Cyber Security Insights for Individuals, Governments & Organizations (Gathered Articles): A North America, Asia, Africa, South America, Oceania & Europe Perspective 1st Edition

RUDOLPH. PATRICK. T. MUTESWA

ISBN: 978-1-77927-319-2

EAN: 9781779273192

Cyber Security Insights for Individuals, Governments & Organizations (Gathered Articles): A North America, Asia, Africa, South America, Oceania & Europe Perspective 1st Edition

for-word quote will only end after proper referencing of open and closed brackets has been done at the end of the verbatim sentence clearly acknowledging the name and year of the source document that has been used by the author as shown (Rudolph, 2019, www.rptmuteswa.ca.us). Furthermore, as the author of this textbook the strategy l am using to write my book is the 'Gathered Articles' writing strategy since l am using direct quotes l have gathered from various publications written by various authors and l later on present them in a logical manner that creates a Book Chapter despite the fact that l will often at times present my own interpreted words in certain parts of the book. I was granted permission by the publishers of the information sources l obtained the information to use during my book writing process. In addition in certain instances there can be a full website link where the article or publication used in writing this textbook can be directly downloaded or viewed by the readers of this textbook for instance: during in-text referencing, the footnotes and or the bibliography section of the chapter as this enables the author of this textbook to clearly show the readers who the original owners of the published work are and also to fully acknowledge them. In addition readers please note that all the information sources used in this book are owned by the publishers/owners of the various websites, books, newspapers, magazines and journals used by the book author. Therefore readers of this textbook if you want to use any of the information from any of these referenced sources please may you directly contact the original owner(s)/publisher(s) of the information source for permission to use their information for whatever purpose you want to use it for.

Author: Rudolph. Patrick .Tawanda. Muteswa

ISBN: 978-1-77927-319-2

EAN: 9781779273192

Author & Book Editor

Rudolph. Patrick. Tawanda. Muteswa is a global Human Resources Management, Entrepreneurship and Business Management Specialist. He received his Master of Commerce (MCom), Bachelor of Commerce Honors (BCom Hons) and Bachelor of Business Administration in Management (BBA) from the University of KwaZulu-Natal in Pietermaritzburg, South Africa. Rudolph P.T. Muteswa is passionate about educating the citizens of various countries around the world such as executive board of directors, managers, entrepreneurs, academics, diplomats, civil society professionals, pilots, tourists, politicians, medical professionals, engineers, journalists, teachers, students and many other professionals about: the importance of – cyber security, world peace, climate change, respecting of human rights, entrepreneurship, human resources management, role of a board of directors, corporate governance, ethics & compliance and tourism information of various countries. Rudolph. P. T. Muteswa in his personal life enjoys doing the following: writing inspirational poetry, athletics, vegetable gardening, rearing chickens/rabbits, listening to music, travelling & learning more about the different cultures found in different parts of the world.

TABLE OF CONTENTS

LIST OF FIGURES:

LIST OF TABLES

PREFACE TO THE FIRST EDITION

Today the Internet has become a key pillar of how individuals, organizations and governments carry-out marketing communications, e-commerce and public relations activities. The Internet has unexpectedly opened new avenues for cyber crime activities and this is one of the many disadvantages that are experienced by individuals and organizations carrying-out business or communications via the Internet. This textbook aims to educate readers about the meaning of cyber crime, the different types of cyber crimes and the different parties involved in a cyber threat. The global pandemic has made it inevitable for every business, institution and government workplace to use virtual or remote workplaces due to the fact that people are more likely to work from home as a result of the global pandemic's government mandatory curfews or lockdown rules in their respective countries. Therefore, another aim of this educational textbook is educate readers about the reasons why the demand for cyber security measures has increased in organizations. The other aim of this educational textbook is to educate readers about the fact that information is a critical ingredient that is used to achieve societal development through shaping its culture, values, thinking, politics, opinions, unity and so on. In addition this book aims to educate readers about the effects of misinformation, disinformation, and malinformation in a society or organization and how this relates to cyber security. This educational textbook aims to educate readers about the fact that organizations and government departments possess personal valuable information in their database systems. Thus as a result this ultimately puts immense pressure on organizations and government departments to make the cyber security training of employees/personnel a key priority in order to enable the organizations and government departments to stay one step ahead in the fight against cyber crime or threats. The other key aim of this educational textbook is that cryptography is now one of the most effective technology tool that can easily be used by organizations to protect data or communications infrastructure. Interestingly, this textbook made an effort to go the 'extra mile' towards educating its readers about some of the tips they can follow to avoid receiving malicious communications or reduce their technical vulnerabilities of their information systems or technology devices. It is strongly advised that readers of this book must ensure that they seek legal or expert professional advice before implementing any information they would have read in this book. Readers of this textbook *please note that the cyber security centres cited in this book do not endorse the personal views expressed in this book or endorse this book.*

Acknowledgement:

I dedicate this book to my future wife and children. I also would like to thank my 6 (*four brothers & two sisters*) siblings for tirelessly supporting me towards my education and personal life goals. I would also like to take this opportunity to greatly thank my late parents, aunties and uncles for the great role they played in my childhood. Furthermore, I shall forever be grateful to the great men and women in the continent of Africa, North America, Europe, Latin America, Middle East, Oceania and Asia who contributed towards the writing of this book in particular all the named organizations & the various information sources cited in this book.

Chapter 1: What is cyber security & threats

After reading this chapter you should be able to:

- Define the following terms ‘cyber’ and ‘information’. Explain the meaning of a ‘cyber threat’ and a ‘cyber threat surface’**.**
- Highlight the actors or parties involved in a ‘cyber threat’. Explain issues about a ‘malicious cyber threat’ activity by exploiting technical vulnerabilities in-depth.
- Discuss what is a ‘cyber crime’. Identify the different types of cybercrimes. Highlight the strategies that can be used to be alert of ‘malicious email messages’.

1.1 Introduction

The Internet is now the foundation that guides most of the decisions and actions taken by people or organizations on a regular basis in this modern day technology-orientated global society and economy therefore this makes the value of cyber security a key area of concern in various global security organizations around the world. Historically immorality has traditionally existed amongst human beings living in a society and surprisingly today immorality now exists in the digital world as well. Nowadays many individuals, organizations and to a certain extent governments pose as a cyber security threat to other nations by carrying-out immoral/illegal activities that are meant to destroy or negatively affect the information systems of organizations, institutions and governments networks for unethical reasons. However, it can also be argued that in some countries cyber security surveillance is often used as a tool to intentionally violate the human rights, democracy and freedoms of citizens by individuals, organizations and or the government. The following section will cover the meaning of terms.

1.2 Define the following terms ‘cyber’ and ‘information’

[1]“**Britannica Dictionary definition of CYBER- :** computer

[1] Britannica (2022) *Cyber*. Available from: https://www.britannica.com/dictionary/cyber- [Accessed May 07, 2022]

• *cyber*café

• *cyber*space" (Britannica, 2022, https://www.britannica.com/dictionary/cyber-). [2]"**Britannica Dictionary definition of INFORMATION** [noncount] **1 :** knowledge that you get about someone or something **:** facts or details about a subject" (Britannica, 2022, https://www.britannica.com/dictionary/information). The next section will cover information about what is a cyber threat and a cyber threat surface in-depth.

1.3 What is a cyber threat and a cyber threat surface?

[3]"Cyber threat**.** A **cyber threat** is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains. The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). [4]According to the Canadian Centre for Cyber Security (2021) **Cyber threat surface.** The cyber threat surface refers to all the available endpoints that a threat actor may attempt to exploit in Internet-connected devices within the cyber threat environment. The many processes that produce, deliver, and rely on information systems connected to the Internet are also potential threat vectors and targets. Services, devices, and data can all be targeted to compromise production and delivery systems, such as supply chains and service management systems. As these processes continue to evolve, the threat surface will expand. In addition, systems that connect physical

[2] Britannica (2022) *Information*. Available from: https://www.britannica.com/dictionary/information [Accessed May 07, 2022] © 2022 Encyclopædia Britannica, Inc.

[3] Canadian Centre for Cyber Security (2022) *Cyber Threats and Cyber Threat Actors.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[4] Canadian Centre for Cyber Security (2022) *Cyber Threat Surface.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-surface [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

entities with the Internet are increasingly common. For example, the smart grid, Internet of Things (IoT) devices, and industrial control systems all present a risk of cyber threat actors interfering with the physical environment of their victims. Internet-connected devices and applications bring great benefits to individuals and to the global economy, but as more physical and information assets become accessible online or have a digital component, cyber threat actors will have more opportunities to conduct malicious cyber threat activity, to access information, disrupt operations, or even have a physical impact (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/cyber-threat-surface). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover information about the parties to a cyber threat in-depth.

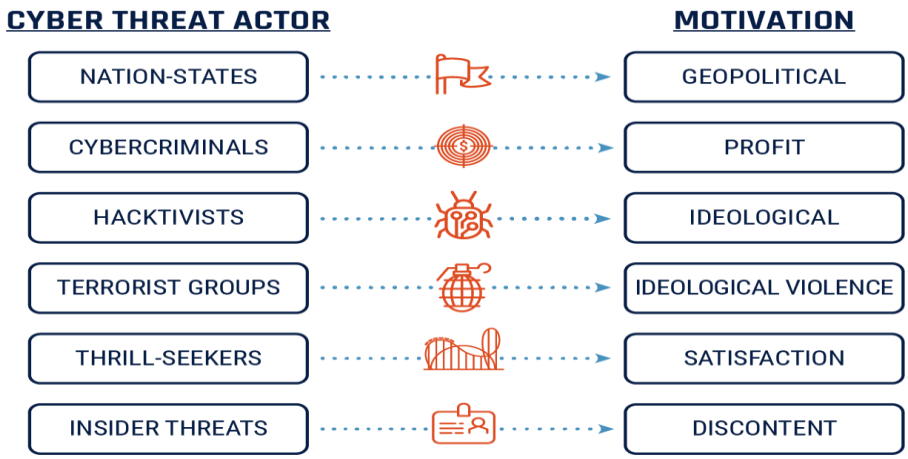
1.4 Parties to a cyber threat

"**Cyber threat actors.** **Cyber threat** actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.

1.4.1 Motivations

Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The actors of cyber threats will be highlighted by Figure 1.1 below.

Figure 1.1: Cyber threat actors



Source: Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/, Long description - Figure 3.1: Cyber threat actors. © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

As highlighted by Figure 1.1 above the cyber threat actors are as follows:

1.4.2 [5]"Sophistication

Cyber threat actors are not equal in terms of capability and sophistication, and have a range of resources, training, and support for their activities. Cyber threat actors may operate on their own or as part of a larger organization (i.e., a nation-state intelligence program or organized crime group). Sometimes, even sophisticated actors use less sophisticated and readily available tools and techniques because these can still be effective for a given task and/ or make it difficult for defenders to attribute the activity.

1.4.2.1Nation-states are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination. Some nation-states have operational relationships with private sector entities and organized criminals.

[5] Canadian Centre for Cyber Security (2022) *Cyber Threats and Cyber Threat Actors.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

1.4.2.2Cybercriminals are generally understood to have moderate sophistication in comparison to nation-states. Nonetheless, they still have planning and support functions in addition to specialized technical capabilities that affect a large number of victims. Threat actors in the top tier of sophistication and skill, capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their strategic goals, are often called **advanced persistent threats (APT)**. This designator is usually reserved for nation-states or very proficient organized crime groups.

1.4.2.3Hacktivists, terrorist groups, and **thrill-seekers** are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation.

1.4.2.4[6]**Insider threats** are individuals working within their organization who are particularly dangerous because of their access to internal networks that are protected by security perimeters. Access is a key component for malicious threat actors and having access privileged access eliminates the need to employ other remote means. Insider threats may be associated with any of the other listed types of threat actors but often include disgruntled employees" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).The following section will cover aspects about malicious cyber threats in-depth.

[6] Canadian Centre for Cyber Security (2022) *Cyber Threats and Cyber Threat Actors.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

1.5 Malicious cyber threat activity by exploiting technical vulnerabilities

““““[7]Cyber threat actors conduct malicious cyber threat activity by exploiting technical vulnerabilities, employing social engineering techniques, or by manipulating social media. A determined and capable adversary will often carefully select the technique most likely to result in successful exploitation after conducting reconnaissance against their target and may use a range of techniques to achieve their goal. The majority of threat actors, however, simply cast a wide net in hopes of exploiting any unsecure network or database.

Technical vulnerabilities are weaknesses or flaws in the design, implementation, operation, or management of an information technology system, device, or service that provides access to cyber threat actors. For example, a threat actor may attempt to install malicious software, called **malware**, or take advantage of existing flaws to exploit the targeted system. In addition to installing malware, threat actors also use tools that directly exploit specific technical vulnerabilities.

[8]Exploitation methods that target human qualities, such as carelessness and trust, are collectively known as social engineering. Threat actors use social engineering to trick an individual into inadvertently allowing access to a system, network, or device. Phishing and spear-phishing are common **social engineering** techniques. (Please see Annex A: The cyber threat toolbox for more information).

Foreign cyber threat actors can also manipulate social media and legitimate advertising and information-sharing tools to conduct **online foreign influence** campaigns that seek to impact domestic events like an election, census, or public health campaign, as well as public discourse more broadly. With a thorough understanding of how traditional media and social media work – and how individuals consume information – cyber threat actors can promote their message to

---

[7] Canadian Centre for Cyber Security (2022) *Cyber Threat Activities.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-activities [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[8] Canadian Centre for Cyber Security (2022) *Cyber Threat Activities.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-activities [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

broader target audiences at a relatively low cost. They can do this by masquerading as legitimate information providers, hijacking social media accounts, or creating websites and new accounts.

Attribution is the act of accurately determining the threat actor responsible for a particular set of activities. Successful attribution of a cyber threat actor is important for a number of reasons, including network defence, law enforcement, deterrence, and foreign relations. However, attribution can be difficult as many cyber threat actors attempt to evade attribution through obfuscating their activities.

Obfuscation refers to the tools and techniques that threat actors use to hide their identities, goals, techniques, and even their victims. In order to avoid leaving clues that defenders could use to attribute the activity, threat actors can use either common, readily available tools and techniques or custom-built tools that covertly send information over the Internet.

Sophisticated threat actors can also use **false flags**, whereby an actor mimics the known activities of other actors with the hope of causing defenders to falsely attribute the activity to someone else. For example, a nation-state could use a tool believed to be used extensively by cybercriminals. The ability of cyber threat actors to successfully obfuscate their actions varies according to their level of sophistication and motivation. In general, nation-states and competent cybercriminals are more adept at obfuscation than other threat actors"[9] (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/cyber-threat-activities). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). In the next section the meaning of cyber crime will be covered.

