Decrypting Ransomware

ANALYZING AND ADDRESSING THE THREAT IN THE CANADIAN CONTEXT

CHARLOTTE CARR
BARRY DENG
SAMI HUAYHUA
KRISTINA IBRAHIM
ALVI JAWAD
FELICITAS JUNG
DYLAN LEVEILLE
DANIELA NAPOLI
ANAÏS PICHÉ-BUSTROS
EMMET ROBINS
SAEED ROSTAMALIZADEH
MOHD SAQIB
MAHMOUD SELIM
DANE VANDERKOOI
CICILIA ZHANG
AND
DR. HALA ASSAL
DR.ANDRÉANNE BERGERON
DR. IVAN PUSTOGAROV

Human-Centric Cybersecurity Partnership

HUMAN-CENTRIC CYBERSECURITY REPORT PROJECT

The 2023 Human-Centric Cybersecurity Report Project brought together postgraduate students from across Canada to work with our partners from both private industry and the public sector to produce reports looking at the problem of ransomware through a transdisciplinary lens.

ABOUT HC2P

The Human-Centric Cybersecurity Partnership (HC2P) is a transdisciplinary group of scholars, government, industry and not-for-profit partners that generate research and mobilize knowledge that will help create a safer, more secure, more democratic and more inclusive digital society.

ACKNOWLEDGEMENTS

We would like to thank Accenture, Bell Canada, The Canadian Centre for Cyber Security (CCCS), Canadian Cyber Threat Exchange (CCTX), Desjardins, Field Effects, GoSecure, Innovation, Science and Economic Development Canada, The National Bank of Canada, The National Cybercrime Coordination Centre (NC3), Public Safety Canada, The Royal Canadian Mounted Police, Statistics Canada, The University of Montreal, and The University of Ottawa for their efforts in supporting this project.

Art by Michael Joyce

Cite as:

Carr, C., Deng, B., Huayhua, S., Ibrahim, K., Jawad, A., Jung, F., Leveille, D., Napoli, D., Piché-Bustros, A., Robins, E., Rostamalizadeh, Saqib, M., Selim, M., Vanderkooi, D., Zhang, C., Assal, H., Bergeron, A., & Pustogarov, I. (2023) Decrypting Ransomware: Analysing and Addressing the Threat in the Canadian Context, Human-Centric Cybersecurity Partnership (HC2P)

Dépôt légal,

ISBN: 978-1-7387249-3-2

The Human-Centric Cybersecurity Partnership is supported in part by funding from the Social Sciences and Humanities Research Council.

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

Canada

Contents

Decrypting Ransomware

ANALYZING AND ADDRESSING THE THREAT IN THE CANADIAN CONTEXT

Executive Summary

Ransomware is a problem that has grown to global proportions, regularly resulting in economic, social and personal harms. Ransomware represents an extortive malicious use of technology that involves and exploits human and social factors to achieve its ends. This report examines the problem of ransomware through a multi-disciplinary lens with the aim of uncovering novel aspects of the problem and shed light on potential new avenues for solutions.

Ransomware is revealed to be a phenomena that evolves when new technology emerges that facilitates successful evolutions of illicit practices. Particularly concerning are its impacts on Critical infrastructure, small businesses, and society generally through emergent harms. The technologies to mitigate ransomware generally exist, however they are often not known, not prioritized or not feasible for the public. There are good solutions to support ransomware mitigation but their implementation needs to be better understood and better resourced.

Key Recommendations

- Consider the impact of Ransomware as the initial event and the series of resulting indirect and emergent harms
- Society wide education to create awareness of not only ransomware and its mitigation but also the institutions in Canada that provide support before during and after a ransomware attack
- Include human-centric defense strategies into technical solutions such as through the use of deceptive technologies and active forensic measures
- Promote and maintain soft regulations (guidelines) for ransomware defense techniques such as backups and encryption at rest.
- Incentivize small businesses to adopt ransomware best practices by including cybersecurity planning in the small business loan and cyberinsurance assessment procedures
- Promote a Security-by-Design approach to application and systems development, to prioritize security at all stages of development
- Work towards cybersecurity training that promotes a collaborative response to ransomware such as communicating concerns and seeking help from IT personnel. These efforts should be customized to the individuals roles within the organization and can include interactive exercises, such as fire drills and table top exercises

> *"ransomware exposes a broad range of cybersecurity issues in a manner that other threats have not."*

1 Introduction

Ransomware is a cybersecurity problem that, by its very nature, demands attention. At its core, Ransomware is a type of malicious software or 'malware' that is designed to encrypt a victim's files and hold them hostage until a ransom is paid. However, the criminal enterprises that ransomware has enabled, those focused on extorting payment in return for the control of data have adopted a range of tools and techniques with which they ply their trade. So it is that ransomware now can be said to include a range of malicious activities that include the illicit installation of malware for the purposes of extracting financial rewards from a victim.

Consequently, ransomware exposes a broad range of cybersecurity issues in a manner that other threats have not. Its effects contrast starkly with the problem of cyberespionage, which while widespread does not result in system outages or the leakage of data. As a consequence, the harms related to cyberespionage are slower to arise and longer term in their effect and more tightly bound, in that they do not so immediately spawn a cascade of direct, indirect and emergent harms. The harms resulting from ransomware range from direct effects such as ransom payments and loss of revenue for e-commerce organizations, indirect effects including deaths due to hospital and emergency services outages and emergent effects such as the destabilization of trust in democratic processes following voting system failures.

The expanded nature of the operation of ransomware and its effects means that it is a grander problem that transcends technology. It affects and is affected by our society, regulation and behaviour in complex ways that require careful examination and influ-

ence our understanding of the problems and responses to it.

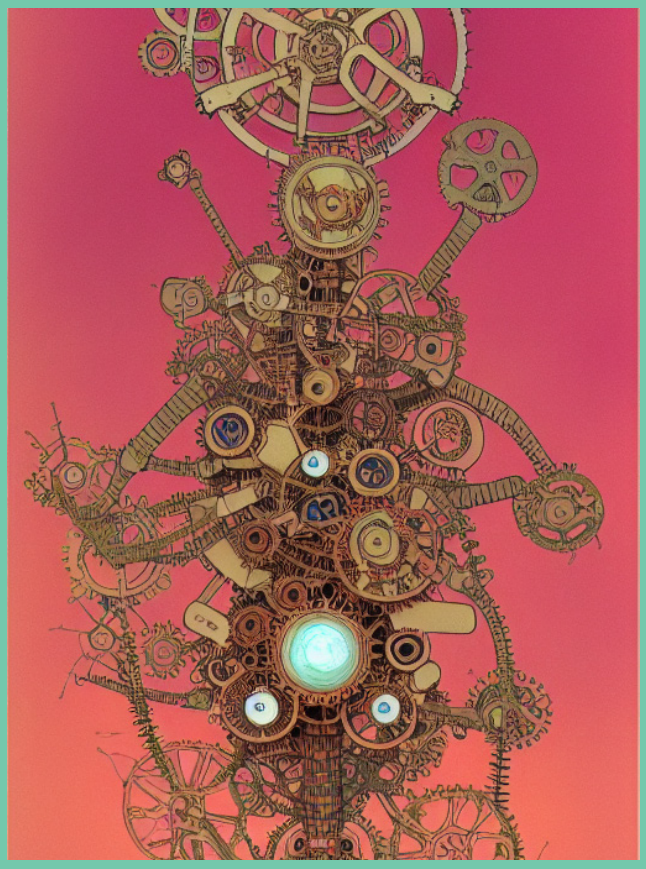
The Human-Centric Cybersecurity Partnership (HC2P) summer program investigated ransomware with each of three multidisciplinary teams focusing their efforts on one of these aspects. The program brought together the knowledge and experiences of expert cybersecurity practitioners and academic researchers from across Canada to guide the research efforts of fifteen graduate-students. This report represents the results of their investigations.

The first section of this report presents ransomware in the frame of its impacts on critical infrastructure in particular, and society in general. It harnesses an evolutionary lens to provide structure to the seemingly chaotic changes in ransomware enabling readers to better predict the future of ransomware development.

The next section examines regulation, both hard and soft in the light of the understood best practices for ransomware. It also focuses on small businesses to find existing mechanisms that could be adjusted to support these Canadian organizations, so they can implement and benefit from regulations that can help them both survive and mitigate ransomware attacks.

The final section highlights the behaviours that lead to ransomware attacks. In an approach that integrates technical and social systems, it identifies the behaviours that introduce vulnerabilities into systems and those that actualize those threats into attacks. By presenting the human involvement in both the creation and operation of technological systems, this section reveals a model of cyber security that highlights new dimensions of the cybersecurity puzzle.

Ransomware is a decades old problem that has grown to a global scale. The complexity of its operations and the severity of its impacts expose the need for solutions that have exceeded the capacities of purely technical fixes. We hope that by providing a human-centric cybersecurity window into the phenomena of ransomware we can inspire new thinking and new approaches that can effectively contribute to a reduction in the frequency and harms of ransomware attacks.



2 Society

2.1 Impact on Critical Infrastructure Sectors

Ransomware attacks on critical infrastructure remain a key security focus in Canada at various levels, including at the local level, from smaller municipalities and towns, all the way up to the federal level as a matter of national security. According to the Canadian Center for Cyber Security 2020 Cyber Threat Bulletin on ransomware, Canada is one of the top countries impacted by ransomware attacks (Canadian Centre for Cyber Security, 2020). Moreover, ransomware attacks against critical infrastructure are on the rise both in terms of their frequency and the ransom amounts demanded. As technological innovations such as artificial intelligence and cryptocurrencies empower hackers to develop more sophisticated forms of ransomware attacks, we must remain ever more vigilant. As such, it should come as no surprise that across the

— Society

past several years, ransomware attacks have affected hundreds of Canadian critical infrastructure service and product providers. The affected critical infrastructure industries range from the power and energy sector to hospitals and all levels of government. For example, in 2019 the Ontario municipal city of Woodstock suffered a loss of over 600,000 dollars CAD due to a ransomware attack that had shut down their computer systems (Saylors, 2019). In another instance, the Northwest Territories Power Corporation was subject to a ransomware attack which disrupted its email system and website (Strong, 2020). Thankfully, in this case, the actual power services were not disrupted, saving the surrounding communities from the potentially devastating impacts. Such a loss of service could have had impacts on the productivity as well as the health and safety of Canadians as such ransomware attacks targeting Canadian critical infrastructure pose a national security risk for Canadian society at large.

2.1.1 What constitutes Canadian Critical Infrastructure?

As of yet, there is not a universal consensus on what precisely constitutes critical infrastructure and consequently formal definitions vary between nations and among academics. We might broadly understand critical infrastructure as defined at a high level, as presented by Barack (2020) as comprising the *"facilities, information processes and systems upon which our society functions and depends"* (pg. 16).

A more detailed definition is provided by the Canadian federal government which provides that:

"Critical infrastructure (CI) refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence" (Public Safety Canada, 2023).

