cross. The Tallinn manual established ninety-five international law 'black-letter rules' related to cyber war conflicts. Some applicable areas are international humanitarian law, sovereignty, the jus ad bellum, state responsibilities and neutrality law.

According to Melzer (2011) the cyber warfare phenomenon does not exist in a legal vacuum but it is subject to well established rules and principles.

Furthermore, cyber warfare has not caused dangerous consequences to human race but to resolve modern issues in the new cyber domain it is necessary to mix classic treaty interpretation with common sense and unanimous policy decisions.

National Cybersecurity Strategies

Many nations are organizing their cyber capabilities in cyberspace by creating and constantly updating a National Cybersecurity Strategy, policy or programme. The Cyber warfare responsibilities mostly belong to a military unit or command but can be shared with a civilian agency or a national cybersecurity organization. Sabillon et al. (2016: 67) define a cybersecurity policy as the instrument developed by nations to communicate and express those aspects that want a state to protect in cyberspace.

NATO (2016) presents in its website some cyber security policies and legal documents especially for NATO nations and partners. International Telecommunication Union (ITU) (2016) highlights that 72 out 193 member states have published a National Cybersecurity Strategy.

DUAL CYBER WARFARE MODEL

In our previous research (Sabillon et al., 2016), we introduced our Dual Cyber Warfare Model (Figure 1) that can be implemented in military and organizational environments to analyze, deter and neutralize cyberattacks. Cyberattacks have been targeting nation's critical infrastructure, national cyber assets and corporations, the attackers could be members of another state, foreign cyber forces and non-state groups like cybercriminals, cyber hacktivists or hackers.

For military cyber commands, units or national cybersecurity centers:

1. Reconnaissance: Counter intelligence of the attacker's intention is gathered
2. Monitor: Monitoring and vigilance for abnormal cyber activities
3. Launch cyber defense measures: Activate cyber active and passive defense measures
4. Cyberdeterrence: Identify attackers and apply cyber retaliation and deterrence as required

5. Perform risk impact: Evaluate all possible scenarios, risk assessment and impact
6. Launch cyber offensive measures: Activate cyber offensive measures as necessary
7. Neutralize: Destroy using force as a last resource
8. Scenario assessment: Debrief mission and present report

For organizations or corporations:

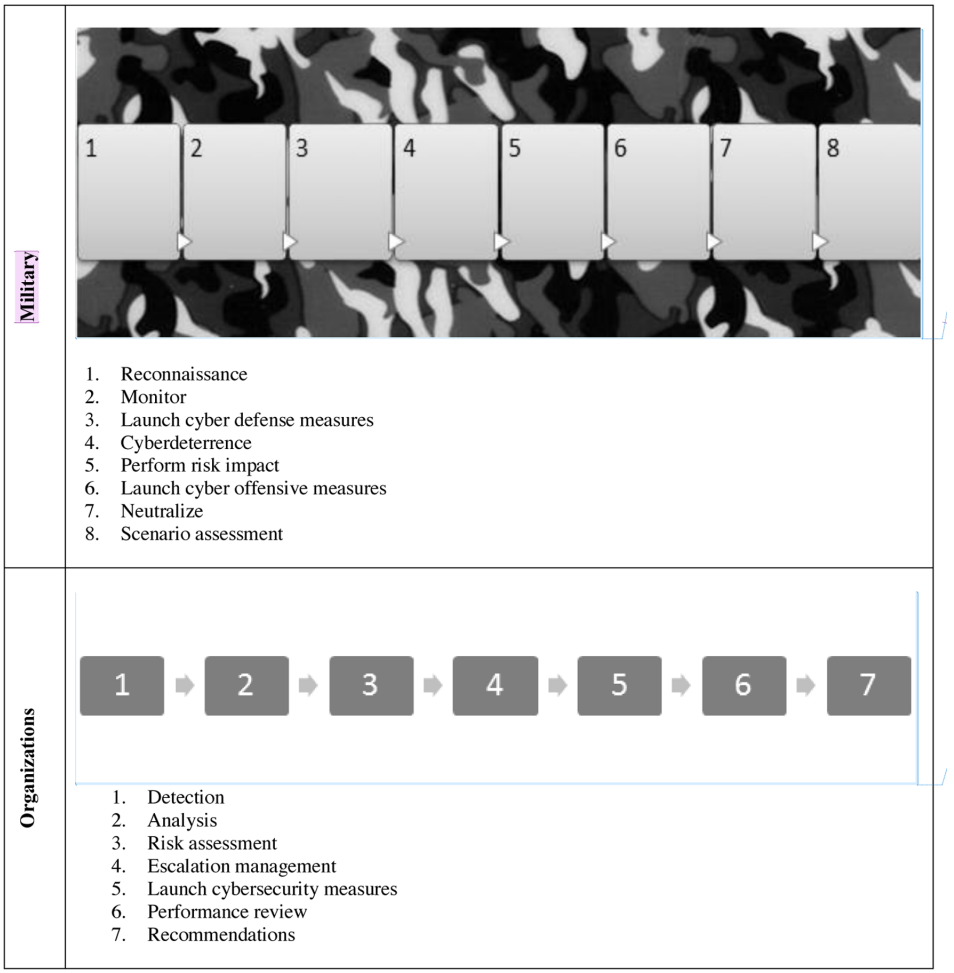
1. Detection: Identify nature of the cyberattack and targets
2. Analysis: Perform vulnerability assessment of the cybersecurity incident
3. Risk assessment: Evaluate all possible risks and consequences of the cyber intrusion
4. Escalation management: Activate incident handling and escalation procedures as necessary
5. Launch cybersecurity measures: Start cybersecurity measures to stop and eradicate impact of the cyberattack
6. Performance review: Perform digital forensics investigation
7. Recommendations: Report findings, detect cyber weaknesses and present a correction plan

CONCLUSION

Cyber warfare is conceivably the most radical repercussion of the Knowledge Era and must be systematically analyzed from both perspectives: empirical-practical and theoretical-conceptual. Moreover, its study is not just an unique matter for military protection or detecting cyber strengths and weaknesses in any national critical infrastructure. The study of the most notorious and recent cyber warfare models allows to confirm that here are many areas that need to focus on additional research for cyber warfare conceptualization such as early warning systems, conducting cyber warfare, cyber warfare phases, cyber warfare ethics, cyber weapons, universal cyber warfare laws and regulations and nation's perspectives on cyberwarfare.

This chapter produces a deep study about all factors and elements involved, strategies, generations and theoretical models, provides the fundamentals for a wide conceptualization of the cyber warfare phenomenon. Cyber warfare like many areas in the cyber domain needs to be accurately understood and many

Figure 1. Dual Cyber Warfare Model (Sabillon et al., 2016)



multidisciplinary areas target to merge to continue researching the separate and intertwined aspects of the cyber domain, cyberspace and cybersecurity.

REFERENCES

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (2nd ed.). Syngress, Elsevier Inc. doi:10.1016/B978-0-12-416672-1.00001-5

Axelos. (2015). *Cyber Resilience Best Practices*. Norwich: TSO (The Stationery Office).

Bendiek, A., & Metzger, T. (2015). *Deterrence theory on the cyber-century: Lessons from a state-of-the-art literature review. Stiftung Wissenschaft und Politik*. German Institute for International and Security Affairs.

Betz, D., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *43*(2), 147–164. doi:10.1177/0967010613478323

Bodeau, D., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework*. MITRE.

Brangetto, P., Çalişkan, E., & Rõigas, H. (2015). *Cyber Red Teaming: Organisational, technical and legal implications in a military context*. CCD COE NATO Cooperative Cyber Defense Centre of Excellence.

Cisco. (2015). *Cisco Security Cyber War Games*. Author.

Citizen, L. & SecDev Group. (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network*. Toronto: Citizen Lab, Munk Centre for International Studies, University of Toronto.

Clifford, R. (2006). *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (2nd ed.). Carolina Academic Press.

Cylance. (2015). Operation Cleaver.

Deibert, R., Rohozinski, R., & Crete, N. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue*, *43*(1), 3–24. doi:10.1177/0967010611431079

Department of Defense. (2015). *Resilient Military Systems and the Advanced Cyber Threat. Defense Science Board*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. Apress. doi:10.1007/978-1-4302-6083-7

Ghionis, A. (2015). *The Limits of Deterrence in the Cyber World: An analysis of deterrence by punishment*. University of Sussex.

Grant, T., Burke, I., & van Heerden, R. (2012). Comparing Models of Offensive Cyber Operations. *Proceedings of the Seventh International Conference on Internet and Web Applications and Services (ICIW 2012)*, 35-55.

Green, J. (2015). *Cyber Warfare: A multidisciplinary analysis*. Routledge Taylor & Francis Group. doi:10.4324/9781315761565

International Telecommunication Unit – ITU. (2016). *National Strategies Repository*. ITU.

ISACA. (2015). *Cybersecurity fundamentals*. Rolling Meadows: ISACA.

Jajodia, S., Shakarian, P., Subrahmanian, V., Swarup, V., & Wang, C. (2015). *Cyber Warfare: Building the Scientific Foundation*. Springer International Publishing. doi:10.1007/978-3-319-14039-1

Joint Staff (2013). *Cyberspace Operations (JP 3-12)*. Washington, DC: Joint Staff Director of Operations (J-3).

Kaplan, J., Bailey, T., Rezek, C., O'Halloran, D., & Marcus, A. (2015). *Beyond Cybersecurity: Protecting your digital business*. John Wiley & Sons. doi:10.1002/9781119055228

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security and Privacy*, *9*(May-June), 49–51. doi:10.1109/MSP.2011.67

Lemieux, F. (2015). Current and emerging trends in cyber operations: Policy, Strategy and Practice. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity. New York: Palgrave Macmillan. doi:10.1057/9781137455550

Lewis, J. (2015). The role of offensive cyber operations in NATO's collective defence. Tallinn Paper No.8. The Tallinn Papers: A NATO CCD COE Publication on Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (the Centre).

Liles, J. (2013). Modern Cyber Deterrence Theory: Norms, Assumptions and Implications. *National Security Policy*, *743*, 1–19.

Lin, P., Allhoff, F., & Rowe, N. (2012). War 2.0: Cyberweapons and ethics. *Communications of the ACM*, *55*(3), 24–26. doi:10.1145/2093548.2093558

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. doi:10.1080/09636412.2013.816122

Lockheed Martin. (2016). *Cyber Kill Chain*. Author.

Mandiant. (2013). *APT1: Exposing one of China's cyber espionage units*. Mandiant Publication.

Maybaum, M., Osula, A., & Lindström, L. (2015). Architecture in Cyberspace. *Proceeding from the Seventh international conference on cyber conflict*, *7*(24), 25-38.

McQuade, S. III. (2006). *Understanding and managing cybercrime*. Pearson/ Allyn and Bacon.

Melzer, N. (2011). Cyberwarfare and International Law. Geneva: United Nations Institute for Disarmament Research (UNIDIR).

NATO. (2013). *The Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

NATO. (2016). *Cyber Security Strategy Documents*. CCD COE.

Oxford English Dictionary. (2016). Oxford University Press.

Ponemon Institute, IBM. (2015). *2015 Cost of data breach study: Global analysis*. Author.

Ponemon Institute, IBM. (2015). *2015 Cost of data breach study: Impact of Business Continuity Management*. Author.

Rattray, G., & Healey, J. (2010). Categorizing and understanding offensive cyber capabilities and their use. In *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy*. Washington, DC: The National Academy of Sciences.

Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, *35*(1), 5–32. doi:10.1080/01402390.2011.608939

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. doi:10.1016/j.cose.2014.11.007

Ryan, J. (2015). *Leading Issues in Cyber Warfare and Security: For researchers, teachers, and students*. Academic Conferences and Publishing International Limited.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67–81.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2016). Cyber Warfare: Challenges within the Cyber domain. *European Journal of Public Order and National Security*, *12*(4), 7–16.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. Oxford University Press.

Suarez, H., & Peláez, J. (2014). *Ciber-Resilencia: Aproximación a un marco de medición*. INTECO-CERT.

Taddeo, M. (2012). An analysis for a just cyber warfare. *Proceeding of Cyber conflict (CYCON). 4TH International Conference*, 1-10.

Thomas, T. (2007). Decoding the virtual dragon. Fort Leavenworth: Foreign Military Studies Office.

Wei, L. (2015). The Challenges of Cyber Deterrence. Pointer. *Journal of The Singapore Armed Forces*, *41*(1), 12–22.

Wihl, L., Kong, J. & Varshney. (2010). Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments. *Proceeding from Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

Chapter 7
Audits in Cybersecurity

ABSTRACT

The objective of this chapter is to provision a comprehensive literature review of the most relevant approaches for conducting cybersecurity audits. The study includes auditing perspectives for specific scopes and the best practices that many leading organizations are providing for security and auditing professionals to follow. The chapter reviews relevant features for auditing approaches in the following order: ISO/IEC 27001:2013, ISO/IEC 27002:2013, Control Objectives for Information and Related Technology (COBIT) 2019, Information Technology Infrastructure Library (ITIL) 4, AICPA, ISACA, NIST SP 800-53, NIST CSF v1.1, IIA, PCI DSS, ITAF, COSO, ENISA, NERC CIP, and CSAM.

INTRODUCTION

This study reviews the most important standards, frameworks, methodologies, guidelines, best practices and models that are used worldwide for planning, execution, reporting and follow-up audit phases in the areas of information security (InfoSec), cybersecurity and information technology.

The chapter reviews relevant features for auditing approaches in the following order: ISO/IEC 27001:2013; ISO/IEC 27002:2013; Control Objectives for Information and Related Technology (COBIT) 2019; Information Technology Infrastructure Library (ITIL) 4, AICPA; ISACA; NIST SP 800-53; NIST CSF v1.1; IIA; PCI DSS; ITAF; COSO; ENISA; NERC CIP and CSAM.

DOI: 10.4018/978-1-7998-4162-3.ch007

Some methodologies have a specific purpose and others provide the audit approaches for certain institutions that have global impact.

ISO/IEC 27001: 2013

This international standard was designed and is maintained by the International Organization for Standardization (ISO). ISO standards are reviewed every five years, previous edition was published in 2005 and the second edition was released in 2013. The ISO/IEC 27001:2013 known as *Information technology - Security techniques – Information security management systems - Requirements*. It is based on the Information Security Management System (ISMS). ISO/IEC 27001:2013 can be used by organizations to establish, implement, maintain and continually improve the ISMS. ISO/IEC 27001:2013 consists of 7 clauses (Table 1), control objectives and controls are aligned with ISO/IEC 27002:2013, which contains 14 control clauses, 35 security categories and 114 controls. Terminology is based on ISO/IEC 27000: *Information technology - Security techniques – Information security management systems – Overview and vocabulary.*

Clauses 9 and 10 provide guidelines for:

1. Monitoring, measurement, analysis and evaluation
2. Internal audit
3. Management review
4. Nonconformity and corrective action
5. And Continual Improvement of the ISMS

Table 1. ISO/IEC 27001:2013 Information Security Management Systems Clauses

ISO/IEC 27001: Security Control Clauses
1. Clause 4: Context of the organization 2. Clause 5: Leadership 3. Clause 6: Planning 4. Clause 7: Support 5. Clause 8: Operation 6. Clause 9: Performance Evaluation 7. Clause 10: Improvement

ISO/IEC 27002: 2013

This international standard was designed and is maintained by the International Organization for Standardization (ISO). ISO standards are reviewed every five years, previous edition was published in 2005 and the second edition was released in 2013. The ISO/IEC 27002:2013 known as *Information technology - Security techniques – Code of practice for information security controls*. It is based on the Information Security Management System (ISMS) from the ISO/IEC 27001. ISO/IEC 27002:2013 can be used by organizations to select controls with any ISMS implementation, implement universally accepted information security controls and to develop information security management guidelines for their specific business environments.

ISO/IEC 27002:2013 contains 14 control clauses (Table 2), 35 security categories (Table 3) and 114 controls.

Table 2. ISO/IEC 27002:2013 Security Control Clauses

ISO/IEC 27002: Security Control Clauses
8. Clause 5: Information Security Policies
9. Clause 6: Organization of Information Security
10. Clause 7: Human Resource Security
11. Clause 8: Asset Management
12. Clause 9: Access Control
13. Clause 10: Cryptography
14. Clause 11: Physical and Environmental Security
15. Clause 12: Operations Security
16. Clause 13: Communication Security
17. Clause 14: System Acquisition, Development and Maintenance
18. Clause 15: Supplier Relationships
19. Clause 16: Information Security Incident Management
20. Clause 17: Information Security Aspects of Business Continuity Management
21. Clause 18: Compliance

In terms of audits, *ISO/IEC 27002:2013* highlights two specific controls for planning and conducting audits:

12.7.1 Information system audit controls: Requirements and activities are to be planned without causing impact to business processes. A guidance implementation is provided that includes 7 guidelines.

18.2.3 Technical compliance review: This controls states that systems should be reviewed constantly to verify compliance with information security policies. This control provides an implementation guidance covering expertise from auditors, appropriate planning of penetration testing and vulnerability

Table 3. ISO/IEC 27002:2013 Security Categories

ISO/IEC 27002: Security Categories
1. Category 5.1: Management direction for information security
2. Category 6.1: Internal organization
3. Category 6.2: Mobile devices and teleworking
4. Category 7.1: Prior to employment
5. Category 7.2: During employment
6. Category 7.3: Termination and change of employment
7. Category 8.1: Responsibilities of assets
8. Category 8.2: Information classification
9. Category 8.3: Media handling
10. Category 9.1: Business requirements of access control
11. Category 9.2: User access management
12. Category 9.3: User responsibilities
13. Category 9.4: System and application access control
14. Category 10.1: Cryptographic controls
15. Category 11.1: Secure areas
16. Category 11.2: Equipment
17. Category 12.1: Operational procedures and responsibilities
18. Category 12.2: Protection from malware
19. Category 12.3: Backup
20. Category 12.4: Logging and monitoring
21. Category 12.5: Control of operational software
22. Category 12.6: Technical vulnerability management
23. Category 12.7: Information systems audit considerations
24. Category 13.1: Network security management
25. Category 13.2: Information transfer
26. Category 14.1: Security requirements of information systems
27. Category 14.2: Security in development and support processes
28. Category 14.3: Test data
29. Category 15.1: Information security in supplier relationships
30. Category 15.2: Supplier service delivery management
31. Category 16.1: Management of information security incidents and improvements
32. Category 17.1: Information security continuity
33. Category 17.2: Redundancies
34. Category 18.1: Compliance with legal and contractual requirements
35. Category 18.2: Information security reviews

assessments and it also includes scope for technical compliance reviews and recommends to use *ISO/IEC TR 27008: Information technology – Security techniques – Guidelines for auditors on information security controls* for conducting technical compliance reviews.

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT) 2019

Control Objectives for Information and Related Technology (COBIT) is a framework for governance and management of enterprise information and

technology for any organization. The COBIT 2019 Core documentation is organized as follows:

1. Framework: Introduction and Methodology
2. Framework: Governance and Management Objectives
3. Design Guide: Designing an Information and Technology Governance Solution
4. Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

COBIT 2019 provides inputs to the COBIT Core where section AP013 is exclusive for Managed Security, then the Core framework publications, adding Design Factors and Focus Areas which result in a tailored enterprise governance system for Information and Technology.

ISACA and ITAF guidelines and procedures can be utilized for planning COBIT audits.

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) 4

ITIL is a framework created to standardize the selection, planning, delivery and maintenance of Information Technology services within any company. The main goal is to improve efficiency and achieve predictable service delivery. ITIL is the global standard for the Information Technology Service Management (ITSM) industry. AXELOS in the United Kingdom (UK), is responsible for maintaining ITIL and all its publications. ITIL is mapped in ISO 20000 Part 1 and its certification scheme can be tailored to adopt and adapt ITIL in alignment with business specific needs.

The core publications map the entire ITIL service lifecycle and are:

1. ITIL Service Strategy
2. ITIL Service Design
3. ITIL Service Transition
4. ITIL Service Operation
5. ITIL Continual Service Improvement

Information Security Management is included in the Service Design (Section 4.6) and contains purpose, goal, objective, scope, value, policies,

principles, basic concepts, the Information Security Management System (ISMS) of ISO 27001, ISMS activities/methods/techniques, security controls, management of security breaches and incidents, triggers/inputs/outputs/interfaces of the Information Security Management (ISM), Key Performance Indicators (KPIs), information management and Challenges/Critical Success Factors (CSFs) and risks of the ISM.

The Continual Service Improvement (CSI) publication provides principles (Section 3), processes (Section 4) and methods and techniques (Section 5).

ITIL can use a series of different criteria for assessment that is presented in Table 4.

Table 4. ITIL assessment criteria

Resource	Description
ITIL Maturity model	A set of 4,000 questions in 30 different questionnaires, that cover 26 processes and 4 functions
ISO/IEC 20000	The ISO standard for service management
COBIT Process Assessment Model	Assessment aligned between COBIT 5 and ISO/IEC 15504 (Standard for IT process assessment)
CMMI-SVC	Capability Maturity Model for services
AXELOS skills framework	Assessment for project and program management, ITSM, leadership and personal management
SFIA	Skills Framework for the Information Age to review the capabilities of IT personnel
European e-Competence Framework	Assessments of IT staff capabilities

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA)

According to AICPA (2017), its Cybersecurity risk management program is a *"Set of policies, processes and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented."*

The Cybersecurity Risk Management Reporting Framework verifies the effectiveness of existing security controls between organization and its stakeholders. The framework consists of the following components:

- Description criteria for management's description of any entity's cybersecurity risk management program
- Trust services control criteria for security, availability and confidentiality
- AICPA Guide reporting on an entity's cybersecurity risk management program

System and Organization Controls (SOCs) are categorized as follows:

- SOC for Cybersecurity guide that includes organization-wide reporting
- SOC 1 Guide that supports controls reporting at service organizations that impact internal controls over financial reporting
- SOC 2 Guide that supports reporting for controls related security, availability, processing integrity, confidentiality and privacy and for restricted-use reporting
- SOC 3 for general-use reporting

Assessments are conducted as audit engagements or engagements for different SOCs (1,2 or 3).

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA)

According to ISACA (2017), cybersecurity is really important to many members of the Board of Directors in part to the fact that bad publicity can be generated once one organization is victim of a major data breach or cyberattack. To invest in proper measures, Companies need to evaluate their current and emerging risks and to audit existing or future controls in order to protect information assets. Control investments should cover awareness, policy, Intrusion Detection Systems (IDS), event logging, incident response, vulnerability scanning, classification of information and cyber assets, forward intelligence and technology/architecture/systems hardening. Cybersecurity audits are organized in three lines of defense:

1. Management: Control Self-Assessments (CSAs), Pen testing, Technical testing, Social testing and Regular Management review
2. Risk Management: Threats/Vulnerabilities/Risks, Risk evaluation, Business Impact Analysis (BIA) and Emerging risk

3. Internal Audit: Internal controls testing, Cybersecurity compliance, Risk acceptance and Digital Forensics investigations

Cybersecurity audits are more complex than any general audit, planning and scoping is shown in Table 5.

Table 5. ISACA's cybersecurity audits by areas and types

Areas	Types of Cybersecurity Audits
Governance	Cybersecurity policy, Technical key operating procedures
Risk	Cybersecurity risk register update, risk treatment, risk reporting
Management	Cybersecurity incident reviews
Assurance	Cybersecurity risk management process

Cybersecurity audits should have specific goals that ought to be aligned with objectives and enterprise outcomes (Table 6).