1.6 What is cyber crime?

[10]""**What is cybercrime?** Cybercrime includes crimes in which technology is the primary target (e.g. malware or ransomware) or crimes that use technology as an instrument to commit crimes

[9] Canadian Centre for Cyber Security (2022) *Cyber Threat Activities.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-activities [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[10] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

(e.g. money laundering or fraud). **Should I report it?** Yes! Whether you are the victim, are reporting for the victim, a business or a witness, we strongly encourage businesses and individuals to report cybercrime to the appropriate law enforcement authorities. You have invaluable information that could make a difference to more than one investigation. For the best outcome, it's important you report the incident within 24 hours of discovering it. **Where do I report a cybercrime?** You should report a cybercrime to your local police department. For geographical areas where the RCMP is the police of jurisdiction, report cybercrimes to the local detachment. File a police report and keep note of the report number for your reference. The following section will cover aspects about the different types of cybercrimes.

1.7 Types of cybercrimes

1.7.1 Types of cybercrimes

1.7.1.1 Ransomware: A type of malware that denies a user's access to files or systems until a sum of money is paid.

1.7.1.2 [11]Phishing: Email or text messages that appear to be from a legitimate source, but contain infected attachments or malicious links. If recipients open the attachments or click on links contained in phishing messages, they may download malware or be directed to malicious websites.

1.7.1.3 Spam: Unsolicited messages, generally sent by email, to many recipients to advertise or to achieve malicious intentions.

1.7.1.4 Fraud: The act of wrongful or criminal deception intended to result in financial or personal gain.

1.7.2 Protect yourself

Follow the best practices below to help enhance your organization's online safety.

[11] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

- Use different user IDs and password combinations for different accounts. Increase the complexity by combining letters, numbers, and special characters, or use passphrases. Change your passwords and passphrases on a regular basis.
- Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates.
- Research applications before downloading to check for possible scams. Only download from trusted sources to avoid phony or malicious applications.
- Review the privacy and security settings for your social media accounts. Be careful what type of information you post online.
- Establish an incident response plan to enhance your ability to recover from an incident quickly with minimal impact to your organization.

1.8.3[12]What can I expect?

The investigation process can seem overwhelming to victims. Knowing what to expect if you fall victim to a cybercrime can make the process much easier. The following section provides insight into the investigative process after you report the cybercrime"" (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

1.7.4 "Initial steps

- Identify potential evidence, preserve it, and ensure nothing is lost or damaged.
- Isolate your network from the Internet and activate your incident response plan.
- Take note of who was present in your organization before, during, and after the incident.

[12] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[12] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

- Appoint a point of contact for law enforcement officers to speak to directly and gather information about the incident.

Note: For ransomware incidents, paying the ransom is a decision for your organization to make. You should know that paying the ransom does not guarantee restored access to your data or prevent it from being leaked. Ransom payments may encourage threat actors to target your devices again or those of another organization as they assume payment will be made. The payment may also fund additional illicit activities.

1.7.5 [13]Investigative process

- Document the report number provided to you by law enforcement.
- Anticipate law enforcement may need access to your equipment to analyze the technological components of the cyber incident. The police will work with you to collect evidence while minimizing the impacts to your business and recovery efforts.
- Provide logs, employee statements, emails, and other similar items as potential evidence.
- Produce a list of key contacts within your organization for law enforcement.

1.7.6 Recovery

- Communicate the incident to staff, business associates, clients, and partners.
- Review your cyber security policies and ensure your staff receive training.
- Consider purchasing anti-malware and anti-virus software for your network and devices.
- Enhance your data security with protective measures (e.g. firewalls, virtual private networks, encryption).

Prepare your organization for the possibility of testifying in court" (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime). © Her

[13] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

1.7.7 "Data breaches

Cybercrime often targets the personal and proprietary data you collect, use, and store. It can be stolen and sold or used for malicious intent by threat actors. In Canada, the *Privacy Act* governs the Government of Canada. Private sector organizations are governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and are required to do the following in the event of a data breach:

- Report any data breach involving personal information that poses a risk of significant harm to individuals to the Privacy Commissioner of Canada.
- Notify individuals affected by the breach.
- Retain records related to the breach"[14] (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021). The following section will cover aspects about how to be alert on issues related to receiving malicious email messages.

1.8 How to be alert of malicious email messages

[15]""**Spotting malicious email messages (ITSAP.00.100).** Organizations and their networks are frequently targeted by threat actors who are looking to steal information. Threat actors are technology savvy, vulnerability conscious, and aggressively agile; a successful intrusion can quickly lead to data and privacy breaches. As an employee, you may have access to sensitive company information, and you should be wary of malicious emails, which threat actors use to

[14] Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[15] Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

infect devices and systems and access information. By learning about malicious emails and phishing attacks, you can help protect and secure your organization's information.

1.8.1 Phishing attacks

[16]Phishing is the act of sending communications that appear to be legitimate but are fraudulent. Phishing emails often contain malicious attachments or links to malicious websites. Threat actors carry out phishing attacks to trick you into disclosing sensitive information, such as credit card numbers, social insurance numbers, or banking credentials. Phishing attacks can take the form of emails, texts, or phone calls, but this document focuses on malicious emails. While some phishing emails may be generic, threat actors can also carefully craft emails that look more convincing or legitimate:

- **Spear-phishing email**: A threat actor sends emails to specific targets, such as an individual, a group, or a company. A spear-phishing email is crafted using the recipient's personal or professional characteristics and interests. Threat actors often use publicly available information from the individual's social media accounts. Spear-phishing emails require more effort from threat actors, but recipients are more likely to respond to the email, open attachments, or click on links.
- **Whaling email**: A threat actor sends emails to high profile individuals or senior executives at a company. Threat actors create targeted and convincing emails by using personal information about the individual or the company they work for. Threat actors may use publicly available information from the company's website or social media accounts.

1.8.2 An effective method of attack

Phishing attacks are effective because threat actors can be highly skilled at creating emails that look legitimate. These emails contain company logos or trademark information. The subject lines are relevant, and the messages are pertinent. Given our desire to trust (and the number of emails

[16] Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

we receive daily), it can be easy to believe the content we read in these emails, click on embedded links, or open attachments. However, the attachments may contain malicious software, and the links may direct you to malicious websites. Even if an email comes from someone you know, you should always think twice before clicking links or opening attachments.

1.8.2.1 No one is immune

Although anyone can be the target of phishing and spear phishing emails, the following individuals are more commonly targeted:

- Senior executives and their assistants
- Help desk staff
- System administrators
- Users who have access to sensitive information
- Users who have remote access
- Users whose jobs involve interacting with members of the public

1.8.2.2 [17]**Beware of quishing**—a phishing attack using malicious "quick response" (QR) codes in emails that re-directs you to phishing websites when the QR code is scanned. Check the website URL to make sure it is the intended site.

1.8.3 Identifying malicious emails

Malicious emails can be difficult to identify, but there are some steps you should take to determine whether emails are legitimate or fake:

- Check that the sender's email address has a valid username and domain name. A suspicious email address could be similar to the one below:
    - **"John Doe <johndoe.%nklo17er@gkmail.com>".**
- Verify that you know the sender of an email and that its tone is consistent with the sender.

[17] Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- Look for grammatical errors or typos in the body of the message. Companies want to maintain a high degree of professionalism and generally do not send out emails that contain these types of errors.
- Consider the tone of the email or what is being offered. If the email is threatening or sounds too good to be true, then it is probably a phishing email.

Pay attention to what is being requested. Most companies do not ask for sensitive or personal information in an email"" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[18]"**Handling malicious emails. Handle suspicious emails with care.** When in doubt, avoid opening suspicious emails and contact the sender by another means (e.g. phone call) to confirm they contacted you. **Do not click on links, attachments or QR codes provided in emails**. If you are being asked to log in to an account for an unsolicited reason, do not click the link. Do not open attached files and avoid scanning QR codes. Instead, visit the company's website by manually entering the URL in your web browser or search for the website through a search engine. **Do not click on links provided in emails.** If you are being asked to log into an account for an unsolicited reason, do not click the link. Instead, visit the company's website by manually entering the URL in your web browser or search for the website through a search engine. **Report suspicious emails.** If you receive a suspicious email or suspect malicious activity on a work device or a work account, report the incident to your organization's IT and security teams. Follow their instructions and avoid forwarding the email to coworkers. You can also report phishing emails to us (cyber.gc.ca) or the Canadian Anti-Fraud Centre. If you receive an offensive, abusive, or potentially criminal message, inform your local police. Save the message as authorities may ask you to provide a copy to help with any subsequent investigations. **Do not send the message to anyone else**.

[18] Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

1.8.4 Interacting with a malicious email

If you accidently interact with a malicious email, remain calm and begin by taking the following actions:

- Stop using your device.
- Disable Wi-Fi or disconnect network cables so the device cannot communicate with the Internet.
- Power off the device.
- Contact your IT security department if you are using a corporate device. They can disable accounts and other device features.
- Change your password, passphrase, or PIN using a different device.
- Scan the device using anti-malware software if possible.
- Restore network connections only when you believe you have a clean system.
- Perform any available updates and security patches on your device.
- Monitor your accounts regularly for suspicious activity"[19] (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The conclusion of this chapter will be covered in the next section.

1.9 Conclusion

It can be concluded that the modern day world is highly dependent on the use of computers and the Internet thus making it impossible for countries to avoid being concerned about protecting their citizens or organizations from cyber security threats. In addition it can be concluded that it has now become a question of 'moral choice' for individuals, institutions, organizations and governments to play a critical role in educating the global society about malicious cyber threats and cybercrimes. Various governments and security institutions are now becoming very

[19] Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

conscious about the technical vulnerabilities of their information systems and how cybercriminals can easily manipulate them to harm the operational activities of their national institutions and organizations. Today cybercriminals are now incorporating strategic thinking when carrying-out their operational activities and this has put more pressure on governments' cyber security programs to be highly innovative and research oriented. It can also be concluded that technology has become a unique and very complicated weapon of choice that is used by criminals to commit cybercrimes in various countries around the world.

1.10 Discussion questions

1) Define the following terms 'cyber' and 'information'? Discuss the meaning of a 'cyber threat' and a 'cyber threat surface'?

2) Identify the actors or parties involved in a cyber threat? Explain issues about a malicious cyber threat activity by exploiting technical vulnerabilities in-depth?

3) Briefly explain what is a cyber crime? List the different types of cybercrimes? Discuss the strategies that can be used to be alert of malicious email messages?

Chapter 2: Increasing cyber security for virtual work & protecting your organization

After reading this chapter you should be able to:

- Define the following terms ‘phishing’ and ‘spoofing’. Highlight the differences between the terms ‘spear-phishing’, ‘spyware’, ransomware’ & [‘virus’, ‘worm’, ‘payload’ & trojan’].
- Discuss how to boost cyber security to protect your virtual work. Explain the various tips on how to increase protection from malware in an organization.
- Identify the various tips on how to keep your passwords safe. Explain the various tips for small & large organizations on cyber security.

2.1 Introduction

Virtual workplaces or remote workplaces have become inevitable for every business, institution and government workplace. Thus this has increased the demand for cyber security measures for remote work in countries, organizations and institutions. In general remote work tends to be more exciting and comforting when people enjoy a sense of security guarantee from cyber threats by using secured networks, information systems and devices. The demand for government cyber security infrastructure has enormously increased. Generally it has become a matter of ‘moral choice’ for government cyber security institutions and their leadership to ensure that they avoid violating the human rights, privacy and freedoms of their citizens or organizations when carrying-out their cyber security operations. Cyber security encompasses almost everything associated with a computer or the internet such as mobile devices, laptops, tablets, networks and so on. Users of mobile devices have the obligation to regularly enhance their devices protection measures to reduce their vulnerability from cyber threats (*scammers, malicious software, phishing and so on*). The following section will cover issues about the meaning of terms.

2.2 Define the following terms 'phishing' and 'spoofing'

The definition of terms when it comes to issues related to cyber security is critical. [20]"**Phishing** is a common method by which threat actors disguise themselves as a trustworthy entity with the intent to lure a large number of recipients into providing information, such as login credentials, banking information, and other personally identifiable information. Phishing is an example of a social engineering technique and is mainly conducted through email spoofing and text messages. Users become victims when they open malicious attachments or click on embedded links. **Spoofing** is the act of masking or forging a website, email address, or phone number to appear as if it originates from a trusted source. After receiving a phishing message, the victim can be enticed into giving away personal, financial, or other sensitive information or clicking on a link or attachment, which can infect a device with malware" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). In the following section the differences

2.3 Differences between the terms 'spear-phishing', 'spyware', ransomware' & ['virus', 'worm', 'payload' & trojan']

There are various complex terms that are used in the field of cyber security and some of them are highlighted in Table 2.1 below.

[20] Canadian Centre for Cyber Security (2022) Annex *Cyber Threat Toolbox.* Available from: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

Table 2.1 Differences between the terms 'spear-phishing', 'spyware', ransomware' & ['virus', 'worm', 'payload' & trojan']

Spear-phishing	Spyware	Ransomware	Virus, Worm, Payload & Trojan
"**Spear-phishing** occurs when a cyber threat actor sends a personally tailored phishing message to a more precisely selected set of recipients or even a single recipient. Spear-phishing relies on social engineering, using details that are believable to the victim as originating from a trusted source. **Whaling** refers to spear-phishing targeted at senior executives or other high-profile recipients with privileged access and authorities" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox).	"**Spyware** is malicious software used to track a user's digital actions and information with or without the user's knowledge or consent. Spyware can be used for many activities, including keystroke logging, accessing the microphone and webcam, monitoring user activity and surfing habits, and capturing usernames and passwords" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox).	"**Ransomware** is malicious software that, in many cases, restricts access to a computer or a device and its data by encrypting its content and demanding that a ransom be paid, usually via a cryptocurrency such as bitcoin, in order for the victim to regain access to systems and information. Ransomware can also lock systems in various ways without the use of encryption, disrupting device performance. Actors may threaten to expose sensitive, personal, or embarrassing information unless a ransom is paid. Ransomware is typically installed using a trojan or a worm deployed via phishing or by visiting a compromised website" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox).	[21]"**Virus, worm, payload, and Trojan** [Virus, ver, charge de virus et cheval de troie]. Malware is commonly delivered through the use of viruses, worms, and trojans with far-reaching consequences. A virus is an executable and replicable program that inserts its own code into legitimate programs with the objective of damaging the host computer (i.e., deleting files and programs, corrupting storage and operating systems). In its simplest state, a worm is a computer program meant to self-replicate and spread to other computers to drain a system's resources. Additionally, just like a virus, a worm has the ability to propagate code that can damage its host. Such code is referred to as a payload (e.g., the ability to encrypt files in ransomware and the installation of system

[21] Canadian Centre for Cyber Security (2022) Annex *Cyber Threat Toolbox.* Available from: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

			backdoors that enable remote access). A trojan is a malicious program disguised as or embedded within legitimate software that has similar objectives to viruses and worms, but, unlike either of them, does not replicate or propagate on its own" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox).

Source: (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

The following section will cover information about how to boost cyber security in order to protect your virtual work.