While this definition could be interpreted very broadly, the practical implications of critical infrastructure are more precisely outlined by the federal government which highlights ten specific sectors that make up Canadian critical infrastructure:

- Energy and Utilities
- Finance
- Food
- Government
- Health
- Information and Communication Technology
- Manufacturing
- Safety
- Transportation
- Water

In addition to their outline of what constitutes Canadian infrastructure, the government has numerous partnerships both foreign and do-

mestic that it works with to help prepare and prevent against cyberattacks targeting critical infrastructure (Public Safety Canada, 2023). Domestically, the federal government partners with several groups including:

- The National Cross Sector Forum (NCSF)
- Multi-Sector Network (MSN)
- Canadian Security Intelligence Service (CSIS)
- Communications Security Establishment (CSE)
- Canadian Centre for Cyber Security
- Public Safety Canada
- Government Operations Centre (GOC)
- Royal Canadian Mounted Police (RCMP)

At the provincial and territorial level, the Public Safety Canada partners with the following government groups:

- Alberta Emergency Management Agency
- Civil Protection, Minister of Public Security (QC)
- Emergency Management (NU)
- Emergency Management and Climate Readiness (B.C.)
- Emergency Management Office (NS)
- Emergency Management Ontario (ON)
- Emergency Management Organization (SK)
- Emergency Measures Organization (MB)
- Emergency Measures Organization (NB)
- Emergency Measures Organization (PEI)
- Emergency Measures Organization (YK)
- Emergency Preparedness (NWT)
- Emergency Services (NL)

At the international level, the Canadian government has partnered with several western governments to focus on critical infrastructure including the following nations:

- Australia
  - Australian Security Intelligence Organization
  - ASIO Business Liaison Unit
  - Trusted Information Sharing Network for Critical Infrastructure Protection
- United Kingdom
  - UK Resilience
  - UK Centre for the Protection of National Infrastructure (CPNI)
- United States
  - US Department of Homeland Security
  - Cybersecurity and Infrastructure Security Agency (CISA)
- New Zealand
  - NZ Department of the Prime Minister and Cabinet (DPMC)
  - NZ Treasury
  - National Infrastructure Unit

2.1.2 Ransomware Attacks Against Critical Infrastructure as a National Security Issue

Public Safety Canada considers critical infrastructure as a key part of their national security defence strategy which seeks to protect the lives and security of Canadians. As the federal government notes, disruptions of critical infrastructure may result in both a loss of life and economic activity which in turn erodes the health, security and safety of Canadians (Public Safety Canada, 2023). Beyond the government's scope, disruptions of critical infrastructure may have social, cultural and political implications such as the erosion of citizens' trust in key public and private institutions.

In terms of mitigating cyberattacks including ransomware against critical infrastructure, the Canadian government has outlined several strategic initiatives.

Public Safety Canada (2023) outlines a National Cyber Security Strategy which is a framework designed to guide the Canadian government to help protect both individuals and organizations from cyber threats, including ransomware attacks.

Another resource is the National Cyber Security Action Plan which serves as a blueprint for specifically implementing the National Cyber Security Strategy. A government program known as the Cyber Security Cooperation Program is an initiative that aims to provide financial support through grants and other funding contributions to assist in improving the security of Canada's critical cyber systems.

A fourth initiative are the Industrial Control Systems (ICS) Security Events whereby Public Safety Canada delivers ICS security events to help strengthen the resilience of critical infrastructure.

A fifth initiative is the Canadian Cyber Security Tool, which is designed for individual critical infrastructure leaders to take part in a self-assessment that can help identify the overall level of cyber-resilience of the specific organization and even offers comparisons of others in the same sector (i.e., banking).

A sixth initiative is the Cy-Phy Exercise Program which can help measure and evaluate how various cyber events may impact critical infrastructure and is open to critical infrastructure leaders. A seventh resource available to critical infrastructure stakeholders is the Critical Infrastructure Gateway, which provides an online portal for critical infrastructure leaders to share information with each other, and also gain access to information and material to enhance awareness concerning various threats and vulnerabilities.

A final initiative is a more recent one known as the Consulting on Canada's Approach to Cyber Security which is an open opportunity for both individuals and organizations to directly contribute their specific knowledge and experience in both cybersecurity in general and the cybercrime environment in relation to how it has impacted themselves, their organization and surrounding communities.

These resources are all available to members of the public to access and learn more about and reflect the Canadian government's commitment to including critical infrastructure as a key component of their overall nation-

al security strategy. Even presently, the government has current and planned future initiatives to increase cyber resilience among critical infrastructure. On the legislative side, in 2022 the government introduced Bill C-26 which amends the Telecommunication Act to modernize the act to reflect the current cyber landscape. A second component introduces the Critical Cyber Systems Protection Act (CCSPA) which aims to develop a regulatory framework to strengthen baseline cybersecurity with regard to critical infrastructure (Justice Canada, 2022).

2.1.3 Vulnerabilities Exposed by Critical Infrastructure

Critical infrastructure in a broad sense, suffers from several key cybersecurity vulnerabilities that create susceptibility with respect to ransomware cyberattacks. At a technical level, academics point to technical vulnerabilities created by industrial control systems which have been integrated into public network systems (Zimba et al., 2018). Older systems were often segmented and isolated from core network system while more modern systems are often fully integrated, meaning if an individual gains access to the general network, they are more easily able to access the industrial control systems. Another key technical vulnerability is legacy systems and the transitioning process toward newer systems. It is not uncommon to find even key critical infrastructures operating on older systems (e.g., Windows 2000), which may no longer be updated to fix security flaws. Such technical issues arise from the upward trends in systems digitization and consolidation and are consequently unlikely be easily resolved.

There are also additional vulnerabilities posed by the inherent human element in any system. In the context of ransomware attacks against critical infrastructure, this manifests in several ways. Humans are at risk of particular forms of cyber-attacks that involve a social interaction component, such as social engineering, which employs several psychological strategies, such as exploiting a tendency towards obedience to authority and ignorance to manipulate unwitting organizational insiders to contribute to harming critical infrastructure (Ghafir et al., 2018). While it may be tempting to question the ignorance of cybersecurity technical controls, it should be understood that many of today's modern critical infrastructure management systems are run by non-technical people such as a teacher using an online e-learning system or a nurse using an IoT patient monitoring system (Ghafir et al., 2018). The difficulties for people attempting effectively manage cybersecurity considerations can be exacerbated by workplace factors such as stress, burnout and security fatigue, wherein employees are simply tired of dealing with security initiatives such as training (Nobles, 2022). Furthermore, as an attacker's success may only depend on a single action on a computer within a network (such as clicking a link), malicious hackers can and take advantage of exceptional distractions such as an employee who may just be having a bad day or going through a divorce.

Another vulnerability presented to information systems by the human is the potential of malicious insider threats, or employees deliberately acting against the network. This might be motivated by bad feelings towards

the company, a disgruntled employee who was passed up for a promotion may knowingly run ransomware on a company system. Employees may even be bribed, for example a low-level employee could be incentivized with a large financial sum to make a few account changes. Both intentional and non-intentional insider threat actions can be leveraged by hackers to gain access to critical infrastructure systems. Together, both human and technical vulnerabilities inherent to modern critical infrastructure systems must be considered by relevant stakeholders if we as a society wish to improve cyber-resilience among these critical cyber systems.

2.2 The trickle-down effects of Ransomware

Ransomware is a type of malware that encrypts the victim's files and demands payment in exchange for the decryption key. While the immediate impact of a ransomware attack is often financial, the downstream effects can be far-reaching, affecting not only the victim but also society at large. Ransomware attacks can also be ideologically or politically motivated and threaten the state's democratic process. These effects can include data breaches and the disruption of essential services. While data extraction is increasingly common in ransomware attacks, data exploitation offers subsequent criminal opportunities for cybercriminals. Furthermore, the democratization of ransomware and artificial intelligence technologies is influencing the evolution of the cybercriminal ecosystem. In this section, we will explore the trickle-down effects of ransomware and its criminal downstream effects, as well as its impact on society at large.

2.2.1 Ransomware as a national security issue

The Canadian Centre for Cyber Security notes that cyber threat actors pose a significant risk to Canada's national security, critical infrastructure, and core institutions. According to the National Cyber Threat Assessment 2023-2024, critical infrastructure is increasingly at risk from cyber threat activity from both cybercriminals and state-sponsored actors (Canadian Centre for Cyber Security, 2023). While the motivation for criminal or financially motivated and politically motivated or state-sponsored actors might be different, they both target critical infrastructure.

2.2.1.1 Financially motivated Ransomware actors

The operation of cybercriminal activities has matured into a complex industry of individual and group actors that interact and exchange knowledge, technology and tools. This has led ransomware software and tools to be commercialized through a franchise business model on Darkweb markets, resulting in the democratization of this type of cybercrime (Meland & al., 2021). The growing "Ransomware-As-A-Service" (RaaS) model makes the use of ransomware techniques, tactics and tools more accessible. It allows malicious actors without technical skills to carry out ransomware attacks. This suggests that ransomware is getting more profitable, and that the "level of entry" to commit these crimes is lowering (Meland & al., 2021; Canadian Centre for Cyber Security, 2023). Consequently, ransomware activities are available to any actor with a financial motivation and a willingness to engage in illegal conduct.

Ransomware actors may target critical infrastructure and supply chains such as food, transportation, healthcare and energy because of their vital role in society's functioning and their short window of acceptable downtime, which could increase the pressure felt by these organizations to pay the ransom (Kay, 2021).

The low tolerance for downtime in Critical Infrastructure supply chains were well illustrated in the case of the ransomware attack on the Colonial Pipeline in 2021. The shutdown of the pipeline, which travels through fourteen US states, disrupted the transportation of oil, rapidly causing fuel shortages and price spikes (Salam, 2021). In turn, this led to national panic and an emergency declaration by the federal government. The company paid the 5$ million USD ransom one day after the attack (Wilkie, 2021).

A cyber-attack on the healthcare sector, such as a hospital, can disrupt information systems essential to the provision of care and jeopardize the security of patients' personal and health data, as well as medical confidentiality. When it causes the interruption of essential medical services, a cyber-attack can directly endanger patients' lives. Because of the risks inherent in cyberattacks on healthcare facilities, the cybersecurity of this type of infrastructure is a national security issue (Achten, 2021).

Cyberattacks against healthcare infrastructure have multiplied in recent years (Zhang-Kennedy & al., 2018; Achten, 2021; ANSSI, 2021; Lachaud, 2021). In 2017, when the WannaCry ransomware managed to infect over 300,000 computers in 150 countries, the British National Health Service (NHS) was affected and the operation of certain services severely impacted. In the USA, four hundred hospitals were reported to have had their computer systems attacked by the end of 2020, causing the permanent closure of at least one hospital (CSIS, 2023).

The impact on society can be harmful, with patients being particularly affected. A 2021 ransomware attack successfully targeted a database managing almost 30 healthcare facilities in Israel. The company responsible for managing this database refused to pay the ransom, which ultimately led to the leak of 290,000 medical records (Achten, 2021). In France, between 2019 and 2021, at least five healthcare centers were reported to have fallen victim to ransomware attacks (Lachaud, 2021). These attacks rendered computer systems unusable, blocked access to medical data, patient contact details, and the software enabling radiotherapy and oncology treatments to be carried out. Vaccination centers against CoVid-19 had to be suspended at the height of the pandemic, surgical procedures had to be rescheduled, and patients admitted to emergency departments had to be redirected elsewhere.

Canada is not immune from financially motivated attacks against healthcare. On October 30, 2021, amid the Covid-19 global pandemic, the computer network of the Newfoundland and Labrador health system fell victim to a ransomware attack (Department of Health and Community Services, 2023). Within a fortnight, the attackers had managed to infiltrate the healthcare network's IT domains using a VPN connection, increased their access and then exfiltrated data from the environment, includ-

ing patient medical records and other personal information. The attack is said to have resulted in computer failure and consequently major disruptions across the province's healthcare network, including blocking access to medical records and delaying thousands of medical appointments and procedures (Department of Health and Community Services, 2023).