Table 6. ISACA's cybersecurity audit goals aligned with business outcomes

Cybersecurity goals	Business outcomes
Proper and effective cybersecurity documentation (Policies, Standards and Procedures)	Audit will review governance, controls for effective and adequate documents
Emerging risk is properly identified, evaluated and treated	Cybersecurity audits will focus on processes, tools and methods
Cybersecurity processes are defined, deployed and measured during business transformation	Cybersecurity reviews will cover transforming processes
Cybersecurity incident response addresses cyberattacks and breaches that are identified and treated appropriately	Cybersecurity (in-depth technical) audits to seek early recognition and identification of cyberattacks in timely and appropriate fashion as specified by corporate documentation

NIST SPECIAL PUBLICATION 800-53

The NIST Special Publication 800-53 Revision 5 is the "Security and Privacy Controls for Information Systems and Organizations", the publication includes a catalog for security and privacy controls. These controls are

flexible, customizable and can be implemented fully or partially in any organization seeking managing security risks. The controls are addressed from a functionality and an assurance perspective.

NIST SP 800-53 provides 20 different security controls (Table7). Each control has objectives, supplemental guidance, related controls, control enhancements and references to other NIST Special Publications. Controls are categorized as common controls, system-specific controls and hybrid controls.

Table 7. Security and Privacy Controls in NIST Special Publication 800-53 v5

NIST Special Publication 800-53 v5: Security and Privacy Control Families
1. Access control
2. Awareness and training
3. Audit and accountability
4. Assessment, authorization and monitoring
5. Configuration management
6. Contingency planning
7. Identification and authentication
8. Individual participation
9. Incident response
10. Maintenance
11. Media protection
12. Privacy authorization
13. Physical and environmental protection
14. Planning
15. Program management
16. Personnel security
17. Risk assessment
18. System and services acquisition
19. System and communications protection
20. System and information integrity

The Audit and accountability family includes the following controls:

1. Audit and accountability policy and procedures
2. Audit events
3. Content of audit records
4. Audit storage capacity
5. Response to audit processing failures
6. Audit, review, analysis and reporting
7. Audit reduction and report generation
8. Time stamps
9. Protection of audit information
10. Non-repudiation
11. Audit record retention

12. Audit generation
13. Monitoring for information disclosure
14. Session audit
15. Alternate audit capability
16. Cross-organizational auditing

NIST CYBERSECURITY FRAMEWORK (CSF) VERSION 1.1

The NIST Cybersecurity Framework (CSF) version 1.1 focuses on business drivers linked to cybersecurity activities and risks. The framework has three main components:

1. Framework Core: Desired cybersecurity outcomes are properly identified
2. Implementation Tiers: Qualitative measure of the organization's cybersecurity risks management
3. Framework Profiles: Alignment between the Framework Core and the organization's requirements, objectives, risk appetite and resources

The main functions of the Framework Core are identified as Identify, Protect, Detect, Respond and Recover. Each function contains categories, subcategories and informative references. The NIST CSF consists of 5 functions, 23 categories, 108 subcategories and 6 informative references (COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001: 2013, NIST SP 800-53 Rev 4 and Center for Internet Security - Top 20 Critical Security Controls (CIS CSC). The framework can be implemented as the foundation of a new cybersecurity program, new cybersecurity risk management, combine with other cybersecurity framework or standard either partially or in a full implementation.

The NIST CSF follows a continuous lifecycle which covers planning, designing, building, deploying, operating and decommissioning phases.

Audits are specified for many subcategories of the core functions of the NIST CSF.

THE INSTITUTE OF INTERNAL AUDITORS (IIA)

According to the Institute of Internal Auditors (IIA), cybersecurity is defined as the technologies, processes and practices designed to protect the information

assets of any organization. Like ISACA, the IIA also considers the "Three Lines of Defense Roles and Responsibilities" to protect cybersecurity related to management, controls and governance. Furthermore, IIA adds roles and responsibilities to the "Three Lines of Defense":

1. First Line of Defense: Chief Technology Officer (CTO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Executive Officer (CEO) and other members of Upper Management
2. Second Line of Defense: IT risk management and IT compliance managers and officers
3. Third Line of Defense: Chief Audit Executive (CAE) and Internal Audit activity

Table 8. IIA's Cybersecurity Risk Assessment Framework

Components	Framework Activities
Cybersecurity Governance	• Risk appetite • Cybersecurity policy • Risk assessment and monitoring • Training • Examination of third-party vendors
Inventory of Information Assets: Data, Infrastructure and Applications	• Data inventory • Device inventory • Software inventory
Standard Security Configurations	• Secure configurations for hardware and software • Secure configurations for networking devices
Information Access Management	• Controlled use of administrative privileges • Account monitoring and control • Controls on *Need to know* access • Population of users
Prompt Response and Remediation	• Continuous improvements • Assessment of vulnerabilities, threat intelligence and gap identification • Performance metrics • Inventory of knowledge, skills and abilities
Ongoing Monitoring	• Malware defenses • Limitation and controls for network ports, protocols and services • Application security • Wireless access controls • Boundary defense • Penetration testing, phishing tests and red teaming exercises • Change event management • Data protection and data loss prevention

IIA utilizes the Cybersecurity Risk Assessment Framework for planning and conducting cybersecurity audits (Table 8).

IIA also recommend specific publications for planning and conducting cybersecurity audits (Table 9).

Table 9. IIA's publications for cybersecurity audits

IIA publication guidance for cybersecurity audits
1. Practice Guide, "Business Continuity Management – Crisis Management"
2. Practice Guide, "Auditing Privacy Risks, 2nd Edition"
3. Global Technology Audit Guide (GTAG), "Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition"
4. Global Technology Audit Guide (GTAG), "Management of IT Auditing, 2nd Edition"
5. Global Technology Audit Guide (GTAG), "Information Technology Outsourcing, 2nd Edition"
6. Global Technology Audit Guide (GTAG), "Identity and Access Management"
7. Global Technology Audit Guide (GTAG), "Developing the IT Audit Plan"
8. Global Technology Audit Guide (GTAG), "Information Security Governance"
9. Global Technology Audit Guide (GTAG), "Auditing IT Governance"
10. Position Paper, "The Three Lines of Defense in Effective Risk Management and Control"

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

PCI DSS is the global standard for the payment industry that involves the major payment cards like American Express, Discover Financial Services, JCB International, Mastercard, Visa Inc and Visa Europe. Compliance with PCI DSS protects merchants and cardholders for the storage, processing and transmission of transaction data. The PCI DSS compliance is a continuous process that includes major phases for assessing, remediating and reporting.

Table 10. PCI DSS's Goals

PCI DSS Goals
1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

The standard has specific goals and requirements that are presented in Tables 10 and 11.

Table 11. PCI DSS's Requirements

Goal alignment	PCI DSS Requirements
1	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
2	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
3	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
4	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
5	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6	12. Maintain a policy that addresses information security for all personnel

The PCI DSS Council is responsible for maintaining the set of standards but each payment card brand is responsible for setting the compliance programs, validation and enforcement. The Council maintains approved

Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) to audit PCI DSS compliance of merchants and the Self-Assessment Questionnaire (SAQ) is another tool to help organizations to self-validate PCI DSS compliance but are not required to submit a Report on Compliance (ROC).

The audit compliance process is generally defined by the following stages:

1. PCI DSS Scoping: Define the audit scope based on risk levels that are determined by the payment card brand. To be conducted at least annually and prior to the annual assessment
2. Assessing: To evaluate compliance in alignment with the audit scope. To be audited once a year
3. Compensating Controls: Qualified Security Assessor (QSA) validate alternative control technologies and processes
4. Reporting: Qualified Security Assessor (QSA) or entity submits the required documentation on an annual basis

5. Clarifications: Qualified Security Assessor (QSA) or entity provides clarifications/updates upon request from the acquiring bank or payment card brand. As required

INFORMATION TECHNOLOGY ASSURANCE FRAMEWORK (ITAF)

The Information Technology Assurance Framework (ITAF) provides standards, guidelines and tools for conducting Information Systems audits and assurance assessments. ITAF also provisions guidance, techniques and tools to plan, design, conduct, report related to any Information Systems (IS) audits and assurance engagements. ITAF standards are mandatory, guidelines are optional, tools and techniques are presented as supplementary material that could be discussion documents, technical directions, white papers, audit programmes or books.

Table 12 presents the ITAF architecture:

Table 12. ITAF architecture

ITAF: IS Audit and Assurance Standards and Guidelines (Third Edition)			
Standards		**Guidelines**	
General Standards	1001-1008	General Guidelines	2001-2008
Performance Standards	1201-1207	Performance Guidelines	2201-2208
Reporting Standards	1401-1402	Reporting Guidelines	2401-2402

The ITAF section 3630.7 Information Security Management provides important guidelines for auditing, the same applies for other ITAF sections like:

- 3450: IT processes
- 3630: Auditing IT General Controls

COMMITTEE OF SPONSORING ORGANIZATIONS (COSO)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Integrated Framework is "*A*

process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Table 13 presents the components of COSO ERM Integrated Framework. These components are used to plan and conduct IT and assurance audits.

Table 13. COSO ERM Integrated Framework

ERM Integrated Framework
Internal Environment: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
Event Identification: Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
Risk Response: Management selects risk responses—avoiding, accepting, reducing or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
Control Activities: Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
Monitoring: The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA)

According to ENISA (2018), information security audits are independent reviews and examinations of system records, activities and related documentation that are intended to improve the level of information security, by avoiding improper designs and by optimizing the efficiency of security processes and safeguards.

Table 14. Security Measures to be reviewed during Information Security audits

Parts	Sub-parts	Security Measures
1. Governance and Ecosystem	1.1 Information system security governance & risk management	1. Information system security risk analysis 2. Information system security policy 3. Information system security accreditation 4. Information system security indicators 5. Information system security audit 6. Human resource security 7. Asset management
	1.2 Ecosystem management	1. Ecosystem mapping 2. Ecosystem relations
2. Protection	2.1 IT Security architecture	1. Systems configuration 2. System segregation 3. Traffic filtering 4. Cryptography
	2.2 IT Security administration	1. Administration accounts 2. Administration information systems
	2.3 Identity and Access management	1. Authentication and identification 2. Access rights
	2.4 IT Security maintenance	1. IT security maintenance procedure 2. Industrial control systems
	2.5 Physical and environmental security	1. Physical and environmental security
3. Defence	3.1 Detection	1. Detection 2. Logging 3. Log correlations and analysis
	3.2 Computer security incident management	1. Information system security incident response 2. Incident response 3. Communication with Competent Authorities and CSIRTs
4. Resilience	4.1 Continuity of operations	1. Business continuity management 2. Disaster recovery management
	4.2 Crisis management	1. Crisis management organization 2. Crisis management process

ENISA has published and is enforcing specific guidelines for planning and conducting information security audits followed by Operators providing Essential Services (OES), Digital Service Providers (DSP) and National Competent Authorities (NCA) of European Union (UE) Member States.

The information security audit guidelines include forms of information security audit, scope, process, outcomes, objectives, EU policy context,

methodology, target audience, goals, principles, good practices, recommendations, relevant information security self-assessment, management frameworks and alignment to control frameworks.

The EU information security audit lifecycle for National Competent Authorities (NCA) consists of three phases:

Pre-audit/planning phase, Audit execution/fieldwork phase and Post-execution phase.

Security measures for Operators providing Essential Services (OES) are highlighted in Table 14.

To facilitate the information security audit processes, ENISA provides the audit methodology for Digital Service Providers (DSP) that presents a mapping of the five elements in Table 15.

Table 15. Digital Service Providers (DSP) audit methodology during Information Security audits

Implementing Regulation Elements	Security Measures
1. Security of systems and facilities	– Physical and environmental security – Access control to network and information systems – Integrity of network components and information systems – Change management – Asset management – Security of data at rest
2. Incident handling	– Security incident detection & response – Security incident reporting
3. Business continuity management	– Business continuity – Disaster recovery capabilities – Secure of supporting utilities
4. Monitoring, auditing and testing	– Monitoring and logging – System tests – Security assessments – Interface security – Software security – Customer monitoring and log access
5. Compliance with (Inter)national Standards	– Compliance – Interoperability and portability

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR CRITICAL INFRASTRUCTURE PROTECTION (NERC CIP)

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority responsible to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

NERC Reliability Standards define all requirements for planning and operation of the bulk power system in North America. The NERC Standards are based on a results-based approach that includes targeting required actions and results. Each NERC Standard utilizes a defense-in-depth methodology by covering *Performance, Risk and Competency.*

In terms of cybersecurity compliance, NERC Standards for Critical Infrastructure Protection (CIP) define a compliance enforcement authority, evidence retentions guidelines, processes for compliance and monitoring assessment that cover:

- Compliance audit
- Self-certification
- Spot checking
- Compliance investigation
- Self-reporting
- Complaint

Severity of compliance elements is categorized in Violation Severity Levels (VSL) that integrate lower, moderate, high and severe VSLs. The NERC CIP Standards are in Table 16.

THE CYBERSECURITY AUDIT MODEL (CSAM)

The CyberSecurity Audit Model (CSAM) is a new exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the

Table 16. NERC Reliability Standards for Critical Infrastructure Protection (CIP)

NERC CIP Standards
1. CIP-002-5.1a Cyber Security – Bulk Electric System (BES) Cyber System Categorization
2. CIP-003-7 Cyber Security – Security Management Controls
3. CIP-004-6 Cyber Security – Personnel & Training
4. CIP-005-5 Cyber Security – Electronic Security Perimeter(s)
5. CIP-006-6 Cyber Security – Physical Security of BES Cyber Systems
6. CIP-007-6 Cyber Security – System Security Management
7. CIP-008-5 Cyber Security – Incident Reporting and Response Planning
8. CIP-009-6 Cyber Security – Recovery Plans for BES Cyber Systems
9. CIP-010-2 Cyber Security – Configuration Change Management and Vulnerability Assessments
10. CIP-011-2 Cyber Security – Information Protection
11. CIP-014-2 Cyber Security – Physical Security

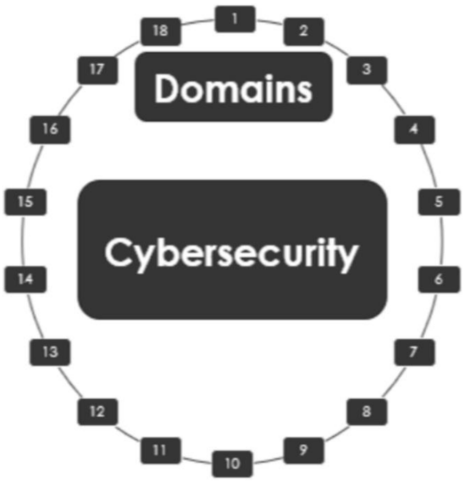
effectiveness of its National Cybersecurity Strategy or Policy already in place. The CSAM can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO).

The aim of this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was envisioned as a seamless and integrated cybersecurity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment for the integration of a national cybersecurity policy, program or strategy at the country level. Many cybersecurity frameworks are mostly oriented towards a specific industry like the *"PCI DSS"* for credit card security, the *"NERC CIP Cyber Security"* for the bulk power system or the *"NIST Cybersecurity Framework"* for protecting national critical infrastructure. Hence, all the existing frameworks do not provide a one-size fits all for planning and conducting cybersecurity audits. The necessity to mapping against specific cybersecurity frameworks is because of regulatory requirements, to satisfy the demands of industry regulators, to comply with internal or external audits, to satisfy business

purposes and customer requirements or simply by improving the enterprise cybersecurity strategy.

The CyberSecurity Audit Model (CSAM) contains overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessment and an evaluation scorecard shown in Figure 1.

Figure 1. The CyberSecurity Audit Model (CSAM)



Domains
1- Nation States
2- Governance and Strategy
3- Legal and Compliance
4- Cyber Assets
5- Cyber Risks
6- Frameworks and Regulations
7- Architecture and Networks
8- Information, Systems and Applications
9- Vulnerability Identification

Domains
10- Threat Intelligence
11- Incident Management
12- Digital Forensics
13- Awareness Education
14- Cyber Assurance
15- Active Cyber Defense
16- Evolving Technologies
17- Disaster Recovery
18- Personnel

CONCLUSION

This chapter provides a comprehensive literature review for standards, frameworks, methodologies, guidelines, best practices and models for information security, cybersecurity and information technology auditing and assurance. In this study, we selected the material based on current practices in the areas of compliance, audit engagements, governance, security risk management, assessments, audits and control verifications. Most methodologies do not cover all cybersecurity domains for auditing planning and execution. In many instances, it is required to combine more than one framework to cover many areas in information security and cybersecurity.

Furthermore, the existing information security/ cybersecurity standards, frameworks, methodologies, guidelines, best practices and models will constantly need to be updated, as the cyberthreat landscape keeps evolving

and cybercriminals find more sophisticated ways to launch their cyberattacks against companies and individuals.

REFERENCES

AICPA. (2017). *Trust Services Criteria*. American Institute of Certified Public Accountants, Inc.

AICPA. (2020). *SOC for Cybersecurity*. Retrieved from https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html

AXELOS. (2016). *ITIL Practitioner Guidance*. The Stationary Office.

AXELOS. (2019). *ITIL Foundation: ITIL* (4th ed.). The Stationary Office.

European Union Agency for Network and Information Security – ENISA. (2018). *Guidelines on assessing DSP and OES compliance to the NISD security requirements: Information Security Audit and Self-Assessment/Management Frameworks*. Retrieved from www.enisa.europa.eu

International Standardization Organization – ISO. (2013). *International Standard ISO/IEC 27002: Information technology – Security techniques – code of practice for information security controls* (2nd ed.). International Standardization Organization – ISO.

International Standardization Organization – ISO. (2013). *International Standard ISO/IEC 27002: Information technology – Security techniques – Information security management systems - Requirements* (2nd ed.). International Standardization Organization – ISO.

ISACA. (2010). *Information Security Management Audit/Assurance Program*. Retrieved from www.isaca.org

ISACA. (2014). *ITAF 3rd Edition: A Professional Practices Framework for IS Audit/Assurance*. Retrieved from www.isaca.org

ISACA. (2017). *Auditing Cyber Security: Evaluating Risk and Auditing Controls*. Retrieved from www.isaca.org

ISACA. (2018). *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. Retrieved from www.isaca.org

ISACA. (2018). *COBIT 2019 Framework: Governance and Management Objectives*. Retrieved from www.isaca.org

ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*. Retrieved from www.isaca.org

ISACA. (2018). *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. Retrieved from www.isaca.org

Lachapelle, E., & Bislimi, M. (2016). *Whitepaper: International Standard ISO/IEC 27002: Information technology – Security techniques – code of practice for information security controls, PECB/ Parabellum Cyber Security*. Retrieved from www.pecb.com

National Institute of Standards and Technology - NIST. (2017). *NIST Special Publication 800-53 Revision 5.* U.S. Department of Commerce. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

National Institute of Standards and Technology - NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. U.S. Department of Commerce. doi:10.6028/NIST.CSWP.04162018

North American Electric Reliability Corporation. (2020). *NERC CIP Reliability Standards*. Retrieved from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Office of Government Commerce. (2007). *ITIL Continual Service Improvement*. The Stationary Office.

Office of Government Commerce. (2007). *ITIL Service Design*. The Stationary Office.

Payment Card Industry Security Standards Council. (2010). *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 2.0*. Retrieved from www.pcisecuritystandards.org

Payment Card Industry Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 3.2.1*. Retrieved from www.pcisecuritystandards.org

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *Proceedings of Second International Conference on Information Systems and Computer Science (INCISCOS)*. 10.1109/INCISCOS.2017.20

The Institute of Internal Auditors - IIA (2016). *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense. Supplemental Guidance - Global Technology Audit Guide (GTAG)*. IIA.

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Cybersecurity Audit: Methodology to verify cybersecurity controls effectiveness and weaknesses.

Cybersecurity Framework: Particular set of rules to plan, implement, validate and audit cybersecurity controls in different organizational areas.

Chapter 8
The CyberSecurity Audit Model (CSAM)

ABSTRACT

This chapter presents the outcome of two empirical research studies that assess the implementation and validation of the cybersecurity audit model (CSAM), designed as a multiple-case study in two different Canadian higher education institution. CSAM can be applied for undertaking cybersecurity audits in any organization or nation state in order to evaluate and measure the cybersecurity assurance, maturity, and cyber readiness. The architecture of CSAM is explained in central sections. CSAM has been examined, implemented, and established under three research scenarios: (1) cybersecurity audit of all model domains, (2) cybersecurity audit of numerous domains, and (3) a single cybersecurity domain audit. The chapter concludes by showing how the implementation of the model permits one to report relevant information for future decision making in order to correct cybersecurity weaknesses or to improve cybersecurity domains and controls; thus, the model can be implemented and sufficiently tested at any organization.

INTRODUCTION

Organizations try to protect cyber assets and put into effect cybersecurity measures and programs, however in spite of this continuing effort it is far unavoidable to avert cybersecurity breaches and cyberattacks.

DOI: 10.4018/978-1-7998-4162-3.ch008

A recent study from Hiscox (2017) highlights that prevalence of cyberattacks is high in British, American and German Companies from unique industries and sectors together with technology, financial, enterprise services, manufacturing, professional services, retail, construction, transport, food and drinks, healthcare, leisure, telecommunication, real estate, media, energy and pharmaceutical and starting from small organizations to large corporations; 57% of the corporations have experienced as a minimum one and 42% of those corporations have dealt with two or more cyberattacks within a year. Most businesses (62%) usually get over a cyber incident in much less than 24 hours; a quarter (26%) usually takes less than an hour to get back to business while some groups spend days or more to recover from a cyberattack. A current trend covers greater spending in cybersecurity budgets, companies that already experienced a cyberattack are willing to put money into acquiring prevention technologies (24%) and detection technologies (23%). Smaller organizations incur with higher economic effect because of cyberattacks in comparison with larger corporations, most companies that participated in this study are taken into consideration as "cyber novices" in relation with the cyber readiness test (Hiscox, 2017) – the gap analysis indicates that investing money or having huge cybersecurity budgets do not help corporations to attain a "Cyber Experts" level. On the contrary, a major financial outlay isn't always the solution but enforcing other strategy and process measures like upper management involvement, cybersecurity awareness training, systematic monitoring and documentation. The costs of a cyberattack vary by geographic zones, for instance with corporations with more than 1,000 employees the financial impact will cost $ 53,131 in Germany, $ 84,045 in the UK and $ 102,314 in the USA.

Meulen et al. (2015) indicate that stakeholders need to comprehend the threat landscape in order to prepare for potential cyberattacks and at the same time to enforce defensive measures for protection. They summarized that there are not unique standards for classifying cyberthreats, the existing evidence suggests that is uncertain when it comes to defining threat assessments; they identified states, cybercriminals and hacktivists as the main threat actors and they also perceived cyberthreats linked to access, disclosure, manipulation of information, obliteration and denial of service.

In spite of enough cybersecurity measures, employees continue to be the weakest link in cybersecurity. Personnel are directly connected to financial losses related to data breaches and cybersecurity incidents (Pendergast, 2016).