2.4 How to boost cyber security to protect your virtual work

""**Cyber security tips for remote work (ITSAP.10.116).** When you work in the office, you benefit from the security measures that your organization has in place to protect its networks, systems, devices, and information from cyber threats. Working remotely provides flexibility and convenience. However, remote work can weaken your organization's security efforts and put you at risk if you don't take precautions. Read through our cyber security tips to ensure that you are practicing good cyber hygiene when working from home, a café, or any other public location.

Mobile devices

[22]Without a dedicated workstation, you rely on mobile devices (e.g. smart phones, laptops, tablets) when working remotely. If possible, work only from corporate devices assigned to you by your employer.

[22] Canadian Centre for Cyber Security (2022) *Cyber security tips for remote work (ITSAP.10.116).* Available from: https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- **Use multi-factor authentication**. You can add an additional layer of security to your devices by changing your settings to require two different factors to unlock it. For example, use a password or PIN **and** a biometric, such as your fingerprint.
- **Keep your devices in sight**. Don't leave them unattended when you're working in a public location and report a lost or stolen device immediately to your IT help desk.
- **Check your surroundings**. Be aware of anyone who might be listening to your phone call or looking over your shoulder as you enter your password.
- **Run updates and patches on your devices**. Updates and patches address and fix security vulnerabilities, ensuring that your device is protected against threat actors.
- **Enable firewalls and anti-virus software**. Firewalls block malicious traffic and anti-virus software scans files for malware[23].

Phishing scams and social engineering

Scammers steal sensitive information by pretending to be someone they're not. They may even use information from your social media accounts to make it seem like they know you — a tactic called social engineering.

- **Be vigilant.** Take care when you receive messages or calls from someone you don't know and requests that come out of nowhere.
- **Trust your gut.** If a phone call or a message is threatening or sounds too good to be true, it probably is.
- **Think twice.** Check a link's URL by hovering your cursor over it and don't open unexpected attachments.
- **Err on the side of caution.** Avoid sending sensitive information over email or texts.

Wi-fi

[24]When working from your home, you should take steps to protect your own Wi-Fi network. Be sure to change the default password that was given to you by your service provider, and make

---

[23] Canadian Centre for Cyber Security (2022) *Cyber security tips for remote work (ITSAP.10.116).* Available from: https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

sure that you are using a passphrase or a strong password that is difficult to guess. The benefit of working remotely is that you can switch up your working location. Whether you are working at home, a library, or a café, you should always use a secure wireless network. Avoid sending sensitive information, whether it's personal or work related, over a public Wi-Fi network. Using a virtual private network (VPN) is another way to protect information. A VPN is a secure encrypted tunnel through which information is sent"" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116). The following section will cover aspects about the tips on how to increase protection from malware in an organization.

2.5 Tips on how to increase protection from malware in an organization

[25]""**Protect your organization from malware (ITSAP.00.057).** Threat actors can use **malware, or malicious software**, to infiltrate or damage networks, systems, and devices. Once malware is installed on your organization's systems and devices, threat actors can gain access to sensitive information. This document introduces some common types of malware, tips for detecting whether your devices have been infected, and steps to protect your organization from being compromised by malware.

Common types of malware

Some of the most common types include the following examples:

- Virus: A computer program that spreads, usually without you knowing, by making copies of itself.

---

[24] Canadian Centre for Cyber Security (2022) *Cyber security tips for remote work (ITSAP.10.116).* Available from: https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[25] Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057).* Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

- Worm: A malicious program that executes independently and self-replicates, usually through network connections, to cause damage (e.g. deleting files, sending documents via email, or taking up bandwidth).
- **Spyware**: Infected software that threat actors use to access your devices and steal sensitive information.
    - Trojan **Horse**: A type of **spyware** disguised as harmless software to fool you into downloading the program.
    - **Adware**: A type of **spyware** that tracks your Internet history and downloads to display pop-up advertisements related to products and services that might interest you.
- [26]Keystroke logger (Keylogger): Software or hardware designed to capture your keystrokes. The keystrokes are stored or transmitted so that threat actors can use them to collect valued information.
- **Rootkit**: Programs that provide threat actors with access to your networks, systems, and devices. A rootkit disguises itself as an operating system component on your device.
- Ransomware: A type of malware that denies your access to data or a system until you pay a sum of money to the threat actor.
- **VPN Filter** Malware: Malware designed to infect routers so that threat actors can collect information, exploit devices, and block network traffic"" (Canadian Centre for Cyber Security, 2020, https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

""**Ways that malware can infect.** Some ways in which you could infect your networks, systems, and devices with malware include the following examples:

- Accepting pop-up advertisements

[26] Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057)*. Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

- Downloading unreliable software (e.g. disguised as a Flash Player update)
- Opening malicious email attachments
- Downloading media and software through untrusted vendors or means
- Sharing files (e.g. peer-to-peer file sharing services)
- Using removable media (e.g. USB, hard drives, CD, DVD) before scanning and verifying it

[27]**Signs of an infected device.** It can be difficult to detect whether your devices have been infected with malware. Some symptoms to look out for include the following examples:

- Pop-up windows appearing on your device
- Homepage changes
- Spam emails sent from your account
- Page or system crashes
- Slow computer performance
- Unknown programs running on your device
- Unauthorized password changes

Tips to protect against malware. Some ways that you can protect your device from malware include the following:

- Back up your devices and information
- Install software updates and patches regularly and as soon as they are made available
- Use anti-virus software and keep it updated
- Use anti-phishing software
    - Align software with the Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy (e.g. email authentication and reporting protocol [domain-name visibility, notification of intrusion])

[27] Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057)*. Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

- Use a host intrusion detection system (HIDS)
- Use a firewall
- Install and execute only authorized applications through using application whitelisting
- Verify that files and attachments are legitimate before downloading them
- Use an ad blocker
- Use a data consumption application (e.g. track data usage on apps, when not in use, for suspicious activity)
- Avoid using public Wi-Fi
- Turn off Wi-Fi, GPS, and Bluetooth when not in use
- Do not share personal information on social media that could help threat actors hack into your other accounts (e.g. home address used as a security question to access banking information)
- Do not jailbreak (e.g. disable security measures imposed by device manufacturer) your device"" (Canadian Centre for Cyber Security, 2020, https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

[28]""**Steps to address infected devices**

If your device has been infected with malware, take the following steps to address the issue:

1. Contact your IT security service desk immediately
2. Disconnect the infected device from the network
3. Turn off Wi-Fi and unplug network-carrying cables (e.g. Ethernet)
4. Connect the device to a clean network and reinstall the operating system
5. Run anti-virus software and scan all back-ups before restoring the device
6. Reconnect the device to your network

[28] Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057)*. Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

7. Monitor traffic and run anti-virus scans to ensure no malware remains"".

Anti-virus software

Anti-virus software defends devices against viruses, Trojans, worms, and spyware. Anti-virus software can identify known malware by scanning start-up files, boot records, and all files that go through the system. It can also monitor common applications.

HIDS

Host intrusion detection systems (HIDS) monitor your system to detect intrusions and unauthorized access. HIDS allows you to see who is accessing and changing files in your system and what they are trying to do.

Firewalls

A firewall is a security barrier that protects the local system's resources from being accessed from the outside. A network firewall restricts traffic from passing from one network to another. A host-based firewall restricts incoming and outgoing network activity for a single host or end points""[29] (Canadian Centre for Cyber Security, 2020, https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020). The following section will cover aspects about the various ways that can be used to keep passwords safe.

2.6 Tips on how to keep your passwords safe

[30]""**Best practices for passphrases and passwords (ITSAP.30.032).** You have passwords for everything: your devices, your accounts (e.g. banking, social media, and email), and the websites

[29] Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057)*. Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

[30] Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032)*. Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

you visit. By using passphrases or strong passwords you can protect your devices and information. Review the tips below to learn how you can create passphrases, strengthen your passwords, and avoid common mistakes that could put your information at risk. For passwords, we recommend that you use a minimum of 12 characters. Keep in mind that websites and applications have different password creation rules that you will have to follow (i.e. the letters, numbers, punctuation marks, and special characters that a password must and must not contain). This will impact your ability to follow our recommended guidance.

Use passphrases. We recommend that you use passphrases, as they are longer yet easier to remember than a password of random, mixed characters. A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces. Your passphrase should be at least 4 words and 15 characters in length. For example, you might create a passphrase by using association techniques, such as scanning a room in your home and creating a passphrase that uses words to describe what you see (e.g. "Closet lamp Bathroom Mug")""[31] (Canadian Centre for Cyber Security, 2019, https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

""**Protect passphrases and passwords.** Threat actors send **phishing** emails to trick you into giving your personal information and, in some cases, installing malware, such as a keylogger. If a **keylogger** is installed on your device, a threat actor can use it to capture the keystrokes you use when entering your passphrases and passwords. Phishing attacks are common, but you can protect yourself by reading the tips in ITSAP.00.100 Spotting Malicious Email Messages and installing anti-malware software on your devices.

Create complex passwords. Use a password that is as complex as possible if you cannot use a passphrase (e.g. a website requires that your password is less than 15 characters). A password

[31] Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032)*. Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password of only lowercase letters. You can also think up a phrase and then use the first letters of each word to create a complex password that is more memorable. For example, the phrase, "My jersey number when I played competitive soccer was 27!" can be used to remember the password, "Mj#wIpcsw27!".

[32]**Use passcodes or PINS.** A passcode or PIN is a sequence of numbers that is at least 4 digits. Passcodes use a minimum of 4 digits because there are other protection mechanisms in place to protect your device or account. Always make sure your PIN is made of random numbers. For example, to access your bank account, a threat actor would need to know your PIN or passcode and have physical access to your bank card.

Two-factor authentication

Two-factor authentication strengthens your device and account security. Two-factor (or multi-factor) authentication makes accounts more secure by requiring at least two items of authentication such as something you know and something you have, (e.g. a password and a token, a password and a fingerprint) to log in. If you use two-factor authentication, you could use a password that is 6 to 8 characters in length because the extra authentication adds another layer of protection. Not all two-factor solutions are equal—but all will improve your overall cyber security posture. Your organization should have user authentication policies that balance security with usability.

Protect passwords, passphrases, and PINs. Passphrases, complex passwords, passcodes, and PINs must be handled, and stored carefully so that they are not compromised. Keep the following tips in mind:

---

[32] Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032)*. Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

- Be aware of your surroundings when entering passwords, passphrases, passcodes, or PINs in public
- Use a different password, passphrase, or PIN for each device and account, especially for accounts with sensitive information
- Do not give out passwords, passphrases, passcodes or PINs online or over the phone
- Do not share passwords, passphrases, passcodes, or PINs with others, even family
- Log off and sign out of accounts and websites when you are done using them

Ensure your sensitive accounts (e.g. banking, CRA) are protected by the strongest passphrase or password possible”” (Canadian Centre for Cyber Security, 2019, https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

[33]““**Avoid common password mistakes.** If created and protected properly, passwords, passphrases, or PINs are an effective way to protect your devices, accounts, and information. Below are some examples of common mistakes to avoid:

- Do not use easily guessed passwords, passphrases, or PINs (e.g. “password”, “let me in”, “1234”), even if they include character substitutions (e.g. p@ssword)
- Do not use common expressions, song titles or lyrics, movie titles, or quotes
- Do not use your personal details (e.g. birthday, hometown, pet’s name)

Know the reasoning behind the rules. The rules around creating passphrases and passwords exist for a reason. If you’re not careful to take precautions with your passphrases and passwords, threat actors can choose from an ever growing list of methods to break into your devices and accounts, and access your information. Many of these methods use a password hash, which is an

[33] Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032)*. Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

encoded version of your clear text password. The hash is what is often used to verify your passwords on apps and websites.

Threat actors can use the following methods:

- **Brute force** is a method of trial and error; all common passwords are entered until one works. This method usually uses password dictionary tables.
- **Rainbow tables** are precompiled lists of password combinations and their associated hashes. These are used to match a known hash to a password that grants access to an account.

Shorter passwords are much easier to hack. You can make it more difficult for threat actors to hack into your devices and accounts if you use lengthy passphrases or more complex passwords.

Password managers. If you feel overwhelmed by the number of passwords that you have, you can use a password manager to generate and track your many passwords. To protect the passwords stored on a password manager, consider the following tips:

- Use them to store passwords for your lower sensitivity accounts, but not for sensitive accounts such as those with administrative privileges or banking credentials.
- Use a strong password and two-factor authentication to secure a password manager.

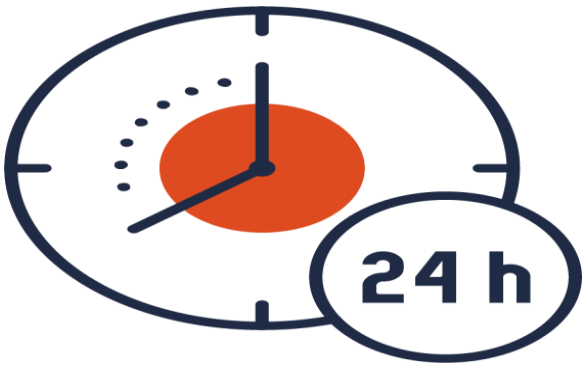
Ensure the password manager is from a secure website, and that it is updated regularly""[34] (Canadian Centre for Cyber Security, 2019, https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019). The following sections will cover information about the key tips for small-large organizations on cyber security issues.

[34] Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032).* Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

2.7 Tips for small & large organizations on cyber security

[35]According to the Canadian Centre for Cyber Security (2021) Looking for steps you can take to protect your organization's networks and information from cyber threats? To get you started, we have summarized the 13 security control categories that are identified in our Baseline Cyber Security Controls for Small and Medium Organizations and form the foundation for the CyberSecure Canada Certification program. By implementing these controls, you can reduce your risks and improve your ability to respond to security incidents. While it isn't always necessary to implement all of the controls, we encourage you to adopt as many as possible to enhance your cyber security (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.1 "Develop an incident response plan



Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

If you have a plan, you can quickly respond to incidents, restore critical systems and data, and keep service interruptions and data loss to a minimum. Your plan should include strategies for backing up data.

[35] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035).* Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

- Developing Your IT Recovery Plan (ITSAP.40.004)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.2 "Use strong user authentication

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Implement user authentication policies that balance security and usability. Ensure your devices authenticate users before they can gain access to your systems. Wherever possible, use two-factor authentication (2FA) or multi-factor authentication (MFA).

- Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)
- Best Practices for Passphrases and Passwords (ITSAP.30.032)
- Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036)"[36](Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[36] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035).* Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.3 "Enable security software

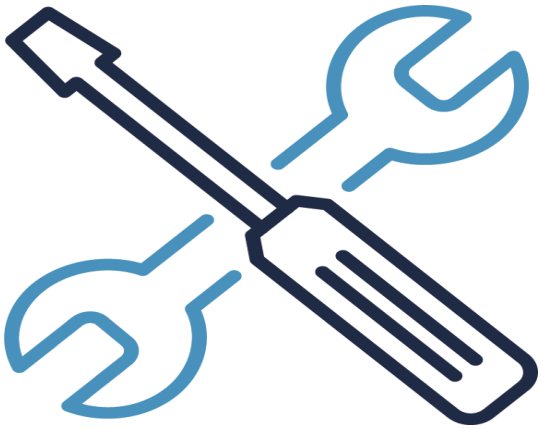
Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Activate firewalls and install anti-virus and anti-malware software on your devices to thwart malicious attacks and protect against malware. Ensure you download this software from a reputable provider. Install Domain Name System (DNS) filtering on your mobile devices to block out malicious websites and filter harmful content.