2.2.1.2 Politically motivated ransomware Actors

The essential nature of CI operations also makes it a prime target for attackers seeking to disrupt the company or cause societal harm. Adversary states may use their cyber capabilities to target democratic institutions and conduct espionage and foreign interference activities against the state to promote their political, economic, military, security and ideological interests, as well as to undermine public confidence in public institutions (Canadian Centre for Cyber Security, 2023).

In April 2023, the National Security Agency (NSA) reported that it had identified ransomware attacks by Russian groups aimed primarily at Ukraine and other European countries that had lent their support to Ukraine (CSIS, 2023). Similarly, a report recently published by Stanford University highlights the political nature of double-extortion attacks perpetrated by ransomware groups. The groups based in Russia reportedly increased the frequency of their attacks prior to elections in major democracies, including Canada (Nershi & Grossman, 2023). A ransomware attack launched during an election period can serve an election meddling and political interference purpose. This can be illustrated by the case of the Louisiana's 2019 gubernatorial election, where a ransomware attack was launched hours after the polls closed. This caused 10% of government computers to go down, followed by the declaration of the state emergency. Although the ransomware group had accessed servers across the state months earlier, they waited six days before the election to launch their attack. The election process ultimately went its course, but this incident had the potential to fuel doubt and mistrust in the election process, undermining public confidence in the country's democratic process (Mehrotra, 2020; Nershi & Grossman, 2023).

The study also found that companies that had curtailed or suspended their activities in Russia following the invasion of Ukraine were more likely to fall victim to attacks by Russian ransomware groups (Nershi & Grossman, 2023).

While these groups are arguably not state-sponsored, an analysis of leaked messages between members of the Conti ransomware group revealed that its leaders maintained links with certain members of the Kremlin, and that the group had reportedly cooperated with the Russian government in at least one state-sponsored cyber-operation (Nershi & Grossman, 2023). The authors concluded that the Kremlin maintains decentralized yet cooperative relations with Russian ransomware groups (Nershi & Grossman, 2023), in addition to benefiting from cyberattacks targeting Western states (Orenstein, 2022). This finding strongly suggests that some cybercriminal groups may commit attacks guided by political ideologies or allegiances.

Intermingled financial and political motivations also can be found with ransomware groups that are more directly state-sponsored. This is the

case with the Lazarus group, a hacking group created and backed by the North Korean state (US. Department of the Treasury, 2019). The group is known for its high-profile cyber attacks such as the Sony hack in 2014 and the WannaCry ransomware attack in 2017 (US. Department of the Treasury, 2019). The Lazarus Group is considered a "state-sponsored hacking organization" by the United States Federal Bureau of Investigation (Hutton, 2023). The group is financially motivated as well as driven by efforts to support North Korea's state objectives (US. Department of the Treasury, 2019), which include military research, industrial espionage, intellectual property theft and the evasion of international sanctions (Page, 2022).

2.2.2 Criminal Downstream Effects

According to Porcedda and Wall (2019), big data and cybercrime allow for "'upstream' big data related cyber-dependent crimes such as data breaches" (p.443). Cyber criminality can be conceived as a perpetually evolving ecosystem that "cascades 'downstream' to give rise to further crimes" (Porcedda and Wall, 2019, p.443). In the same way, a ransomware attack does not simply end when the ransom is paid – rather, data extraction renders new subsequent criminal opportunities where the data can be further exploited for monetization (VMWare, 2022 ; Canadian Center for Cybersecurity, 2023). Data breaches can be harnessed for double-extortion, phishing and spear-phishing, intellectual property theft and more recently, deep fake attacks. In turn, additional criminal prospects arise from these new cyber-attacks.

Double extortion, an increasingly common tactic used by ransomware attackers, happens when cybercriminals use the extracted data for extortion by threatening to release sensitive information if their demands are not met (VMware, 2022). After paying the ransom, victims have no guarantee their data aren't still in the hands of the attacker. This can result in further blackmail and extortion, putting pressure on the victim to pay more ransom money after the initial ransom payment. Moreover, it's possible the data will be leaked online even if the victim pays the ransom (VMware, 2022).

When the stolen data is used by the attacker or sold on the dark web, new criminal opportunities emerge (VMware, 2022; Canadian Center for Cybersecurity, 2023). In the cybercrime chain, data extraction and sale enable additional criminal opportunities for new malicious actors, not just the initial ransomware attackers (Meland & al., 2021). In this context, the cascading effects involve new malicious actors who can commit new types of crime.

Sensitive personal information such as financial information, social security numbers, and medical records can be stolen and used for identity theft or financial fraud (Canadian Center for Cybersecurity, 2023). This can have long-lasting impacts on the individual's credit score, financial stability, and overall well-being. Additionally, the individual may face emotional distress and a loss of privacy because of their personal information being exposed (Kelly, 2021).

When personal data is leaked or sold, it can be used by cybercriminals to carry out targeted or cross-referenced attacks such as phish-

ing and spear-phishing (MS-ISAC, 2021). With access to personal data, attackers can craft highly convincing phishing emails or targeted phishing attacks that appear to come from a legitimate source, such as the victim's bank, government agency or postal service (MS-ISAC, 2021).

Intellectual property theft is another potential consequence of a ransomware attack. Attackers can extract sensitive business information such as trade secrets for their own use (as may be the case with a nation state actor) or sell it to competitors (Canadian Center for Cybersecurity, 2023).

Finally, data extraction during a ransomware attack can potentially be used for more insidious attack types, such 'Deepfake' attacks (Poremba, 2021). Deepfakes are synthetic media in which a person's likeness is replaced with someone else's likeness using artificial intelligence (VMware, 2022). If an attacker can extract personal data such as images or videos during a ransomware attack, they may use this information to make Deepfakes more realistic (Poremba, 2021). Deepfakes can be used for a variety of malicious purposes, including fraud, extortion, and disinformation (Department of Homeland Security, 2022; VMware, 2022). The use of Deepfakes can have large scale impacts on nations, governments and society if they are used by hostile states trying to achieve social polarization or political interference (Department of Homeland Security, 2022). According to the US Department of Homeland Security (2022), the technology is rapidly advancing and will be part of an emerging threat landscape "wherein the attacks will become easier and more successful" (p.18).

The increasing accessibility of AI tools has the potential to change the way cyber-attacks are conceived and launched. It is possible to argue that since "cybercrime is an ever-changing and constantly evolving threat" (Porcedda & Wall, 2019), new technologies will impact the evolution of the cybercrime ecosystem. It is therefore possible to argue that just as RaaS has lowered the barriers to entry for committing ransomware attacks, the democratization of artificial intelligence represents a new component in the evolution of the cybercriminal ecosystem.

The rise of RaaS in recent years (Meland & al., 2021), combined with the democratization of AI tools (Department of Homeland Security, 2022), generates new opportunities for cybercriminals. They may be able to use them to carry out more sophisticated attacks at a faster pace (Department of Homeland Security, 2022). For example, attackers may use AI to create highly convincing deepfakes for use in social engineering attacks (Department of Homeland Security, 2022). They may also use AI to automate the process of discovering vulnerabilities in systems or to create malware that can evade traditional detection methods (Canadian Center for Cybersecurity, 2023). Moreover, this has the potential to change the cybercrime ecosystem, attracting new malicious actors with less technical knowledge and expertise who may use ransomware attacks for financial, ideological, or political motives.

2.2.3 Societal Downstream Effects: Lack of trust & Socio-Political Polarization

Ransomware attacks could be understood as initiating a ripple of negative downstream ef-

fects across society. While it may be easy to intuit the direct effects of ransomware, such as using stolen data or system outages to enable further crimes (Porcedda & Wall, 2019), these effects can also take on an emergent form. Emergent effects occur from a complex situation but are unexpected and categorically different from their causes. Emergent effects, within the context of ransomware, can be operationalized as problems created as a result of ransomware that are not directly connected to the original crime (Dupont, 2019). Hence, ransomware attacks can cause effects that were unlikely to be forecast.

Ransomware victimization can be the first step in the dissolution of trust in digital media and services. When a ransomware attack occurs, the victim loses their autonomy of their data, files, or computer (Porcedda & Wall, 2019). The victimization may then continue through the exploitation of exposed personal information with crimes such as identity theft. According to the Canadian Centre for Cybersecurity (2023) only 42% of Canadian organizations who ended up paying their ransom had their data fully restored. This combined with the difficulties that police organization face in servicing victims and the apparent low rate of arrests for cybercriminals results in a poor set of outcomes for victims. This makes it difficult for them to put trust in institutions or organizations, adding to their unlikeliness of disseminating between trusted information and fake information. These cascading effects display how data exfiltration goes through processes of linked stages which can eventually have negative consequences on society (Porcedda & Wall, 2019).

This low trust environment creates a set of circumstances that could result in further emergent harms. The exacerbation of the lack of trust prevalent within a ransomware context is fuelled by growing ability to generate fake information using AI. According to Dupont et al. (2018), deepfakes are a malicious example of how AI can be used to manipulate individuals. Expanding on the image editing functions of software such as Adobe Photoshop , Deepfakes allows for automation that facilitates the editing of sounds and videos (Dupont et al., 2018). Often used through a tool called “FakeApp”, these tools can learn an individual’s facial features and make a video of them saying whatever the creator wants. This makes it increasingly easy for hackers to exploit individuals through impersonation or blackmail. This form of easily producible fake information adds to the lack of trust people have in society, organizations, and the government.

According to the Communications Security Establishment (2023), heightened occurrences of disinformation, used to provoke emotional responses, cause a general lack of trust amongst Canadians. Disinformation in this context, refers to as false information that has been deliberately created to invoke harm. This form of information spreads easily and quickly with the help of social media. Leveraging the ease with which they are able to spread disinformation, foreign states attempt to destabilize Canada’s democracy through “spreading false information, influencing voter decisions, polarizing opinions, discrediting people and institutions, and undermining trust in the democratic process” (Communications Security Establishment, 2023). Spreading fake information is a way foreign actors can destabilize micro levels of society such as

individuals and organizations, which then ripples into affecting the macro sphere such as the government or society at large.

Connected to the societal impacts of lack of trust and disinformation comes socio-political polarization. Creating conflict allows for a wedge to be driven within a society. Rapid Response Mechanism Canada (2022) express that disinformation distorts the public sense of reality. Ultimately, this threatens the pillars of democracy and shrinks the power of free speech (Rapid Response Mechanism Canada, 2022). This form of polarization is dangerous as it undermines the citizenry's trust in democratic institutions. While polarization is not something new, the rise of ransomware attacks creates an emergent environment in which actors can further manipulate massive groups of people resulting in socio-political instability. An example of this that occurred in January and February of 2022 is the 'freedom convoy' protests in which Truckers caused disruptions by occupying Canada's capital, Ottawa (McLaren, 2022). This example displayed how easily individuals can become divided, with some citizens supporting the convoy while others were firmly against it.

Ransomware is an issue which has societal, intelligence, and diplomatic consequences (Wilner et al., 2019). While the initial impacts are readily understood the cascading and emergent effects can result in a wide set of issues. These ramifications require analyses from multiple angles, with a core element focusing on social behaviour. While the technological environment is highly dynamic, it is consistently people who are conducting and developing cybercrime, which affects society and public safety as a whole (Wilner et al., 2019). While the full range of emergent effects are difficult to

understand, at the very least, the emergent effects that appear after a ransomware attack include a lack of trust and socio-political polarization.