IT audits are being redefined to include cybersecurity however there aren't clear guidelines or unison to which areas, sub-areas, domains or sub-

domains to incorporate in a cybersecurity audit. The CyberSecurity Audit Model (CSAM) was designed to address the limitations and inexistence of cybersecurity controls to handle comprehensive cybersecurity or domain-specific cybersecurity audits. An comprehensive cybersecurity audit model is needed to support the information security function. Furthermore, a model to deliver cybersecurity awareness training based on company roles is also necessary to change the traditional awareness programs.

We present the results of two empirical studies that assessed the implementation and validation of the CSAM through extensive cybersecurity audits. These studies were motivated by the lack of universal guidelines to conduct comprehensive cybersecurity audits and the existing weaknesses of general programs to deliver cybersecurity awareness training.

Our multi-case studies were conducted to answer the following questions:

How can we evaluate and measure the cybersecurity assurance, maturity and cyber readiness in any organization or Nation State?

Why it is necessary to increase cyber awareness at the organizational and personal levels?

BACKGROUND

This chapter look into an innovative model for creating, developing, planning, delivering and maintaining a CyberSecurity Audit (CSA) methodology or program that was corroborated in two different Canadian Higher Education organizations under unrelated projects and schedules. The implementations in both organizations were part of a multi-case study research along with the Cybersecurity Awareness TRAining Model (CATRAM); another innovative model to conduct and deliver cybersecurity awareness training.

The CyberSecurity Audit Model (CSAM) was conceived distinctively to conduct partial or complete cybersecurity audits classified by a specific domain, selected domains or the full audit of all domains within any organization. CSAM was designed to be functional for any type of organization, no matter the size nor the industry or sector where the organization is positioned.

In this chapter, CSAM was endorsed as the foundational model of our target organizations. These organizations did not have any policy in place for cybersecurity audits and CSAM was validated to introduce cybersecurity audits for their security domains and existing security controls. These days, CSAM is being adopted to develop the future cybersecurity audit programs for these higher education organizations.

LITERATURE REVIEW

Whenever a team of auditors might be participating in an IT, Information Security or compliance audit, there will be constant phases like planning, defining objectives and scope, clarifying engagement boundaries, running the audit, confirming evidence, assessing risks, presenting the audit findings and book follow up tasks. Planning any cybersecurity assessment is not different than any type of audit but can take countless resources due to the complexity of many cybersecurity domains.

ISACA points out the relevance of incorporating security controls as part of a complete framework and strategy, cyber assurance might be accomplished by management reviews, cyber risk assessments and cybersecurity controls audits. Hollingsworth recapitulated from his cybersecurity audit study, that the integral audit process produced evidence and remediation requirements to develop better cybersecurity controls; the involved audit team was able to remediate system documentation and nonconformities during the pre-audit phase and he concluded that upper management support and attention to cybersecurity audits turn into a standard for organizations.

Cybersecurity is located as the premier technology challenge for Information Technology (IT) audit managers and professionals; thus, companies should consider reviewing on a continuously their IT audit plans to address the cybersecurity threats and emerging technologies (Protiviti, 2017a). This research shows that managing cybersecurity audits are more important in certain geographic areas than others – North America (70%), Europe (58%), Latin America (56%), Oceania (53%), Middle East (50%), Africa (49%) and Asia (35%). However, North America is the only area where overseeing cybersecurity audits are within the Top 3 priorities when it comes to auditing. It is also revealed several imperative key considerations for directors including culture, competitiveness, compliance and cybersecurity (Protiviti, 2017b). Cybersecurity internal audits can support board of directors and senior management in these particular ways:

Evaluation of corporate processes to measure the attention to high-value information and systems

More effectively awareness of the cyberthreat landscape

Appraisal of the organizational cyber incident response readiness

The significance of conducting internal audits to verify the cybersecurity control's effectiveness, cyber risk management is based on roles and responsibilities (Deloitte, 2015):

First Line of defense: Business and Information Technology operations
Second Line of defense: Information and technology risk management
Third Line of defense: In-house audits

Deloitte's cybersecurity framework entitles that a few cybersecurity domains may be assessed through current IT audits, however the majority of cyber capabilities are not assessed by using the internal audits' scope. This framework includes risk and compliance management, development cycle, security program, third-party vendor management, information/ asset control, access control, threat/vulnerability control, data control and protection, risk analytics, crisis control and resiliency, safety operation and security awareness and training. Moreover, Deloitte's framework is aligned with industry frameworks just like the National Institute of Standards and Technology (NIST), Information Technology Infrastructure Library (ITIL), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and International Organization for Standardization (ISO).

ISACA (2016) designed an audit and assurance program primarily based on the NIST Cybersecurity Framework (CST) for comparing cybersecurity controls. This sort of audit program will review configuration management, incident management processes, networks, servers, awareness, enterprise continuity management, information security, governance administration practices for any company, its departments and relationships with third party vendors. The converting nature of cyberthreats demands businesses to develop cyber resilience and versatility as far as possible, by imposing cyber-by-layout in all their initiatives together with continuous assessments and cyber risks re-evaluations (ICAEW, 2016). Cybersecurity training and awareness are very important, but cybersecurity/InfoSec practices should be a component of any organizational culture.

A cybersecurity survey conducted by means of Deloitte and the National Association of State Chief Information Officers (NASCIO) highlights that the most important cybersecurity tasks for 2016 had been training and awareness, cybersecurity monitoring, strategy, governance, cybersecurity operations, risk assessments, cybersecurity metrics, regulatory and legislative compliance and access management. Additionally, cybersecurity budgets went through an increase from 37% in 2014 to 48% in 2016 respectively for the cybersecurity audit costs and the recurrent evaluation activities had been code reviews, cyber risk assessments, penetration testing, application safety vulnerability testing, cyberthreat intelligence analytics, privacy impact assessments, wargaming, business continuity exercises, disaster recovery exercises, protection tracking and operations center tasks (Deloitte University

Press, 2016). The 2017 version covers vital cybersecurity adoptions together with frameworks based on countrywide standards, awareness education, InfoSec culture, strategic plans, metrics to measure applications and cyber insurance (NASCIO, 2017).

For example, one global assignment in reviewing cybersecurity preparedness is the absence of standards to execute cybersecurity audits (Ross, 2015). Simple, precise and substantial approaches need to be targeted to deal with measures against cyberattacks, to make clear cybersecurity audit processes, to affirm that sensitive information is encrypted and to ensure patch management best practices.

Furthermore, there aren't any metrics to determine cybersecurity audits and the cybersecurity audit topic is badly understood as it renews really quickly. In order to cover a meaningful scope for planning a cybersecurity audit, the auditors must include all relevant areas in any organization; these areas are customer operations, finance, human resources, IT systems and applications, legal, purchasing, regulatory affairs, physical security and all applicable third parties that have relationships with the business (Khan, 2016).

Audit reporting isn't always about generating more than one report about information security weaknesses with out recommending the adequate solutions (Messier, 2016). The IT auditor team does not forget tips as a mandatory section when drafting the final audit report, but it is really useful that consists of corrective, preventive or immediate actions for the subsequent audit or a follow-up audit. The intention of cybersecurity audits should grasp on providing real evaluations of cybersecurity controls, standards, frameworks, procedures, strategies and recommendations to management.

Leidos (2017) designed the "Cyber Defense Maturity Evaluation (CDME)" that evaluates 13 key process areas and these areas must reach an *"ideal state/ level 4.0"* for the domains:

- Organization and Mission
- Executive Support
- Architecture and Engineering
- Security Technology
- Enterprise User Awareness
- Enterprise Visibility and Monitoring
- Malware Analysis
- Response and Mitigations
- Analysis Process and Skills
- Defender Operations

- Intelligence Management
- Metrics and Measuring Success
- Supporting Programs

This comprehensive enterprise defense framework was conceived on "how" approach instead of focusing on the basic "what", the framework itself is helping organizations to defend, sustain and outpace evolving cyber attackers. Leidos (2017) also enabled the Core Security Framework (CSF) assessment that evaluates cybersecurity implementations including 5 functions and 22 categories based on the Commerce Department's National Institute of Standards and Technology (NIST) security framework. The CSF utilizes metrics for risk management principles and best practices for cybersecurity.

Conducive to cyber readiness studies, Hathaway et al. (2015) established the leading comprehensive methodology that has been applied to 125 countries and available in 6 languages; Arabic, Chinese, English, French, Russian, and Spanish. Furthermore, the authors developed unique Cyber Readiness Index (CRI) country profiles for France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, United Kingdom and United States of America. The Cyber Readiness Index 1.0 was originally disseminated in November 2013 and is now superseded by The Cyber Readiness Index 2.0 edition of November 2015. This methodology stresses that *"No country is cyber ready"* and evaluates the nation's level of preparedness to deal with cyber risks, the identification of critical areas related to the cyber domain and the focus to implement certain initiatives to protect their economy and connectivity in terms of cybersecurity.

In terms of financial and cybersecurity audits, financial auditors have been engaged for many years by assessing IT controls since 1974 (SAS3), 1982 (SAS 44), 1992 (SAS70), 1997 (WebTrust), 1999 (SysTrust), 2003 (Trust Services Principles & Criteria - TSPC), 2010 (SSAE 16), 2011 (SOC1), 2016 (SSAE 18) and most recently in 2017; following the criteria from the Cybersecurity Risk Management Reporting Framework and Examination. The Center for Audit Quality recommends these cybersecurity frameworks as foundations to implement and assess a corporate cybersecurity risk management program including NIST Framework for improving critical infrastructure cybersecurity, ISO/IEC 27001/27002, US Securities and Exchange Commision (SEC) Cybersecurity Guidelines and Trust Services Criteria (TSC), (CAQ, 2017).

Moreover, the American Institute of Certified Public Accountants (AICPA) developed its own cybersecurity framework – the Cybersecurity Reporting Framework is an entity-level cybersecurity risk management framework

focused towards upper management's description, upper management's assertion and the opinions of Certified Public Accountants (CPAs).

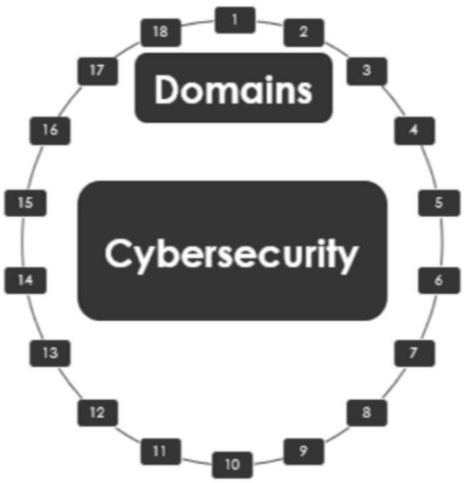
THE CYBERSECURITY AUDIT MODEL (CSAM)

The CyberSecurity Audit Model (CSAM) is a new exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place. The CSAM can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO).

The aim of this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was envisioned as a seamless and integrated cybersecurity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment for the integration of a national cybersecurity policy, program or strategy at the country level. Many cybersecurity frameworks are mostly oriented towards a specific industry like the *"PCI DSS"* for credit card security, the *"NERC CIP Cyber Security"* for the bulk power system or the *"NIST Cybersecurity Framework"* for protecting national critical infrastructure. But, all the existing frameworks do not provide a one-size fits all for planning and conducting cybersecurity audits. The necessity to mapping against specific cybersecurity frameworks is because of regulatory requirements, to satisfy the demands of industry regulators, to comply with internal or external audits, to satisfy business purposes and customer requirements or simply by improving the enterprise cybersecurity strategy.

The CyberSecurity Audit Model (CSAM) contains overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessment and an evaluation scorecard shown in Figure 1.

Figure 1. The CyberSecurity Audit Model (CSAM)



Domains
1- Nation States
2- Governance and Strategy
3- Legal and Compliance
4- Cyber Assets
5- Cyber Risks
6- Frameworks and Regulations
7- Architecture and Networks
8- Information, Systems and Applications
9- Vulnerability Identification

Domains
10- Threat Intelligence
11- Incident Management
12- Digital Forensics
13- Awareness Education
14- Cyber Assurance
15- Active Cyber Defense
16- Evolving Technologies
17- Disaster Recovery
18- Personnel

Overview

This section introduces the model organization, the working methodology and the possible options for implementation.

Resources

This component provides links to additional resources to help understanding some of the cybersecurity topics:

Cybersecurity: NIST Computer Security Resource Center, Financial Industry Regulatory Authority (FINRA) cybersecurity practices and Homeland Security cybersecurity.

National Cybersecurity Strategy (NCS): North Atlantic Treaty Organization (NATO) cybersecurity strategy, European Union Agency for Network and Information Security (ENISA) cybersecurity strategy and Organisation for

Economic Co-operation and Development (OECD) comparative analysis of national cybersecurity strategies.

Governance: PricewaterhouseCoopers Board cybersecurity governance and MITRE cybersecurity governance.

Cyber Assets: NERC critical cyber assets.

Frameworks: Foresite common cybersecurity frameworks, United States Computer Emergency Readiness Team (US-CERT) framework and ISACA's implementing the NIST cybersecurity framework.

Architecture: Trusted Computer Group (TCG) architect's guide and US Department of Energy's IT security architecture.

Vulnerability Management: SANS vulnerability assessment and Homeland Security vulnerability assessment and management.

Cyber Threat Intelligence: SANS – Who's using cyberthreat intelligence and how?

Incident Response: Computer Security Incident Response Team (CSIRT) frequent asked questions.

Digital Forensics: SANS forensics whitepapers.

Awareness: National Cyber Security Alliance – Stay safe online and PCI DSS -Best practices for implementing security awareness program.

Cyber Defense: SANS- The sliding scale of cybersecurity.

Disaster Recovery: Financial Executives International (FEI) Canada – Cybersecurity and business continuity.

Personnel: Kaspersky – Top 10 tips for educating employees about cybersecurity.

Domains

The CSAM contains 18 domains. Domain 1 has been designed specifically for Nations States and domains 2-18 are applicable to any organization as illustrated in Table 1.

Sub-Domains

All domains have at least one sub-domain but in certain cases there might be several sub-domains per domain.

Table 1. The CyberSecurity Audit Model (CSAM) domains

The CyberSecurity Audit Model (CSAM) domains	
	Domains
The CyberSecurity Audit Model (CSAM)	1. Nation States 2. Governance and Strategy 3. Legal and Compliance 4. Cyber Assets 5. Cyber Risks 6. Frameworks and Regulations 7. Architecture and Networks 8. Information, Systems and Applications 9. Vulnerability Identification 10. Threat Intelligence 11. Incident Management 12. Digital Forensics 13. Awareness Education 14. Cyber Assurance 15. Active Cyber Defense 16. Evolving Technologies 17. Disaster Recovery 18. Personnel

The sub-domains are:

- Cyberspace
- Governance
- Strategy
- Legal and Compliance
- Cyber Asset Management
- Cyber Risks
- Frameworks and Regulations
- Architecture
- Networks
- Information
- Systems
- Applications
- Vulnerability Management
- Threat Intelligence
- Incident Management
- Digital Forensics
- Awareness Education
- Cyber Insurance
- Active Cyber Defense
- Evolving Technologies

- Disaster Recovery
- Onboarding
- Hiring
- Skills
- Training
- Offboarding

Controls

Each domain has sub-domains that are assigned a reference number. Controls are identified by clause numbers and an assigned checklist. In order to verify the control evaluation, the cybersecurity control is either in place or inexistent.

Checklists

Each checklist is linked to a specific domain and the subordinated sub-domain. The checklist verifies the validity of the cybersecurity sub-controls in alignment with a control clause. The cybersecurity auditors have the option to collect evidence to verify the sub-control compliance.

Guideline Assessment

The guideline assessment only applies to the Nation States domain. The guidelines are evaluated for cybersecurity culture, National Cybersecurity Strategy (NCS), cyber operations, critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy.

Evaluation Scorecard

The control, guideline and sub-control evaluation is calculated after the audit has been completed. The evaluation consists in assigning scores and ratings for each control, guideline and sub-control.

We calculate the final cybersecurity maturity rating of the Nation States domain by using the following criteria. The score can be mapped to a specific maturity level:

Immature (I): 0-30

The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy (NCS) or Policy is inexistent.

Developing (D): 31-70

The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace.

Mature (M): 71-90

While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters.

And for domains 2-18, we calculate the final cybersecurity maturity rating of any organization by using the following criteria:

The score can be mapped to a specific maturity level:

Immature (I): 0-30

The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program.

Developing (D): 31-70

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations.

Mature (M): 71-90

While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

METHODOLOGY

The goal of this study was to investigate and provide comprehensive models for the challenges that may arise when planning and delivering cybersecurity audits along with deploying cybersecurity awareness training.

Case studies are considered the most relevant of observational studies, any case study results are limited in generalizability and broader applications

(Edgard and Manz, 2017). Some authors prefer to design their case studies using the research methodology provided by Yin (2009). Bartnes and Brede (2016) presented their research using data collection, data analysis, scenario and case content sections. Meszaros and Buchalcevova (2016) designed the Online Services Security Framework (OSSF) and their research methods were organized in a process with the following activities:

1. Problem identification and motivation
2. Define the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

On a different approach, the case study of Bartnes et al. (2016) compiled the research method in an industrial case context, data collection and analysis and privacy and confidentiality issues sections.

According to Yin (2014), a definition of a case study encloses the following:

A case study investigates a contemporary phenomenon in a real-world context, a case study will have more variables of interest than data points, the main research questions are "how" or "why", case studies can include single or multiple cases, case studies are limited to quantitative evidence and are useful methods for evaluation. (Yin, 2014)

Following this statement, we designed, implemented and validated a multiple-case study based on Yin (2018) of three exercises - A cybersecurity audit and a cybersecurity awareness training in a Canadian higher education institution and cybersecurity audit in a second Canadian higher education institution. We cannot disclose further details to protect the confidentiality and anonymity of our target organizations and its participants, that allowed us to complete this multi-case study research. We conducted our multi-case study following the research methodology proposed by Yin (2018).

We recognized that the main problems are linked to conduct cybersecurity audits in a comprehensive and timely fashion by including the proper domains to be audited. Furthermore, how to deliver the appropriate cybersecurity awareness training to target different corporate groups in conjunction with topics that are aligned with the current cyberthreat landscape. Our motivation aimed to design a model that included an all in one approach to plan and

conduct cybersecurity audits at any organization with the ability to assess national cybersecurity strategies as well. In addition, we discovered that it was necessary to deal with the lack of knowledge to face cyberattacks and cyberthreats, as a result we ended up designing an organizational cybersecurity awareness training model that can be implemented to create the foundations of any cybersecurity awareness program.

We designed two theoretical cybersecurity models (CSAM & CATRAM) in order to be functional for any type of organization, no matter the size nor the industry or sector where the organization is positioned. The case study research proposition was to validate the execution of our models. The case involved the active participation of all levels of staff in our target organization in order to benefit by the case study research outcomes. The lessons learned from our study may help other organizations for further testing and implementations of our models.

Once we designed our cybersecurity models, we approached upper management of our initial target organization and presented our case study research proposal. We decided to conduct a cybersecurity pre-assessment to understand the organizational cybersecurity function and from there, plan to implement CSAM (Sabillon et al., 2017) while simultaneously delivering our cybersecurity awareness training based on CATRAM (Sabillon et al., 2018), and the results of the model's validation will be instrumental to understand the current cybersecurity status of the organization. The target organization management felt that this case study research was a win-win opportunity for the institution and for the researchers. The first author conducted interviews, observations, online surveys and collected documentation pertinent to the scope of the case study. The same approach was followed for our second target institution.

During the pre-assessment stage, the first author collected data using online surveys from IT staff, the IT manager and the registrar director. While delivering the cybersecurity training based on CATRAM, we collected survey data from all different groups including the board of directors, executives, managers, IT staff and end users. Thus, we collected evidence when conducting the cybersecurity audits based on CSAM (Sabillon, 2018) and organized by cybersecurity domains. The data collection phase allowed us to gather evidence from multiple sources like documents, policies, archival records, open-ended interviews, observations, structured interviews, structured surveys, multiple site visits, presentations, meetings, and computer and server logs. Data collection was similar in our second target institution.

The authors utilized a variety of approaches for data analysis. For the CATRAM dataset, we created flowcharts, charts, graphics and tabulated the data provided from the cybersecurity awareness training sessions. On the other hand, the biggest dataset came from the CSAM audit where the data was recorded in our control forms, sub-control forms and checklists for each cybersecurity domain and sub-domain that we audited.

We focused the dissemination of our multi-case study research, its results and our cybersecurity models to academic audiences, IT audit teams, cybersecurity audit teams and IT auditors. We presented a final report of our case study research to the executives of our target organizations, by highlighting the results and providing recommendations to address existing cybersecurity weaknesses. The authors designed a linear-analytic structure for this exploratory multi-case study research.

RESULTS

The CSAM was implemented and validated using three different scenarios at two different Canadian higher education institutions. In order to implement and validate the CSAM, we also designed the CATRAM that was simultaneously implemented along with the CSAM in our first target organization.

Scenario I: Cybersecurity audit of all model domains

The following tables provide a series of results to present the findings in the research scenario I. We illustrate the assessment of the CSAM cybersecurity domains and its main controls. Table 2 and Table 3 summarize the results and domain ratings for the research scenario where all CSAM cybersecurity domains were audited in our target organization 1 and target organization 2.

Scenario II: Cybersecurity Audit of Several Domains (Governance and Strategy, Legal and compliance, Cyber Risks, Frameworks and Regulations, Incident Management, Cyber Insurance and Evolving Technologies)

The following tables provide a series of results to present the findings in the research scenario II. We illustrate the assessment of seven cybersecurity

Table 2. Multiple Cybersecurity domain score (Scenario I) for Target Organization 1

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	35%
3	Legal and Compliance	☐	☐	☒	☐	90%
4	Cyber Assets	☒	☐	☐	☐	30%
5	Cyber Risks	☐	☒	☐	☐	60%
6	Frameworks and Regulations	☒	☐	☐	☐	30%
7	Architecture and Networks	☐	☒	☐	☐	67%
8	Information, Systems and Apps.	☐	☒	☐	☐	55%
9	Vulnerability Identification	☒	☐	☐	☐	30%
10	Threat Intelligence	☐	☒	☐	☐	60%
11	Incident Management	☒	☐	☐	☐	10%
12	Digital Forensics	☒	☐	☐	☐	30%
13	Awareness Education	☐	☒	☐	☐	60%
14	Cyber Insurance	☐	☐	☒	☐	90%
15	Active Cyber Defense	☒	☐	☐	☐	5%
16	Evolving Technologies	☐	☐	☐	☒	100%
17	Disaster Recovery	☒	☐	☐	☐	30%
18	Personnel	☐	☐	☒	☐	77%
Multiple Domain -Cybersecurity Maturity Rating						
Developing (D): 31-70 The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations.		☐	☒	☐	☐	**51%**

domains and its main controls. Table 4 and Table 5 summarize the results and domain ratings for the research scenario II where multiple cybersecurity domains were audited in our target organization 1 and target organization 2.