- Preventative Security Tools (ITSAP.00.058)"[37](Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[37] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.4 “Patch operating systems and applications



Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

When software issues or vulnerabilities are identified, vendors release patches to fix bugs, address known vulnerabilities, and improve usability or performance. Where possible, enable automatic patches and updates for all software and hardware to prevent threat actors from exploiting these issues or security vulnerabilities.

- How Updates Secure Your Devices (ITSAP.10.096)”(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.5 "Back up and encrypt data

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[38]Copy your information and critical applications to one or more secure locations, such as the cloud or an external hard drive. If a cyber incident or natural disaster happens, these copies can help you continue business activities and prevent data loss. Backups can be done online or offline and can also be done in three different iterations: full, differential or incremental. Test your backups regularly to ensure you can restore your data.

Tips for Backing Up Your Information (ITSAP.40.002)" (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[38] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035).* Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.6 "Train your employees

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Tailor your training programs to address your organization's cyber security protocols, policies, and procedures. Having an informed workforce can reduce the likelihood of cyber incidents.

- Offer Tailored Cyber Security Training to your Employees (ITSAP.10.093)

How to use these controls

These controls are not a one-size-fits-all approach to cyber security. They are guiding principles that you can use to create your organization's own cyber security framework.

[39]You should scope and tailor these controls based on your organization's needs and requirements. Implement as many of these controls as possible to enhance your cyber security posture and help minimize the risk of cyber attacks. Starting with the following four controls will strengthen your organization's security:

1. Develop an Incident Response Plan
2. Patch Operating Systems and Applications
3. Use Strong User Authentication
4. Backup and Encrypt Data

[39] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Before implementing the controls, keep the following tips in mind:

- Identify the critical information assets and systems to which you will apply these controls.
- Understand the main threats to your organization.
- Identify your valuable information and systems and apply risk management plans to enhance your security posture.

Implement some or all of these controls and you will see a significant impact on improving your organization's resilience and protection against cyber threats" (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.7 "**Secure cloud and outsourced services**

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Get to know a service provider before you contract them. Make sure the service provider has measures in place to meet your security requirements and needs.

[40]Know where a service provider's data centres are located. Different countries have different privacy laws and data protection requirements.

[40] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

- Benefits and Risks of Adopting Cloud-Based Services in Your Organization (ITSE.50.060)
- Models of Cloud Computing (ITSAP.50.111)
- Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.8 "Secure mobile devices

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Choose a device deployment model. Will your organization provide employees with corporately owned devices or will you allow employees to use personal devices for work?

Ensure employees can only use approved applications and can only download applications from trusted sources.

- Security Considerations for Mobile Device Deployments (ITSAP.70.002)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.9 "Establish basic perimeter defences

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[41]Defend your networks from cyber threats. For example, use a firewall to defend against outside intrusions by monitoring incoming and outgoing traffic and filtering out malicious sources.

Use a virtual private network (VPN) when employees are working remotely to secure the connection and protect sensitive information.

- Virtual Private Networks (ITSAP.80.101)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[41] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.10 "Secure portable media

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Storing and transferring data using a portable media device, like a USB key, is convenient and cost-effective, but they can be prone to loss or theft. Maintain an inventory of all assets. [42]Use encrypted portable storage devices, if possible, and sanitize devices properly before reusing or disposing of them.

- Security Tips for Peripheral Devices (ITSAP.70.015)
- Sanitization and Disposal of Electronic Devices (ITSAP.40.006)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[42] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.11 “Secure websites

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Protect your website and the sensitive information it collects. Encrypt sensitive data, ensure your certificates are up to date, use strong passwords or passphrases on the backend of the site, and use HTTPS for your site.

If you have outsourced your website, ensure your site’s host has security measures in place.

- Website Defacement (ITSAP.00.060)”(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.12 "Access control and authorization

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[43]Apply the principle of least privilege to prevent unauthorized access and data breaches. Employees should only have access to the information that they need to do their jobs. Each user should have their own set of log-in credentials, and administrators should have separate administrative accounts and general user accounts.

- Managing and Controlling Administrative Privileges (ITSAP.10.094)"(Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[43] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Figure 2.13 "Configure devices securely

Source: (Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Take the time to review your device's default settings and make modifications as required. At a minimum, we recommend changing default passwords (especially administrative passwords), turning off location services, and disabling unnecessary features.

- Cyber Security at Home and in the Office: Secure Your Devices, Computers and Networks (ITSAP.00.007)"[44](Canadian Centre for Cyber Security, 2021, https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021). The conclusion of this chapter is covered next.

2.8 Conclusion

It can be concluded that historically over the past centuries numerous civil wars have been experienced on the continents of Europe, Africa, North America, the Middle East, Asia and

[44] Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)***.** Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035 [Accessed May 21, 2022] "*Reproduced with the permission of the* Minister of National Defence*, 2021*". © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

South America and nowadays this has evolved to cyber warfare as a result of technology innovations. Nowadays the various parties or actors to cybercrimes intentionally target networks or information systems to install virus, malicious software, copy passwords and so on. Thus cyber criminals are now installing virus, malicious software or passwords in order to gain access to critical information for personal gain and in certain instances such illicit activities can place a country's or organization's network security at risk. Small – large businesses are also vulnerable to cyber threats if they do not invest in their cyber security. It can also be concluded that some of the cyber security tips or measures that may help individuals and organizations are now being easily made available at local government security institutions, higher learning institutions and private cyber security consulting organizations.

2.9 Discussion questions

1) Define the following terms 'phishing' and 'spoofing'? Identify the differences between the terms 'spear-phishing', 'spyware', ransomware' & ['virus', 'worm', 'payload' & trojan']?

2) Explain how to boost cyber security to protect your virtual work? List the various tips on how to increase protection from malware in an organization?

3) Discuss the various tips on how to keep your passwords safe? List the various tips for small & large organizations on cyber security?

Chapter 3: What is misinformation, disinformation & malinformation

After reading this chapter you should be able to:

- Define the following terms 'formjacking' and 'password cracking'. Explain how individuals or organizations can easily notice misinformation, disinformation, and malinformation (MDM).
- Highlight the measures implemented to reduce misinformation, disinformation, and malinformation (MDM). List the various tips on how to maximize protection of your mobile device when travelling.
- Identify the various tips for business travelers to protect their mobile devices. Discuss aspects about bluetooth technology and cyber security.

3.1 Introduction

"Information is the lifeblood that flows in the entire system of each and every society with the aim of shaping its culture, values, thinking, politics, opinions, development, governance and unity while on the other-hand 'without it' the whole society ceases to effectively function in a manner that is conducive to its inhabitants (*people, organizations, government & so on*). In general a society is more likely to prosper when it's fully educated and kept well-informed about its surrounding environment on various relevant topics (*such as politics, economics, technology, health, climate change, world peace, human rights and so on*) on a day-to-day basis" (Rudolph. Patrick. Tawanda. Muteswa, 2022). [45]According to the Canadian Centre for Cyber Security (2022) The effects of misinformation, disinformation, and malinformation (MDM) cost the global economy billions of dollars each year. Often known colloquially as "fake news", MDM are damaging to public trust in institutions and, during elections, may even pose a threat to

[45] Canadian Centre for Cyber Security (2022) *How to Identify Misinformation, Disinformation and Malinformation.* Available from: https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

democracy itself. MDM has become a serious concern for consumers and organizations of all sizes. New technologies such as machine learning, natural language processing, and amplification networks are being used to discredit factual information. Disinformation campaigns may use artificial intelligence (AI) to spread false and misleading information, such as deepfakes. Deepfakes refer to artificially generated images, audio, and videos used in place of the original image, audio, or video. This document offers consumers and organizations information on identifying MDM and implementing the appropriate security measures for mitigation strategies (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover aspects about the definition of terms.

3.2 Define the following terms 'formjacking' and 'password cracking'

[46]"**Formjacking** is when cybercriminals inject malicious code into a webpage form, such as a payment page, to compromise it and steal credit card details and other information that is entered by users on these pages. **Password cracking** is an attempt to directly access accounts. Two common forms of password cracking are **brute force** and dictionary-based. Brute force cracking uses an exhaustive number of randomly generated passwords to attempt to gain access, while **dictionary-based** cracking checks against a list of commonly used passwords" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover aspects about how to easily misinformation, disinformation, and malinformation (MDM).

[46] Canadian Centre for Cyber Security (2022) Annex *Cyber Threat Toolbox.* Available from: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

3.3 Can individuals or organizations easily notice misinformation, disinformation, and malinformation (MDM)

[47]““**How to identify MDM.** Evaluate the information landscape critically and take the time to review the sources and messaging. When viewing content, in any form, ask yourself the following questions:

- Does it provoke an emotional response?
- Does it make a bold statement on a controversial issue?
- Is it an extraordinary claim?
- Does it contain clickbait?
- Does it have topical information that is within context?
- Does it use small pieces of valid information that are exaggerated or distorted?
- Has it spread virally on unvetted or loosely vetted platforms?

These are a few guiding questions that can help you identify MDM. Even if one of these questions applies to a source, it does not automatically discredit the information. It is an indication to conduct more research on the item before trusting it. MDM can be identified as three main forms of informational activity that can cause minor or major harm. **Misinformation** refers to false information that is not intended to cause harm. **Disinformation** refers to false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction. **Malinformation** refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm. Information that is **valid** means that it is factually correct, is based on data that can be confirmed, and is not misleading in any way. **Inaccurate** information is either incomplete or manipulated in a way that portrays a false narrative. **False** information is incorrect and there is data that disproves it. **Unsustainable** information can neither be confirmed nor disproved based

[47] Canadian Centre for Cyber Security (2022) *How to Identify Misinformation, Disinformation and Malinformation.* Available from: https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

on the available data”” (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover aspects about the measures implemented to reduce misinformation, disinformation, and malinformation (MDM).

3.4 Measures implemented to reduce misinformation, disinformation, and malinformation (MDM)

[48]““**How can organizations take action against MDM?** Organizations can protect themselves from the threat of MDM by applying the following strategies and controls:

- Set up social media and web monitoring, as well as alerting services for identifying and tracking fake news related to your brand and organizations. These services often let you monitor not only your own social media profiles, but also public posts, web forums, websites, reviews, mentions, etc
- Use search engine optimization (SEO) along with transparent, high quality content on any web presence. SEO is used to optimize your site and social media listings on search engines such as Google and can make the difference of being displayed above or below a website with MDM that is targeting your organization
- Use answer engine optimization (AEO) which focuses on voice assistants such as Google Home, Amazon Alexa, or Siri to optimize answers from these devices so that they point to facts about your organization and not false information
- Use amplification networks to increase the reach and visibility of your content and prevent false information from overpowering the truth. Amplification networks act as loudspeakers for the truth and can include organizational partners, brand ambassadors, and existing customers

[48] Canadian Centre for Cyber Security (2022) *How to Identify Misinformation, Disinformation and Malinformation.* Available from: https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- Encourage engagement with your customers and users to ensure trust is established and maintained. For example, search engines use reviews by customers and users to gauge the trustworthiness of a brand
- Create a response team to indirectly counteract any MDM campaigns and ensure a response occurs as soon as possible
- Do not directly engage with MDM. Responses should be passive in nature and not within the conversation, post, or thread that they are posted on. Instead, you could post the response on your website. Ensure that a response to MDM includes detailed, transparent, factual answers. This may vary depending on the organization

[49]**How can consumers take action against MDM?** As a consumer of information, you can take these actions to investigate content further and protect yourself from MDM:

- Look for out of place design elements such as unprofessional logos, colours, spacing, and animated gifs
- Verify domain names to ensure they match the organization. The domain name may have typos or use a different Top Level Domain (TLD) such as .net or .org
- Check that the organization has contact information listed, a physical address, and an 'About Us' page
- Perform a WHOIS lookup on the domain to see who owns it and verify that it belongs to a trustworthy organization. WHOIS is a database of domain names and has details about the owner of the domain, when the domain was registered, and when it expires
- Conduct a reverse image search to ensure images are not copied from a legitimate website or organization
- Use a fact–checking site to ensure the information you are reading has not already been proven false

[49] Canadian Centre for Cyber Security (2022) *How to Identify Misinformation, Disinformation and Malinformation.* Available from: https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- Do not automatically assume information you receive is correct, even if it comes from a valid source (such as a friend or family member)
- Ensure the information is not out of date""(Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover aspects about mobile device protection by travelers.

3.5 Tips on how to maximize protection of your mobile device when travelling

[50]""**Mobile device guidance for high profile travellers (ITSAP.00.088).** If you're someone who is in a high-profile position, such as a politician or a senior executive, you need to protect the security of your mobile devices when you travel. Mobile devices contain sensitive information and they are high-value targets for cyber threat actors. If your device or the information on it is compromised, it could be used against you or the organization you represent. Below, we cover some of the common threats and the security measures you should take before, during, and after you travel to protect your mobile devices.

Threats

Threat actors use different techniques to gain access to devices and sensitive information. Someattack methods practiced are included in the following examples:

- **Shoulder-surfing:** Using in-person visibility to steal your sensitive information.
- Phishing**:** Sending fraudulent emails or texts that include malicious files, malicious links, or requests for personal information.
- **Network spoofing:** Masquerading as another network.
- **Signal jamming:** Interfering with, disrupting, or blocking communications signals and services.

[50] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- **In-the-middle attacks:** Exploiting vulnerabilities to intercept communications.
- Ransomware**:** Using malicious software to encrypt files or lock systems and devices until the victim pays a sum of money.

[51]For more information on these types of threats, refer to ITSAP.00.100 Don't Take the Bait: Recognize and Avoid Phishing Attacks, ITSAP.80.009 Protecting Your Organization While Using Wi-Fi, and ITSAP.00.099 Ransomware: How to Prevent and Recover.

Risks

Travel is considered **high-risk** if a traveller's identity is well-known or high-profile. This is especially true when the high-profile traveller is going to a widely known event or conference (e.g. The World Economic Forum), or the traveller's destination is considered high risk by Global Affairs Canada. When travelling, threat actors from foreign intelligence services, criminal groups, or competitor organizations may attempt to compromise your devices. As someone in a high-profile position, the information you deal with may be highly sensitive. Threat actors target technical, political, strategic, military, financial, and personal data. If your devices, or the information contained on them, are compromised, it could be used against you or the organization you represent. Your organization should consider any risks introduced by international travel and determine its level of tolerance. You and your organization should implement measures to mitigate those identified risks"" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). Figure 3.1 below will help highlight the Travelers Guide for Mobile Devices.