2.3 Evolution of Ransomware Tactics

2.3.1 Ransomware and Natural Selection

The phenomenon of ransomware can be understood as evolving through a process of natural selection, where the most effective and successful variants survive and proliferate, while less successful ones fade away. As the environment in which ransomware exists has

changed dramatically over time, ransomware operations that have more effectively capitalized on these changes have become prevalent. While the future of ransomware may appear unpredictable, it can be appreciated through a historical analysis of its historical evolutionary process, which can be traced back to the late 1980s.

2.3.2 Early days

In the early days of ransomware, traditional physical (i.e., letter) mail was the main method of both payment and distribution. The PC CYBORG/AIDS Information Trojan was one of the first known cases of ransomware (Giri et al., 2006). In 1989 the author of the malware mailed to numerous people, a floppy disk containing a Trojan; a type of malware that disguises itself within legitimate software code or data files to trick users into executing or installing it. The recipients were likely unaware that the package contained ransomware. Once installed on the system, the Trojan would encrypt all of the user's files and demand a payment of $378 to recover the files, instructing them to mail the amount to an address in Panama (Giri et al., 2006). This form of ransomware could be understood as being reliant on the increasing availability of personal computers, the standardization of the floppy disk as a storage medium and the relative ubiquity of the DOS operating system.

2.3.3 The Internet

The use of mail as a distribution and payment channel gradually declined with the rise of the internet. As a result, there was a period of relative inactivity in ransomware attacks until May of 2005 when GPCoder emerged as one of the earliest modern ransomware variants (Giri et al., 2006). While the PC CYBORG/AIDS Trojan relied on floppy disks for distribution, GPCoder capitalized on the internet's connectivity and email services, allowing it to spread more efficiently and target a larger number of potential victims (Richardson & North, 2017). This marked a significant milestone in the evolution of ransomware as it adapted to the changing technological landscape and embraced online platforms for its malicious activities. While both ransomware variants demanded payment from their victims to regain access to their encrypted files, GPCoder started the trend of using online payment methods. These methods, such as e-gold and Liberty Reserve enabled attackers to receive ransom payments without revealing their identities or location, increasing the difficulty for law enforcement to track them down (Giri et al., 2006). These services, while providing a degree of anonymity, were themselves legal entities with centralized control of their platforms and were eventually targeted by law enforcement actions due to their association with various illegal activities, including ransomware payments.

2.3.4 Cryptocurrencies

With law enforcement agencies stepping up their efforts to control the illicit movement of funds through established online financial service providers, ransomware operators sought alternative payment methods that offered greater privacy and decentralization. This shift coincided with the rise of cryptocurrencies, which gradually replaced e-gold and Liberty Reserve as the preferred payment option for ransom demands.

CryptoLocker, one of the most famous ransomware strains, exemplifies this transition. When CryptoLocker emerged in August of 2013, it distinguished itself with its high level of sophistication compared to earlier ransomware (Richardson & North, 2017). It utilized strong encryption algorithms, making it extremely difficult for victims to recover their data without paying the ransom. Most notably, it demanded ransom payments in Bitcoin. Bitcoin allows for two parties to transact without an intermediary, hence, is not regulated by governments and banks (Wilner et al., 2019). This is a form of innovation in the ransomware sphere because of how difficult it is to track and trace, providing cybercriminals with a more efficient and anonymous method of receiving payments. The impact of CryptoLocker became even more apparent by the end of 2015, when the FBI estimated that $27 million in ransom payments had been made by victims to authors of CryptoLocker (Richardson & North, 2017).

However, the increased use of Bitcoin resulted in law enforcement agencies developing an increased capacity for blockchain analysis and the tracing of Bitcoin transactions. Consequently, in order to continue to be successful, ransomware operators needed better techniques to launder their profits effectively. To obscure the origins of the ransom payments and distance themselves from the illegal funds, cybercriminals turned to cryptocurrency exchanges, mixers, and tumblers.

Cryptocurrency exchanges played a crucial role in converting the received ransom payments into other cryptocurrencies or even fiat currencies, government-issued currencies, such as US dollars or euros (Matthijsse et al., 2023). By creating accounts on multiple exchanges that allowed anonymous or minimal identity verification, the ransomware operators could move funds in a way that obscured their origins and made tracing difficult.

Mixers and tumblers provided a way to further increase the anonymity of the received cryptocurrencies (Canadian Centre for Cyber Security, 2023). These services mix digital coins from multiple sources, making it challenging for blockchain analysis tools to link transactions to specific addresses. As a result, the ransomware operators could more effectively launder the funds and prevent investigators from following the money trail.

Additionally, some ransomware groups started demanding payments in privacy-centric cryptocurrencies. Bitcoin and alike cryptocurrencies such as Ethereum operate on a public blockchain, that has all transfers and transactions visible to the public. However, privacy-oriented cryptocurrencies such as Monero were deliberately crafted to obscure transactions and ensure user anonymity, increasing their popularity amongst cybercriminals (Canadian Centre for Cyber Security, 2023). Payments made in these cryptocurrencies made it even more challenging for investigators to track the flow of funds and identify the recipients. Despite this the spread of ransomware continued to be limited by operational factors. The effective operation of ransomware infrastructure is technically complicated and the number of operators that have both the technical skills to effectively implement a ransomware campaign and manage the laundering of funds and other operational aspects of a criminal enterprise.

2.3.5 Ransomware as a Service

The evolutionary nature of ransomware continued to progress with the introduction of a new and significant development in 2015, ransomware-as-a-service (Oz et al., 2022). This marked a pivotal shift in the evolution of ransomware, as it enabled a more streamlined and accessible model for cybercriminals to engage in ransomware attacks.

The RaaS model operated like a legitimate software-as-a-service (SaaS) business, with experienced ransomware developers offering their malware as a service to aspiring cybercriminals. They would gain access to user-friendly dashboards and tools provided by the developers, enabling them to customize, deploy, and execute ransomware attacks quickly and inexpensively without technical skills. Ransomware delivered in this way overcomes some of the limitations by separating the technical skills from operational requirements of ransomware functions, allowing RaaS ransomware to become more prevalent. The RaaS model significantly lowered the barrier to entry for conducting ransomware attacks, resulting in a vast and diverse ecosystem of ransomware variants (Oz et al., 2022).

2.3.6 Multiple Extortion

The increasing likelihood of ransomware could be viewed as precipitating a greater investment in ransomware resistant information systems. The large ransomware ecosystem, in turn, fostered the evolution and diversification of ransomware techniques, most notably introducing the concept of double extortion, as exemplified by the infamous Maze ransomware (Razaulla et al., 2023). Before encrypting the victims' databases, the attackers would steal sensitive information. Using this

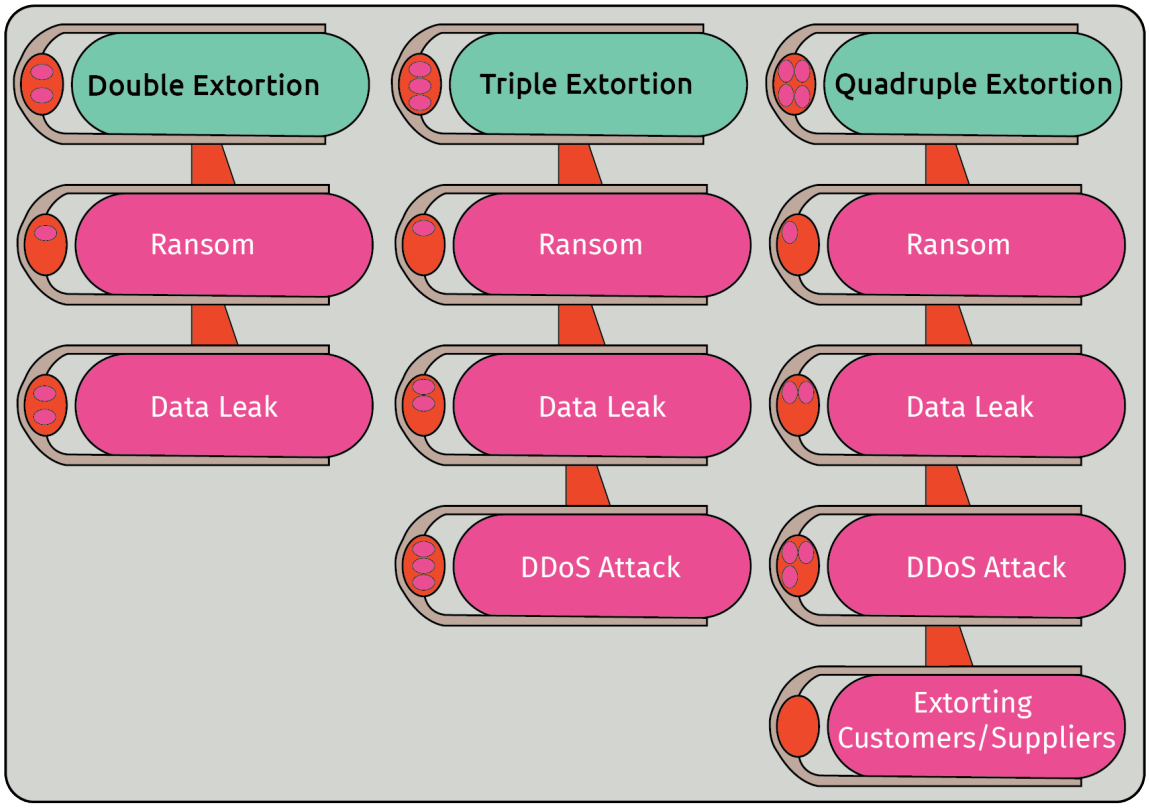


Figure 1- Multiple Extorsion Ransomware Techniques

stolen data as leverage, they would threaten to publish it on their "Name and Shame" website unless ransom demands are met, putting pressure on the victims to comply (Kerns et al., 2022).

As double extortion became more widely recognized and countered by cybersecurity measures, attackers evolved their strategies to maintain their effectiveness. This led to the emergence of triple and even quadruple extortion tactics. SunCrypt, a prominent RaaS operator, emerged as the pioneer of triple extortion in 2020 (Warikoo, 2023). In this advanced form, attackers would not only threaten data publication and demand a ransom, but also add a layer of coercion by deploying Distributed Denial of Service (DDoS) attacks on the victims' networks or websites. These DDoS attacks flood the system with an overwhelming volume of traffic, which causes service disruptions, and prevents legitimate users from accessing the system, leading to further financial losses for the victim. Quadruple extortion encompasses a ransom payment, data publication, DDoS attacks, and, additionally, involves attackers directly contacting the compromised company's customers or suppliers for further extortion (Warikoo, 2023). The first occurrence of this phenomenon was also observed in 2020 when hackers obtained access to a medical company's patient data (Robinson et al., 2022). Patients of a compromised Finnish psychotherapy company began receiving emails, with hackers demanding €200 in bitcoin in order to prevent their sensitive therapy conversations from being made public.

With the advent of RaaS platforms and new ways to further extort victims, the scale and complexity of ransomware attacks escalated. Cybercriminals refined their techniques and started focusing on larger corporations with substantial assets and financial capabilities. The average ransom payment witnessed a remarkable increase, rising from around $300 in 2015 to a staggering $111,605 in 2020, indicating that ransomware has evolved into a highly lucrative criminal enterprise (Connolly & Borrion, 2022).