Scenario III: A single cybersecurity domain audit (Awareness Education)

Before conducting our case study research, our target organization did not have any cybersecurity awareness model or any cybersecurity awareness education program whatsoever. The CATRAM delivery allowed the organization, to

Table 3. Multiple Cybersecurity domain score (Scenario I) for Target Organization 2

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	42%
3	Legal and Compliance	☐	☐	☐	☒	100%
4	Cyber Assets	☐	☐	☒	☐	80%
5	Cyber Risks	☐	☒	☐	☐	70%
6	Frameworks and Regulations	☐	☐	☒	☐	90%
7	Architecture and Networks	☐	☐	☒	☐	80%
8	Information, Systems and Apps.	☐	☐	☒	☐	87%
9	Vulnerability Identification	☐	☐	☐	☒	100%
10	Threat Intelligence	☐	☐	☐	☒	95%
11	Incident Management	☐	☐	☐	☒	92%
12	Digital Forensics	☐	☐	☒	☐	85%
13	Awareness Education	☐	☐	☐	☒	95%
14	Cyber Insurance	☐	☐	☒	☐	85%
15	Active Cyber Defense	☐	☒	☐	☐	60%
16	Evolving Technologies	☐	☐	☒	☐	80%
17	Disaster Recovery	☐	☐	☒	☐	89%
18	Personnel	☐	☐	☒	☐	85%
Multiple Domain -Cybersecurity Maturity Rating		☐	☒	☐	☐	**83%**
Mature (M): 71-90 While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.						

build a strong foundation for a future implementation of a comprehensive cybersecurity awareness training program. The cybersecurity audit of the awareness education domain was conducted after the successful delivery and implementation of CATRAM.

We provide a series of tables to present the findings in the research scenario III for both organizations. Table C1 illustrates the assessment of the main cybersecurity awareness education controls. Table 6 and 7 summarize the results and domain rating for awareness education in our target organization 1 and target organization 2.

Table 4. Multiple Cybersecurity domain score (Scenario II) for Target Organization 1

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	35%
3	Legal and Compliance	☐	☐	☒	☐	90%
5	Cyber Risks	☐	☒	☐	☐	60%
6	Frameworks and Regulations	☒	☐	☐	☐	30%
11	Incident Management	☒	☐	☐	☐	10%
14	Cyber Insurance	☐	☐	☒	☐	90%
16	Evolving Technologies	☐	☐	☐	☒	100%
Multiple Domain -Cybersecurity Maturity Rating						
Developing (D): 31-70 The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations.		☐	☒	☐	☐	**59%**

Table 5. Multiple Cybersecurity domain score (Scenario II) for Target Organization 2

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☒	☐	☐	42%
3	Legal and Compliance	☐	☐	☐	☒	100%
5	Cyber Risks	☐	☒	☐	☐	70%
6	Frameworks and Regulations	☐	☐	☒	☐	90%
11	Incident Management	☐	☐	☐	☒	92%
14	Cyber Insurance	☐	☐	☒	☐	85%
16	Evolving Technologies	☐	☐	☒	☐	80%
Multiple Domain -Cybersecurity Maturity Rating						
Mature (M): 71-90 While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.		☐	☐	☒	☐	**80%**

DISCUSSION

This study presents the architecture and the dual validation of the CyberSecurity Audit Model (CSAM). The aim of this model is to introduce a cybersecurity

Table 6. Overall Cybersecurity domain rating (Scenario III) in Target Organization 1

Cybersecurity Audit Model (CSAM)			
Domain	**13-Awareness Education**		
Control Evaluation	**Ratings**		**Score**
	Immature	☐	
	Developing	☒	**60%**
	Mature	☐	
	Advanced	☐	
Developing (D): 31-70 The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The Awareness Education domain is developing. The organization has a foundation model for cybersecurity awareness and additional efforts are required to develop a complete cybersecurity awareness program.			

Table 7. Overall Cybersecurity domain rating (Scenario III) in Target Organization 2

Cybersecurity Audit Model (CSAM)			
Domain	**13-Awareness Education**		
Control Evaluation	**Ratings**		**Score**
	Immature	☐	
	Developing	☐	
	Mature	☐	
	Advanced	☒	**95%**
Advanced (A): 91-100 The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits. The Awareness Education domain is advanced. The organization has a foundation model for cybersecurity awareness and additional efforts are required to develop a complete cybersecurity awareness program that includes all staffing level and customers.			

audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was designed as a seamless and integrated cybersecurity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment

for the integration of a national cybersecurity policy, program or strategy at the country level.

Several cybersecurity frameworks are mostly oriented towards a specific industry like the *"PCI DSS"* for credit card security, the *"NERC CIP Cyber Security"* for the bulk power system or the *"NIST Cybersecurity Framework"* for protecting national critical infrastructure. Hence, all the existing frameworks do not provide a one-size fits all for planning and conducting cybersecurity audits. The needs for mapping against specific cybersecurity frameworks is because of regulatory requirements, to satisfy the demands of industry regulators, to comply with internal or external audits, to satisfy business purposes and customer requirements or simply by improving the enterprise cybersecurity strategy.

We compared our model in Table 8, to emphasize the main features against *"The Cybersecurity Framework (CSF) Version 1.1: NIST (2017)"* and *"The Audit First Methodology: Donaldson et al. (2015)"*. The CSAM is not for a specific industry, sector or organization – On the contrary, the model can be utilized to plan, conduct and verify cybersecurity audits everywhere. The CSAM has been conceived to conduct partial or complete cybersecurity audits either by a specific domain, several domains or the comprehensive audit for all domains.

CONCLUSION

The main objectives of this multi-case study were to design and validate two cybersecurity models; the CyberSecurity Audit Model (CSAM) along with the Cybersecurity Awareness TRAining Model (CATRAM) to address the challenges to conduct comprehensive cybersecurity audits and to deliver cybersecurity awareness training based on staff roles respectively. The cybersecurity models including all its components were successfully validated by a multiple case study performed in two Canadian higher education institutions.

The CSAM is not for a specific industry, sector or organization – On the contrary, the model can be utilized to plan, conduct and verify cybersecurity audits everywhere. The CSAM has been designed to conduct partial or complete cybersecurity audits either by a specific domain, several domains or the comprehensive audit for all domains. Likewise, the CATRAM can support the implementation of a foundation for consolidating a cybersecurity awareness training program at any organization.

Table 8. Comparison of some cybersecurity audit models

Audit Model or Framework	Description
The Cybersecurity Framework (CSF) Version 1.1: NIST (2017)	The first version was conceived in 2014 to improve cybersecurity of critical infrastructure. The version 1.1 manages cybersecurity risks for critical infrastructure. It includes of the Framework Core, the Framework Implementation Tiers and the Framework profiles. The Framework Core includes five functions – Identify, Protect, Detect, Respond and Recover; then each of these functions have categories and subcategories. In addition, the Core contains Informative resources like cybersecurity standards, guidelines and best practices. The Tiers define cybersecurity context organized from partial to adaptive tier. The Profile presents the outcomes based on organizational needs. The current profile can later be compared with a target profile.
The Audit First Methodology: Donaldson et al. (2015)	This approach considers other cybersecurity controls and leaves preventive control execution until the end. This audit includes five different stages: 1. Threat analysis: This phase identifies Confidentiality, Integrity and Availability (CIA) threats that may impact IT and corporate data. Threat impact and indicators are defined. 2. Audit controls: It includes the design of threat audit controls. 3. Forensic controls: This phase helps to implement the required forensic controls for the enterprise cybersecurity functional areas: 1) Systems administration 2) Networks 3) Applications 4) Endpoints, servers and devices 5) Identity, authentication and access 6) Data protection and cryptography 7) Monitoring, vulnerabilities and patch management 8) Availability, disaster recovery and physical protection 9) Incident management 10) Supply chain and asset management 11) Policy, audit, e-Discovery and training 4. Detective controls: Detective controls are designed to alert, detect, stop and repel cyberattacks. 5. Preventive controls: These controls block undesired activities and stop them from occurring.
The CyberSecurity Audit Model (CSAM): Sabillon et al. (2017)	The CSAM includes overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessments and an evaluation scorecard. Domain 1-Guideline assessment are specific for Nation States and domains 2-18 are applicable to any type of organization. Several domains have specific sub-domains where controls are evaluated. Then the checklists verify compliance about specific sub-controls based on domain/sub-domain. The scorecard results determine the domains rating and score that will produce the overall cybersecurity maturity rating.

The results of this study show that cybersecurity audits conducted by domains can be very effective to evaluate controls and responses to cyberthreats. Thus, the delivery of cybersecurity training based on organizational roles and

responsibilities tend to motivate personnel to create and maintain awareness in their workplaces as well in their personal lives.

The limitation of our study is that both models were validated in a single organization, time constraints, lack of interest for the topics and lack of engagement were some of the challenges that we have to overcome from some of the participants. For that reason, CSAM was also valiudated in second organization. Hence, future testing will enhance the model results by engaging more organizations.

The case study findings have implications for our target organizations but at the same time, implications for future research to review and expand our proposed cybersecurity models.

REFERENCES

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of Using Gaming Technologies for Cyber-Security Awareness. *International Journal of Information Security Research*, *6*(2), 660–666. doi:10.20533/ijisr.2042.4639.2016.0076

Axelos. (2015). *Cyber Resilience Best Practices.* Norwich: Resilia.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A., & Passingham, N. (2015). *Awareness is only the first step: A framework for progressive engagement of staff in cyber security*. Hewlett Packard Enterpise.

Beyer, R., & Brummel, B. (2015). *Implementing Effective Cyber Security Training for End Users of Computer Networks*. Society for Human Resource Management and Society for Industrial and Organizational Psychology.

Cano, J. (2016). La educación en seguridad de la información. Reflexión pedagógicas desde el pensamiento de sistemas. *Memorias 3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz"*.

Cano, J. (2016). Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información, 24-29.

Cyber, X. (2019). 2019 Global ICS & IIoT Risk Report. A data-driven analysis of vulnerabilities in our industrial and critical infrastructure. *CyberX Labs.* Retrieved from https://cyberx-labs.com/resources/risk-report-2019/

ESET. (2017). *ESET Cybersecurity Awareness Training.* ESET Canada. Retrieved from https://www.eset.com/ca/cybertraining/

Fujitsu. (2017). *The Digital Transformation PACT*. Retrieved from https://www.fujitsu.com

Gartner. (2016). *2016 Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors.* Gartner, Inc.

Gartner. (2018). *How to Build an Enterprise Security Awareness Program.* Gartner, Inc.

Gartner. (2018). *How to Secure the Human Link.* Gartner, Inc.

Gartner. (2018). *Magic Quadrant for Security Awareness Computer-Based Training*. Gartner, Inc.

Hayden, L. (2016). *People-Centric Security: Transforming your Enterprise Security Culture*. Mc Graw Hill.

Hollingsworth, C. (2016). Auditing fro FISMA and HIPAA: Lessons Learned Performing an In-House Cybersecurity Audit. *ISACA Journal*, *5*, 1–6.

International Organization for Standardization - ISO. (2005). *ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*. ISO.

International Organization for Standardization -ISO. (2012). *ISO/IEC 27032:2012 – Information Technology – Security Techniques – Guidelines for Cybersecurity*. ISO.

ISACA. (2017). *Auditing Cyber Security: Evaluating Risk and Auditing Controls*. ISACA.

LeClair, J., Abraham, S., & Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Worforce. *Proceedings of Information Security Curriculum Development Conference*, 71-78.

MediaPro. (2017). *A Best Practices Guide for Comprehensive Employee Awareness Programs*. MediaPro.

MITRE. (2010). *The Importance of Using EARNEST.* The MITRE Corporation. Retrieved from https://www.mitre.org/sites/default/files/pdf/mitre_earnest.pdf

MITRE. (2017). *Cybersecurity Awareness & Training*. The MITRE Corporation.

Monahan, D. (2014). *Security Awareness Training: It's not just for Compliance-Research Report Summary. Enterprise Management Associates*. EMA.

National Institute of Standards and Technology – NIST. (2003). *Building an Information Technology Security Awareness and Training Program.* NIST Special Publication 800-50.

National Institute of Standards and Technology – NIST. (2017). *An Introduction to Information Security.* NIST Special Publication 800-12 Revision 1.

Nguyen, T.N., Sbityakov, L., & Scoggins, S. (2018). *Intelligence-based Cybersecurity Awareness Training- an Exploratory Project*. CoRR, abs/1812.04234.

NTT Group. (2017). *Embedding cybersecurity into digital transformation - a journey towards business resilience.* NTT Security. Retrieved from https://www.nttsecurity.com

PCI Security Standards Council - PCI DSS. (2014). *Best Practices for Implementing a Security Awareness Program*. PCI DSS.

Penderdast, T. (2016). How to Audit the Human Element and Assess Your Organization's Security Risk. *ISACA Journal*, *5*, 1–5.

PhishMe. (2017). PhishMe CBFree. *PhishMe Headquarters*. Retrieved from https://phishme.com/resources/cbfree-computer-based-training/

Ponemon Institute. (2018). Assessing the DNS Security Risk. Research report sponsored by Infoblox. Ponemon Institute LLC.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *Proceedings of Second International Conference on Information Systems and Computer Science (INCISCOS)*. 10.1109/INCISCOS.2017.20

Sabillon, R., Serra-Ruiz, J., Cavaller, V., Jeimy, J., & Cano, M. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39. doi:10.4018/JCIT.2019070102

SANS Institute. (2017). 2017 Security Awareness Report: It's time to communicate. *SANS Security Awareness*. Retrieved from https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf

Security Awareness, S. A. N. S. (2017). *2017 Security Awareness Report*. SANS Institute.

Symantec. (2014). *Symantec Security Awareness Program: Mitigate information risk by educating your employees*. Symantec Corporation.

Ward, M. (2016). *Security Awareness and Training: Solving the unintentional insider threat*. Cyber Safe Worforce LLC.

Whitman, M. E., & Mattord, H. J. (2019). *Management of Information Security* (6th ed.). Cengage Learning, Inc.

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). Sage Publications.

Yin, R. K. (2018). *Case Study Research and Applications* (6th ed.). Sage Publications.

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Cybersecurity Audit: Audit to be conducted to verify cybersecurity controls.

Cybersecurity Domains: Cybersecurity areas that support a cybersecurity program in any organization.

Cybersecurity Maturity: Level of experience that an organization has implemented and acquired for cybersecurity practices.

APPENDIX 1

Template for Overall Cybersecurity Rating for Domain 1 (Nation States)

Table 9. Overall Cybersecurity Rating for Domain 1 (Nation States)

Cybersecurity Audit Model (CSAM)					
Domain	**1-Nation States**				
Sub-Domain: 1.1 Cyberspace	**Ratings**				**Score**
	I	**D**	**M**	**A**	
1.1.1 Cybersecurity Culture	☐	☐	☐	☐	
1.1.2 National Cybersecurity Strategy	☐	☐	☐	☐	
1.1.3 Cyber Operations	☐	☐	☐	☐	
1.1.4 Critical Infrastructure	☐	☐	☐	☐	
1.1.5 Cyber Intelligence	☐	☐	☐	☐	
1.1.6 Cyber Warfare	☐	☐	☐	☐	
1.1.7 Cybercrime	☐	☐	☐	☐	
1.1.8 Cyber Diplomacy	☐	☐	☐	☐	
Final Cybersecurity Maturity Rating	☐	☐	☐	☐	

Rating

If your score is:

Immature (I): 0-30

The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy or Policy is inexistent.

Developing (D): 31-70

The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace.

Mature (M): 71-90

While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters.

Template for Overall Cybersecurity Rating for Domains 2-18

Table 10. Overall Cybersecurity Rating for Domains 2-18

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
2	Governance and Strategy	☐	☐	☐	☐	
3	Legal and Compliance	☐	☐	☐	☐	
4	Cyber Assets	☐	☐	☐	☐	
5	Cyber Risks	☐	☐	☐	☐	
6	Frameworks and Regulations	☐	☐	☐	☐	
7	Architecture and Networks	☐	☐	☐	☐	
8	Information, Systems and Apps.	☐	☐	☐	☐	
9	Vulnerability Identification	☐	☐	☐	☐	
10	Threat Intelligence	☐	☐	☐	☐	
11	Incident Management	☐	☐	☐	☐	
12	Digital Forensics	☐	☐	☐	☐	
13	Awareness Education	☐	☐	☐	☐	
14	Cyber Insurance	☐	☐	☐	☐	
15	Active Cyber Defense	☐	☐	☐	☐	
16	Evolving Technologies	☐	☐	☐	☐	
17	Disaster Recovery	☐	☐	☐	☐	
18	Personnel	☐	☐	☐	☐	
Final Cybersecurity Maturity Rating		☐	☐	☐	☐	

Rating

If your score is:

Immature (I): 0-30

The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program.

Developing (D): 31-70

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations.

Mature (M): 71-90

While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

APPENDIX 2

We have included all CSAM checklists in this appendix. Appendix 2 contains checklists for all sub-domains:

- Cyberspace
- Governance
- Strategy
- Legal and Compliance
- Cyber Asset Management
- Cyber Risk
- Frameworks and Regulations
- Architecture
- Networks
- Information
- Systems
- Applications
- Vulnerability Management
- Threat Intelligence
- Incident Management
- Digital Forensics
- Awareness Education

- Cyber Insurance
- Active Cyber Defense
- Evolving Technologies
- Disaster Recovery
- Personnel Onboarding
- Personnel Hiring
- Personnel Skills
- Personnel Training
- Personnel Offboarding

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.1 (Cybersecurity Culture)

Table 11. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.1	1	Does the Nation State promote the adoption of a national cybersecurity culture for the society and its citizens?	☐	☐	☐		
1.1.1	2	Does the Nation State have involved all sectors of the society to create and develop a national cybersecurity culture?	☐	☐	☐		
1.1.1	3	Does the Nation State have cybersecurity awareness training programs for its citizens?	☐	☐	☐		
1.1.1	4	Does the Nation State have involved academia with cybersecurity research and development initiatives?	☐	☐	☐		
1.1.1	5	Does the Nation State have involved the private sector with cybersecurity research and development initiatives?	☐	☐	☐		
1.1.1	6	Does the Nation State have incentive mechanisms to encourage new cybersecurity products and services?	☐	☐	☐		
1.1.1	7	Does the Nation State have government incentives to encourage cybersecurity education, knowledge sharing and skills development?	☐	☐	☐		
1.1.1	8	Does the Nation State have introduced mechanisms to reduce the digital divide? Do Internet and Telecommunication services will be improved?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.2 (NCSS)

Table 12. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.2	1	Is the NCSS regularly reviewed? Are there any mechanisms to review and audit the NCSS?	☐	☐	☐		
1.1.2	2	Does the NCSS involve the participation of all related national main agencies, industries, sectors, military, police and academia?	☐	☐	☐		
1.1.2	3	Does the Nation State have designated an agency to deal with all national cybersecurity matters?	☐	☐	☐		
1.1.2	4	Does the Nation State have a national CSIRT to monitor and protect cyberspace?	☐	☐	☐		
1.1.2	5	Does the Nation State have clear coordination and communication procedures for all its agencies in case of different levels of cyberattacks?	☐	☐	☐		
1.1.2	6	Does the Nation State have designated a military unit in charge of developing military cyber capabilities?	☐	☐	☐		
1.1.2	7	Is the NCSS integrated with the Nation State security strategies?	☐	☐	☐		
1.1.2	8	Does the NCSS include a secure, resilient and reliable cyberspace?	☐	☐	☐		
1.1.2	9	Is the NCSS evaluating all possible risks that may affect national information and communication technologies?	☐	☐	☐		
1.1.2	10	Is the NCSS continually identifying various stakeholders to develop cyber offensive and defensive capabilities?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.3 (Cyber Operations)

Table 13. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.3	1	Does the Nation State have a national cyber operations center?	☐	☐	☐		
1.1.3	2	Is the Nation State continually implementing and enhancing cyber defensive operations?	☐	☐	☐		
1.1.3	3	Is the Nation State continually implementing and enhancing cyber offensive operations?	☐	☐	☐		
1.1.3	4	Does the Nation State have recruited qualified staff to operate and manage the national cyber operations center?	☐	☐	☐		
1.1.3	5	Does the Nation State have monitoring capabilities for cyberspace?	☐	☐	☐		
1.1.3	6	Does the Nation State have all the required tools and technologies at the national cyber operations center?	☐	☐	☐		
1.1.3	7	Does the Nation State have case management capability at the national cyber operations center?	☐	☐	☐		
1.1.3	8	Does the Nation State have detection, analysis, and response operations at the national cyber operations center?	☐	☐	☐		
1.1.3	9	Does the Nation State have clear standard operating procedures and policies to run the national cyber operations center?	☐	☐	☐		
1.1.3	10	Does the Nation State have a metric program to measure the effectiveness of the national cyber operations? Are Cyber Red/White/Blue Team exercises planned and executed?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.4 (Critical Infrastructure -CI)

Table 14. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.4	1	Does the Nation State have identified all its national critical infrastructure/ critical infrastructure information, systems, cyber assets, data and capabilities?	☐	☐	☐		
1.1.4	2	Does the Nation State have developed plans to protect all its national critical infrastructure services?	☐	☐	☐		Anomalies, events, incidents, 24/7 monitoring, detection processes
1.1.4	3	Does the Nation State have implemented measures to detect cybersecurity events?	☐	☐	☐		
1.1.4	4	Does the Nation State have implemented plans to respond to specific cybersecurity incidents?	☐	☐	☐		
1.1.4	5	Does the Nation State have implemented resilience and recovery plans after the impact of a cybersecurity incident?	☐	☐	☐		
1.1.4	6	Does the State Nation is following a specific cybersecurity framework to protect CI?	☐	☐	☐		
1.1.4	7	Does the State Nation have implemented *Information Exchange* to protect CI?	☐	☐	☐		
1.1.4	8	Does the State Nation have defined clear roles and responsibilities for all CI stakeholders?	☐	☐	☐		
1.1.4	9	Does the State Nation have defined communication procedures in case of any incident affecting CI?	☐	☐	☐		
1.1.4	10	Does the State Nation review and audit its cybersecurity program to protect CI?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.5 (Cyber Intelligence)

Table 15. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.5	1	Does the Nation State have Cyber Intelligence capabilities?	☐	☐	☐		
1.1.5	2	Does the Nation State have Cyber Counter Intelligence capabilities?	☐	☐	☐		
1.1.5	3	Does the Nation State have Cyber Intelligence services to address cyberthreats?	☐	☐	☐		Information collection, verification, aggregation, analysis and intelligence sharing
1.1.5	4	Does the Nation State Cyber Intelligence support operational, tactical and strategic environments?	☐	☐	☐		
1.1.5	5	Does the Nation State Cyber Counter Intelligence support operational, tactical and strategic environments?	☐	☐	☐		
1.1.5	6	Does the Nation State assign resources to increase the Cyber Intelligence capabilities?	☐	☐	☐		
1.1.5	7	Does the Nation State assign resources to increase the Cyber Counter Intelligence capabilities?	☐	☐	☐		
1.1.5	8	Do national intelligence agencies collaborate gathering cybersecurity intelligence?	☐	☐	☐		
1.1.5	9	Does the Nation State collect intelligence related to the latest APTs and cyber-espionage?	☐	☐	☐		
1.1.5	10	Does the Nation State analyze the current cyber threat landscape? Are there any collaboration with international agencies?	☐	☐	☐		Five eyes, NSA, 9 eyes, 14 eyes, 41 eyes

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.6 (Cyber Warfare)