[51] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

Figure 3.1 Travelers Guide for Mobile Devices

Source: (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[52]"""**Before you go**

- Use corporately owned, temporary devices ("burner devices") if possible.
- Enforce multifactor authentication (MFA) to access devices and accounts.
- Install anti-virus and spyware protection and a firewall.
- Run updates and install patches for operating systems and applications.
- Back up devices for possible recovery when returned.
- Remove unnecessary data and applications from devices.
- Install a virtual private network (VPN) on your devices to securely transfer data.
- Configure a sandbox to securely access organizational data apart from other device applications.
- Limit administrative privileges to secure software settings and restrict downloadable applications

[52] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- Configure devices to run anti-virus software on storage devices (e.g. USB drives) upon installation.
- Implement appropriate network security settings for devices (e.g. restrict Wi-Fi connectivity to secure networks, disable hot-spot discovery).
- Configure mobile devices to disable external connection access (e.g. Wi-Fi and Bluetooth) while accessing the organization's secure network (i.e. internal network).
- Turn off devices before going through customs and security.
    - Inform IT if your device is inspected by security.

[53]During your trip

- Encrypt sensitive information.
- Avoid using personal accounts, if possible.
    - If necessary, secure with MFA, inform IT, and change passwords when returned home.
- Disable Bluetooth and Wi-Fi.
- Assume that communications transmitted over public carriers can be intercepted.
- Avoid using hotel, and public Wi-Fi and Bluetooth.

- Use your organization's network and VPN to access and send sensitive information.
- Maintain control of chargers, cables, and peripherals at all times.
- Avoid using storage media (e.g. USB) and peripherals given to you by external sources.
- Keep your devices in your possession and be aware of your surroundings at all times

When you return

Monitor your devices for unusual behaviours. Indicators such as your device acting slow or pop-ups disappearing before you can read them will need to be brought to the attention of your

[53] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

IT security team. Compare the device's image with a backup for signs of malicious activity"" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). Figure 3.2 will help highlight how investigation will be needed if a mobile device has exposed to a cyber security violation or breach.

Figure 3.2 How a mobile device that has been exposed to a cyber threat must be investigated

Source: (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[54]"If your device has been compromised, forensic research is recommended and a factory reset to restore the device is recommended. Use a secure back up to restore the device before further use. If you notice suspicious activity on your device during or after travel, follow these security measures:

1. Disconnect your device from the Internet and any other devices.

[54] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

2. Use another device to contact your service provider and your IT team to begin the appropriate incident management processes.
3. Keep the device disconnected for the rest of your trip.

4. Examine the device in your organization's secure environment once returned from travel.
5. Eliminate the threat from the device and use the latest secure backup to restore the device.
6. Replace the device's SIM card"[55] (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover information about the protection of mobile devices by business travelers.

3.6 Tips for business travelers to protect their mobile devices

[56]""**Mobile devices and business travellers (ITSAP.00.087).** As a business traveller, you should carefully consider the potential risks of using mobile devices during your travel. A compromised device can allow unauthorized access to your organization's network, placing not only your information at risk, but also that of your organization. This document offers information on the threats and risks to mobile devices during travel and how to best prevent these risks from becoming a reality. **Threats and risks.** Mobile devices are a prime target for theft. If stolen, a threat actor may be able to access the information contained on your device and use the device or the information for malicious purposes. Everyone should take precautions to protect their mobile devices when travelling. However, individuals who hold senior positions or work with valuable information may have a higher risk of being targeted by threat actors. Threat actors

[55] Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[56] Canadian Centre for Cyber Security (2022) *Mobile devices and business travellers (ITSAP.00.087)***.** Available from: https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

can use commercial eavesdropping devices (e.g. International Mobile Subscriber Identity [IMSI] catchers) to do the following:

- Identify and target mobile devices
- Deliver malicious code to the device
- Use the device's network connections (e.g. Wi-Fi, Bluetooth)
- Access the device and track your location
- Activate the microphone or camera on the device
- Intercept communications

In some countries, hotel business centres and phone networks are monitored, and rooms may be searched. Users should assume that there is no privacy in offices, hotels, Internet cafes, or other public areas"" (Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

""**Before you travel.** Before you travel, take the following actions:

- Disable features such as Bluetooth and wireless headset capabilities
- Remove unnecessary data
- Take only the devices that you need to do the job
- Change your passphrases and passwords before you leave
- Back up your data

[57]**While you travel.** While you travel, you can take the following actions to protect yourself:

- Keep possession of your phone at all times. If you must leave the device unattended, remove the battery, if possible, and the SIM card and keep them with you.

[57] Canadian Centre for Cyber Security (2022) *Mobile devices and business travellers (ITSAP.00.087)*. Available from: https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

- Power off devices while going through customs or other inspection points.
- Empty your Trash and **Recent** folders after every use. Clear your browser after each use (delete history files, caches, cookies, URL, and temporary internet files).
- Be aware of your surroundings and be mindful of shoulder surfers trying to view your screen or keyboard.
- **Do not use** the Remember Me feature on websites. Enter your log-in credentials every time.
- **Do not use** unknown, unsecured, or public Wi-Fi networks and charging kiosks.
- **Do not** store or communicate information above the approved classification of the device.
- Keep an eye on your cables, chargers and peripherals. Modern cables can be programmed to compromise your device since they can contain microcontroller components.
- **Do not** open emails, attachments, or click on links sent from unknown sources.
- Do not accept chargers
- Contact your IT Security department right away if your device is stolen or misplaced, or if you have a security concern""(Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[58]""**After you travel.** When you return from your trip, take the following actions:

- Report suspected security concerns to your IT security department.
- Change the passphrases, passwords, or PINs on your devices or accounts that you accessed while abroad.

High risk travel

Travel can be considered high risk if the traveller's identity is well known or is high-profile (e.g. Chief Executive Officer), if the event or conference is widely known about (e.g. The World

[58] Canadian Centre for Cyber Security (2022) *Mobile devices and business travellers (ITSAP.00.087)*. Available from: https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

Economic Forum), or if the destination is high-risk (as defined by Global Affairs Canada). If you are unsure of the risk, contact your IT Security department.

High-risk travel requires the following special considerations:

- Do not use your regular business or personally owned devices. If you must use a personal device, turn off Bluetooth, Wi-Fi and location sharing and use a VPN.
- Ask your IT department if they have an inventory of devices for travel or "burner devices" and "burner accounts" for high-risk, high-threat environments.
- Assume that all communications transmitted over public carriers are at risk of being intercepted. Encrypt all sensitive information on your mobile devices before your trip.
- Assume that hotel Internet connections, photocopiers, or fax machines are monitored. Only use them for non-sensitive information.
- Report any unusual device performance issues or any other associated security concerns to your IT Security department""[59](Canadian Centre for Cyber Security, 2022, https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022). The following section will cover aspects about Bluetooth technology.

3.7 Bluetooth technology and cyber security

[60]""**Using bluetooth technology (ITSAP.00.011).** Many business and personal devices use Bluetooth technology. Bluetooth is a wireless technology used to transfer and synchronize data between devices without the use of physical cables (e.g. a laptop and headphones, a fitness tracker and an app). Bluetooth is also used by exposure notification applications with signal

[59] Canadian Centre for Cyber Security (2022) *Mobile devices and business travellers (ITSAP.00.087)*. Available from: https://cyber.gc.ca/en/guidance/mobile-devices-and-business-travellers-itsap00087 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

[60] Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011)*. Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

distribution to perform effectively (e.g. COVID Alert). As Bluetooth technology evolves, newer versions of Bluetooth can transfer data between devices at increased speed and range. Overall, it is a low-cost and effective way to connect your devices. However, threat actors can exploit vulnerabilities in this technology to gain access to your devices and steal sensitive information.

Security considerations when using bluetooth

Use updated versions of Bluetooth. Devices that use earlier versions of Bluetooth don't have the same security features, making them vulnerable to interception and attacks. If you connect two devices and one of them uses an earlier version of Bluetooth, then the entire connection is vulnerable. Although newer versions of Bluetooth have improved security measures, you should still use Bluetooth with caution.

Protect sensitive information. Avoid transferring sensitive information over Bluetooth connections. For example, avoid using Bluetooth enabled keyboards to enter sensitive information or passwords, as this information can be intercepted (e.g. keystroke logging). When using Bluetooth technology, such as a wireless mouse, keep in mind that your computer is vulnerable to remote attacks if the wireless adaptor in the mouse, which enables the Bluetooth connection, is exploited and compromised.

Disable discovery mode. Discovery mode is a state in which a Bluetooth-enabled device can search for and connect with other devices that are in range. When using discovery mode to connect devices, you should connect only with devices you know and trust. Turn off discovery mode when you're not using it.

Use devices with appropriate security measures. Choose Bluetooth devices that use security mechanisms, such as changeable passwords. Some Bluetooth products do not use PINs or passwords, or they use fixed passwords (e.g. 0000 pin). With a changeable passwords, you can make it more difficult for a threat actor to connect to and access your devices.

[61]**Authenticate and authorize devices.** Protect your devices and information by authenticating and authorizing other devices. Always verify that a listed device is one that you know and trust before you pair it with your device. To authorize and verify connections, pairing codes and passkeys are used. Be wary if you receive a pairing request if you haven't initiated it. Keep in mind that once paired, devices remain on your list of paired devices. Always remove lost or stolen devices from your paired devices list"" (Canadian Centre for Cyber Security, 2021**,** https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

""**Bluetooth-enabled cars.** By connecting devices to Bluetooth-enabled cars, drivers and passengers can make hands-free calls, send texts or emails, stream music, and connect to the Internet. When you pair your device with your car, your personal information is stored on the car's system. Your call logs, contacts, and messages, such as texts, emails, or any app based messaging, can be accessed on the car screen through Bluetooth. This might not seem like an issue if you own the car, but it is a concern when you sell or rent a car. Make sure to delete stored data and devices when you are selling your car. It's best to avoid pairing your devices with rental cars altogether. If you need to use hands-free calling when using a rental car, use the built-in speakerphone on your device or pair your device with a personal Bluetooth device.

[62]**Threats to be aware of.** Bluetooth-enabled devices are susceptible to general cyber threats. Threat actors use different attack methods to connect to your devices, eavesdrop, and steal information. Some of these attack methods are included in the following:

Protocol attacks: A threat actor broadcasts packets (e.g. small pieces of data) or impersonates a device to bypass authentication and encryption.

---

[61] Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011)***.** Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[62] Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011)***.** Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Denial-of-Service (DoS) attacks: A threat actor jams the signal to prevent your device from connecting to another device. DoS attacks are often used with protocol attacks to deny access to intended devices and redirect you to connect with a spoofed device.

Once a threat actor connects to your device, they can carry out additional attacks, such as the following examples:

Eavesdropping attacks: A threat actor captures and decodes sensitive information in your Bluetooth transmissions (e.g. password typed into a Bluetooth keyboard).

[63]**Impersonation attacks:** A threat actor uses direct spoofing or person-in-the-middle attacks to access your device contents and services to download contents and change settings. Internet of Things devices are often vulnerable to these types of attacks. In addition to these methods, threat actors can take advantage of device, software, and application vulnerabilities to access and gain control of your Bluetooth devices. Once your device is compromised, threat actors can steal information, track locations, and change device settings without your knowledge. Keeping your devices, software, and applications updated can address vulnerabilities and protect you from cyber threats. Be sure to run updates and patches regularly.

Summary of security tips

Bluetooth technology continues to evolve, but you can continue to protect your data and devices with a few simple actions:

- Keep all Bluetooth devices up to date (e.g. phones, headphones, keyboards, gaming equipment)
- Turn off Bluetooth when you're not using it[64]Footnote*
- Turn off discovery mode when you're not connecting devices
- Avoid pairing devices in public spaces

---

[63] Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011)***.** Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

[64] "Note: Exposure notification applications (e.g. COVID Alert) need Bluetooth to be continuously enabled. In this case, you should consider removing any paired devices that are not in use and restrict your device permissions" (Canadian Centre for Cyber Security, 2021**,** https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011).

- Pair only with devices that you know and trust
- Never transfer sensitive information over Bluetooth
- Avoid using Bluetooth-enabled keyboards to enter sensitive information or passwords
- Remove lost or stolen devices from your list of paired devices
- Delete all stored data and devices from Bluetooth enabled cars
- Avoid pairing devices with rental cars

Be sure to check out ITSAP.00.001 Using Your Mobile Device Securely for more tips on keeping your devices safe""[65] (Canadian Centre for Cyber Security, 2021**,** https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011). © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021). The conclusion of this chapter is covered next.

3.8 Conclusion

It can be concluded that information is the most critical element in each and every institution in a society yet it still remains the most vulnerable due to manipulation. The Internet is full of misinformation and disinformation thus resulting in the eradication of the correct narration of truthful facts since society can no longer separate between fake news and factual news. Trust is built on truthful communications in a society therefore when misinformation, disinformation, and malinformation (*MDM*) become the new 'world order' in various parts of the world it leads to public trust being easily diminished. It can also be concluded that cyber security institutions are the key determinants to a truth based future since it helps to protect the integrity of society.

[65] Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011).* Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] "*Reproduced with the permission of the* Minister of National Defence*, 2021*". © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

3.9 Discussion questions

1) Define the following terms ‘formjacking’ and ‘password cracking’? Explain how individuals or organizations can easily notice misinformation, disinformation, and malinformation (*MDM*)?

2) Discuss the various measures implemented to reduce misinformation, disinformation, and malinformation (*MDM*)? Explain the various tips on how to maximize protection of your mobile device when travelling?

3) List the various tips for business travelers to protect their mobile devices? Discuss the various aspects related bluetooth technology and cyber security?

Chapter 4: How to implement or improve personnel security in the private & public sector

After reading this chapter you should be able to:

- Define the term 'data security' & 'digital preservation'. Identify the differences between 'public data', 'public network infrastructure', 'public switched telephone network', 'security risk', 'security risk appetite' & 'security risk management'.
- Highlight the objectives of training & development in an organization. Describe the different methods of training.
- Discuss how to conduct cyber security informative training.

4.1 Introduction

Nowadays both private and public organizations are placing more emphasis on providing their employees at all levels of the organizational hierarchy with training and development programs that focus on cyber security. It has naturally become inevitable for employers such as government departments to omit cyber security training in their human resources development plans. In almost each and every country various government departments' possess or store critical personal information of their citizens, organizations including 'confidential national data'. Therefore this has put immense pressure on many governments to make cyber security training of employees/personnel a key priority in order to stay one step ahead of avoiding cyber crime or threats. [66]It is important to point-out the fact that every training & development program that is carried-out in both the private and public sector (*even for cyber security training purposes*) must first be aligned with the objectives of the employees and the organization so that the program can easily be made applicable in the day-to-day operational activities of the organization (Rudolph. Patrick. Tawanda. Muteswa, 2019:228). The following section will cover aspects about the definition of terms in-depth.