Furthermore, the evolution in ransomware has been influenced not only by financially motivated cybercriminals but also by state actors driven by political motivations. State-sponsored ransomware attacks, executed by sophisticated hacking groups backed by nation-states, have emerged as a significant concern (Fiore et al., 2023). For instance, the WannaCry ransomware emerged in May 2017, exploiting a vulnerability in Microsoft Windows operating systems. The attackers demanded a ransom between $300 - $600, payable in bitcoin. However, the attack's impact extended beyond the financial, as several hospitals were compromised, experiencing shutdowns. This incident marked one of the first examples of a ransomware operation targeting destruction rather than solely seeking financial gain and it was attributed to a North Korean government sponsored cybercriminal organization (US. Department of Justice, 2018). Such attacks, aimed at disrupting critical infrastructure, corporate entities, and influencing political agendas, hold far-reaching implications beyond monetary motives. The involvement of state actors adds a new layer of complexity to the evolving ransomware threat, blurring the lines between traditional cybercrime and political strategies.

Ransomware has come a long way since its early days of letter mail distribution and

modest ransom demands. Over the years, it has adapted and evolved in response to changing technological landscapes, financial incentives, and law enforcement actions. This ever-evolving nature of ransomware exemplifies the relentless pursuit of adaptability and resilience in the competitive cyber landscape. Just as nature selects the fittest organisms for survival, the cyber landscape selects the most effective and evasive ransomware variants for proliferation. As the evolutionary trajectory of ransomware progresses, it becomes evident that combating this diverse and sophisticated cyber threat requires continual vigilance, collaboration, and innovative security measures from the cybersecurity community and law enforcement agencies. By understanding and anticipating ransomware's evolutionary pathways, we can better prepare to defend against this continuously developing threat and protect the digital world from its detrimental effects.

2.4 New means for the attacker

As ransomware attacks continue to evolve, cyber attackers capitalize on the advancements in technology, using them to their advantage in exploiting victims more efficiently. Innovations such as cryptocurrencies, artificial intelligence (AI), and the Internet of Things (IoT) have opened new avenues for these malicious actors, making their nefarious activities more challenging to track and combat and could consequently be playing a role in the current evolution of ransomware threats.

2.4.1 Cryptocurrencies

The advent of cryptocurrency has significantly fuelled ransomware attacks, as evidenced by the case of the first CryptoLocker attack (Conti et al., 2018). As we have discussed in the previous section on evolution, with the launch of Bitcoin, cybercriminals found an ideal tool to execute their malicious deeds. Beyond Bitcoin, attackers are also leveraging alternative digital currencies such as Ethereum, Ripple, and Monero, drawn by the additional layers of anonymity they provide. To complicate matters further, attackers have delved into the realm of custom coins or tokens, specifically designed for ransomware campaigns, evading public trading and raising victims' apprehensions about engaging with rare digital currencies. Seeking to elude law enforcement and cybersecurity scrutiny, attackers have turned to tumblers and mixers, which pool and mix funds to obscure transaction origins. By funnelling ransom payments through these services, attackers effectively blur the money trail, impeding investigators from tracing funds back to specific individuals or groups. The development of online currencies and related institutions facilitating their transfer and conversion could be important to the development of ransomware schemes should more efficient or anonymous schemes be realized.

2.4.2 Automated System Vulnerability Detection

Artifical Intelligence (AI) assumes a pivotal role in detecting system vulnerabilities with remarkable ease (Khan, S., & Parkinson, S., 2018). Additionally, 'explainable AI' (XAI) provides invaluable insights into these vulner-

abilities, offering a deeper understanding to both defenders and attackers alike. Although this technological advantage aids cybersecurity professionals in fortifying their defenses, it also empowers attackers by automating processes and rendering cracking systems more flexible. The capability of AI to analyze vast amounts of data in a single click saves time for cybercriminals, facilitating swift identification of vulnerabilities. Once weaknesses are pinpointed, attackers employ XAI to gain in-depth knowledge about the vulnerable code snippets, enabling them to launch precise and targeted attacks on these areas of vulnerability. The continuous development and application of AI in cybersecurity demand vigilance and innovation to safeguard against emerging threats in the ever-evolving digital realm.

2.4.3 IoT Ecosystem

The Internet of Things (IoT) ecosystem is a diverse realm, encompassing a vast array of devices like smart home appliances, wearable gadgets, industrial sensors, and medical devices. However, these devices often bear the burden of limited processing power and memory, posing challenges in implementing robust security measures. Additionally, the absence of standardized security implementations leaves IoT devices vulnerable to exploitation. As the Internet of Things continues to expand, it inadvertently creates a favourable environment for ransomware attackers seeking potential targets (Humayun et al., 2021). The use of IoT as an entry point to corporate networks through the homes of teleworkers pursuit of standardized security protocols and innovative cybersecurity measures becomes paramount to safeguarding the integrity and privacy of our interconnected world.

2.4.4 Social Engineering

Attackers consistently adapt to defensive measures through processes of social engineering. Social engineering focuses on targeting individuals and using techniques derived from behavioural science and psychology to manipulate them into providing hackers with the means for access into their networks or accounts (Conteh & Schmink, 2021). This attack strategy focuses more targeting humans rather than relying purely on technological innovation (Dupont et al., 2018). Through the use of deception and forging trust with users, hackers can access information relatively undetected, as it seems like authorized access (Conteh & Schmink, 2021). With the rising use of social engineering, attacks have become more targeted. Examples of this are seen through personalized phishing attacks, coined as spear phishing, where attackers frame emails as if they are legitimate in attempts to collect personal information. This practice continues to evolve; hackers find new creative ways to trick individuals into believing their phishing emails through finding catered personal information of the victim (Beaman et al., 2021). This form of personalized adaptation makes it difficult to discern between correct information and disinformation in emails, causing victims to easily fall for deception.

2.4.5 Extended Software Supply Chains

Supply chain effects are another software attack that hackers are growing accustomed to. These attacks “occur when attackers com-

promise a block of code at its source, such as a software update that then infects any business or customer that uses it" (Robinson et al., 2022). For example, say there is a large software development company that creates a contract with another smaller company to execute some processes for them. Hackers could see an opportunity to attack the smaller company that has less security. Through breaching the security of the small company, a successful ransomware attack can occur. This chain of supply makes software that are distributed over the internet difficult to remain compromised (Robinson et al., 2022). Hackers take advantage of this which is why risks of supply chain attacks has never been higher, adding to the fact that hackers consistently adapt their attacks based on new technologies.

2.5 Future Risks

Future era of technology, where anonymity and e-personas prevail, making the task of tracking ransomware increasingly challenging. As technology advances, so do the opportunities for the evolution of cybercrime threats. In order to put in place the measures to reduce the harm from the future development of ransomware, the analysis of near future technologies could provide crucial insights.

2.5.1 AI-driven social engineering

AI is increasingly being leveraged to fuel ransomware attacks, enabling cybercriminals to conduct large-scale and sophisticated assaults (Poudyal, S., & Dasgupta, D., 2020). AI-driven social engineering tactics further enhance the attackers' ability to compromise victims and coax them into downloading ransomware as Trojans (Krombholz et al., 2015). In today's digitally connected world, where individuals' details and activities are easily tracked through social media, cyber attackers exploit this wealth of data to evoke specific emotional responses from their targets, such as fear, urgency, curiosity, or trust. Employing personalized Trojan messages and convincing negotiations, automated social engineering techniques craft highly authentic-looking emails and communications that appear to originate from trusted sources, making it difficult for recipients to discern malicious intent. This manipulation not only influences victims to pay the ransom but also enables attackers to adjust ransom amounts and time limits based on their analysis of the victim's behaviour. As a result, AI-driven social engineering could provide an avenue for not only securing access but also facilitating a providable outcome which would be invaluable for attackers, during, and after an attack.

2.5.2 Smart cities and e-governance

The world is witnessing a sweeping transformation towards smart cities and a futuristic e-governance landscape (Bajpai, P., & Enbody, R., 2020). Fuelling this evolution is a myriad of cutting-edge technologies that promise to make our world more dynamic and connected than ever before. Smart cities, powered by the Industrial Internet of Things (IIoT), manage critical infrastructures like energy, water supply, and transportation, raising concerns about potential vulnerabilities (Bajpai, P., & Enbody, R., 2020). Furthermore, e-governance presents both opportunities and challenges,

offering the potential for efficiencies in the management of communities and increasing access to services but also presenting a vast mine of personal information for ransomware attackers to target (Nershi, K., & Grossman, S., 2022). The developing digitization of the institution of democracy also presents potential targets. An illuminating study by Stanford reveals that election times are particularly prone to cyber attacks, compromising politician communications and highlighting the pressing need for robust cybersecurity measures in this digital age (Nershi, K., & Grossman, S., 2022). The development of these aspects of our cities and government present opportunities for the development of criminal operations that could shape the future ransomware techniques.

2.6 Technical Solutions

2.6.1 Unlocking the Power of Ransomware Defense

Strategies for more effectively countering ransomware could make effective use of not only cutting-edge approaches such as defense-in-depth, defending forward and deception strategies, but also long-standing techniques such as widespread system logging. This concept combines the prowess of canary files and logging, creating an enticing trap for attackers while empowering organizations to stay one step ahead of the cyber threat. By strategically deploying alluring Trojan canary files in unauthorized areas of the system and network, attackers are lured into revealing their presence in a system, setting the stage for their undoing. The interaction with these deceptive decoys does more than just raise alerts; they stealthily record every move of the intruders. On activation the keylogger component of the canary file springs into action, capturing critical data, including the attackers' IP addresses, encryption methods, and even decryption keys. The deployment of strategies such as these could increase the cost of running ransomware operations, as operators would need to constantly defend while attacking on all systems, due to the possibility of the system employing this form of defense. This form of active and deceptive defense would potentially change the game, increasing possibility of resilience against ransomware threats.

2.6.2 AI-driven system behaviour detection

In the ever-evolving landscape of cybersecurity, AI emerges as a formidable weapon in the fight against ransomware. One of its key roles is to monitor system behaviour, identifying anomalies that could signal a potential ransomware attack. Through network traffic monitoring, tracking suspicious API calls, and automating intrusion detection, AI-powered systems can swiftly spot signs of malicious activity. Notably, ransomware-infected systems exhibit unusual behaviour, as highlighted in a recent study (Hampton et al., 2018), where researchers discerned specific API features associated with ransomware-infected operations. By harnessing these cutting-edge technologies, organizations can more rapidly thwart ransomware attacks and safeguard their data and operations from harm before the threat materializes. Embracing AI as a preventive measure is a crucial step towards fortifying our cyber defenses and ensuring a secure digital future.

2.7 Recommendations for Organizations and the Public

In the ever-evolving landscape of the digital era, the rise of ransomware attacks has become an alarming concern. As technology advances and the digital realm expands, the sophistication and frequency of these attacks have reached unprecedented levels. Despite numerous efforts to eliminate ransomware, the perpetrators behind these malicious acts have proven to be incredibly resilient, continually finding innovative ways to exploit vulnerabilities in our systems and networks.