Table 16. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.6	1	Is the Nation State prepared to protect its cyber domain?	☐	☐	☐		
1.1.6	2	Is the Cyber domain strategy aligned with the NCSS?	☐	☐	☐		
1.1.6	3	Does the Nation State include cyber defense to protect its cyberspace?	☐	☐	☐		Cyber defensive and offensive operations
1.1.6	4	Does the Nation State include strategic cyber operations?	☐	☐	☐		
1.1.6	5	Does the Nation State have specific battlefield cyber capabilities?	☐	☐	☐		
1.1.6	6	Does the Nation State have a tactical military cybersecurity unit?	☐	☐	☐		
1.1.6	7	Does the Nation State have organized cyber warrior forces?	☐	☐	☐		
1.1.6	8	Does the Nation State have formal programs to recruit, train and hire cybersecurity specialists?	☐	☐	☐		Either military and/or civilian personnel
1.1.6	9	Is the Nation State able to apply cyber retaliation and cyber deterrence in order to prevent or stop full scale-neutralize cyber attacks?	☐	☐	☐		
1.1.6	10	Does the Nation State have the ability to measure the effectiveness any cyber scenario?	☐	☐	☐		Briefing and Debriefing, Present reports

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.7 (Cybercrime)

Table 17. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.7	1	Does the Nation State have laws to prosecute cybercrime?	☐	☐	☐		
1.1.7	2	Does the Nation State have several organizations that are fighting national and international cybercrime?	☐	☐	☐		
1.1.7	3	Does the Nation State have national cybersecurity awareness programs to prevent cybercrime?	☐	☐	☐		
1.1.7	4	Does the Nation State have a multi-angled program with government agencies and private sector to prevent and report cybercrime?	☐	☐	☐		
1.1.7	5	Does the police have cybercrime units to investigate and prosecute cybercrime? Do these cybercrime units have the required training and tools to tackle the modus operandi of cybercriminals?	☐	☐	☐		
1.1.7	6	Does the national police have cross-links and information exchanges with foreign cybercrime police units? Are these programs part of bilateral collaborations or exchange between international police organizations?	☐	☐	☐		Interpol, Europol
1.1.7	7	Does the national judiciary system cover prosecution of new forms of cybercrime?	☐	☐	☐		
1.1.7	8	Do digital investigations are protected by the national civil, criminal and judiciary systems?	☐	☐	☐		
1.1.7	9	Does the Nation State regulate ISPs and telecommunication carriers in order to inform of any actor that may incur in cybercrime operations?	☐	☐	☐		
1.1.7	10	How is the Nation State dealing with jurisdiction, sovereignty and international cooperation issues to fight cybercrime?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyberspace: 1.1.8 (Cyber Diplomacy)

Table 18. Domain: 1-Nation States

Clause	No.	Guidelines Assessment	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
1.1.8	1	Does the Nation State participate actively in global Internet governance initiatives?	☐	☐	☐		IAB, IETF, ICANN, ITU, IGF, IEEE
1.1.8	2	Does the Nation State participate actively in cyber diplomacy to improve global cybersecurity?	☐	☐	☐		
1.1.8	3	Does the Nation State participate in bilateral agreements to reduce tensions in cyberspace?	☐	☐	☐		
1.1.8	4	Does the Nation State participate in multilateral agreements to reduce tensions in cyberspace?	☐	☐	☐		
1.1.8	5	Does the Nation State participate in pro action initiatives related to cyber diplomacy?	☐	☐	☐		
1.1.8	6	Does the Nation State participate in prevention initiatives related to cyber diplomacy?	☐	☐	☐		
1.1.8	7	Does the Nation State participate in preparation initiatives related to cyber diplomacy?	☐	☐	☐		
1.1.8	8	Does the Nation State participate in response initiatives related to cyber diplomacy?	☐	☐	☐		
1.1.8	9	Does the Nation State participate in recovery initiatives related to cyber diplomacy?	☐	☐	☐		
1.1.8	10	Does the Nation State participate in after care initiatives related to cyber diplomacy?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Governance

Table 19. Domain: 2-Governance and Strategy

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
2.1.1	1	Is there a valid metric framework in place?	☐	☐	☐		
2.1.2	2	Are the roles and responsibilities for each line of defense clearly described?	☐	☐	☐		
2.1.4	3	The organization has defined a taxonomy for cybersecurity risks?	☐	☐	☐		
2.1.2	4	Have the organization clearly defined responsibilities to support cybersecurity governance?	☐	☐	☐		
2.1.4	5	Management actions are in accordance with the organization's governance?	☐	☐	☐		
2.1.2	6	Do staff support the organization's strategy and objectives?	☐	☐	☐		
2.1.3	7	Does management encourage periodical cybersecurity reviews?	☐	☐	☐		
2.1.4	8	Are the external contracting practices evaluated based on the organization's strategies and objectives?	☐	☐	☐		
2.1.1	9	Do the organization's policies, standards and procedures support the governance and strategy?	☐	☐	☐		
2.1.5	10	Are the cybersecurity risk management practices properly managed?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Strategy

Table 20. Domain: 2-Governance and Strategy

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
2.2.1	1	The organization has established a cybersecurity policy?	☐	☐	☐		
2.2.2	2	Is the organization implementing a cybersecurity strategy aligned with IT and InfoSec strategies?	☐	☐	☐		
2.2.2	3	The scope of the cybersecurity strategy reflects the size and the sector/industry of the organization?	☐	☐	☐		
2.2.1	4	Is the cybersecurity strategy aligned with the organization governance?	☐	☐	☐		
2.2.1	5	Is the cybersecurity strategy linked to other relevant organizational policies?	☐	☐	☐		
2.2.5	6	Has the organization defined strategic, tactical and operational plans for cybersecurity initiatives?	☐	☐	☐		
2.2.4	7	The organization encourages monitoring and reporting of preventive, detective and corrective measures	☐	☐	☐		
2.2.1	8	Do you ensure that cybersecurity is incorporated with the organization's values and objectives?	☐	☐	☐		
2.2.1	9	Does your organization adopt cybersecurity governance rules?	☐	☐	☐		
2.2.3	10	Does cybersecurity governance include continual improvement practices and progress monitoring?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Legal and Compliance

Table 21. Domain: 3-Legal and Compliance

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
3.1.1	1	The organization is complying with statutory, regulatory and contractual requirements?	☐	☐	☐		
3.1.2	2	What legislations are applicable to your institution?	☐	☐	☐		
3.1.3	3	What are the measures to protect your business records?	☐	☐	☐		
3.1.4	4	Provide proof of protection controls for data and privacy of personal information	☐	☐	☐		
3.1.5	5	List controls to avoid misuse of information and premises	☐	☐	☐		
3.1.6	6	What methodologies of cybersecurity frameworks are you following?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyber Assets

Table 22. Domain: 4-Cyber Assets

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
4.1.1	1	Does your organization have identified primary assets that support cybersecurity?	☐	☐	☐		
4.1.1	2	Does your organization have identified secondary assets that support cybersecurity primary assets?	☐	☐	☐		
4.1.2	3	Does the organization keeps track of physical asset inventory?	☐	☐	☐		
4.1.2	4	Does the organization keeps track of software asset inventory?	☐	☐	☐		
4.1.5	5	Does the organization have information classification guidelines to ensure protection?	☐	☐	☐		
4.1.4	6	Has the organization adopted procedures to label and handle information?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyber Risks

Table 23. Domain: 5-Cyber Risks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
5.1.1	1	Does the organization define risk scope and boundaries?	☐	☐	☐		
5.1.1	2	What criteria is used to assess cyber risks?	☐	☐	☐		
5.1.1	3	What methodology is used to deal with identified risks?	☐	☐	☐		
5.1.3	4	How do you manage residual risks?	☐	☐	☐		
5.1.4	5	What procedures are in place to manage risk acceptance?	☐	☐	☐		
5.1.1	6	Are there any risk communication and consultation processes?	☐	☐	☐		
5.1.1	7	Do you have procedures for risk monitoring?	☐	☐	☐		
5.1.1	8	How often do you review your risk management processes?	☐	☐	☐		
5.1.2	9	What criteria was used to define your cyber asset classification?	☐	☐	☐		
5.1.5	10	What are the goals and objectives of your cyber risk management?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Frameworks

Table 24. Domain: 6-Frameworks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
6.1.1	1	Is your organization following one or more best practices from an IT, information security or cybersecurity framework?	☐	☐	☐		
6.1.2	2	Is your organization certified on a specific cybersecurity framework? If not, do you consider this approach will be useful to your business?	☐	☐	☐		If the organization is certified or planning to certify on a specific framework, then a separate framework audit must be conducted.

6.1.3 Are you interested or planning to implement either partially or completely best practices from the following frameworks?

ITIL ☐ ISO 27001 ☐ NIST SP800-53 ☐ ISC^2 CBK ☐ NIST Cybersecurity ☐
COBIT ☐ SANS 20 ☐ DHS CRR ☐ Australian DSD ☐ PCI DSS ☐
HIPAA ☐ HITRUST CSF ☐ NERC CIP ☐ ISO 27032 ☐ ISACA audit and assurance ☐
NERC ☐ ITAF ☐ COSO ☐ ISF ☐ Other: _____

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.1 (Data Centres)

Table 25. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.1	1	Does the organization control physical access to data centres and server rooms? Do you keep an access log?	☐	☐	☐		
7.1.1	2	Does the organization have proper equipment hosting requirements?	☐	☐	☐		Water-cooled equipment, weight, electrical supply, receipt of new equipment, diagrams, maintenance, decommissioning
7.1.1	3	Is Power management adequate to the facilities?	☐	☐	☐		
7.1.1	4	Do you monitor environmental conditions and alert systems?	☐	☐	☐		Temperature, humidity, air quality
7.1.1	5	Are the facilities in compliance with safety standards and legislation?	☐	☐	☐		
7.1.1	6	Do you coordinate routine maintenance accordingly?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.2 (IT Operations)

Table 26. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.2	1	Do you incorporate security measures in all your IT Operations?	☐	☐	☐		
7.1.2	2	Do you keep up-to-date documentation for critical processes or functions?	☐	☐	☐		Standard Operating Procedures (SOPs), Operation logs, Operations schedules
7.1.2	3	Do you monitor events, incidents, routine operational activities and status/performance of systems?	☐	☐	☐		
7.1.2	4	Do you manage job scheduling accordingly?	☐	☐	☐		
7.1.2	5	Do you have a backup management plan? Are your backup tapes or media stored outside the main building? Are you able to restore any specific data based on corrupt data, lost data, disaster recovery or historical data?	☐	☐	☐		
7.1.2	6	Do you have a Print management plan? Have you changed the default settings/passwords on your printers? Have you implemented secure printing for confidential printouts?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.3 (Servers)

Table 27. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.3	1	Do you restrict physical and logical access to servers to authorized technical staff?	☐	☐	☐		
7.1.3	2	Do you keep a patch management plan for all your servers? Do you follow approved change management for new updates and patches?	☐	☐	☐		
7.1.3	3	Do you have configuration and alerts in place to monitor server uptime/downtime?	☐	☐	☐		
7.1.3	4	Do you inspect/review your servers regularly in order to hardening security?	☐	☐	☐		
7.1.3	5	Have you implemented virtualization? Do you keep inventory of your virtual servers and host machines? Have you encrypted server communications (SSL or IPSec)? Do you restrict access to the virtual server management console and hypervisors?	☐	☐	☐		
7.1.3	6	Do you perform regular maintenance on all your physical/virtual servers?	☐	☐	☐		
7.1.3	7	Do you have procedures for old server decommissioning and disposal?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.4 (Storage)

Table 28. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.4	1	Have you defined a data storage policy for all your storage devices?	☐	☐	☐		HDDs, NAS, SANs, DAS, CAS
7.1.4	2	Have you implemented a storage naming convention and hierarchy?	☐	☐	☐		
7.1.4	3	Are you enforcing freedom of information, data protection and IT governance regulations for your stored data?	☐	☐	☐		
7.1.4	4	Do you have an archiving policy?	☐	☐	☐		
7.1.4	5	Are you able to retrieve archived data as necessary?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.5 (Defense-in-Depth)

Table 29. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.5	1	Have you implemented cybersecurity defense-in-depth?	☐	☐	☐		
7.1.5	2	Which type of defense have you implemented?	☐	☐	☐		Concentric rings, overlapping redundancy, segregation or a combination
7.1.5	3	What vulnerabilities are you addressing per layer?	☐	☐	☐		
7.1.5	4	How are the layers weakening the vulnerabilities?	☐	☐	☐		
7.1.5	5	What kind of interactions exist between layers?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.6 (Physical Security)

Table 30. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.6	1	Do you have policies and procedures to limit unauthorized access to restricted facilities?	☐	☐	☐		
7.1.6	2	Do you have methods in place to control access to your secure areas?	☐	☐	☐		
7.1.6	3	Is your computing area physically secured?	☐	☐	☐		
7.1.6	4	Do you have a screen saver policy? Do screens automatically lock after inactivity?	☐	☐	☐		Via GPO
7.1.6	5	Have you implemented procedures to avoid laptop or equipment theft?	☐	☐	☐		Cable locks, secure storage

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.7 (Third Party Products and Services)

Table 31. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.7	1	Do you have strict processes for selecting suppliers, vendors and consultants?	☐	☐	☐		
7.1.7	2	Do you limit access to suppliers, vendors and consultants?	☐	☐	☐		
7.1.7	3	Do you monitor unauthorized changes or systems reconfiguration related to your infrastructure and architecture?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.8 (Frameworks)

Table 32. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.8	1	Do you follow a specific security architecture framework?	☐	☐	☐		SABSA, TOGAF
7.1.8	2	Do you follow architecture process models or framework models?	☐	☐	☐		
7.1.8	3	Do you have a centralized, decentralized or hybrid IT architecture?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.9 (OSI model)

Table 33. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.9	1	Have you taken measures to ensure smooth flowing of data throughout the OSI layers?	☐	☐	☐		
7.1.9	2	Have you implemented security solutions for all seven OSI layers?	☐	☐	☐		
7.1.9	3	Have you enforced network port security for TCP and UDP?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.10 (Interconnection devices)

Table 34. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.10	1	Have you enforced security measures for hubs, repeaters and NICs?	☐	☐	☐		
7.1.10	2	Have you enforced security measures for layer 2 switches, bridges and Wireless Access Points (WAPs)?	☐	☐	☐		
7.1.10	3	Have you enforced security measures for layer 3 switches and routers?	☐	☐	☐		
7.1.10	4	Have you enforced security measures for layer 4 switches?	☐	☐	☐		
7.1.10	5	Have you enforced security measures for gateways?	☐	☐	☐		
7.1.10	6	Have you enforced security measures for modems?	☐	☐	☐		
7.1.11	7	Have you enforced security measures for PBXs?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.11 (Network Segmentation)

Table 35. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.11	1	Have you implemented isolation and segmentation to hardening network security?	☐	☐	☐		
7.1.11	2	Have you implemented secure VLANs?	☐	☐	☐		
7.1.11	3	Have you implemented server isolation?	☐	☐	☐		
7.1.11	4	Have you implemented domain isolation?	☐	☐	☐		
7.1.11	5	Have you implemented a Demilitarized Zone (DMZ)	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.12 (Encryption)

Table 36. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.12	1	Do you protect data/information using encryption techniques?	☐	☐	☐		
7.1.12	2	Have you implemented VPNs?	☐	☐	☐		
7.1.12	3	Have you implemented symmetric key encryption?	☐	☐	☐		
7.1.12	4	Have you implemented asymmetric key encryption?	☐	☐	☐		
7.1.12	5	Have you implemented PKI?	☐	☐	☐		
7.1.12	6	Have you implemented SSL and TLS?	☐	☐	☐		
7.1.12	7	Have you implemented digital signatures?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Architecture: 7.1.13 (Monitoring and Detection)

Table 37. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.1.13	1	Do you monitor ingress, egress and data loss prevention (DLP) in your organization?	☐	☐	☐		
7.1.13	2	Have you configured and monitored corporate antivirus?	☐	☐	☐		
7.1.13	3	Have you configured and monitored corporate anti-malware or security suite?	☐	☐	☐		
7.1.13	4	Do you have an IDS in place? Do you monitor it?	☐	☐	☐		
7.1.13	5	Do you have an IPS in place? Do you monitor it?	☐	☐	☐		
7.1.13	6	Do you have a SIM, SIEM or SEM in place? Do you monitor it?	☐	☐	☐		
7.1.13	7	Do you have a firewall in place? Do you monitor it?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.1 (Connectivity)

Table 38. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.1	1	Do you enforce security on your wired and Wi-Fi networks connectivity?	☐	☐	☐		
7.2.1	2	Have you implemented security on your Internet nodes?	☐	☐	☐		
7.2.1	3	Have you implemented security on your Intranet nodes?	☐	☐	☐		
7.2.1	4	Have you implemented security on your Extranet nodes?	☐	☐	☐		
7.2.1	5	Have you considered a security assessment for your IoT devices?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.2 (Telecom carriers and ISPs)

Table 39. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.2	1	Does your carrier and/or ISP offer security on your dedicated private channel and Internet link?	☐	☐	☐		
7.2.2	2	Does your carrier and/or ISP offer monitoring tools for your upload link?	☐	☐	☐		
7.2.2	3	Does your carrier and/or ISP offer monitoring tools for your download link?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.3 (Pen Testing)

Table 40. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.3	1	Do you plan your pen testing accordingly?	☐	☐	☐		
7.2.3	2	Do you define a clear scope when performing a pen test?	☐	☐	☐		
7.2.3	3	Do you approve a written permission for any pen test?	☐	☐	☐		
7.2.3	4	Do you ensure that your pen tests include **"Do not harm"** procedures?	☐	☐	☐		
7.2.3	5	Do you verify that your pen testers are highly qualified to conduct the work?	☐	☐	☐		
7.2.3	6	Do you release communication and escalation plans to your organization during the tests?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.4 (Fault Management)

Table 41. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.4	1	Have you implemented fault management to detect, log, alert and fix network issues?	☐	☐	☐		
7.2.4	2	Does your network management include network discovery and topology mapping features?	☐	☐	☐		
7.2.4	3	Have you configured properly your networks to discover events related to fault detection?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.5 (Configuration Management)

Table 42. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.5	1	Have you implemented configuration management so you can easily track network/systems configuration linked to hardware and software?	☐	☐	☐		
7.2.5	2	Are you able to discover your network devices using a specific tool?	☐	☐	☐		
7.2.5	3	Are you able to discover software and firmware versions in order to schedule future network updates?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.6 (Accounting Management)

Table 43. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.6	1	Have you implemented accounting management in order to measure network utilization parameters?	☐	☐	☐		
7.2.6	2	Are you measuring the utilization of all your network resources?	☐	☐	☐		
7.2.6	3	Are you analyzing data gathered to detect usage patterns?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.7 (Performance Management)

Table 44. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.7	1	Have you negotiated with your carrier or ISP a SLA to include metrics to evaluate the performance level of network services?	☐	☐	☐		
7.2.7	2	Are you evaluating input queue drops, output queue drops and ignored packets?	☐	☐	☐		
7.2.7	3	Are you evaluating CPU utilization, buffer allocation and memory allocation?	☐	☐	☐		Device level: Relationship between network protocols and buffer availability
7.2.7	4	Are you evaluating performance for any WAN?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.8 (Network Security)

Table 45. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.8	1	Have you hardening network authentication security?	☐	☐	☐		
7.2.8	2	Have you hardening network firewalls security?	☐	☐	☐		
7.2.8	3	Have you hardening network authorization security?	☐	☐	☐		
7.2.8	4	Have you hardening network segmentation security?	☐	☐	☐		
7.2.8	5	Have you hardening IDS/IPS security?	☐	☐	☐		
7.2.8	6	Have you implemented alert notification and remediation for attempted cyberattacks?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.9 (Endpoints)

Table 46. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.9	1	Are you regularly running inventories of authorized and unauthorized devices in your organization?	☐	☐	☐		
7.2.9	2	Are you regularly running inventories of authorized and unauthorized software in your organization?	☐	☐	☐		
7.2.9	3	Do you keep master images of laptops, mobile devices, laptops, workstations and servers? Are these images stored on a secure server?	☐	☐	☐		
7.2.9	4	Have you implemented continuous vulnerability assessment and remediation for your endpoints?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Networks: 7.2.10 (Firewalls)

Table 47. Domain: 7-Architecture and Networks

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
7.2.10	1	What kind of firewalls do you have in place?	☐	☐	☐		Hardware/ Software, Packet filtering, application systems, stateful inspection, NGFW, network layer, transport layer, context aware, proxy server, reverse proxy server, NAT, host-based
7.2.10	2	What kind of approach do you follow to configure your firewalls?	☐	☐	☐		Block by default, allow specific traffic, etc.…
7.2.10	3	Do you follow specific procedures to create firewall rules?	☐	☐	☐		Form, approval request
7.2.10	4	Do you follow the least privilege principle for granting network access through your firewalls? Do you configure access rules with minimal access rights?	☐	☐	☐		
7.2.10	5	Do you filter ICMP messages?	☐	☐	☐		
7.2.10	6	Do you grant mobile devices access by using MAC filtering?	☐	☐	☐		
7.2.10	7	Have you enforced security to access firewall consoles?	☐	☐	☐		Internal and external ports
7.2.10	8	Do you restrict network access and resources to visitors, temporary workers and consultants?	☐	☐	☐		
7.2.10	9	Do you document all firewall rule changes?	☐	☐	☐		
7.2.10	10	Do you perform firewall audits every semester? Do you schedule regular firewall maintenance for every firewall? Do you backup your firewall configurations?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.1 (Service Desk)

Table 48. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.1	1	Is your Help Desk enforcing best security practices?	☐	☐	☐		
8.1.1	2	Are you using a ticketing system to track all security events and incidents?	☐	☐	☐		
8.1.1	3	Is your Help Desk able to deal with cybersecurity events and incidents?	☐	☐	☐		
8.1.1	4	Are your Help Desk analysts escalating cybersecurity issues whenever is required?	☐	☐	☐		
8.1.1	5	Is your Help Desk creating and updating your knowledge base to deal with recurrent incidents?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.2 (Desktop Support)

Table 49. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.2	1	Are you enforcing desktop and laptop security policies?	☐	☐	☐		
8.1.2	2	Do you have a desktop and laptop image program in place?	☐	☐	☐		
8.1.2	3	Are you deploying releases, upgrades, patches and hot fixes through a release management program?	☐	☐	☐		
8.1.2	4	Do you monitor and audit your organization's desktop and laptop computers?	☐	☐	☐		
8.1.2	5	Are your laptops using an encryption program?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.3 (InfoSec Management)

Table 50. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.3	1	Do you have policies to manage and protect organizational data?	☐	☐	☐		
8.1.3	2	Have you defined data ownership in your organization?	☐	☐	☐		
8.1.3	3	Are you protecting sensitive information?	☐	☐	☐		
8.1.3	4	Are you in compliance with federal and provincial legal requirements for data and information?	☐	☐	☐		
8.1.3	5	Are you collecting personal data? Are you ensuring that personal data is protected against misuse, modification, unauthorized access and disclosure?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.4 (Documentation)

Table 51. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.4	1	Do you have an IT documentation policy?	☐	☐	☐		
8.1.4	2	Are you documenting your critical processes and procedures?	☐	☐	☐		
8.1.4	3	Have you implemented standardized documentation formats?	☐	☐	☐		
8.1.4	4	Are you following proper version controls and retirement controls?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.5 (Project Management)