[66] Rudolph. Patrick. Tawanda. Muteswa (2019) *The Importance of Human Resources Management & Business Leadership in the Boardroom (Gathered Articles): A North America, Asia, Africa, Oceania & Europe Perspective* 1st Edition, Educational EBook, ISBN 978-1-77920-215-4, p1-305.

4.2 Define the term 'data security' & 'digital preservation'

The definition of terms is critical in the field of technology and cyber security. [67]"*Data security* – Measures used to protect the confidentiality, integrity and availability of data. *Digital preservation* - The coordinated and ongoing set of processes and activities that ensure long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span the information is required" (Australian Cyber Security Centre – Information Security Manual, 2022:164). © Commonwealth of Australia 2022. The following section will cover the differences of six terms in-depth.

4.3 Differences between 'public data', 'public network infrastructure', 'public switched telephone network', 'security risk', 'security risk appetite' & 'security risk management'

It is important to point-out the fact that there is a high distinction between the terms 'public data', 'public network infrastructure', 'public switched telephone network', 'security risk', 'security risk appetite' & 'security risk management'. In general it is more likely that some people (or professionals) may confuse these six terms and end up assuming they share the same meaning whilst this assumption is not correct. Table 4.1 below will help to explain the key difference between six cryptography terminology in-depth.

Table 4.1 Differences of terms explained

Term	Explanation
"public data	Data that has been formally authorised for release into the public domain

[67] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

public network infrastructure	Network infrastructure that an organisation has no control over, such as the internet
Public Switched Telephone Network	Public network infrastructure used for voice communications
security risk	Any event that could result in the compromise, loss of integrity or unavailability of data or resources, or deliberate harm to people measured in terms of its likelihood and consequences[68]
security risk appetite	Statements that communicate the expectations of an organisation's senior management about their security risk tolerance. These criteria help an organisation identify security risks, prepare appropriate treatments and provide a benchmark against which the success of mitigations can be measured.
security risk management	The process of identifying, assessing and taking steps to reduce security risks to an acceptable level" (Australian Cyber Security Centre – Information Security Manual, 2022:170-172).

Source: Table Created By The Author Using Information From: (Australian Cyber Security Centre – Information Security Manual, 2022:170-172, https://www.cyber.gov.au). © Commonwealth of Australia 2022.

The following section will cover aspects pertaining to the objectives of training & development in an organization in-depth.

[68] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

4.4 Objectives of training & development in an organization

[69]Training mainly aims to enable the employees, executive directors and board of directors to learn new knowledge and discover new capabilities that are usually highlighted in training programs so that they may implement their newly acquired knowledge in their day-to-day work activities. The various aims of training & development in an organization include the following:

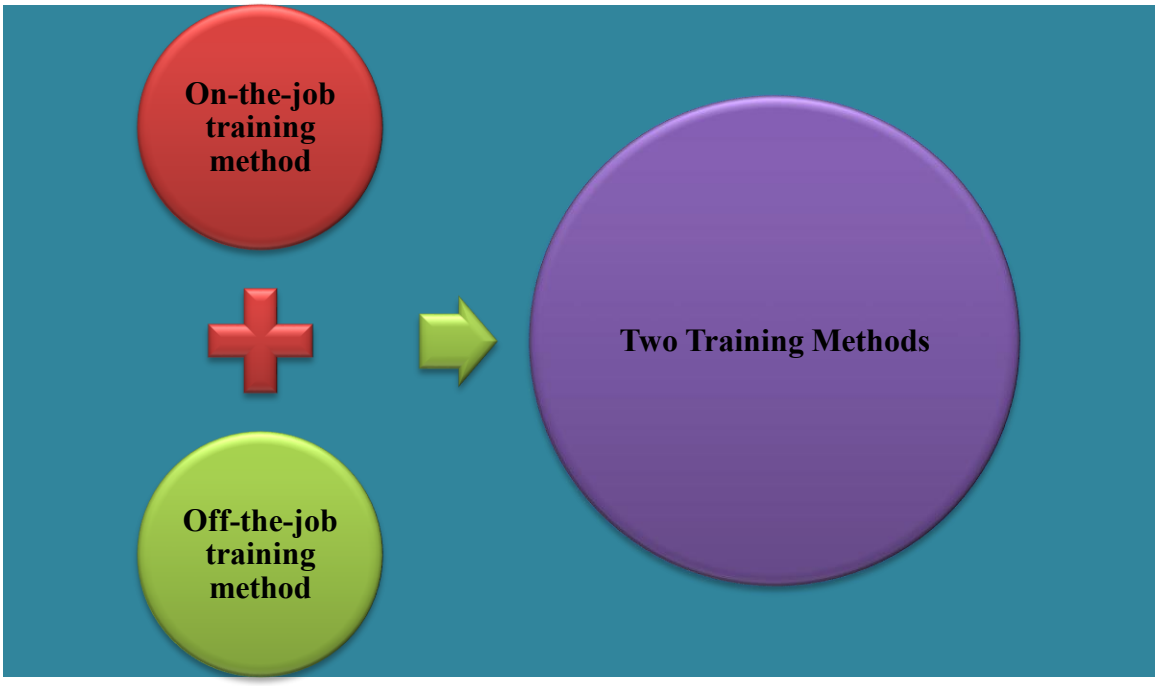
• To help trigger quick, analytical and decisive thinking in employees, executive directors and board of directors' as this often results in most of the organization's problems being easily resolved,
• To entrench the culture of ethical behavior amongst the employees, executive directors and board of directors,
• To entrench a culture of adhering to the set rules of good corporate governance amongst the employees, executive directors and board of directors,
• To ensure that the current employees, executive directors and board of directors' in the organization are consistently kept abreast of the new latest skills, knowledge and concepts so that they may easily cope with changes pertaining to the following: technology, innovation, cyber security and so on,
• To provide the organization with well educated, highly productive and skilled employees, executive directors and board of directors' who are able to improve the organization's current strategic planning, oversight, corporate image and market position through attaining reduced cyber security risk and high quality work results (Rudolph. Patrick. Tawanda. Muteswa, 2019:229). The following section will cover the two methods of training in-depth.

4.5 Methods of training

The two forms of training are clearly highlighted by Figure 4.1 below.

[69] Rudolph. Patrick. Tawanda. Muteswa (2019) *The Importance of Human Resources Management & Business Leadership in the Boardroom (Gathered Articles): A North America, Asia, Africa, Oceania & Europe Perspective* 1st Edition, Educational EBook, ISBN 978-1-77920-215-4, p1-305.

Figure 4.1 Two methods of training



Source: (Rudolph. Patrick. Tawanda. Muteswa, 2019:237-238)

As depicted by Figure 4.1 the two methods of training are further discussed as follows:

4.5.1'On-the-job' training

[70]*'On-the-job training'* occurs when informal training is conducted and one of its most significant characteristic is that trainees receive their new knowledge or skills whilst on-the-job. Today it is a very popular method of job training used by many organizations around the world. [71]The common forms of 'on-the-job' training include: job rotation and coaching & mentoring (Human Resources Institute of New Zealand, 2018, https://www.hrinz.org.nz/ cited in Rudolph. Patrick. Tawanda. Muteswa, 2019:237-238). One of the key advantage of 'on-the-job' training is that the employee is quickly introduced to the new methods of doing things therefore their newly

[70] Rudolph. Patrick. Tawanda. Muteswa (2019) *The Importance of Human Resources Management & Business Leadership in the Boardroom (Gathered Articles): A North America, Asia, Africa, Oceania & Europe Perspective* 1st Edition, Educational EBook, ISBN 978-1-77920-215-4, p1-305.

[71] Human Resources Institute of New Zealand (2018) *Coaching.* Available from: https://www.hrinz.org.nz/Site/My_HR_Career/Coaching/What_is_Coaching.aspx [Accessed 2018, 03 May]

acquired skills are quickly reinforced in their day-to-day work activities because learning is done on-the-job (Rudolph. Patrick. Tawanda. Muteswa, 2019:235).

4.5.2 'Off-the-job' training

In general any form of job training that is done at a site away from the workplace whilst the employees, executive directors and or the board of directors are not working is referred to as *off-the-job training*. In addition, off-the-job training puts more emphasis on learning than the carrying-out of the job tasks by the trainee. The common methods of off-the-job training methods include: case studies, the lecture method, computer-aided, role playing, audio-visual methods and so on. The advantages that are offered by off-the-job training is that it is carried-out by highly skilled experts (*for example cyber security academics*) and it also helps to reduce work-related stress or distractions that might affect the trainees/employees to learn properly (Rudolph. Patrick. Tawanda. Muteswa, 2019:237-238). The following section will cover aspects about cyber security informative training in-depth.

4.6 Cyber security informative training

4.6.1 [72]""""**Guidelines for Personnel Security. Cyber security awareness training.** Providing cyber security awareness training. An organisation should ensure that cyber security awareness training is provided to all personnel in order to assist them in understanding their security responsibilities. Furthermore, the content of cyber security awareness training should be tailored to the needs of specific groups of personnel. For example, personnel with responsibilities beyond that of a normal user will require tailored privileged user training. [73][74]*Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A Cyber security awareness training is undertaken annually by all personnel and covers:*

---

[72] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

[73] Control: ISM-1565; Revision: 0; Updated: Jun-20; Applicability: All; Essential Eight: N/A
Tailored privileged user training is undertaken annually by all privileged users.

[74] Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight

- *the purpose of the cyber security awareness training*
- *security appointments and contacts*
- *authorised use of systems and their resources*
- *protection of systems and their resources*
- *reporting of cyber security incidents and suspected compromises of systems and their resources.*

Managing and reporting suspicious changes to banking details or payment requests. [75]Business email compromise, a form of financial fraud, is when an adversary attempts to scam an organisation out of money or assets with the assistance of a compromised email account. An adversary will typically attempt to achieve this via invoice fraud, employee impersonation or company impersonation. With invoice fraud, an adversary will compromise a vendor's email account and through it have access to legitimate invoices. The adversary will then edit contact and bank details on invoices and send them to customers with the compromised email account. Customers will then pay the invoices, thinking that they are paying the vendor, but instead be sending money to the adversary's bank account. With employee impersonation, an adversary will compromise an organisation's email account and impersonate an employee via email. This is then used to commit financial fraud in a number of ways. One common method is to impersonate a person in a position of authority, such as a Chief Executive Officer or Chief Financial Officer, and have a false invoice raised. Another method is to request a change to an employee's banking details. The funds from the false invoice or the employee's salary is then sent to the adversary's bank account. With company impersonation, an adversary registers a domain with a name similar to another organisation. The adversary then impersonates that organisation in an email to a vendor and requests a quote for a quantity of expensive assets, such as laptops, and subsequently negotiates for the assets to be delivered to them prior to payment. The assets are then delivered to a location specified by the adversary, with the invoice being sent to the legitimate organisation who

[75] Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.

never ordered or received the assets. To mitigate business email compromise, personnel should be educated to look for the following warning signs:

- an unexpected request for a change of banking details
- an urgent payment request, or threats of serious consequences if payment is not made
- unexpected payment requests from a person in a position of authority, particularly if payment requests are unusual from this person
- an email received from a suspicious email address, such as an email address not matching an organisation's name.

In dealing with such situations, personnel should have clear guidance to verify bank account details; think critically before actioning unusual payment requests; and have a process to report threatening demands for immediate action, pressure for secrecy, or requests to circumvent normal business processes and procedures. Reporting suspicious contact via online services**.** [76]Online services, such as email, internet forums, messaging apps and direct messaging on social media, can be used by an adversary in an attempt to elicit sensitive or classified information from personnel. As such, personnel should be advised of what suspicious contact via online services is and how to report it. [77]Posting work information to online services. [78]Personnel should be advised to take special care not to post work information to online services unless authorised to do so, especially in internet forums and on social media. Even information that appears to be benign in isolation could, along with other information, have a considerable security impact. In addition, to ensure that personal opinions of individuals are not misinterpreted, personnel should

[76] Control: ISM-0817; Revision: 4; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Personnel are advised of what suspicious contact via online services is and how to report it.

[77] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

[78] Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

be advised to maintain separate work and personal accounts for online services, especially when using social media. Posting personal information to online services. [7980]Personnel should be advised that any personal information they post to online services, such as social media, could be used by an adversary to develop a detailed understanding of their lifestyle and interests. In turn, this information could be used to build trust in order to elicit sensitive or classified information from them, or influence them to undertake specific actions, such as opening malicious email attachments or visiting malicious websites. Furthermore, posting information on movements and activities may allow an adversary to time attempted financial fraud to align with when a person in a position of authority will be uncontactable, such as attending meetings or travelling. Finally, encouraging personnel to use any available privacy settings for online services can reduce security risks by restricting who can view their information as well as their interactions with such services. Sending and receiving files via online services. When personnel send and receive files via unauthorised online services, such as messaging apps and social media, they often bypass controls put in place to detect and quarantine malicious code. Advising personnel to send and receive files via authorised online services instead will ensure files are appropriately protected and scanned for malicious code"" (Australian Cyber Security Centre – Information Security Manual, 2022, https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security). © Commonwealth of Australia 2022.

4.6.2 [81]""**Access to systems and their resources.** [82]Security clearances. Where these guidelines refer to security clearances, it applies to Australian security clearances or security clearances

[79] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

[80] Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.

[81] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

from a foreign government which are formally recognised by Australia. System access requirements. Documenting access requirements for a system and its resources can assist in determining if personnel have the appropriate authorisation, security clearance, briefings and need-to-know to access the system and its resources. Types of users for which access requirements should be documented include unprivileged users, privileged users, foreign nationals and contractors. User identification. [83]Having uniquely identifiable users ensures accountability for access to a system and its resources. Furthermore, where a system processes, stores or communicates Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access to the system, it is important that the foreign nationals are identified as such. Unprivileged access to systems. Personnel seeking access to systems, applications and data repositories should have a genuine business requirement validated by their manager or another appropriate authority. Finally, to assist with incident response activities, it is important that unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. Unprivileged access to systems by foreign nationals. Due to the extra sensitivities associated with AUSTEO, AGAO and REL data, foreign access to such data is strictly controlled. Privileged access to systems. Privileged accounts are considered to be those which can alter or circumvent a system's controls. [84]This can also apply to users who have only limited privileges, such as software developers, but can still bypass controls. A privileged account often has the ability to modify system configurations, account privileges, event logs and security configurations for applications. Privileged users, and in some cases privileged service accounts, are often targeted by an adversary as they can potentially give full access to systems. As such, ensuring that privileged

---

[82] Control: ISM-0432; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Access requirements for a system and its resources are documented in its system security plan.

[83] Control: ISM-0414; Revision: 4; Updated: Aug-19; Applicability: All; Essential Eight: N/A
Personnel granted access to a system and its resources are uniquely identifiable.