The traditional approach to combating ransomware has revolved around attempts to eradicate it completely. However, this strategy has proven to be ineffective as the threat actors behind these attacks adapt rapidly and evolve their tactics. Each time a security loophole is patched, or a defense mechanism is implemented, cybercriminals are quick to identify new vulnerabilities and develop strategies to bypass them. As a result of this reality, society needs to accept that ransomware is now a part of our lives and is not going away any time soon. We must be able to quickly adapt to the new attempts cybercriminals use and understanding that ransomware is a persistent and pervasive threat is crucial for devising effective strategies to mitigate its impact.

Ransomware attacks are inevitable and know no borders. Knowing this means that society needs to come together to mitigate these attacks, rather than sweeping them under the rug. The foundations for ensuring this are spreading awareness and transparency, along with focusing on altering the culture of cybersecurity attacks. From a societal standpoint, ransomware attacks are still taboo. Organizations and individuals feel a sense of shame when suffering from an attack and this only contributes to limiting solutions to the problem. To help mitigate this, the culture of ransomware needs to change.

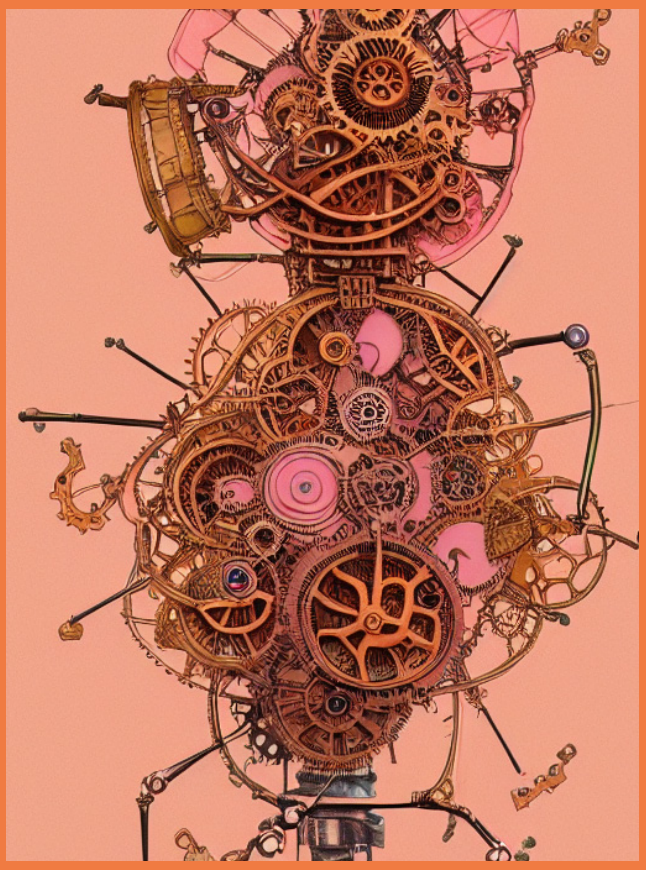
Shifting the culture of ransomware starts with spreading awareness. This can happen through implementing awareness in starting from a young age, helping with normalizing the reality of these attacks as the population grows. These learning experiences can be made fun to keep children invested in understanding and learning about cybersecurity. Various exercises teaching them the importance of the issue, such as through games, quizzes, collaborative exercises, etc. can make the topic approachable. To assist with the rest of the population, implementing education within organizations that focuses on the emotional, business, and mental impacts of ransomware can help. Receiving so much information on important initiatives is difficult, so it is crucial to make awareness campaigns relatable and impactful.

Just as campaigns like “Lives not Knives” in the United Kingdom have successfully appealed to the youth, we can design similar initiatives to engage, educate, and empower young minds to stay away from cybercriminal activities (Lives Not Knives, n.d.) By highlighting the harsh reality that being a cybercriminal does not pay well, we can scatter the illusion of quick gains and showcase the abundance of opportunities in legitimate technology careers. Demonstrating the positive impact of legal professions, where their skills can be

harnessed for the greater good, can inspire them to pursue legitimate jobs and contribute positively to society. In addition, mentorship programs and workshops led by cybersecurity experts can create role models who can demonstrate the fulfilling, rewarding path of a cybersecurity professional. By creating engaging and relatable awareness campaigns, we can create a culture that not only discourages cybercrime, but also nurtures and celebrates the younger generations potential to become technology leaders of the future.

Cybersecurity is something that we need to continuously learn about and practice. Cybercriminals are always evolving and figuring out new ways to attack. To mitigate this, learning about protecting oneself online from a young age, along with constant learning as one grows up can add to strengthening society's knowledge on the topic. An example of this can be done through implementing phishing training within organizations. Not only does this continue the education of the realities of what can happen through ransomware attacks, but it allows for training for avoiding these occurrences. Central to these training situations needs to be an activism aspect to assist with changing the culture and ideologies surrounding being a victim of ransomware attacks.

Centralization of resources is an aspect of awareness that can help with showing people that they have a place to go to learn or report ransomware attacks. There is a multitude of resources available, but it is overwhelming not knowing where to specifically go. Knowledge paradox has become so common, so having a central website or phone number to call for cybersecurity information is helpful. Having that guidance and a central guide can add to the awareness and transparency need of ransomware. For instance, when there is a typical real-world crime (e.g., a robbery) there is most often one number to call, e.g., '911'. For a cybercrime, there are many resources available, but which would you contact first? Public Health and Safety? The local police? The RCMP? On top of having to manage the stress of dealing with a cyber incident, not having an immediate resource to contact can further aggravate the already immense pressure. Having a single point of contact, that upon calling, could direct the victim towards the appropriate resource(s) could go a long way, regardless of size. For example, a smaller critical infrastructure operator such as a small-town power grid when faced with a ransomware attack may be directed towards a more appropriate resource versus the power grid operator of a major area such as Toronto which would require a more serious resource. Centralizing the initial contact point can help save time and resources during a cyber crisis.



Regulation

3 Regulation

3.1 The Impact of Ransomware on Small Businesses

Small businesses are a vital component of the Canadian economy. According to the Small Business Branch of Innovation, Science and Economic Development Canada (2022), enterprises with 1-9 employees make up 74.1% of all businesses in Canada, and when combined with businesses of up to 99 employees, the number increases to 97.9%. These small businesses are responsible for creating jobs, with nearly 70% of employee working for small businesses and driving innovation, accounting for 36.7% of Canada's GDP in 2019 (Innovation, Science

and Economic Development Canada, 2022). While small businesses are thriving in Canada, in recent years they have faced a meteorically rising threat: ransomware attacks. Data from the Canadian Ransomware report by Telus indicates that 61% of small businesses have been affected by ransomware, with the average ransomware payment (across businesses of all sizes) exceeding $250,000 (National Cyber Threat Assessment, 2022; Telus, n.d). Small businesses have become increasingly popular targets of ransomware attacks in recent years, and the impacts of victimization can be devastating. In the wake of a ransomware incident, small enterprises are left cash strapped and forced to allocate significant time and resources towards getting back on their feet. Some businesses experience a blow to their reputation, especially when data is leaked, and others go out of business entirely (Telus, n.d;).

Despite the growing threat of ransomware, small business owners may be unaware of their vulnerability, with many failing to employ basic cyber security practices. Others may underestimate their likelihood of being victimized, an overly confident mindset linked to the failure to take appropriate preventative measures (Bekkers, Van 'T Hoff-de Goede, Misana-ter Huurne, Van Houten, Spithoven, & Leukfeldt, 2023; De Kimpe, Walrave, Verdegem & Ponnet, 2022). In many cases, business owners are aware of the impact of ransomware, but they do not feel that their business are a lucrative enough target for ransomware attackers. However, almost every business nowadays requires IT infrastructure to run their business, and the lack of proper cybersecurity preparation and incident response policies may make operations complicated when they face a ransomware attack. Therefore, it is important for entrepreneurs to be aware of the risks of ransomware attacks and take appropriate measures to protect their businesses.

The Canadian government provides a range of resources and guidelines for small businesses seeking to mitigate ransomware, such as the Ransomware Playbook provided on the Canadian center for cyber security website (Canadian Centre for Cyber Security, 2021; Ransomware Playbook, 2021). Beyond these guidelines, however, there is a scarcity of available information nor regulations specifically focused on the risks of ransomware for small businesses. Furthermore, while most of the resources are freely available, additional steps are required to actively inform the business owners about them to help form a better cybersecurity hygiene. As small businesses are the backbone of our economy, we argue that it is crucial for the government to take a more proactive role in protecting small businesses who may otherwise lack the resources, technical abilities, and education required to contend with the complex criminal threat that is ransomware.

The purpose of this section of the report is to provide an overview of the existing regulatory bodies in Canada related to ransomware (Section 3.2). Based on our exploration of the related literature and cooperation with the partners, we detail three recommendations to be considered when forming future regulations and how they relate to existing regulations (Section 3.4). Finally, we highlight the challenges in the adoption of regulations and discuss some possible regulatory actions to support the adoption of our recommendations (Section 3.5).

Our research reveals how data encryption, regular data backups, and Security Education and Training Awareness (SETA) can help small businesses form a solid cybersecurity strategy against ransomware. In doing so, we highlight technical and legal challenges, and dive beyond formal regulations to discuss how cyber-insurance and initiatives such as bank loans for small businesses could be leveraged along with regulatory actions to support the adoption ransomware-resilient practices in Canada.

3.2 Existing Regulatory Frameworks in Canada

Cybersecurity law is a legal framework that aims to protect individual rights and privacy, economic interests, and national security by promoting the confidentiality, integrity, and availability of public and private information, systems, and networks (Kosseff, 2017). It includes both hard and soft measures to compel and advise individuals, companies, and organizations to safeguard their IT infrastructures, information technology, computer systems, networks, and data against various cyber threats such as unauthorized access.

Cyber security laws in Canada include various legislative and regulatory frameworks. While various federal and provincial laws address cyber security such as the Criminal Code of Canada, the Privacy Act, the Access to Information Act, the Personal Information Protection and Electronic Documents Act, Canada's Anti-Spam Law (CASL), and the proposed Bill C-26, only two of them directly impose obligations on businesses. In addition, there are various public and private centers and organizations that are involved in overseeing and enforcing cyber security regulations.

In order to mitigate cyber risks (i.e., take preventive measures) and their potential financial and legal consequences, organizations and business entities operating in Canada must have a proper understanding of relevant regulations and legal obligations.

In this section, we provide a brief overview of the evolving landscape of Canadian cyber law. Having a comprehensive understanding of this law subsequently enables organizations and business entities to develop their approach to cyber risk management and implement necessary preventive and recovery plans for cyber-attacks.

3.2.1 Hard Regulations

Hard law are legally binding obligations that are clearly defined or can be made defined through legal proceedings or the issuance of detailed regulation (Summer, 2000).

Although there are various definitions of hard law, the existing literature in this field has a consensus that hard law represents rules that have a binding nature. Such laws impose binding obligations on individuals and entities under their strict legal jurisdiction, and violation or failure to comply with those binding obligations, may result in fines or penalties (Zajc, 2016).

3.2.1.1 Bill C-26: An Act Respecting Cyber Security (ARCS)

As cyber-attacks such as ransomware represent a continuing threat to Canada's security and economic well-being, the Canadian gov-

ernment introduced Bill C-26 on June 14, 2022. This bill aims to implement substantial cybersecurity requirements for federally regulated industries and introduce new national security mandates for the telecommunications sector. The proposed Bill aims to create a framework regulate the security of critical infrastructure in Canada and strengthen the oversight of telecommunications security.