Table 52. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.5	1	Are you using project management methodologies and best practices for all your projects?	☐	☐	☐		
8.1.5	2	Are you considering security for all the projects that you plan to implement in your organization?	☐	☐	☐		
8.1.5	3	Do your PM methodologies ensure that all internal and external resources follow best cybersecurity practices?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.6 (Change Management)

Table 53. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.6	1	Have you implemented change management in your organization?	☐	☐	☐		
8.1.6	2	Have you identified the change approvers in your organization?	☐	☐	☐		
8.1.6	3	Have you defined a change impact and risk categorization matrix?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.7 (Records Management)

Table 54. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.7	1	Have you implemented document control and records management in your organization?	☐	☐	☐		
8.1.7	2	Are your maintaining physical and electronic records?	☐	☐	☐		
8.1.7	3	Have you implemented security measures to protect your physical and electronic records?	☐	☐	☐		
8.1.7	4	Have you implemented procedures for data retention?	☐	☐	☐		
8.1.7	5	Have you implemented procedures for data destruction?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.8 (Privacy)

Table 55. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.8	1	Have you taken security measures to protect privacy?	☐	☐	☐		
8.1.8	2	Have you developed a Privacy Impact Analysis (PIA)?	☐	☐	☐		Based on Technology, Processes and People
8.1.8	3	Do you provide notice prior to collecting personal information?	☐	☐	☐		
8.1.8	4	Do you offer *opt-in* and *opt-out* information options?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Information: 8.1.9 (Audits)

Table 56. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.1.9	1	Do you conduct audits to ensure that the organization is protected and controlled?	☐	☐	☐		
8.1.9	2	Do you verify general control procedures?	☐	☐	☐		
8.1.9	3	Do you verify preventive, detective and corrective security controls?	☐	☐	☐		
8.1.9	4	Do you achieve assurance by continuous auditing and monitoring?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.1 (Operating Systems)

Table 57. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.1	1	Do you regularly schedule operating systems maintenance and support?	☐	☐	☐		
8.2.1	2	Do you regularly inventory and maintain your systems scripts?	☐	☐	☐		
8.2.1	3	Do you regularly inventory and maintain your systems programs?	☐	☐	☐		
8.2.1	4	Do you monitor interfaces to hardware and identify any failure?	☐	☐	☐		
8.2.1	5	Are you hardening authentication security?	☐	☐	☐		
8.2.1	6	Are you hardening authorization security?	☐	☐	☐		
8.2.1	7	Are you hardening file system permissions security?	☐	☐	☐		
8.2.1	8	Are you hardening access privileges security?	☐	☐	☐		
8.2.1	9	Have you implemented Single Sign-On (SSO) to log on multiple systems?	☐	☐	☐		
8.2.1	10	Do you regularly inventory and verify your organization's GPOs?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.2 (Access Management)

Table 58. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.2	1	Have you implemented a strong password policy for systems administrators and end users?	☐	☐	☐		
8.2.2	2	Have you implemented an access control policy?	☐	☐	☐		
8.2.2	3	Have you implemented a formal procedure for granting and blocking user's access?	☐	☐	☐		
8.2.2	4	Have you implemented privilege management based on the principle of least privilege?	☐	☐	☐		
8.2.2	5	Have you implemented user rights management based on job roles and segregation of duties?	☐	☐	☐		
8.2.2	6	Have you implemented a clear desk policy?	☐	☐	☐		
8.2.2	7	Have you implemented a clear screen policy?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.3 (Logging and monitoring)

Table 59. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.3	1	Is audit logging enabled on all your systems?	☐	☐	☐		
8.2.3	2	Do you monitor all your systems?	☐	☐	☐		
8.2.3	3	Have you taken security measures to protect logs against tampering and unauthorized access?	☐	☐	☐		
8.2.3	4	Are all your systems synchronized?	☐	☐	☐		
8.2.3	5	Is logging enabled for systems administrators and operators?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.4 (Databases)

Table 60. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.4	1	Have you implemented DB standards and policies?	☐	☐	☐		
8.2.4	2	Do you keep inventory of all your existing databases?	☐	☐	☐		
8.2.4	3	Have you taken security measures to avoid database manipulation?	☐	☐	☐		
8.2.4	4	Have you defined triggers that will generate alerts?	☐	☐	☐		
8.2.4	5	Do you perform database maintenance and monitoring?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.5 (Licensing)

Table 61. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.5	1	Do you keep track of all your software licensing?	☐	☐	☐		Contracts, keys, tokens, subscriptions, upgrades, OEMs
8.2.5	2	Have you implemented software licensing management?	☐	☐	☐		
8.2.5	3	Do you have processes in place for managing the software licensing phases?	☐	☐	☐		Requirements, design, evaluate, procure, build, deploy, operate, optimize and retire

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.6 (Web Management)

Table 62. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.6	1	Have you taken security measures to protect websites, web-based applications and Internet services?	☐	☐	☐		
8.2.6	2	Are you able to mitigate any cyber threat that could impact your websites, web-based applications and Internet services?	☐	☐	☐		
8.2.6	3	Do you monitor your website and web-based applications?	☐	☐	☐		Availability, resilience and security

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.7 (TPS)

Table 63. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.7	1	Have you taken security measures to protect TPS?	☐	☐	☐		
8.2.7	2	Do you protect confidential information generated by TPS?	☐	☐	☐		i.e. Payroll, bookstore
8.2.7	3	Do your flowcharts have strict security controls for the TPS?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.8 (ERP)

Table 64. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.8	1	Have you taken security measures to protect ERP?	☐	☐	☐		
8.2.8	2	Do you protect confidential information generated by ERP?	☐	☐	☐		
8.2.8	3	Do your flowcharts have strict security controls for the ERP?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.9 (e-Commerce)

Table 65. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.9	1	Have you taken security measures to protect e-Commerce?	☐	☐	☐		
8.2.9	2	Do you protect confidential information generated by e-Commerce systems?	☐	☐	☐		
8.2.9	3	Do your flowcharts have strict security controls for the e-Commerce systems?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.10 (Systems utilities)

Table 66. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.10	1	Do you keep track of all your systems utilities?	☐	☐	☐		
8.2.10	2	Have you implemented security measures for remote desktop connections?	☐	☐	☐		
8.2.10	3	Have you implemented security measures for virtual desktop access?	☐	☐	☐		
8.2.10	4	Do you regularly uninstall utilities that are no longer needed?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Systems: 8.2.11 (MAM)

Table 67. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.2.11	1	Have you hardening security on all mobile devices through your Mobile Application Management (MAM)?	☐	☐	☐		
8.2.11	2	Have you implemented controls to wipe data/ block any stolen/lost mobile device?	☐	☐	☐		
8.2.11	3	Have you implemented procedures to report and deal with stolen/lost mobile devices?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.1 (SDLC)

Table 68. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.1	1	Have you implemented security measures during all SDLC phases? From planning to maintenance?	☐	☐	☐		
8.3.1	2	Have you included vulnerability and control testing?	☐	☐	☐		
8.3.1	3	Have you included security during the code review process?	☐	☐	☐		
8.3.1	4	Have you separated system development, testing and production environments?	☐	☐	☐		
8.3.1	5	Do you have different access controls for system development, testing and production environments?	☐	☐	☐		
8.3.1	6	Do you stay current on application vulnerabilities?	☐	☐	☐		
8.3.1	7	Do you have procedures for media sanitization and destruction?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.2 (Cybersecurity apps)

Table 69. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.2	1	Is your antivirus program up-to-date?	☐	☐	☐		
8.3.2	2	Is your cybersecurity program up-to-date?	☐	☐	☐		
8.3.2	3	Is your anti-malware program up-to-date?	☐	☐	☐		
8.3.2	4	Is your firewall program up-to-date?	☐	☐	☐		
8.3.2	5	Is your IDS program up-to-date?	☐	☐	☐		
8.3.2	6	Is your IPS program up-to-date?	☐	☐	☐		
8.3.2	7	Is your SEM program up-to-date?	☐	☐	☐		
8.3.2	8	Is your SIM program up-to-date?	☐	☐	☐		
8.3.2	9	Is your SIEM program up-to-date?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.3 (Open source)

Table 70. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.3	1	Have you installed open source software on your organization critical servers?	☐	☐	☐		
8.3.3	2	Do you have specific requirements when selecting an open source software?	☐	☐	☐		
8.3.3	3	When installing free software are you ensuring that code does not contain malicious instructions?	☐	☐	☐		Spyware, surveillance software
8.3.3	4	When using freeware, shareware or any open source software, are you ensuring that is fully patched and using the latest versions?	☐	☐	☐		To avoid zero day attacks
8.3.3	5	Do you allow your end users to install their own open source software?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.4 (Merchant)*

Table 71. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.4	1	Do you maintain security network?	☐	☐	☐		
8.3.4	2	Do you protect cardholder data?	☐	☐	☐		
8.3.4	3	Do you maintain a vulnerability management program?	☐	☐	☐		
8.3.4	4	Have you implemented access control measures?	☐	☐	☐		
8.3.4	5	Do you monitor your networks?	☐	☐	☐		
8.3.4	6	Do you have an information security policy?	☐	☐	☐		

*Additional security controls may apply based on PCI DSS requirements

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.5 (Social Media)

Table 72. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.5	1	Have you changed the default privacy settings on all your social media apps?	☐	☐	☐		
8.3.5	2	Have you taken measures to deal with impersonation?	☐	☐	☐		
8.3.5	3	Are your familiar with the acceptable use policies?	☐	☐	☐		
8.3.5	4	Do you keep a strong password?	☐	☐	☐		
8.3.5	5	Are you taking measures to keep a good online presence and reputation?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.6 (Network Management)

Table 73. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.6	1	Are your network management applications up-to-date?	☐	☐	☐		
8.3.6	2	Is your app. monitoring physical and logical access to diagnostic and configuration ports?	☐	☐	☐		
8.3.6	3	Are you restricting networks connections?	☐	☐	☐		
8.3.6	4	Have you configured session time-out limits?	☐	☐	☐		
8.3.6	5	Have you implemented network routing controls?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.7 (VoIP)

Table 74. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.7	1	Are you enforcing Session Initiation Protocol (SIP)?	☐	☐	☐		
8.3.7	2	Are you provisioning on all your VoIP devices?	☐	☐	☐		Disabling admin interfaces, changing default passwords, limiting network access
8.3.7	3	Have you disabled voice portal dialing?	☐	☐	☐		
8.3.7	4	Do you check for weak passwords across the network?	☐	☐	☐		
8.3.7	5	Do you check for international forwarding?	☐	☐	☐		
8.3.7	6	Do you check for accounts without authentication?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.8 (Unified Communication)

Table 75. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.8	1	Have you taken security measures to protect video, chat, email, VoIP and presence?	☐	☐	☐		
8.3.8	2	Have you disabled unused services?	☐	☐	☐		
8.3.8	3	Do you monitor your call logs?	☐	☐	☐		
8.3.8	4	Do you use built-in UC security tools?	☐	☐	☐		
8.3.8	5	Have you implemented Quality of Service (QoS)?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.9 (Input controls) *

Table 76. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.9	1	Does the app have data checks and validation controls to ensure data is accurate, complete and authorized?	☐	☐	☐		
8.3.9	2	Does the app have approval and override controls to ensure data is accurate, complete and authorized?	☐	☐	☐		
8.3.9	3	Does the app have pended items controls to ensure data is accurate, complete and authorized?	☐	☐	☐		

*These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.10 (Access controls) *

Table 77. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.10	1	Does the app have authorization and approval rights controls to ensure data is accurate, complete and authorized?	☐	☐	☐		
8.3.10	2	Does the app have automated segregation of duties controls to ensure data is accurate, complete and authorized?	☐	☐	☐		
8.3.10	3	Does the app have access rights controls to ensure data is accurate, complete and authorized?	☐	☐	☐		

**These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.11 (Transmission controls) *

Table 78. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.11	1	Does the app have completeness and validity of content controls to ensure files are received from a trustful source and follow an accurate and complete processing?	☐	☐	☐		
8.3.11	2	Does the app have data transmission controls to ensure files are received from a trustful source and follow an accurate and complete processing?	☐	☐	☐		

*These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.12 (Processing controls) *

Table 79. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.12	1	Does the app have automated file identification and validation controls to ensure data is accurate and complete?	☐	☐	☐		
8.3.12	2	Does the app have automated functionality and calculations controls to ensure data is accurate and complete?	☐	☐	☐		
8.3.12	3	Does the app have data extraction, filtering and reporting controls to ensure data is accurate and complete?	☐	☐	☐		
8.3.12	4	Does the app have interface balancing, aging processing and duplicate checks controls to ensure data is accurate and complete?	☐	☐	☐		

**These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.13 (Output controls) *

Table 80. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.13	1	Does the app have general ledger controls to ensure data is accurate and complete?	☐	☐	☐		
8.3.13	2	Does the app have subledger posting controls to ensure data is accurate and complete?	☐	☐	☐		

**These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.14 (Integrity controls) *

Table 81. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.14	1	Does the app have processing data controls to ensure data is consistent and correct?	☐	☐	☐		
8.3.14	2	Does the app have monitoring and storage controls to ensure data is consistent and correct?	☐	☐	☐		
8.3.14	3	Does the app have update authorization controls to ensure data is consistent and correct?	☐	☐	☐		

**These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.15 (Audit trails) *

Table 82. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.15	1	Does the app have automated tracking of changes controls to ensure data is consistent and correct?	☐	☐	☐		
8.3.15	2	Does the app have automated tracking of overrides controls to ensure data is consistent and correct?	☐	☐	☐		
8.3.15	3	Does the app evaluate the effectiveness of other controls to ensure data is consistent and correct?	☐	☐	☐		

*These controls can apply to any application

Cybersecurity Audit Checklist: CSAM-Applications: 8.3.16 (e-mail)

Table 83. Domain: 8-Information, Systems and Applications

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
8.3.16	1	Have you implemented an antispam tool?	☐	☐	☐		
8.3.16	2	Have you enforced the avoidance of opening attachments or clicking on suspect links?	☐	☐	☐		This could trigger malware, spyware, ransomware
8.3.16	3	Have you enforced training on phishing techniques?	☐	☐	☐		Users can become victims of identity theft or financial scams
8.3.16	4	Do you enforce with your end users that email is not a tool to share personal or confidential information?	☐	☐	☐		
8.3.16	5	Are you using/encouraging personal email accounts for work purposes?	☐	☐	☐		
8.3.16	6	Do you verify any spoofed/suspicious email before replying to it?	☐	☐	☐		
8.6.16	7	Do you enforce with your end users to avoid connecting to public Wi-Fi's?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Vulnerability Management

Table 84. Domain: 9-Vulnerability Identification

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
9.1.2	1	Has the organization identified where all assets reside? This applies to physical and logical assets	☐	☐	☐		
9.1.3	2	Does your organization perform host-based vulnerability scans? List tools	☐	☐	☐		
9.1.3	3	Does your organization perform network-based vulnerability scans? List tools	☐	☐	☐		
9.1.5	4	Does the organization evaluate technical, process, organizational and emergent vulnerabilities?	☐	☐	☐		
9.1.6	5	What actions do you take as part of your vulnerability remediation?	☐	☐	☐		
9.1.1	6	Do you have proper reporting and metrics mechanisms related to vulnerability management?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Threat Intelligence

Table 85. Domain: 10-Threat Intelligence

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
10.1.1	1	Do you analyze information in order to identify and predict cyber capabilities and cyber threats?	☐	☐	☐		
10.1.1	2	Do you possess the mechanisms and tools to monitor and analyze the current cyber threat landscape?	☐	☐	☐		
10.1.2	3	Do you have measures that keep threats from exploiting vulnerabilities?	☐	☐	☐		
10.1.2	4	Do you have measures in place to identify and isolate malware?	☐	☐	☐		
10.1.3	5	Do you monitor logs, systems reports and security alerts?	☐	☐	☐		
10.1.4	6	Do you have plans to develop CTI skills in-house or outsource them?	☐	☐	☐		
10.1.4	7	Which CTI tools and tactics are you currently using?	☐	☐	☐		Examples are SIEM. SIM, SEM, IDS, IPS, firewalls, Forensics tools
10.1.1	8	Do you gather CTI from vendors, public feeds, law enforcement, private feeds, social media or open source feeds?	☐	☐	☐		
10.1.5	9	What best practices can you use to improve and integrate CTI into your systems?	☐	☐	☐		
10.1.5	10	What challenges is the organization facing to develop and integrate CTI capabilities?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Incident Management

Table 86. Domain: 11-Incident Management

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
11.1.1	1	Do you have a cybersecurity incident response plan in place?	☐	☐	☐		
11.1.5	2	Have you implemented processes for detection, identification, analysis and response to cybersecurity incidents?	☐	☐	☐		
11.1.2	3	Have you established escalation and communication processes to handle incidents?	☐	☐	☐		
11.1.4	4	Do you have formal plans to respond and document cybersecurity breaches?	☐	☐	☐		
11.1.2	5	Have you developed processes to communicate with internal parties and external stakeholders in case of a security incident?	☐	☐	☐		
11.1.1	6	Do you have a plan to organize and train teams to respond to cybersecurity incidents?	☐	☐	☐		
11.1.5	7	Do your conduct continuous reviews to your incident handling processes?	☐	☐	☐		
11.1.5	8	Do you keep record of all cybersecurity incidents?	☐	☐	☐		
11.1.5	9	Do you identify lessons learned and review incident response handling?	☐	☐	☐		
11.1.1	10	Have you categorized cybersecurity and reporting time frames for your organization?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Digital Forensics

Table 87. Domain: 12-Digital Forensics

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
12.1.1	1	Is the organization able to perform in-house digital forensic investigations?	☐	☐	☐		
12.1.2	2	Is any third-party vendor hired for internal digital investigations?	☐	☐	☐		
12.1.1	3	Is the technical staff familiar with all phases of digital forensics?	☐	☐	☐		
12.1.1	4	Is the organization able to provide validation of the occurrence of a cyberattack?	☐	☐	☐		
12.1.3	5	Can the organization gather digital evidence in case of any future prosecution?	☐	☐	☐		
12.1.4	6	Is your technical staff proficient with evidence management?	☐	☐	☐		
12.1.5	7	Is the organization capable of complying with any e-discovery case for litigation support?	☐	☐	☐		
12.1.1	8	Is your technical staff proficient in the use of DF procedures, tools and methodologies?	☐	☐	☐		
12.1.1	9	Is your technical staff able to deal with Anti-Forensics tactics, techniques and procedures(TTPs)?	☐	☐	☐		
12.1.3	10	Have you established capabilities to investigate cyberattacks and/or any type of cybercrime that could impact your operations?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Awareness

Table 88. Domain: 13-Awareness Education

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
13.1.1	1	Does your organization have a cybersecurity awareness program?	☐	☐	☐		
13.1.1	2	Do you provide some kind of cybersecurity training to your staff?	☐	☐	☐		
13.1.2	3	Is training delivered on a regular recurring basis?	☐	☐	☐		
13.1.1	4	Do employees are following security policies of the organization?	☐	☐	☐		
13.1.1	5	Are you delivering training to recognize and deal with social engineering?	☐	☐	☐		
13.1.1	6	Do your staff know how to recognize and report a security incident?	☐	☐	☐		
13.1.1	7	Is your personnel able to detect and respond to any cybersecurity emergency?	☐	☐	☐		
13.1.1	8	Do you enforce privacy and confidentiality requirements in your organization?	☐	☐	☐		
13.1.1	9	Are your employees following security procedures for data and information protection?	☐	☐	☐		
13.1.4	10	Is your awareness training focused and delivered to specific audiences like end users, managers, IT, C-Suite executives and Board of Directors?	☐	☐	☐		
13.1.1	11	Is your awareness training covering multidimensional topics?	☐	☐	☐		
13.1.1	12	Does your training outline cover technical, social and user behaviour areas?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Cyber Insurance

Table 89. Domain: 14-Cyber Insurance

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
14.1.1	1	What kind of cyber insurance coverage would your organization seek? Would you include first party and/or third party coverage?	☐	☐	☐		Options could be cyber omissions & errors, privacy, media protection and computer networks
14.1.5	2	Is your organization aware that cyber insurance cannot offer coverage for weaknesses in your cybersecurity architecture or program?	☐	☐	☐		
14.1.3	3	Are you prepared to fulfill a cybersecurity audit requirement in order to get a cyber insurance policy?	☐	☐	☐		
14.1.3	4	Would you implement a recommended cybersecurity framework, standard or good practice in order to acquire a cyber insurance?	☐	☐	☐		
14.1.2	5	How would you handle your current cybersecurity weaknesses in a potential cyber insurance risk assessment?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Active Cyber Defense

Table 90. Domain: 15- Active Cyber Defense

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
15.1.1	1	Does the organization have implemented passive defense to protect its networks, architecture and systems?	☐	☐	☐		
15.1.1	2	What ACD measures have you implemented?	☐	☐	☐		
15.1.3	3	What controls are in place to detect and analyze cyberattacks?	☐	☐	☐		
15.1.4	4	What controls are in place to mitigate cyberattacks?	☐	☐	☐		
15.1.5	5	Do you have any countermeasures in place?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Evolving Technologies

Table 91. Domain: 16- Evolving Technologies

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
16.1.1	1	Do you consider security when buying new assets for your organization?	☐	☐	☐		
16.1.1	2	Do you evaluate cybersecurity matters with external stakeholders, outsourcing companies and vendors?	☐	☐	☐		
16.1.4	3	Do you follow a specific procedure for acquiring/ hiring new security technologies, products or services?	☐	☐	☐		
16.1.4	4	What measures do you adopt when implementing new digital technologies?	☐	☐	☐		
16.1.4	5	Do you have a policy to manage mobile technology vulnerabilities, threats and risks?	☐	☐	☐		
16.1.4	6	Do you encourage a Bring-Your-Own-Device (BYOD) policy at your workplace?	☐	☐	☐		
16.1.5	7	Do you allow telework, work from home and digital collaborations?	☐	☐	☐		
16.1.4	8	Do you manage any kind of cloud computing?	☐	☐	☐		
16.1.4	9	Have you enforced policies to hardening security for social networks?	☐	☐	☐		
16.1.4	10	Do you assess associated cybersecurity issues, vulnerabilities and risks when acquiring a new technology?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Disaster Recovery

Table 92. Domain: 17- Disaster Recovery

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
17.1.1	1	Have you identified cyberassets that are critical to the continuous operation of your organization?	☐	☐	☐		
17.1.2	2	Have you taken measures to protect your critical services and infrastructure?	☐	☐	☐		
17.1.3	3	Have you taken any measures in case of a cybersecurity disaster?	☐	☐	☐		
17.1.1	4	Do you have formal and current Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) in place?	☐	☐	☐		
17.1.3	5	Have you followed Business Impact Analysis (BIA) to determine your critical cybersecurity processes?	☐	☐	☐		
17.1.4	6	Do you include cybersecurity testing while reviewing your BCP?	☐	☐	☐		
17.1.3	7	Is BCP/DRP training material content aligned with current business status?	☐	☐	☐		
17.1.6	8	Is the backup of business-critical systems, data, applications and documentation properly managed?	☐	☐	☐		
17.1.1	9	Has the Business Impact Analysis (BIA) covered time frames, priorities, resources and interdependencies that support key processes of the organization?	☐	☐	☐		
17.1.1	10	Have you determined Recovery Point Objectives (RPOs) for your critical processes?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Personnel Hiring