[84] Control: ISM-1649; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Just-in-time administration is used for administering systems and applications.

accounts do not have the ability to access the internet, email and web services minimises opportunities for these accounts to be compromised. Finally, to assist with incident response activities, it is important that privileged access event logs and privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. Privileged access to systems by foreign nationals. [85][86]As privileged accounts often have the ability to bypass a system's controls, it is strongly encouraged that foreign nationals are not given privileged access to systems that process, store or communicate AUSTEO, AGAO or REL data. Suspension of access to systems. Removing or suspending access to systems, applications and data repositories can prevent them from being accessed when there is no longer a legitimate business requirement for their use, such as when personnel change duties, leave an organisation or are detected undertaking malicious activities. Recording authorisation for personnel to access systems. Retaining records of system account requests will assist in maintaining personnel accountability. This is needed to ensure there is a record of all personnel authorised to access a system, their user identification, who provided the authorisation, when the authorisation was granted and when the access was last reviewed. *Control: ISM-0407; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A*

A secure record is maintained for the life of each system covering:

- *all personnel authorised to access the system, and their user identification*
- *who provided authorisation for access*
- *when access was granted*
- *the level of access that was granted*
- *when access, and the level of access, was last reviewed*
- *when the level of access was changed, and to what extent (if applicable)*

[85] Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.

[86] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

- *when access was withdrawn (if applicable).*

Temporary access to systems. [87][88]Under strict circumstances, temporary access to systems, applications or data repositories may be granted to personnel who lack an appropriate security clearance or briefing. In such circumstances, personnel should have their access controlled in such a way that they only have access to data required for them to undertake their duties. Emergency access to systems. It is important that an organisation does not lose access to their systems. As such, an organisation should always have a method for gaining access during emergencies. Typically, emergencies would occur when access to systems cannot be gained via normal authentication processes, such as due to misconfigurations of authentication services, misconfigurations of security settings or due to a cyber security incident. In these situations, a break glass account (also known as an emergency access account) can be used to gain access. As break glass accounts generally have the highest level of privileges available for systems, extreme care should be taken to both protect them and to monitor for any signs of compromise or abuse. When break glass accounts are used, any administrative activities performed will not be directly attributable to an individual, and systems may not generate event logs. As such, additional controls need to be implemented in order to maintain the system's integrity. In doing so, an organisation should ensure that any administrative activities performed using a break glass account are identified and documented in support of change management processes and procedures. This includes documenting the individual using the break glass account, the reason for using the break glass account and any administrative activities performed using the break glass account. As the custodian of each break glass account should be the only party who knows the account's credentials, credentials will need to be changed and tested by custodians after any

---

[87] Control: ISM-0441; Revision: 8; Updated: Jun-22; Applicability: All; Essential Eight: N/A
When personnel are granted temporary access to a system, effective controls are put in place to restrict their access to only data required for them to undertake their duties.

[88] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

authorised access by another party. [89]Modern password managers that support automated credential changes and testing can assist in reducing the administrative overhead of such activities. Finally, to assist with incident response activities, it is important that break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected"" (Australian Cyber Security Centre – Information Security Manual, 2022, https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security). © Commonwealth of Australia 2022. The conclusion of this chapter is covered in the next section.

4.7 Conclusion

It can be concluded that the training & development (*in the area of cyber security*) of employees, executive management and board of directors in an organization both in the private and public sector has become a matter of strategic importance. The fact that organizations and or government departments possess personal valuable information in their database systems ultimately puts immense pressure on both private and public sector organizations to make cyber security training of employees/personnel a key priority. When cyber security training is made a key priority in both the private and public sector organizations it helps them to stay one step ahead in the fights against cyber crime or threats. It can also be concluded that in order for any training & development program to be successful in any organization (*both in the private and public sector*) it must be aligned with the objectives of the trainees (*employees, executive management & board of directors*) and the organization. One of the key aim of carrying-out cyber security informative training in an organization is to educate employees, executive management & board of directors about the critical role they can play to implement cyber security and what is expected of them to do it in-good faith. The two most effective methods of carrying-out training in an organization include: 'on-the-job' and 'off-the-job' training methods.

[89] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

4.8 Discussion questions

1) Define the term ‘data security’ & ‘digital preservation’? Identify the differences between ‘public data’, ‘public network infrastructure’, ‘public switched telephone network’, ‘security risk’, ‘security risk appetite’ & ‘security risk management’?

2) Discuss the objectives of training & development in an organization? Describe the key methods of training?

3) Explain what is Cyber security informative training?

Chapter 5: Cryptograph

After reading this chapter you should be able to:

- Define the following terms ‘key material’ & ‘key management’.
- Differences between ‘cryptographic algorithm’, ‘cryptographic equipment’, ‘cryptographic hash’, ‘cryptographic protocol’, ‘cryptographic software’ & ‘cryptographic system’.
- Explain how to implement cryptography in a private or public sector organization

5.1 Introduction

Traditionally cyber criminals have for the past decades used simple activities such as hacking to breach communications privacy. When cyber criminals breach communications privacy for individuals or organizations (*for instance in their database management system, email network, telephone infrastructure and so on*) the negative consequences that are experienced by the victims are severe and in certain instances some organizations end up closing down their operations and or alternatively they experience prolonged public relations crisis’s. The arrival of cryptography as a cyber security tool that individuals and organizations can use to protect their data or communications has significantly reduced security risks and threats to cyber crime. In general the magnificence of cryptography is that it keeps evolving to become much better in order to block any previous vulnerabilities that were allowing cyber criminals to successfully breach communications privacy for individuals or organizations. Today cryptography is a cost saving activity in organizations since it helps to protect the organization from: (1) fraud related incidences, (2) litigation costs as a result of leakages of confidential customers information and (3) it also helps to protect the image of the organization from bad publicity (*for instance it helps to avoid bad incidences such as fraud or hacking*). The following section will cover aspects about the definition of terms in-depth.

5.2 Define the following terms 'key material' & 'key management'

There are various definitions in the field of cryptography and in general the simplifying of terms helps readers to easily grasp the meaning, usage and logic of each term. [90]"*Key material* - Cryptographic keys generated or used by cryptographic equipment or software. *Key management* – The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction" (Australian Cyber Security Centre – Information Security Manual, 2022:167). The following section will cover aspects about the differences in six cryptography terminology in-depth.

5.3 Differences between 'cryptographic algorithm', 'cryptographic equipment', 'cryptographic hash', 'cryptographic protocol', 'cryptographic software' & 'cryptographic system'

It is important to point-out the fact that there is a high distinction between the terms 'cryptographic algorithm', 'cryptographic equipment', 'cryptographic hash', 'cryptographic protocol', 'cryptographic software' & 'cryptographic system'. In general it is more likely that some people (or professionals) may confuse these six terms and end up assuming they share the same meaning whilst this assumption is not correct. Table 5.1 below will help to explain the key difference between six cryptography terminology in-depth.

[90] Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

Table 5.1 Differences of terms explained

Term	Explanation
"cryptographic algorithm	An algorithm used to perform cryptographic functions, such as encryption, integrity, authentication, digital signatures or key establishment.
cryptographic equipment	A generic term for commercial cryptographic equipment and High Assurance Cryptographic Equipment
cryptographic hash	An algorithm (the hash function) which takes as input a string of any length (the message) and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
cryptographic protocol	An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, authentication and non-repudiation of data.
cryptographic software	Software designed to perform cryptographic functions.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage and the administrative framework in which it operates" (Australian Cyber Security Centre – Information Security Manual, 2022:163).

Source: Table Created By The Author Using Information From: (Australian Cyber Security Centre – Information Security Manual, 2022:163, https://www.cyber.gov.au).

The next section will cover aspects about how to implement cryptography in a private or public sector organization.

5.4 How to implement cryptography in a private or public sector organization

[91]““**Guidelines for Cryptography. Cryptographic fundamentals**. Purpose of cryptography. The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data. In doing so, confidentiality protects data by making it unreadable to all but authorised entities, integrity protects data from accidental or deliberate manipulation by entities, authentication ensures that an entity is who they claim to be, and non-repudiation provides proof that an entity performed a particular action. Using encryption. Encryption of data at rest can be used to protect sensitive or classified data stored on ICT equipment and media. In addition, encryption of data in transit can be used to protect sensitive or classified data communicated over public network infrastructure. However, when an organisation uses encryption for data at rest, or data in transit, they are not reducing the sensitivity or classification of the data, they are simply reducing the immediate consequences of the data being accessed by an adversary. [92]Cryptographic key management processes and procedures. Well documented cryptographic key management processes and procedures can assist with the secure use and management of cryptographic keys and associated hardware and software. In doing so, cryptographic key management processes and procedures should cover cryptographic key generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction. Encrypting data at rest. When encryption is applied to data at rest it provides an additional layer of defence against unauthorised access by an adversary. In doing so, it is important that full disk encryption is used as it provides a greater level of protection than file-based encryption. This is due to the fact that while file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system.

[91] Australian Government: Australian Signals Directorate - Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Cryptography.* Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography [Accessed July 29, 2022] © Commonwealth of Australia 2022.

[92] Control: ISM-0507; Revision: 4; Updated: Jun-22; Applicability: All; Essential Eight: N/A
Cryptographic key management processes, and supporting cryptographic key management procedures, are developed and implemented.

When selecting cryptographic equipment or software for this purpose, the level of assurance required will depend on the sensitivity or classification of the data. Encrypting data in transit. When data is communicated over network infrastructure, encryption should be used to protect the data from unauthorised access or manipulation. When selecting cryptographic equipment or software for this purpose, the level of assurance required will depend on the sensitivity or classification of the data and the environment in which it is being applied. Data recovery. To ensure that access to encrypted data is not lost due to the loss, damage or failure of an encryption key, it is important that where practical cryptographic equipment and software provides a means of data recovery. Handling encrypted ICT equipment and media. When a user authenticates to the encryption functionality of ICT equipment or media, encrypted data is made available. At such a time, the ICT equipment or media should be handled according to its original sensitivity or classification. Once the user deauthenticates from the encryption functionality, such as shutting down a device or activating a lock screen, the ICT equipment or media can be considered to be protected by the encryption functionality again. Transporting cryptographic equipment. Transporting cryptographic equipment in a keyed state may expose its keying material to potential compromise. Therefore, if cryptographic equipment is transported in a keyed state it should be done based on the sensitivity or classification of its keying material. [93]Reporting cryptographic-related cyber security incidents. If cryptographic equipment or associated keying material is compromised, or suspected of being compromised, then the confidentiality and integrity of previous and future communications may also be compromised. In such cases, the cyber security incident should be reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs and all keying material should be changed"" (Australian Government: Australian Signals Directorate - Australian Cyber Security Centre – Information Security Manual, 2022, https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography). © Commonwealth of Australia 2022. The conclusion of this chapter will be covered in the following section.

[93] Australian Government: Australian Signals Directorate - Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Cryptography.* Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography [Accessed July 29, 2022] © Commonwealth of Australia 2022.

5.5 Conclusion

It can be concluded that breaches in communications privacy or cyber crime targeting organizations or individuals has severe consequences on the victims. Cryptography is now one of the most effective technology tool that can be used by organizations to protect data or communications infrastructure. One key advantage of cryptography is that it helps protect the organization from: fraud related incidences and it also helps to maintain a positive image of the organization.

5.6 Discussion questions

1) Define the following terms 'key material' & 'key management'?

2) Differences between 'cryptographic algorithm', 'cryptographic equipment', 'cryptographic hash', 'cryptographic protocol', 'cryptographic software' & 'cryptographic system'?

3) Explain how to implement cryptography in a private or public sector organization?

References:

Chapter 1

1) Britannica (2022) *Cyber*. Available from: https://www.britannica.com/dictionary/cyber- [Accessed May 07, 2022] © 2022 Encyclopædia Britannica, Inc.
2) Britannica (2022) *Information*. Available from: https://www.britannica.com/dictionary/information [Accessed May 07, 2022] © 2022 Encyclopædia Britannica, Inc.
3) Canadian Anti-Fraud Centre (2022) *Canadian Anti-Fraud Centre.* Available from: https://www.antifraudcentre-centreantifraude.ca [Accessed May 21, 2022]
4) Canadian Centre for Cyber Security (2022) *Cyber Threats and Cyber Threat Actors.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
5) Canadian Centre for Cyber Security (2022) *About.* Available from: https://cyber.gc.ca/en/ [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
6) Canadian Centre for Cyber Security (2022) *Ransomware.* Available from: https://cyber.gc.ca/en/glossary/ransomwire [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
7) Canadian Centre for Cyber Security (2022) *Phishing.* Available from: https://cyber.gc.ca/en/glossary/phishing [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
8) Canadian Centre for Cyber Security (2022) *Cyber Threats.* Available from: https://cyber.gc.ca/en/glossary/cyber-threat [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
9) Canadian Centre for Cyber Security (2022) *Cyber Threat Surface.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-surface [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

10) Canadian Centre for Cyber Security (2022) *Cyber Threat Activities.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-activities [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
11) Canadian Centre for Cyber Security (2021) *Have you Been a Victim of Cyber Crime.* Available from: https://cyber.gc.ca/en/guidance/have-you-been-victim-cybercrime [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).
12) Canadian Centre for Cyber Security (2022) *Spotting Malicious Email Messages (ITSAP00100).* Available from: https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

Chapter 2

1) Canadian Centre for Cyber Security (2022) Annex *Cyber Threat Toolbox.* Available from: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
2) Canadian Centre for Cyber Security (2022) *Cyber security tips for remote work (ITSAP.10.116).* Available from: https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
3) Canadian Centre for Cyber Security (2022) *Benefits and Risks of Adopting Cloud-Based Services in Your Organization (ITSE.50.060)*. Available from: https://cyber.gc.ca/en/guidance/benefits-and-risks-of-adopting-cloud-based-services-in-your-organization-itse50060 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
4) Canadian Centre for Cyber Security (2022) *Models of Cloud Computing (ITSAP.50.111)*. Available from: https://cyber.gc.ca/en/guidance/models-of-cloud-computing-itsap50111 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

5) Canadian Centre for Cyber Security (2022) *Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)*. Available from: https://cyber.gc.ca/en/guidance/cyber-security-considerations-of-consumers-of-managed-services [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
6) Canadian Centre for Cyber Security (2022) *Security Considerations for Mobile Device Deployments (ITSAP.70.002*. Available from: https://cyber.gc.ca/en/guidance/security-considerations-for-mobile-device-deployments.itsap70002 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
7) Canadian Centre for Cyber Security (2022) *VPN.* Available from: https://cyber.gc.ca/en/glossary/VPN [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
8) Canadian Centre for Cyber Security (2022) *Virtual Private Networks (ITSAP.80.101).* Available from: https://cyber.gc.ca/en/guidance/virtual-private-networks-itsap80101 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
9) Canadian Centre for Cyber Security (2022) *Security Tips for Peripheral Devices (ITSAP.70.015).* Available from: https://cyber.gc.ca/en/guidance/security-tips-for-peripheral-devices-itsap70015 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
10) Canadian Centre for Cyber Security (2022) *Sanitization and Disposal of Electronic Devices (ITSAP.40.006).* Available from: https://cyber.gc.ca/en/guidance/sanitization-and-disposal-of-electronic-devices-itsap40006 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
11) Canadian Centre for Cyber Security (2022) *Website Defacement (ITSAP.00.060).* Available from: https://cyber.gc.ca/en/guidance/website-defacement-itsap00060 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