Bill C-26 consists of two main sections. The first section sets out to amend the Communications Act by focusing on the security of Canada's telecommunications systems, while the second section tries to enact the Critical Cyber Systems Protection Act (CCSPA). The CCSPA establishes comprehensive regulatory frameworks to protect critical cyber infrastructure systems that are vital to national and public security. This Act would apply to operators that provide critical services such as telecommunications, energy, finance transport and banking, requiring them to develop a "cyber security program" within 90 days that takes the following five steps:

"(a) identify and manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and services;

(b) protect its critical cyber systems from being compromised;

(c) detect any cyber security incidents affecting, or having the potential to affect, its critical cyber systems;

(d) minimize the impact of cyber security incidents affecting critical cyber systems; and

(e) do anything that is prescribed by the regulations."

(Bill C-26, 2021, c9-1)

The operators are also required to report cyber incidents to the Communications Security Establishment (CSE) and follow mitigation recommendations provided by the CSE.

3.2.1.2 The Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy legislation for private-sector organizations including all businesses (large, medium-sized, and small businesses) in Canada. It establishes guidelines for how businesses must handle personal information during their commercial activities.

Even though PIPEDA may not be classified as a cyber security law, many of the challenges for cyber security are at the same time challenges for privacy and data protection. As businesses try to collect vast amounts of their customers' data to develop their operations and adapt to new technologies, the collected personal data and information may be exposed to cyber threats such as unauthorized access and pose risks to both privacy and security.

Organizations or businesses subject to PIPEDA are expected to adequately safeguard their clients' data and personal information. They are required to prevent any unauthorized use, access, or disclosure as may result from ransomware attacks.

An important aspect of PIPEDA is Principle

7 — Safeguards, which requires businesses to deploy appropriate "security measures" for example, by "the use of passwords and encryption" in order to "protect all personal information (regardless of how it is stored) against loss, theft, or any unauthorized access, disclosure, copying, use or modification" (PIPEDA, 2000, C-4.7).

The main point here is that PIPEDA does not provide specific security measures to safeguard personal data, instead, it assigns this responsibility to the organization or businesses subject to the law, requiring them to develop and implement a security policy to protect personal information and use appropriate security measures to provide the necessary protection.[1]

3.2.2 Soft Regulations

Emerging technologies such as artificial intelligence, Internet of Things, blockchain, digital currencies, and others present a set of challenges and risks that are quite complex which make it very hard for traditional legal and regulatory systems to keep up with of rapid advancements in those technologies. One of the approaches that has been recently proposed to address the challenges raised by new technologies suggest the adoption of soft laws. Soft law expresses requirements, recommendations, provisions, and guidelines that are not directly enforceable by government regulators or the judicial system. It may include private standards, codes of conduct, certification programs, principles, guidelines, and voluntary initiative, which can be quickly adopted, updated or revised without the complexities of adopting traditional hard laws (Marchant, 2020).

This section provides an overview of the main organizations and centers involved in addressing cyber-crimes and provide related guidance. The Canadian government established various centers and departments in order to enhance cyber security among small and medium-sized businesses within the country and safeguard them against cyber threats while increasing public trust in the digital economy. These centers provide recommendations and guidelines (soft law) in four main areas:

- **Public awareness;**
- **Professional advice and guidance;**
- **Cybercrime and fraud reporting systems;**
- **Cybersecurity training and certification programs.**

3.2.2.1 The Canadian Centre for Cyber Security

The Cyber Centre is an open and collaborative initiative under the Canada's National Cyber Security Strategy which is currently part of the Communications Security Establishment (CSE). As Canada's professional authority on cyber security, the centre cooperates with different public and private organizations such as federal and provincial departments, municipalities, critical infrastructures, academics, banks and Canadian businesses to offer cybersecurity related services. (https://www.cyber.gc.ca/en). The centre works to increase the country's cybersecurity capacity by developing and sharing specialized cyber defence technologies and tools as well as providing guidance and awareness, such as through the "Get Cyber Safe" Campaign. (https://www.getcybersafe.gc.ca/en)

With regards to ransomware specifically, the center has developed professional cybersecurity advice and guidance that focuses on this issue and is tailored to small and medium-sized businesses. This documentation is freely available online and includes the documents noted in the table below.

In particular, the Ransomware Playbook, provides detailed information on Ransomware, the attacker's motivation, and outlines the measures that businesses may take to prevent cyber-attacks. It also proposes strategies to protect the businesses' data and systems against the impacts of cyber-attacks.

As a baseline cybersecurity recommendation, the Center advises that small and medium-sized businesses comply with "IT security risk management: A lifecycle approach (ITSG-33)" to increase their cyber resilience against cyber threats and incidents. The ITSG-33 is the Canadian equivalent of the NIST Cyber Security Framework or ISO/IEC 27001:2013 and accordingly provides a comprehensive set of recommendations, guidance, and security controls at the technical, operational, and management levels of a business. These measures can help companies and organizations to manage their cyber security risks more effectively.

3.2.2.2 The National Cybercrime Coordination Unit (NC3)

The National Cybercrime Coordination Unit (NC3) was established as mandated in Canada's National Cyber Security Strategy and the RCMP Cybercrime Strategy. The NC3 works with various public and private sectors to help them mitigate the risks and impacts of cybercrime threats and potential victimization throughout the country. It mostly focuses on cybercrime investigations in Canada, provides investigative advice, guidance and actionable cybercrime intelligence for Canadian police (Government of Canada, 2020).

One of the interesting initiatives of the NC3 is to implement a new and publicly accessible national cybercrime reporting system with the Canadian Anti-Fraud Centre (CAFC). This system not only makes cybercrime and fraud reporting process much easier and simple for individuals and businesses (victims or witnesses of cyber-

Resource Title	Resource Link
Baseline cyber security controls for small and medium organizations	https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)	https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035)
Get Cyber Safe Guide for Small and Medium Businesses	https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-and-medium-businesses)

Table 1 - Canadian Federal Government Cybersecurity Guidance for SMEs

crimes and frauds), but also allows police and law enforcement to better understand the constantly changing cyber threat landscape.

3.2.2.3 CyberSecure Canada

Cybersecure Canada is a cybersecurity program developed and led by Innovation, Science and Economic Development Canada (ISED) and the Communications Security Establishment (CSE). It provides a voluntary cybersecurity certification program for small and medium sized businesses. This program includes a free self-paced eLearning series which is designed to help businesses improve their cybersecurity knowledge and learn how to implement necessary and basic cybersecurity practices in order to prevent cyberattacks against their systems and IT infrastructure without the need to hire IT technicians.

3.3 Recommendations for Future Regulations

Following the evolution and growth of ransomware attacks in the last few years, it is not hard to imagine a future where ransomware becomes big enough of a threat to society at large that organizations need to be regulated. Based on our exploration of the existing literature and information exchanges with government, academic, and industry partners, we suggest three recommendations to reduce the impact of a ransomware attack and assess their feasibility.

3.3.1 Recommendation 1: Having a Good Backup Policy

The goal of ransomware attacks has traditionally focused on preventing the victims from accessing their systems. The permanent loss of files is one of the most significant aspects of ransomware victimization, as it may take a small organization months to recover. This even pertains to organizations who decide to pay a ransom to the threat actor in exchange for decryption keys, as it is not uncommon for threat actors to not provide decryption keys despite being paid (Canadian Centre for Cyber, 2019). An analysis of businesses who were victimized by ransomware found that a lack of backups devastated some companies (Yuryna Connolly & Borrion, 2022). For example, one SME in the IT sector that was faced with a ransom demand that they elected to pay but did not have the immediate capital to afford and they were not given the opportunity to negotiate. The organization did not have their files backed up, and since they could not decrypt their files, they went bankrupt (Yuryna Connolly & Borrion, 2022).

Safely and correctly backing up important documents such as financial records, creative files, and copyright materials can help small businesses restore their operations after an attack. Having a system backup allows the victimized organizations to roll the changes back to the time that the backup was made, which if it is before the commencement of the attack is enough to remove the ransomware and restore the system with its files. A file backup of critical data for the organization, on the other hand, creates a copy of individual data files, allowing targeted restoration of files and is useful to regain access to the unencrypted data when a ransomware attack targets specific files of folders for encryption. The two methods come with their own sets of bene-

fits and drawbacks. However, regardless of the type, backups are known to be the one of the most effective strategies against ransomware attacks that demand a ransom in exchange of system or data access and is suggested by the ransomware Playbook (Canadian Centre for Cyber Security, 2021).

The Canadian Centre for cyber security provides comprehensive advice for small businesses to avoid prevent and recover from ransomware attacks (Canadian Centre for Cyber Security, 2021). The guide highlights the 3 ways in which a corporation can backup their files: full, differential, and incremental. A full backup is the most expensive and time-consuming option, but it creates a complete copy of all data. A differential backup only creates a copy of data that has changed since the last full backup. Incremental backups only store the data that has changed since the last full or differential backup, and each increment is saved as an incremental volume. The document also recommended 'deduplicating' data to reduce costs and ensure efficient backup and storage. Furthermore, their guide highlights the 3 methods an organization can use to store their backups: namely onsite, offsite, and cloud based. Onsite backups are stored within the physical space of organizations and are convenient and time-efficient, but they may still be vulnerable to data loss if your facility is affected by a physical disaster, such as a fire or flood. Offsite backups are stored in a separate location and can help prevent data loss but require organizations to trust a 3rd party vendor to safely store their precious data. Finally, cloud-based backups are stored on a remote server and can be beneficial in many ways, including freeing up resources for your organization and offering enhanced security features. They specifically recommend opting for offline backups instead of online, as they are disconnected from the internet and therefore offer greater protection against a ransomware attack (Canadian Centre for Cyber Security, 2021).

3.3.1.1 Feasibility

While having regular backups so that we can recover our files in the event of a ransomware attack sounds like a great idea, it may not be as simple in practice. There are many aspects to consider to ensure backups are effective.

Ensuring that backups are scheduled properly and are being done regularly is challenging. Most organizations would use backup software to automatically backup system data. However, it is important to clearly assign the responsibility of backup administration (or the role of backup administrator) to ensure that the backups are being effectively generated to the schedule. Organizations can specify in their organizational policy how frequently they backup their data. Given the constraints of small businesses, we suggest that they consider performing a file backup for their critical data at least monthly and they perform a full system backup at least quarterly.

Completed backups must also be checked to ensure they are reliable as the backup process can fail. If the end product is not checked properly, the organization can end up with a corrupted version of the backup that is impossible to recover any data from. Even if the backups themselves are fine, the backup restoration system can fail to restore the data. Automatic backups can also end up getting encrypted by ransomware when not monitored

properly. If the ransomware persists within the system and a scheduled backup is done, the backup may contain partially or completely encrypted datasets. In this case, recovering data from the backup becomes ineffective as an organization will only be able to recover the encrypted data. Thus, completed backups should be regularly tested by the backup administrator, or person assigned this responsibility to ensure that usable files are able to be restored. This process involves the regular restoration and access of a backed up file and system to ensure the systems are operating effectively.