Table 93. Domain: 18- Personnel

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
18.2.1	1	Does the organization highlight the importance of any new hire's behaviour that is aligned with policies and standards?	☐	☐	☐		
18.2.2	2	Does the organization have clear disciplinary actions for staff that may infringe cybersecurity policies and standards?	☐	☐	☐		
18.2.2	3	Do disciplinary actions include security breaches committed by employees, consultants or third-party stakeholders?	☐	☐	☐		
18.2.3	4	Does the organization provide assigned office space and computing devices to the new hire?	☐	☐	☐		
18.2.3	5	Does the organization provide assigned telecom and wireless services to the new hire?	☐	☐	☐		
18.2.3	6	Does the organization provide the proper permissions and access to the new hire in order to work remotely?	☐	☐	☐		
18.2.3	7	Does the organization provide any kind of building security device or physical access?	☐	☐	☐		Access cards, tokens, biometric, alarm code, keys
18.2.3	8	Does the organization provide any kind of logical security?	☐	☐	☐		Passwords, FOBs, folder access, drive access
18.2.3	9	Does the organization enforce Ethernet port security?	☐	☐	☐		
18.2.1	10	Does the organization have proper procedures for 'Leave of absence request' and 'Return from Leave of absence'?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Personnel Onboarding

Table 94. Domain: 18- Personnel

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
18.1.1	1	Does the organization clearly state the job responsibilities in the job profile?	☐	☐	☐		
18.1.2	2	Does the organization ask for criminal background check prior to any job offer?	☐	☐	☐		
18.1.2	3	Does the organization ask for credit check prior to any job offer?	☐	☐	☐		
18.1.2	4	Does the organization ask for security clearance prior to any high-profile job offer?	☐	☐	☐		
18.1.3	5	Does the organization stress enough to the new hire the responsibilities when it comes to organizational cybersecurity matters?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Personnel Offboarding

Table 95. Domain: 18- Personnel

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
18.5.1	1	Does the organization have a clear termination request process?	☐	☐	☐		
18.5.1	2	Does the organization have an immediate termination request process?	☐	☐	☐		
18.5.1	3	Does the organization have a clear change of position request process?	☐	☐	☐		

Cybersecurity Audit Checklist: CSAM-Personnel Skills

Table 96. Domain: 18- Personnel

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
18.3.1-3	1	Does the organization encourage skills and competencies development based on roles?	☐	☐	☐		
18.3.1-3	2	Are goals defined for the acquisition of cybersecurity skills and competencies?	☐	☐	☐		
18.3.1-3	3	Does the organization know its current status for cybersecurity skills and competencies?	☐	☐	☐		
18.3.1-3	4	Does the organization encourage cybersecurity knowledge transfer based on Good Practices?	☐	☐	☐		
18.3.1-3	5	Which skills and competencies the organization wants its employees to develop and improve?	☐	☐	☐		Governance, cybersecurity strategy, cyber risks, architecture, cyber operations, assessments, audits, testing, compliance

Cybersecurity Audit Checklist: CSAM-Personnel Training

Table 97. Domain: 18- Personnel

Clause	No.	Checklist Questions	Findings			Supporting Evidence	Comments
			Compliant	Minor Nonconformity	Major Nonconformity		
18.4.1	1	Does the organization deliver an orientation training for new hires?	☐	☐	☐		
18.4.2	2	Does the orientation training cover basics of organizational cybersecurity?	☐	☐	☐		
18.4.3	3	Does the organization have valid training for departmental systems, apps and controls?	☐	☐	☐		
18.4.4	4	Does the organization have valid training for corporate systems, apps and controls?	☐	☐	☐		
18.4.2	5	All new hires participate in a cybersecurity awareness training?	☐	☐	☐		

Chapter 9
The Cybersecurity Awareness Training Model (CATRAM)

ABSTRACT

This chapter presents the outcome of one empirical research study that assess the implementation and validation of the cybersecurity awareness training model (CATRAM), designed as a multiple-case study in a Canadian higher education institution. Information security awareness programs have become unsuccessful to change people's attitudes in recognizing, stopping, or reporting cyberthreats within their corporate environment. Therefore, human errors and actions continue to demonstrate that we as humans are the weakest links in cybersecurity. The chapter studies the most recent cybersecurity awareness programs and its attributes. Furthermore, the authors compiled recent awareness methodologies, frameworks, and approaches. The cybersecurity awareness training model (CATRAM) has been created to deliver training to different corporate audiences, each of these organizational units with peculiar content and detached objectives. They concluded their study by addressing the necessity of future research to target new approaches to keep cybersecurity awareness focused on the everchanging cyberthreat landscape.

INTRODUCTION

A satisfactory Cybersecurity Awareness Program must include adequate training that is aligned with the organization's objectives, the focus to raise cybersecurity awareness while performing employee's duties and an

DOI: 10.4018/978-1-7998-4162-3.ch009

interactive communication between all stakeholders for any cybersecurity matter. Awareness programs may be unsuccessful if they are not designed to change people's attitude towards cyber incidents and likewise if a positive impact on any organization cannot be achieved. A cybersecurity awareness program is an organizational long-term investment that will help to create a cybersecurity culture if training is delivered on a continuous basis. A more energetic vision of the awareness aim is to go beyond the prevention of cybersecurity incidents.

We consider that the Cybersecurity Awareness TRAining Model (CATRAM) can represent a substantial foundation for the implementation of any organizational cybersecurity awareness program. CATRAM can also review any awareness training model that is steady and updated with the current cyberthreat landscape.

Cano (2016) points out that one of the consequences of current information security training methodologies is the "Bottom-up delegation"; this scenario does not allow end users to practice freedom and autonomy when it comes to data protection but instead follow and tolerate certain organizational information security policies.

BACKGROUND

This chapter look into an innovative model for creating, developing, planning, delivering and maintaining a Cybersecurity Awareness Training methodology or program that was validated in a Canadian Higher Education organization. The implementations in our target organization were part of a multi-case study research along with the CyberSecurity Audit Model (CSAM); another innovative model to conduct and deliver cybersecurity audits.

The Cybersecurity Awareness TRAining Model (CATRAM) was created distinctively to deliver cybersecurity awareness training to specific groups within any organization. CATRAM was designed to deliver the awareness training for the members of the Board od Directors, Top Executives, Managers, IT (Information Technology) staff and of course, end-users.

In this particular research scenario, CATRAM was implemented as the foundational model of our target organization. This organization did not have any Information Security policy in place for awareness training and CATRAM was validated to introduce cybersecurity awareness for their employees. These days, CATRAM is being used to develop the future cybersecurity awareness training program of this higher education organization.

LITERATURE REVIEW

As reported by the Gartner Magic Quadrant (2016) for Security Awareness Computer-Based Training (CBT) where leaders, visionaries, challengers and niche players are positioned. The Leaders are SANS Institute, Wombat Security Technologies, PhishMe, MediaPro, Security Innovation, Inspired eLearning, Terranova WW, PhishLine, Global Learning Systems, The Security Awareness Co.; Visionary vendors are Popcom Training and Security Mentor; Challenger vendors are BeOne Development, KnowBe4 and Optiv Security and last but not least are niche players like Junglemap, Digital Defense, Symantec (Blackfn Security) and Secure Mentem. Two years later (Gartner, 2018), we have seen relevant changes for the Security Awareness Computer-Based Training market where positions are different in all quadrants. The Leaders are Proofpoint (Wombat Security), MediaPro, Cofense, KnowBe and Terranova.; Visionary vendors are Inspired eLearning and Barracuda (PhishLine); Challenger vendors are SANS Institute, InfoSec Institute and Global Learning Systems and finally are the niche players like Junglemap, Security Innovation and Sophos. The new vendors placed as leaders, clearly identified market needs and incorporate new features on their CBT products, by including security topics aligned with the everchanging cyberthreat landscaping. Vendors continue to separate security awareness products and services by introducing a variety of formats, lengths and styles, by providing gamification, multilanguage support, supplemental internal marketing content like newsletters, intranet postings and security alerts, and integration with partnerships to offer endpoint detection and response, endpoint protection and data security. Another research study from Gartner (2018), indicates that by 2023 organizations that have implemented security awareness programs will go through 75% fewer account takeover attacks in comparison with other organizations, that is because effective security awareness programs must have a commitment from upper management and be in alignment with any organization's needs, practices and culture. Organizations face many challenges when deciding, delivering, implementing and maintaining a cybersecurity awareness training that is tailored to their specific business environment, strategy, needs and objectives. For example, choosing which topics to include when delivering the training, how to deliver training to personnel, how to verify the effectiveness of the training, updating the training program, implementing control measures to test cyber behaviors in the workplace and defining the frequency to re-train stakeholders.

A study from Ponemon Institute (2018) surveyed 1,021 IT and IT security practitioners in the USA and Europe, the Middle East and Africa (EMEA) to study Domain Name System (DNS) architecture, implementation and to identify responsibilities that manage cybersecurity activities in organizations. According to the results of the study, Ponemon Institute and Infoblox created the DNS Risk Index by categorizing five different areas: visibility, DNS attack protection, data protection and malware mitigation, threat intelligence and security operations. The most salient findings of this study show that most companies do not have dedicated staff to address DNS security, most companies are not tracking or identifying cyber assets, traffic analysis from firewalls is mostly used for malware mitigation and data assets protection, use of threat intelligence feeds is ineffective, measures to protect data assets include antivirus, endpoint security and data encryption and most cyberthreat investigations are conducted manually. The results show that the greatest concerns in terms of cyberattacks are advanced malware (63%), Advanced Persistent Threats (APTs – 59%), DNS-based data exfiltration (54%), unauthorized network access (51%), Ransomware (46%) and phishing/social engineering (45%).

The Global Security Awareness Report from SANS (2017), highlights that time and communication were identified as the critical takeaways to a thriving awareness program. The findings highlighted poor communication to engage people, the problem of time and lack of resources being assigned to a corporate awareness program. The participants revealed that they implemented awareness and behavior change (54.6%), had a compliance awareness program (27.1%), achieved long-term sustainment and culture change (9.8%), defined a program with robust metrics (0.9%) and did not have a cybersecurity awareness program at all (7.6%).

Symantec (2014) suggests that poorly trained personnel increases the risks of disclosure and loss of sensitive data like Personally Identifiable Information (PII) and Intellectual Property (IP). Its Security Awareness Program reduces vulnerabilities by creating a corporate culture and train employees to protect any organization critical assets from cyberattacks, exploitation, fraud and unauthorized access. The fundamental topics of Symantec's training program are information security, threats, vulnerabilities, countermeasures, securing the workplace, securing mobile users, protecting Internet information, social media mobile device security.

A study from Enterprise Management Associates (EMA, 2014) reported that 56% of personnel, not including IT and security staff, have not received any security awareness training in their organizations and 84% of participants

recognized that the awareness training from their workplaces was also used to decrease cyber risks at home. In addition, the study findings confirmed that the existing security awareness programs lack the appropriate delivery periodicity, content and quality. Moreover, Company size, market and budgets have a significant impact on the existence and maturity of their corporate awareness training.

ESET (2017) provision free online cybersecurity awareness training to train employees and get a certification. The topics consist of an overview of threats like malware, phishing and social engineering; best practices for password management; best practices for email protection and preventive measures that cover best practices for cyber hygiene at the workplace and at home. PhishMe also provides access to a free of charge Computer Based Training (CBT) course called PhishMe CBFree which contains seventeen security awareness modules and four compliance training modules. The course is available in seven languages (English, Chinese, French, German, Portuguese, Spanish and Japanese). The Compliance modules are General Data Protection Regulation (GDPR), Payment Data, Personal Data and Health Care; The security awareness modules cover cybersecurity awareness, cloud computing, advanced spear phishing, business email compromise, ransomware, surfing the Web, data protection, insider threats, malicious links, malware, mobile devices, security outside of the office, passwords, physical security, social engineering, social networking and spear phishing (PhishMe, 2017). Table 1 introduces an overview of most models and frameworks linked to best practices for the definition and consolidation of cybersecurity awareness programs.

Industrial and critical infrastructure organizations can also be targets of any cyberattack, as these organizations rely their businesses on Industrial Control Systems (ICS). Global malware attacks such as NotPetya, WannaCry and Emotet as well more targeted ICS cyberattacks such as Industroyer and TRITON, are just a few examples that can impact production outages, clean-ups, catastrophic safety and environmental incidents. The Global ICS & Industrial Internet of Things (IIOT) risk report (Cyberx, 2019) analyzed data from 850 production ICS networks using Network Traffic Analysis (NTA) in conjunction with deep packet inspections. The major findings included that 40% of industrial sites have at least one direct connection to the Internet, 53% of sites have obsolete Windows systems, 69% of sites have plain-text passwords traversing their networks, 57% of sites are not running anti-virus solutions that include automatic signature updates, 16% of sites have at least a misconfigured Wireless Access Point (WAP) and 84% of industrial sites

have at least one remotely accessible device without multifactor authentication controls.

Our literature review approach used mixed methods (Qualitative and Quantitative studies), to select the material as initial references in our multi-case study. The lead researcher used computerized databases and the Internet searching for keywords like "security training"; "information security training"; "SETA"; "cybersecurity awareness training"; "cybersecurity awareness training program"; "cybersecurity training framework" and "security awareness training program."

Axelos (2015) indicates that cyber-resilience specific training should be delivered on a regular basis, training should be designed and tailored to specific organizational roles and responsibilities of employees, awareness campaigns should be created to raise awareness and to address specific cyber risks. Nonetheless, we have to come up with finding innovative ways to deliver cybersecurity awareness training and most of all, keep people engaged with cybersecurity awareness activities.

THE CYBERSECURITY AWARENESS TRAINING MODEL (CATRAM)

The Cybersecurity Awareness TRAining Model (CATRAM), is an innovative model that can be implemented at any organization to consolidate the awareness foundations of a corporate Cybersecurity Awareness Program or to start the implementation of an organizational Cybersecurity Awareness Training Program (See Figure 1). The model design answers our main research question:

Why it is necessary to increase cyber awareness at the organizational and personal levels?

The aim of this research was to design a model for delivering cyber awareness training to support awareness education in any organizational environment. The Cybersecurity Awareness TRAining Model (CATRAM) has been created to deliver the initial cybersecurity awareness training at any organization or to re-introduce a better awareness training approach to an existing cybersecurity or information security awareness training program.

CATRAM has been designed to provide specific cybersecurity awareness training for personnel:

Table 1. Cybersecurity Awareness frameworks and methodologies

Framework or Methodology that focuses on cybersecurity awareness	Phases
ISO/IEC 27001:2005 (2005)	There aren't any specific phases or recommendations for the security awareness delivery. Clause 5.2.2 highlights the importance of necessary personnel competencies to support the Information Security Management System (ISMS), providing training to satisfy needs, maintaining training records and that the organization is responsible for the awareness training of relevant personnel
ISO/IEC 27032 (2012)	Section 2.4 covers the training and awareness program. Defining training needs, designing and planning training, defining awareness program requirements and setting up training and awareness evaluation
Hewlett Packard Progressive Engagement Framework (Beyer et al., 2015)	1. Awareness Profiling · Company profiling · Awareness assessment · Gap analysis · Awareness maturity level report 2. Awareness Planning · Communication, education and training concept · Awareness improvement plan 3. Transformation · Creation, production and measures implementation · Support of internal core team 4. Optimization · Comparison between target and actual state · Adjust and optimize accordingly
SANS Security Awareness Maturity Model (2017)	This Awareness Maturity Model is organized in five sections: 1. Non-Existent: An awareness program does not exist 2. Compliance Focused: The awareness program is either aligned with a compliance or audit requirements 3. Promoting awareness and behavior change: This program is focused on training topics that have greatest impacts to support the mission of the organization 4. Long-Term Sustainment and Culture Change: This program is aligned with a corporate cybersecurity program. It has processes, resources and leadership support 5. Robust Metrics Framework: This is a mature awareness program with a robust metrics framework in place
MediaPro Adaptive Awareness Framework (2017)	1. Analyze: Use data to inform about the program 2. Plan: Draw a roadmap for planning the awareness program 3. Train: Build training to achieve real behavior changes 4. Reinforce: Battle the forgetting curve
Beyer-Brummel Comparative Cybersecurity Training Framework (2015)	Organized by levels: 1. Targeted: To produce non-IT cybersecurity skills to exact role specific performance 2. Education: To cultivate IT security insight and understanding 3. Advanced: To equip IT security professionals to address assurance, policy and training
NIST- Key steps leading to the implementation of the awareness and training program (2014)	1. Design Awareness and Training Program 2. Develop Awareness and Training material 3. Implement Program 4. Post-Implementation
PCI Data Security Standard (PCI DSS)- Best Practices for Implementing a Security Awareness Program (2014)	1. Assemble the Security Awareness Team 2. Determine Roles for Security Awareness 3. Target delivery of relevant material to the appropriate audience in an efficient and timely way 4. Define the Security Awareness training content 5. Define assessment metrics of the awareness training 6. Follow the Security Awareness Program checklist

continued on following page

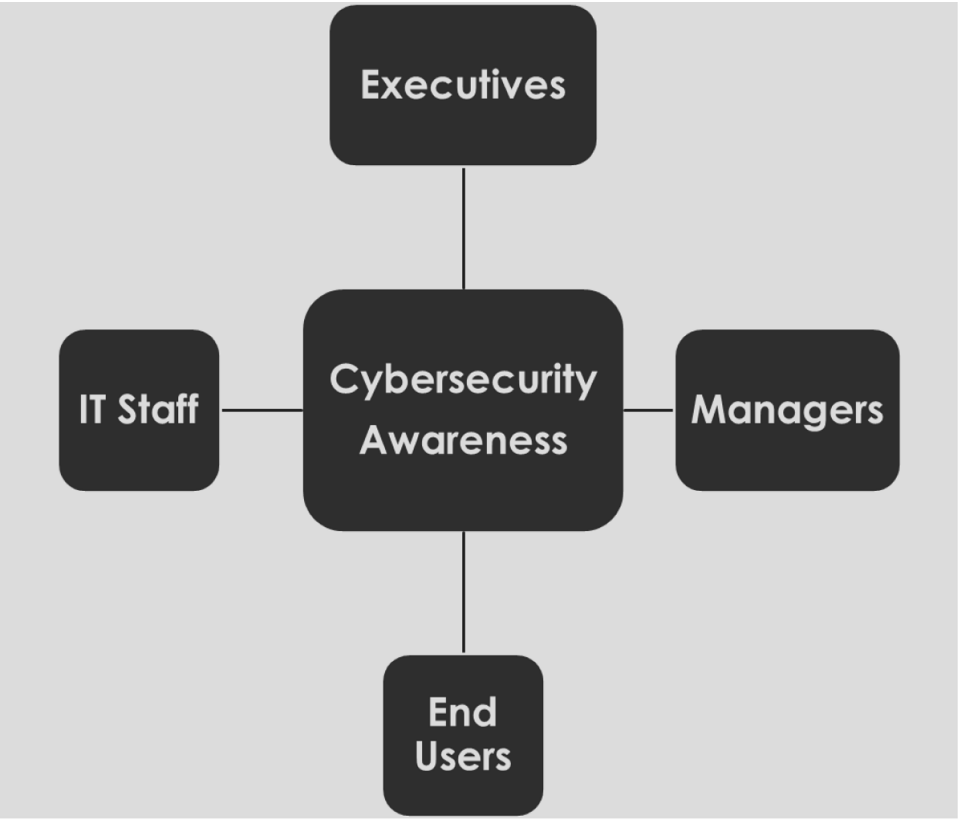
Table 1. Continued

Framework or Methodology that focuses on cybersecurity awareness	Phases
Cano – Basic Model of the level of maturity of the Organizational Information Security Culture (2016)	To measure the maturity of several elements of the InfoSec culture Elements: 1. Culture foundations 2. Access foundations 3. Information understanding 4. Basic Instruments 5. Management compromise Maturity indicators: 1. Reactive 2. Unstable 3. Proactive 4. Sustainable
MITRE- Model to question the validity of any email (2010)	EARNEST utilizes a series of questions to challenge the validity of an electronic message: Expected: It the email expected? Ambiguous: Is it asking to open attachments? Relationship: Any prior relationship with sender? Normal: Are context, grammar, syntax and spelling consistent from your contact? Exposed: Any malicious links in your email? Sense: Does it make sense to receive a link or attachment? Time: Is there any time factor for responding?
Cyber Safe Workforce – Security Awareness and Training Program (2016)	The awareness lifecycle comprises the following phases: 1. Identify and Define: Define and create training plan 2. Baseline: Gather initial set of data for future trainining scope 3. Train: Deliver guidance and information training 4. Track & Measure: Audit participation and gather good metrics 5. Evaluate & Update: Keep updating your training program all the time
Whitman and Mattord - Framework of Security Education, Training, and Awareness (2019)	The Framework includes six components that are applicable to Awareness, Training and Education: 1. Attributes: It seeks teaching members the importance of security by focusing on what, how and why 2. Levels: Knowledge transfer from basic, detailed and in-depth levels 3. Objectives: Based on threat recognition, effective responses using learned skills and engagement of active defense 4. Teaching methods: Some examples include informal training, hands-on practice and seminars 5. Assessments: By using different evaluation techniques like problem solving and essays 6. Impact timeframe: Short-term, intermediate and long-term
Nguyen et al. – InCAT (Intelligence-based Cybersecurity Awareness Training). (2018)	A model for delivering cybersecurity training with a strong focus on drilling deep into the shared contexts among collected cyber awareness training results, cyberthreat intelligence reports, and other cybersecurity related data logs. InCAT feedback loop includes 8 steps: 1. Threat reports 2. Annotation model flow to knowledge discovery model 3. Derived knowledge from threat reports 4. Tests for users 5. Initial user reports 6. User report verification by the annotation model 7. User assessment reports 8. Final results in control dashboard system

1. Board of Directors and Executives: Members of this group are trained based on the organizational cybersecurity strategy, governance and program.
2. Managers: Department managers are trained to support and lead cybersecurity initiatives in their corporate environment.

3. End Users: This group gets awareness training to improve cybersecurity practices in the workplace and their personal lives.
4. IT Staff: Information Technology specialists are trained in the use of advanced cybersecurity techniques, methods, procedures and best practices to support the corporate awareness program and the cybersecurity program.

Figure 1. The Cybersecurity Awareness TRAining Model (CATRAM)



Each awareness course has been developed with a specific outline, objectives, content and cybersecurity topics in alignment with the target audience, the organizational scope and aim, the cybersecurity awareness program and the corporate cybersecurity program. Cybersecurity topic choice are based on

the group's main responsibilities and also on the cybersecurity domains that this group will be dealing with in the workplace on their daily tasks.

Awareness Course for the Board of Directors and Executives

The course lasts 2 hours and can be delivered in two different sessions. It is advisable that this course could be delivered in a classroom or board meeting environment.