12) Canadian Centre for Cyber Security (2022) *Managing and Controlling Administrative Privileges (ITSAP.10.094).* Available from: https://cyber.gc.ca/en/guidance/managing-and-controlling-administrative-previleges-itsap10094 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
13) Canadian Centre for Cyber Security (2022) *Cyber Security at Home and in the Office: Secure Your Devices, Computers and Networks (ITSAP.00.007).* Available from: https://cyber.gc.ca/en/guidance/cyber-security-at-home-and-in-the-office-secure-your-devices-computers-and-networks-itsap00007 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
14) Canadian Centre for Cyber Security (2022) *Worm.* Available from: https://cyber.gc.ca/en/glossary/Worm [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
15) Canadian Centre for Cyber Security (2022) *Authentication.* Available from: https://cyber.gc.ca/en/glossary/Authentication [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
16) Canadian Centre for Cyber Security (2022) *Antivirus software.* Available from: https://cyber.gc.ca/en/glossary/Anti-virus-software [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
17) Canadian Centre for Cyber Security (2022) *Phishing.* Available from: https://cyber.gc.ca/en/glossary/phishing [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
18) Canadian Centre for Cyber Security (2022) *Two factor authentication.* Available from: https://cyber.gc.ca/en/glossary/Two-facor-authentication [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
19) Canadian Centre for Cyber Security (2022) *Baseline Cyber Security Controls for Small and Medium Organizations.* Available from: https://cyber.gc.ca/en/guidance/baseline-

cyber-security-controls-for-small-and-medium-organizations [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

20) Canadian Centre for Cyber Security (2022) *Home.* Available from: https://cyber.gc.ca/eic/site/137.nsf/eng/home [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
21) Canadian Centre for Cyber Security (2022) *Developing your IT recovery plan.* Available from: https://cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
22) Canadian Centre for Cyber Security (2022) *Trojan.* Available from: https://cyber.gc.ca/en/glossary/Trojan [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
23) Canadian Centre for Cyber Security (2022) *Keystroke logger.* Available from: https://cyber.gc.ca/en/glossary/Keystrokelogger [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
24) Canadian Centre for Cyber Security (2022) *Ransomware.* Available from: https://cyber.gc.ca/en/glossary/ransomware [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
25) Canadian Centre for Cyber Security (2022) *Malware.* Available from: https://cyber.gc.ca/en/glossary/malware [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
26) Canadian Centre for Cyber Security (2022) *Virus.* Available from: https://cyber.gc.ca/en/glossary/virus [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
27) Canadian Centre for Cyber Security (2022) *Phishing.* Available from: https://cyber.gc.ca/en/glossary/phishing [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

28) Canadian Centre for Cyber Security (2022) *Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030).* Available from: https://cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-with-multi-factor-authentication-itsap30030 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

29) Canadian Centre for Cyber Security (2022) *Best Practices for Passphrases and Passwords (ITSAP.30.032).* Available from: https://cyber.gc.ca/en/guidance/best-practices-for-passphrases-and-passwords-itsap.30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

30) Canadian Centre for Cyber Security (2022) *Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036).* Available from: https://cyber.gc.ca/en/guidance/rethink-your-password-habits-to-protect-your-accounts-from-hackers-itsap30036 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

31) Canadian Centre for Cyber Security (2022) *Cyber Threats and Cyber Threat Actors.* Available from: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

32) Canadian Centre for Cyber Security (2020) *Protect your organization from malware (ITSAP.00.057).* Available from: https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2020).

33) Canadian Centre for Cyber Security (2019) *Best practices for passphrases and passwords (ITSAP.30.032).* Available from: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2019).

34) Canadian Centre for Cyber Security (2021) *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035).* Available from: https://cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-

organizations-itsap10035 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).

Chapter 3

1) Canadian Centre for Cyber Security (2022) Annex *Cyber Threat Toolbox.* Available from: https://cyber.gc.ca/en/guidance/annex-cyber-threat-toolbox [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
2) Canadian Centre for Cyber Security (2022) *How to Identify Misinformation, Disinformation and Malinformation.* Available from: https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
3) Canadian Centre for Cyber Security (2022) *Mobile device guidance for high profile travellers (ITSAP.00.088).* Available from: https://cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
4) Canadian Centre for Cyber Security (2021) *Using bluetooth technology (ITSAP.00.011)***.** Available from: https://cyber.gc.ca/en/guidance/using-bluetooth-technology-itsap00011 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2021).
5) Canadian Centre for Cyber Security (2022) *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi.* Available from: https://cyber.gc.ca/en/guidance/Protecting-your-organization-while-using-wi-fi-itsap8009 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
6) Canadian Centre for Cyber Security (2022) *ITSAP.00.099 Ransomware: How to Prevent and Recover.* Available from: https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).

7) Canadian Centre for Cyber Security (2022) *ITSAP.00.100 Don't Take the Bait: Recognize and Avoid Phishing Attacks.* Available from: https://cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
8) Canadian Centre for Cyber Security (2022) *Ransomware.* Available from: https://cyber.gc.ca/en/glossary/Ransomware [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
9) Canadian Centre for Cyber Security (2022) *VPN.* Available from: https://cyber.gc.ca/en/glossary/VPN [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
10) Canadian Centre for Cyber Security (2022) *Phishing.* Available from: https://cyber.gc.ca/en/glossary/Phishing [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
11) Canadian Centre for Cyber Security (2022) *ITSAP.00.001 Using Your Mobile Device Securely.* Available from: https://cyber.gc.ca/en/guidance/using-your-mobile-device-securely-itsap00001 [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (National Defence), (2022).
12) Global Affairs Canada (GAC) (2022) *Global Affairs Canada*. Available from: https://travel.gc.ca/travelling/advisories [Accessed May 21, 2022] © Her Majesty the Queen in Right of Canada, as represented by the Minister of (Global Affairs), (2022).

Chapter 4

1) Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.
2) Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Personnel Security*. Available from: https://www.cyber.gov.au/acsc/view-

all-content/advice/guidelines-personnel-security [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022

3) Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.

4) Control: ISM-1565; Revision: 0; Updated: Jun-20; Applicability: All; Essential Eight: N/A Tailored privileged user training is undertaken annually by all privileged users.

5) Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight

6) Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.

7) Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

8) Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: N/A Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.

9) Control: ISM-0824; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A Personnel are advised not to send or receive files via unauthorised online services.

10) Control: ISM-1146; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A Personnel are advised to maintain separate work and personal accounts for online services.

11) Control: ISM-0432; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A Access requirements for a system and its resources are documented in its system security plan.

12) Control: ISM-0434; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A Personnel undergo appropriate employment screening and, where necessary, hold

an appropriate security clearance before being granted access to a system and its resources.

13) Control: ISM-0435; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A Personnel receive any necessary briefings before being granted access to a system and its resources.

14) Control: ISM-0414; Revision: 4; Updated: Aug-19; Applicability: All; Essential Eight: N/A Personnel granted access to a system and its resources are uniquely identifiable.

15) Control: ISM-0415; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

16) Control: ISM-1583; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Personnel who are contractors are identified as such.

17) Control: ISM-0420; Revision: 11; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A Where a system processes, stores or communicates AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.

18) Control: ISM-0405; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A Requests for unprivileged access to systems, applications and data repositories are validated when first requested.

19) Control: ISM-1566; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A Use of unprivileged access is logged.

20) Control: ISM-1714; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A Unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

21) Control: ISM-0409; Revision: 8; Updated: Jun-22; Applicability: S, TS; Essential Eight: N/A Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL data unless effective controls are in place to ensure such data is not accessible to them.

22) Control: ISM-0411; Revision: 7; Updated: Jun-22; Applicability: S, TS; Essential Eight: N/A Foreign nationals, excluding seconded foreign nationals, do not have access to

systems that process, store or communicate AGAO data unless effective controls are in place to ensure such data is not accessible to them.

23) Control: ISM-1507; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3. Requests for privileged access to systems and applications are validated when first requested.
24) Control: ISM-1508; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML3 Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.
25) Control: ISM-1175; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Privileged user accounts are prevented from accessing the internet, email and web services.
26) Control: ISM-1733; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A Requests for privileged access to data repositories are validated when first requested.
27) Control: ISM-1653; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3 Privileged service accounts are prevented from accessing the internet, email and web services.
28) Control: ISM-1649; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3 Just-in-time administration is used for administering systems and applications.
29) Control: ISM-0445; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.
30) Control: ISM-1509; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Use of privileged access is logged.
31) Control: ISM-1650; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Changes to privileged accounts and groups are logged.
32) Control: ISM-1651; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3 Privileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

33) Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.
34) Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.
35) Control: ISM-0430; Revision: 7; Updated: Sep-19; Applicability: All; Essential Eight: N/A Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.
36) Control: ISM-1591; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.
37) Control: ISM-1404; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A Unprivileged access to systems and applications is automatically disabled after 45 days of inactivity.
38) Control: ISM-1648; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Privileged access to systems and applications is automatically disabled after 45 days of inactivity.
39) Control: ISM-1716; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A Access to data repositories is automatically disabled after 45 days of inactivity.
40) Control: ISM-1647; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3 Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.
41) Control: ISM-1734; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A Privileged access to data repositories is automatically disabled after 12 months unless revalidated.
42) Control: ISM-0407; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
43) Control: ISM-0441; Revision: 8; Updated: Jun-22; Applicability: All; Essential Eight: N/A When personnel are granted temporary access to a system, effective controls are

put in place to restrict their access to only data required for them to undertake their duties.

44) Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicability: S, TS; Essential Eight: N/A Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

45) Control: ISM-1610; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

46) Control: ISM-1611; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Break glass accounts are only used when normal authentication processes cannot be used.

47) Control: ISM-1612; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Break glass accounts are only used for specific authorised activities.

48) Control: ISM-1614; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Break glass account credentials are changed by the account custodian after they are accessed by any other party.

49) Control: ISM-1615; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A Break glass accounts are tested after credentials are changed.

50) Control: ISM-1613; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A Use of break glass accounts is logged.

51) Control: ISM-1715; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A Break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

52) Further information on access to government resources, including required security clearances, can be found in the Attorney-General's Department's Protective Security Policy Framework, Access to information policy.

53) Further information on access to highly sensitive government resources, including required briefings, can be found in the Government Security Committee's *Australian Government Security Caveat Guidelines*. This publication is available from the Protective

Security Policy GovTEAMS community or the Australian Security Intelligence Organisation by email.

54) Further information on restricting the use of privileged accounts can be found in the ACSC's Restricting Administrative Privileges publication.

55) Further information on event logging can be found in the event logging and monitoring section of the Guidelines for System Monitoring.

56) Further information on telephone system usage can be found in the telephone systems section of the Guidelines for Communications Systems.

57) Further information on fax machine and multifunction device usage can be found in the fax machines and multifunction devices section of the Guidelines for Communications Systems.

58) Further information on mobile device usage can be found in the mobile device usage section of the Guidelines for Enterprise Mobility.

59) Further information on removable media usage can be found in the media usage section of the Guidelines for Media.

60) Further information on email usage can be found in the email usage section of the Guidelines for Email.

61) Further information on web usage can be found in the web proxies section of the Guidelines for Gateways.

62) Further information on detecting socially engineered messages be found in the Australian Cyber Security Centre (ACSC)'s Detecting Socially Engineered Messages publication.

63) Further information on business email compromise can be found in the ACSC's Protecting Against Business Email Compromise publication.

64) Further information on the use of social media can be found in the ACSC's Security Tips for Social Media and Messaging Apps publication.

65) Further information on the sanitisation of documents before posting them to authorised online services can be found in the ACSC's An Examination of the Redaction Functionality of Adobe Acrobat Pro DC 2017 publication.

66) Human Resources Institute of New Zealand (2018) *Coaching.* Available from:https://www.hrinz.org.nz/Site/My_HR_Career/Coaching/What_is_Coaching.aspx [Accessed 2018, 03 May]

67) Rudolph. Patrick. Tawanda. Muteswa (2019) *The Importance of Human Resources Management & Business Leadership in the Boardroom (Gathered Articles): A North America, Asia, Africa, Oceania & Europe Perspective* 1st Edition, Educational EBook, ISBN 978-1-77920-215-4, p1-305.

Chapter 5

1) Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Information Security Manual*. Available from: https://www.cyber.gov.au/sites/default/files/2022-06/Information%20Security%20Manual%20%28June%202022%29.pdf [Accessed July 29, 2022] p1-177, © Commonwealth of Australia 2022.
2) Australian Cyber Security Centre – Information Security Manual (ISM) (2022) *Guidelines for Cryptography.* Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography [Accessed July 29, 2022] © Commonwealth of Australia 2022.
3) Control: ISM-1080; Revision: 5; Updated: Jun-22; Applicability: All; Essential Eight: N/A An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.
4) Control: ISM-0507; Revision: 4; Updated: Jun-22; Applicability: All; Essential Eight: N/A Cryptographic key management processes, and supporting cryptographic key management procedures, are developed and implemented.
5) Control: ISM-0501; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.
6) Control: ISM-0142; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.

7) Control: ISM-1091; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A Keying material is changed when compromised or suspected of being compromised.
8) Control: ISM-0469; Revision: 6; Updated: Jun-22; Applicability: All; Essential Eight: N/A An ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect data when communicated over network infrastructure.
9) Control: ISM-0462; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A When a user authenticates to the encryption functionality of ICT equipment or media, it is treated in accordance with its original sensitivity or classification until the user deauthenticates from the encryption functionality.
10) Control: ISM-0455; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A Where practical, cryptographic equipment and software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.
11) Control: ISM-0465; Revision: 9; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.
12) Control: ISM-0467; Revision: 10; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A HACE is used to protect SECRET and TOP SECRET data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.
13) Control: ISM-0457; Revision: 9; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.
14) Control: ISM-0460; Revision: 11; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A HACE is used when encrypting media that contains SECRET or TOP SECRET data.

15) Control: ISM-0459; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition, is implemented when encrypting data at rest.
16) Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules and National Institute of Standards and Technology (NIST) Special Publication (SP) 180-140, FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 are United States standards based upon ISO/IEC 19790:2012 and ISO/IEC 24759:2017.
17) Further information on cryptographic key management practices can be found in NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 – General.
18) Further information on cryptographic key management practices for HACE is available from the ACSC.
19) Further information on evaluated products can be found in the evaluated product acquisition section of the Guidelines for Evaluated Products.
20) Further information on the evaluation of cryptographic modules, including testing requirements, is available as part of the Cryptographic Module Validation Program which is jointly operated by NIST and the Canadian Centre for Cyber Security.
21) Further information on the protection of ICT equipment and media can be found in the Attorney-General's Department's Protective Security Policy Framework, Physical security for entity resources policy.
22) International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules, and ISO/IEC 24759:2017, Information technology – Security techniques – Test requirements for cryptographic modules, are international standards for the design and validation of hardware and software cryptographic modules.