Objectives

1. Provide a high-level overview of an effective cybersecurity awareness training for your organization
2. Create cybersecurity awareness for the Board of Directors and C-Suite Executives

Cybersecurity Awareness Topics

Initial Survey
Cybersecurity Introduction
Cybersecurity and Cybercrime Statistics
A Corporate Cybersecurity Program
Cybersecurity Strategy
Responsibilities of Stakeholders (Board of Directors and C-Suite Executives)
Cyberthreat Landscape
Cybersecurity Risk Management
Cybersecurity Frameworks
Cybersecurity Awareness and Training
Cybersecurity Business Continuity
Incident Response Management
Conclusions
Final Survey

Awareness Course for Managers

The course lasts 2 hours and can be structured in two different sessions. The course can be delivered in a classroom setting, online or a blended environment.

Objectives

1. Provide a high-level overview of an effective cybersecurity awareness training for your organization
2. Create cybersecurity awareness for Managers
   Cybersecurity Awareness Topics
   Initial Survey
   Cybersecurity Introduction
   Cybersecurity and Cybercrime Statistics
   A Corporate Cybersecurity Program
   Cybersecurity Strategy
   Responsibilities of Stakeholders (Department Managers)
   Cyberthreat Landscape
   Cybersecurity Risk Management
   Cybersecurity Frameworks
   Cybersecurity Awareness and Training
   Cybersecurity Business Continuity
   Incident Response Management
   Conclusions
   Final Survey

Awareness Course for End Users

The course lasts 4 hours and can be established in two or four different sessions. The course can be delivered in a classroom setting, online or a blended environment. It is recommended to add a short video clip from YouTube as additional learning resource for your audiences.

Objectives

1. Educate end users to help protecting the confidentiality, availability and integrity of your organization's information and cyber assets
2. Create awareness of the importance of cybersecurity and cybersecurity controls
   Cybersecurity Awareness Topics
   Initial Survey
   Cybersecurity Introduction
   Cybersecurity and Cybercrime Statistics
   You are a target for cybercriminals
   Cybercrime

Hackers
Cyberthreats
Social Engineering
Phishing
Internet Browsing
Social Networks
Mobile device security
Passwords
Encryption
Data security
Identity Theft
Wi-Fi Security
Working remotely
Physical security
Protecting your online profile
Protecting your home network
Protecting our children online
Privacy
Avoiding Scams
Have you been hacked?
Conclusions
Final Survey

Awareness Course for IT Professionals

The course lasts 20 hours and can be structured in ten or twenty different sessions. The course can be delivered in a classroom setting, online, self-paced e-doing or a blended environment.

Objectives

1. Understand cybersecurity concepts
2. Recognize key cybersecurity objectives for the protection of cyber assets
3. Understand cybercrime operations
4. Recognize cybersecurity threat agents that could impact your organization
5. Understand any cyberattack architecture
6. Identify most common cyberattacks
7. Apply cybersecurity measures to defend against cyberattacks
8. Understand a cybersecurity program architecture and operation

9. Recognize the importance of developing, enforcing and maintaining cybersecurity policies
10. Understand the fundamentals of ethical hacking
11. Understand the architecture of penetration testing
12. Get familiar with most cybersecurity frameworks
13. Understand the basics of cyber threat intelligence
14. Understand the importance of proper cybersecurity training
15. Raise cybersecurity awareness in your organization
16. Apply cybersecurity architecture principles
17. Recognize the importance of hardening security in data, voice and video networks
18. Recognize the importance of security hardening for information, systems and applications
19. Identify cybersecurity vulnerabilities
20. Remediate existing cybersecurity vulnerabilities
21. Recognize the cybersecurity implications of new and evolving technologies
22. Understand the principles of Cybersecurity Incident Response and Management
23. Understand the fundamentals of Digital Forensics
24. Recognize the importance of the continual evaluation of a corporate cybersecurity program
25. Recognize the value of corporate cyber wargames to test cybersecurity
26. Identify the opportunities for cybersecurity education and professional development

Cybersecurity Awareness Topics
Initial Survey
Cybersecurity Fundamentals
Cybercrime
Cyberattacks
Corporate Cybersecurity Program
Cybersecurity Policies
Ethical Hacking
Penetration Testing
Cyber Operations
Cybersecurity Frameworks
Cyber Threat Intelligence
Cybersecurity Awareness and Training Program
Architecture and Networks

Information, Systems and Applications
Vulnerability Management
Evolving Technologies
Incident Response Management
Digital Forensics
Enterprise Cybersecurity Assessment
Cybersecurity Corporate Wargames
Cybersecurity Education
Final Survey

Alotaibi et al. (2016) point out that one of the best ways to deal with cybercrime is by creating awareness and by adopting effective cybersecurity practices for people.

MEASURING THE MODEL RESULTS

The results of CATRAM can be assessed once all training courses have been delivered. Most of the assessment could be measured at the end user level by evaluating changes in security behaviors and alignment with corporate cybersecurity compliance. If possible, end users must be advised that the effectiveness of the awareness training will be evaluated by performing announced assessments, and the delivery of non-announced assessment exercises as well.

Table 2 presents suggested awareness areas and participating groups to assess the compliance and the impact of the cybersecurity awareness model.

Hayden (2016) presents a model to measure the levels of security culture strength. The strength of the security culture could be a function of the organizational awareness and training program or it could the result of a highly regulated industry: A weak security culture (80% occurrence of a bad decision); a moderate security culture (50% occurrence of a bad decision) and a strong security culture (20% occurrence of a bad decision).

We assess the cybersecurity awareness by measuring compliance by addressing the following criteria:

- Does your organization have a cybersecurity awareness program?
- Do you provide some kind of cybersecurity training to your staff?
- Is training delivered on a regular recurring basis?
- Do employees are following security policies of the organization?

Table 2. CATRAM Metric Identifiers and Objectives

Metric Identifier	Group	Metric Objectives
Cybersecurity Awareness and Training Effectiveness	Executives	Identify training gap needs and approve training courses
Cyber policy-making assessment	Executives	Review, update and approve cybersecurity policies
Cyber monitoring, metric definition and reporting	Executives	Approve required cybersecurity metrics
Awareness training completion	Managers	Verify that all staff completes training for every department
Communication flow	Managers	Enforce the distribution of awareness communication and proper training documentation
Cybersecurity incidents volume	IT	Evaluate Help Desk monthly report
Cybersecurity skills	IT	Evaluate new cybersecurity skills of technical staff that is consistent with the organization growth and operations
Infected digital devices	IT	Identify percentage on a monthly basis
Phishing awareness and detection	End Users	Identify phishing victims and users that are able to avoid phishing attacks
Social Media risks	End Users	Evaluate percentage of user's time
Password management	End Users	Assess user's behavior for password management

- Are you delivering training to recognize and deal with social engineering?
- Do your staff know how to recognize and report a security incident?
- Is your staff able to detect and respond to any cybersecurity emergency?
- Do you enforce privacy and confidentiality requirements in your organization?
- Are your employees following security procedures for data and information protection?
- Is your awareness training focused and delivered to specific audiences like end users, managers, IT, C-Suite executives and Board of Directors?
- Is your awareness training covering multidimensional topics?
- Does your training outline cover technical, social and user behavior areas?

Evaluation Scorecard

We calculate the final cybersecurity maturity rating of the cybersecurity awareness training domain by using the criteria from Table 3. The score can be mapped to a specific maturity level.

Gartner (2018) suggests that security and risk management leaders must provision awareness training to employees in order to focus on protecting their online security and the personal aspects of cybersecurity, knowledge transfer of good practices to protect intellectual property and data in corporate environments. Gartner also suggests a series of best practices to develop and maintain a cybersecure worforce:

1. By nurturing a holistic cybersecure personal lifestyle that includes good hygiene for identity management and security awareness
2. By committing to training and awareness behavior that encircles corporate training, workshops and the use of the proper tools
3. By building trust that verifies employees' online behavior through timely tests of cybersecure hygiene

METHODOLOGY

The Cybersecurity Awareness TRAining Model (CATRAM) has been tested, implemented and validated along with the CyberSecurity Audit Model (CSAM) in a Canadian higher education institution (Sabillon et al., 2019). The research project did audit the cybersecurity organizational strategy, implemented the CyberSecurity Audit Model (CSAM) and delivered cybersecurity awareness training to more than one hundred participants based on the Cybersecurity Awareness TRAining Model (CATRAM). The CyberSecurity Audit Model (CSAM) is an exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization. The CyberSecurity Audit Model (CSAM) contains overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessment and an evaluation scorecard.

Table 3. Cybersecurity Awareness Training Maturity Rating

Rating	Description
Immature (I): 0-30	The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program nor an awareness training program.
Developing (D): 31-70	The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The Awareness Education domain is developing. The organization has a foundation model for cybersecurity awareness and additional efforts are required to develop a complete cybersecurity awareness program.
Mature (M): 71-90	While the organization has a mature cybersecurity awareness environment. Improvements are required to the key areas that have been identified with weaknesses.
Advanced (A): 91-100	The organization has excelled in implementing cybersecurity awareness training best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

The mutiple case study research included several phases like plan, design, preparation, collection, analysis, sharing and dissemination. We intended to perform qualitative research by utilizing interpretive material practices such as online and paper surveys, interviews, classroom and online training and analysis of documentation, processes and procedures of the target institution. We completed a multi-case study research following Yin's methodology (2018; 2014) to plan, design, prepare, collect, analyze and share phases by creating, implementing and validating two innovative cybersecurity models (CATRAM & CSAM). This initial validation of the CATRAM and CSAM took place in a Canadian Higher Education Institution. More recently, the CSAM has been validated for the second time in a larger Canadian Higher Education Institution.

The target organization provided their staff time to support the case study research, resources to conduct the cybersecurity audit, the provision of classroom space and time, computer use, Internet access for the delivery of the cybersecurity awareness training courses, the access to their computer systems to conduct the research and to design the online courses in their Learning Management System (Moodle).

Table 4. Control Evaluation of the Cybersecurity Awareness Education

Control evaluation of the Cybersecurity Awareness Education domain						
Reference	**Sub Area**	**Clause**	**Steps**	**Control Evaluation**		**Checklist**
				Yes	**No**	**CSAM-Awareness**
13.1	Awareness	13.1.1	Organization deploys a cybersecurity awareness program	□	ý	
		13.1.2	The awareness training program is delivered on an annual basis	ý	□	
		13.1.3	Employees are aware of the need of this kind of training program	□	ý	
		13.1.4	The training program is designed for different staffing levels	ý	□	
		13.1.5	Training material is constantly updated as new cyber threats emerge	ý	□	

Table 5. Control Evaluation of the Cybersecurity Awareness Education

Cybersecurity audit checklist: CSAM – Awareness Education (Domain 13)					
Clause	**No.**	**Checklist Questions**	**Findings**		
			Compliant	**Minor Nonconformity**	**Major Nonconformity**
13.1.1	1	Does your organization have a cybersecurity awareness program?	□	□	ý
13.1.1	2	Do you provide some kind of cybersecurity training to your staff?	ý	□	□
13.1.2	3	Is training delivered on a regular recurring basis?	ý	□	□
13.1.1	4	Do employees are following security policies of the organization?	ý	□	□
13.1.1	5	Are you delivering training to recognize and deal with social engineering?	ý	□	□
13.1.1	6	Do your staff know how to recognize and report a security incident?	□	ý	□
13.1.1	7	Are your personnel able to detect and respond to any cybersecurity emergency?	□	□	ý
13.1.1	8	Do you enforce privacy and confidentiality requirements in your organization?	□	□	ý
13.1.1	9	Are your employees following security procedures for data and information protection?	□	□	ý
13.1.4	10	Is your awareness training focused and delivered to specific audiences like end users, managers, IT, C-Suite executives and Board of Directors?	ý	□	□
13.1.1	11	Is your awareness training covering multidimensional topics?	ý	□	□
13.1.1	12	Does your training outline cover technical, social and user behavior areas?	ý	□	□

RESULTS

Before initiating our case study research, our target organization did not own any cybersecurity awareness model nor any cybersecurity awareness education program whatsoever. The CATRAM delivery let the organization, to build a strong foundation for a future implementation of a comprehensive cybersecurity awareness training program. The cybersecurity audit of the awareness education domain was executed after the successful delivery and implementation of CATRAM. We conducted the audit of the awareness education based on the CSAM and the most relevant noncompliances are the lack of a corporate cybersecurity awareness training program and the confirmation that staff are aware that cyber training is not being delivered and it exists the necessity to eradicate this weakness (Table 4). The critical controls that need immediate attention are that the target organization does not have a valid cybersecurity awareness program, and employees were not aware how important is to keep training them in cyber topics to increase awareness and show a proactive participation in order for their potential awareness training program to be successful.

A series of tables are included to present the findings in this research scenario. Table 4 illustrates the assessment of the main cybersecurity awareness education controls. Table 5 contains the sub-controls findings based on the audit checklist. Major nonconformities need to addressed and corrected. Staff need to able to identify and report any cybersecurity incident, enforce privacy, confidentialy and protection for any Personally Identifiable Information (PII) for the internal and stakeholders of the institution.

Table 6 corroborates that the cybersecurity awareness training is at a '*developing stage'* and consequently needs improvement in our target organization. The higher education institution needs to implement a full cybersecurity awareness and training program for all stakeholders. Partial awareness training is ineffective. The validation of the CATRAM helped the target organization to implement a foundation for their future cybersecurity awareness training program. While the CATRAM implementation was delivered for the Board of Directors, C-Suite Executives, Managers, IT staff and end users thus a critical recommendation was to train their students and external stakeholders as well.

With regard to recommendations, we did suggest the creation and implementation of the corporate cybersecurity awareness training program, to define ownership to maintain the training program and the CATRAM

Table 6. Overall Cybersecurity Awareness Rating

Cybersecurity Awareness TRAining Model (CATRAM)			
Domain	**13-Awareness Education**		
Control Evaluation	**Ratings**		**Score**
	Immature	□	
	Developing	ý	60%
	Mature	□	
	Advanced	□	
Developing (D): 31-70 The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The Awareness Education domain is developing. The organization has a foundation model for cybersecurity awareness and additional efforts are required to develop a complete cybersecurity awareness program.			

update on an annual basis or as new cyberthreats emerge, to conduct "Train the Trainer" sessions for designated instructors or facilitators and, last but not least the constant evaluation of staff using scheduled and non-scheduled assessments to evaluate and understand cybersecurity awareness and behaviors.

CONCLUSION

The main objective of this multi-case study was to design and validate a cybersecurity awareness model; the Cybersecurity Awareness TRAining Model (CATRAM) to address the challenges to deliver cybersecurity awareness training based on staff roles. The cybersecurity model including all its components were successfully validated by a multi-case study performed in a Canadian higher education institution.

CATRAM could support the implementation of a foundation or for consolidating a cybersecurity awareness training program at any organization. The results of this research show that the delivery of cybersecurity training based on organizational roles and responsibilities tend to motivate personnel to create and maintain awareness in their workplaces as well in their personal lives.

The limitation of our case study is that CATRAM was validated in a single organization, time constraints, lack of interest for the topics and lack of engagement were some of the challenges that we have to overcome from

some of the participants. Hence, future testing will enhance the model results by engaging more organizations. The case study results have implications for our target organization but at the same time, implications for future research to review and expand our proposed cybersecurity model. Future work would propose to transform CATRAM into a cybersecurity awareness training framework.

REFERENCES

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of Using Gaming Technologies for Cyber-Security Awareness. *International Journal of Information Security Research*, *6*(2), 660–666. doi:10.20533/ijisr.2042.4639.2016.0076

Axelos. (2015). *Cyber Resilience Best Practices.* Norwich: Resilia.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A., & Passingham, N. (2015). *Awareness is only the first step: A framework for progressive engagement of staff in cyber security.* Hewlett Packard Enterprise.

Beyer, R., & Brummel, B. (2015). *Implementing Effective Cyber Security Training for End Users of Computer Networks*. Society for Human Resource Management and Society for Industrial and Organizational Psychology.

Cano, J. (2016). La educación en seguridad de la información. Reflexión pedagógicas desde el pensamiento de sistemas. *Memorias 3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz".*

Cano, J. (2016). Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información, 24-29.

Cyber, X. (2019). 2019 Global ICS & IIoT Risk Report. A data-driven analysis of vulnerabilities in our industrial and critical infrastructure. *CyberX Labs.* Retrieved from https://cyberx-labs.com/resources/risk-report-2019/

ESET. (2017). *ESET Cybersecurity Awareness Training*. ESET Canada. Retrieved from https://www.eset.com/ca/cybertraining/

Fujitsu. (2017). *The Digital Transformation PACT*. Retrieved from https://www.fujitsu.com

Gartner. (2016). *2016 Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors.* Gartner, Inc.

Gartner. (2018). *How to Build an Enterprise Security Awareness Program.* Gartner, Inc.

Gartner. (2018). *How to Secure the Human Link.* Gartner, Inc.

Gartner. (2018). *Magic Quadrant for Security Awareness Computer-Based Training*. Gartner, Inc.

Hayden, L. (2016). *People-Centric Security: Transforming your Enterprise Security Culture*. Mc Graw Hill.

International Organization for Standardization - ISO. (2005). *ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*. ISO.

International Organization for Standardization -ISO. (2012). *ISO/IEC 27032:2012 – Information Technology – Security Techniques – Guidelines for Cybersecurity*. ISO.

LeClair, J., Abraham, S., & Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Worforce. *Proceedings of Information Security Curriculum Development Conference*, 71-78.

MediaPro. (2017). *A Best Practices Guide for Comprehensive Employee Awareness Programs*. MediaPro.

MITRE. (2010). *The Importance of Using EARNEST.* The MITRE Corporation. Retrieved from https://www.mitre.org/sites/default/files/pdf/mitre_earnest.pdf

MITRE. (2017). *Cybersecurity Awareness & Training*. The MITRE Corporation.

Monahan, D. (2014). *Security Awareness Training: It's not just for Compliance-Research Report Summary. Enterprise Management Associates*. EMA.

National Institute of Standards and Technology – NIST. (2003). *Building an Information Technology Security Awareness and Training Program.* NIST Special Publication 800-50.

National Institute of Standards and Technology – NIST. (2017). *An Introduction to Information Security.* NIST Special Publication 800-12 Revision 1.

Nguyen, T.N., Sbityakov, L., & Scoggins, S. (2018). *Intelligence-based Cybersecurity Awareness Training- an Exploratory Project*. CoRR, abs/1812.04234.

NTT Group. (2017). Embedding cybersecurity into digital transformation - a journey towards business resilience. *NTT Security*. Retrieved from https://www.nttsecurity.com

PCI Security Standards Council - PCI DSS. (2014). *Best Practices for Implementing a Security Awareness Program*. PCI DSS.

Penderdast, T. (2016). How to Audit the Human Element and Assess Your Organization's Security Risk. *ISACA Journal*, *5*, 1–5.

PhishMe. (2017). PhishMe CBFree. *PhishMe Headquarters*. Retrieved from https://phishme.com/resources/cbfree-computer-based-training/

Ponemon Institute. (2018). Assessing the DNS Security Risk. Research report sponsored by Infoblox. Ponemon Institute LLC.

Sabillon, R. (2018). Scenario III: Data for a single cybersecurity domain audit (Awareness Education). *Mendeley Data, 2*. doi:10.17632/m4dk8n9sx7.2

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *Proceedings of Second International Conference on Information Systems and Computer Science (INCISCOS)*. 10.1109/INCISCOS.2017.20

Sabillon, R., Serra-Ruiz, J., Cavaller, V., Jeimy, J., & Cano, M. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39. doi:10.4018/JCIT.2019070102

SANS Institute. (2017). *2017 Security Awareness Report: It's time to communicate. SANS Security Awareness.* Retrieved from https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf

SANS Security Awareness, . (2017). *2017 Security Awareness Report*. SANS Institute.

Symantec. (2014). *Symantec Security Awareness Program: Mitigate information risk by educating your employees*. Symantec Corporation.

Ward, M. (2016). *Security Awareness and Training: Solving the unintentional insider threat*. Cyber Safe Worforce LLC.

Whitman, M. E., & Mattord, H. J. (2019). *Management of Information Security* (6th ed.). Cengage Learning, Inc.

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). Sage Publications.

Yin, R. K. (2018). *Case Study Research and Applications* (6th ed.). Sage Publications.

ADDITIONAL READING

Choi, Y. (2018). *Selected Readings in Cybersecurity*. Cambridge Scholars Publishing.

KEY TERMS AND DEFINITIONS

Cybersecurity Awareness: Perception of cybersecurity matters to be incorporated at any job function.

Cybersecurity Awareness Education Maturity: Level of experience that an organization has implemented and acquired for cybersecurity training in accordance with the cyberthreat landscaping.

Cybersecurity Awareness Training: Cybersecurity areas that will be taught to any stakeholder in order to increase awareness and remediation.

APPENDIX 1

Template for Overall Cybersecurity Rating for Domain 13 (Awareness Education)

Table 7. Overall Cybersecurity Rating for Domain 13 (Awareness Education)

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	**D**	**M**	**A**	
13	Awareness Education	☐	☐	☐	☐	
Final Cybersecurity Maturity Rating of Awareness Education		☐	☐	☐	☐	

Immature (I): 0-30	The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program nor an awareness training program.
Developing (D): 31-70	The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The Awareness Education domain is developing. The organization has a foundation model for cybersecurity awareness and additional efforts are required to develop a complete cybersecurity awareness program.
Mature (M): 71-90	While the organization has a mature cybersecurity awareness environment. Improvements are required to the key areas that have been identified with weaknesses.
Advanced (A): 91-100	The organization has excelled in implementing cybersecurity awareness training best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

About the Author

Regner Sabillon is a Ph.D. Candidate in Network and Information Technologies (NIT) and researcher at the Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Spain. Canadian researcher in Cybersecurity, Cyber law, Cyberforensics and Cybercrime areas. Faculty member at the School of Computing and Information Systems (SCIS), Athabasca University and at the School of Information and Communication Technologies (ICT), Southern Alberta Institute of Technology – SAIT Polytechnic, Canada. ICT/ Cybersecurity specialist with more than 20 years of experience.

Index

A

C

D

E

H

I

N

S

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM

With the continued progression of technologies such as mobile computing and the internet of things (IoT), cybersecurity has swiftly risen to a prominent field of global interest. This has led to cyberattacks and cybercrime becoming much more sophisticated to a point where cybersecurity can no longer be the exclusive responsibility of an organization's information technology (IT) unit. Cyber warfare is becoming a national issue and causing various governments to reevaluate the current defense strategies they have in place.

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM provides emerging research exploring the practical aspects of reassessing current cybersecurity measures within organizations and international governments and improving upon them using audit and awareness training models, specifically the Cybersecurity Audit Model (CSAM) and the Cybersecurity Awareness Training Model (CATRAM). The book presents multi-case studies on the development and validation of these models and frameworks and analyzes their implementation and ability to sustain and audit national cybersecurity strategies. Featuring coverage on a broad range of topics such as forensic analysis, digital evidence, and incident management, this book is ideally designed for researchers, developers, policymakers, government officials, strategists, security professionals, educators, security analysts, auditors, and students seeking current research on developing training models within cybersecurity management and awareness.

Topics Covered

- Awareness Training
- Cyber Governance
- Cyber Monitoring
- Cyber Warfare
- Cybersecurity Audit Model (CSAM)
- Cybersecurity Awareness Training Model (CATRAM)
- Digital Evidence
- Electronic Discovery
- Forensic Analysis
- Incident Management
- Metric Reporting
- Security Auditing

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

701 E. Chocolate Avenue
Hershey, PA 17033, USA
www.igi-global.com

ISBN 978-1-7998-5609-2
90000
9 781799 856092