Backup storage that is physically connected or connected through a local network connection, can compromised during a ransomware attack, as the malware maybe about to propagate to them. **Isolated or air-gapped backups** (Perot, 2019) refer to offsite backups that cannot to targeted by remote cyberattacks as they are physically detached from the system (i.e. there is an air gap between their ports and the system). While this type of backup is typically less accessible, it acts as a last line of defense against targeted and organized ransomware attacks. Therefore, having two copies of backups (one isolated) is vital so that the organization retains at least one copy of the data and lessens the possibilities of ransomware propagation or backup hunting, where the attacker targets the backup data first for deletion before revealing the existence of the ransomware. The traditional 3-2-1 rule of backups (Malecki, 2021) which suggests that businesses keep at least three backup copies of their data, two onsite on separate media, and one backup copy kept offsite (isolated backup) is a practice that offers this air gapping protection along with additional protection against physical threats to the media (e.g. theft, flood, fire).

Prioritizing critical data becomes more and more important as the system grows in size. The size of the backup increases with the increase in the amount of data that the organization deals with, making the backup process more time-consuming. Hence, it becomes very important to determine what data is essential for the organization to continue its regular operations, label it as critical data, and at the very least keep multiple copies of backup of that portion of the data. As an additional layer of protection, following privacy by design principles will reduce the amount of critical data that needs to be stored while offering additional protection from data exfiltration or data breach type incidents.

The organizational policy should include the above considerations about what data is critical for the system, what tool (e.g., a third-party application) would be used for the backup, and the frequency of scheduled backups. The policy should also include human considerations to ensure that backups are performed correctly. This includes assigning responsibility for backup administration as well as ensuring that the person or persons have the capacities and resources required for the task. For small businesses, if they lack the technical expertise, they might require third-party services or and additional personnel for performing and checking the backups. Additionally, how many copies of backups to make, where to keep the copies (e.g., onsite or offsite, in the cloud or in a physical hard drive), and who keeps the backups (e.g., the business owner) are also essential consider-

ations. Policies for the safe management of these backups are important to ensure not only that the backups are effective in reducing the harm of ransomware, but also to ensure that the backups themselves do not become a burden or a source of harm to the business (e.g., if they are not disposed of safely or are misplaced).

3.3.1.2 Relations to existing regulations

All the three documents developed by the Canadian Centre for Cyber Security (including Baseline cyber security controls for small and medium organizations, Get Cyber Safe Guide for Small and Medium Businesses and ITSAP.10.035) advise small and medium-sized business to:

- Back up regularly all essential business information to an external secure location.
- Store back-ups in a secure, encrypted state.
- Have clear procedures on how to restore data from backups.
- Test backups regularly.
- Another document that provides detailed information specifically on baking-up data is the document titled “Tips for backing up your information (ITSAP.40.002)” developed by the Canadian Centre for Cyber Security. ((Canadian Centre for Cybersecurity, n.d.))

3.3.2 Recommendation 2: Encryption of critical data at rest

The evolution of Ransomware attacks have resulting many offenders employing a multiple extortion scheme (Payne & Mienie, 2021). Even after a ransom has been paid and the attacker provides the decryption keys to the organization to recover their files and resume regular business operations, another threat remains. If the attackers have managed to exfiltrate sensitive data (e.g., customer credentials, or patient health information), they may then extort another ransom payment by threatening to disclose that data to the competitors, media, or the general public (Whitwam, 2019). An example of this form of ransomware attack on can be seen in the case of BMO and Simplii in 2018, where the attackers threatened to reveal customer names, account numbers, passwords, security questions and answers, as well as extremely sensitive information such as social insurance numbers and account balances (Evans, 2018). The Canadian postal operator Canada Post was also hit by a ransomware in May of 2021, where the ransomware data exfiltration of shipping manifest data included sender and receiver contact information, names, and mailing addresses for over 950,000 receiving customers was used to extort payment (Abrams, 2021). Some criminal organizations have decided to focus completely on this aspect of ransomware and forget about encrypting the data altogether, and this trend is only expected to continue (Li & Liao, 2022). Therefore, it is not enough to have only a backup of the critical system data to mitigate the impacts of ransomware.

Having proper cryptographic measures in place (i.e. strong encryption) is a common and mature

approach to reduce the threat of attackers exfiltrating the data and threatening to leak it (Ullah et al., 2018). When the critical data within a system is encrypted at rest (i.e., when it is stored), it reduces the value of any exfiltrated data to the attacker. On a similar note, leaking the data no longer poses a threat since no one will be able to read that data. Thus, having a strong encryption scheme can go a long way in preparing an organization for a future ransomware attack. Additionally, it can make many other cyberattacks less-effective, especially those whose primary impact is the breach and disclosure of data.

3.3.2.1 Feasibility

From the organization's perspective, the recommendation to encrypt the data at rest may impose some additional burdens on the firm. For example, users of the system (e.g., employees) will need to provide a password to access any encrypted data. For example, in a Windows system, the users can use BitLocker Drive Encryption to encrypt the data. The system will then ask for a password and the associated key to decrypt and access the files. This also leads to other cybersecurity issues related to creating, remembering, and safekeeping of passwords in general. In environments where urgency weighs more than security considerations (e.g., hospitals), the users of the system (e.g., doctors and nurses) may use shared devices or reject 'slow' authentication procedures, further complicating the situation.

The choice of an encryption scheme becomes extremely important when the future capabilities of quantum computers are considered. While organizations need to choose a strong encryption scheme, ideally it should also be quantum-safe, i.e., it does not collapse under the enhanced searching and factoring capabilities of quantum computers. This is important as data that is exfiltrated and made public could be stored by criminals or other malicious actors waiting for the encryption to become vulnerable by means of quantum computers in the future. The advanced encryption standard (AES) is regarded as a quantum-safe scheme (Wang et al., 2021), and AES-128 (key size of 128), AES-192, or AES-256 can provide strong encryption while still being reasonably fast in performance (Nadeem & Javed, 2005). There is also some **performance overhead** that should be considered when encryption is added to the regular system processes. Encryption of large amounts of data can impact system performance and encrypting the data both at rest and during transmission can be very expensive in terms of performance. Therefore, we suggest that the organizations at least encrypt the data at rest to build one layer of defense against ransomware.

The **system encryption keys need to be securely stored and isolated** from the normal system data, so that the attackers do not get them during the data exfiltration process. Therefore, there needs to be isolation in terms of the system storage and the organization's IT architecture may not be a suitable platform for that. One option is to use an USB flash drive to isolate the keys from the system storage, and that adds the burden of carrying the USB drive and keeping it safe to access the system. The use of a third-party external encryption system such as Microsoft's Azure key vault or Google's cloud key management can help keep the encryption keys secret in

the cloud.

There is some management overhead in involving encryption in the organizational structure. Not all organizations have the technical expertise readily available to encrypt their entire database and/or parts of it that contain more critical data. Organizations may lack the policies to determine what parts of the data is considered critical, and whether it is critical ethically (e.g., important to the customers) or for business continuity. The organization may have to hire a, external security service or purchase automated tools. This can also become quite expensive and not all organizations, especially smaller organizations, may have the budget allocated to support it.

This approach only reduces the threat of disclosure of data and is not enough to prevent the attacker from asking for a ransom on its own. For example, the attacker can still encrypt the system database on top of the system encryption (double encryption) and make the system unusable. The organization will need to decrypt the outer layer of encryption done by the ransomware attacker, and the keys needed can only be gained by paying a ransom to the attacker. However, having a scheduled backup policy in collaboration with the encryption of critical data can greatly help mitigate the two most consequential aspects of ransomware.

It must be noted that while encryption does reduce the risk from data exfiltrated from the system, it does not guarantee that sensitive data will not be compromised. In order to be useful, system data must be accessible to legitimate users of the system, Consequently , techniques such as remote access Trojans (RAT) can covertly view and modify user files and functionalities, bypassing the encryption algorithms altogether (Kara & Aydos, 2019) these now have turned into attacks that demand ransom or steal user's information. Malware designed for these purposes cause losses of reputation, customer and market loss problems in addition to user's financial losses.

3.3.2.2 Relations to existing regulations

Under PIPEDA, businesses are responsible to use appropriate security safeguard measures to protect personal information against loss, theft, or any unauthorized access, disclosure, copying, use or modification which obviously includes the case of cyber-attacks like ransomware.

PIPEDA does not provide specific security measures to safeguard personal data, instead, it assigns this responsibility to the organization or businesses subject to the law, requiring them to develop and implement a security policy to protect personal information and use appropriate security measures to provide the necessary protection

Under PIPEDA, businesses are required to:

- Report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals;
- Notify affected individuals about those breaches; and
- Keep records of all breaches.

While issues regarding Ransomware may not seem directly related to PIPEDA, this may not be precisely true. The first ransom following a ran-

somware attack is demanded in exchange for restored system and data availability. Many attackers often follow up with a data disclosure threat, where they threaten to disclose previously exfiltrated sensitive data (e.g., customer name, passwords, location, social insurance number, and credit card credentials). In other cases, this malicious action is followed by a threat to sell the data to interested parties (e.g., associates, competitors, nation states). The fact that the possibility exists for sensitive data to be already exfiltrated whenever a ransomware attack first occurs is enough for it to be considered a possible data breach. Ransomware attacks should be reported to law enforcement agencies and like the Canadian Centre for Cyber Security and failure to report that to the Office of the Privacy Commissioner of Canada (OPC) and affected individuals or businesses may be subject to court action, regulatory compliance audits initiated by OPC based on victim complaints, and public disclosures that can harm their organizational reputation (TELUS Business, n.d.).

3.3.3 Recommendation 3: Security Education and Training Awareness (SETA)

Ransomware cannot be studied in complete isolation from other forms of cybercrime, as various activities, namely phishing, are often intertwined in the process of a ransomware attack.

Threat actors deploy ransomware on a corporation's computer or servers) using access gained via phishing emails that direct the recipient to infected websites or to download compromised files (Mitre, n.d). Unsuspecting businesses and employees receive these emails, unaware of the malicious content, leading to the entire organization falling victim to the ransomware attack. In recent years, threat actors have honed their tactics, utilizing sophisticated and unique forms of phishing that are particularly challenging to detect, such as spear phishing, which involves personally targeted individuals receiving well-crafted and contextually relevant messages (Jampen et al., 2020) Incidents such as the WannaCry Ransomware attack illustrate how phishing presents legitimate threat to systems around the world.

Given the prevalence of phishing and ransomware attacks, it is evident that small businesses need to address the risks posed to their operations. The research presented in the following section underscores the importance of enhancing the average computer user's ability to identify suspicious emails, especially in professional environments, where a single malicious file downloaded on one computer can jeopardize an entire system. Human behaviour plays a significant role in combating phishing attempts, making it a crucial protective measure against ransomware. (Jampen et al., 2020)

3.3.3.1 Recommendations

With Canada witnessing a significant increase in ransomware attacks (Canadian Centre for Cybersecurity [CCCS], 2021) ,small businesses must take proactive measures to safeguard themselves from financial ruin and reputational damage resulting from victimization (Ransomware Playbook, 2021; CCCS, 2021). An essential challenge in addressing phishing is the lack of awareness among users. Many indi-

viduals remain unaware of how to spot signs of scams and attacks, rendering them vulnerable to phishing and social engineering attempts. While small businesses may not be able to implement expensive and complex security systems, they can prioritize completing basic Security Education Training and Awareness (SETA). This training could drastically reduce their risk by limiting the impact of ransomware threats leveraging phishing to gain initial access to systems.

Although relevant government bodies have developed cohesive, practical, and cost-effective best practices, this information is generally posted this information online rather than being directly distributed to small businesses. Our policy recommendation is to use alternative mechanisms to distribute the already developed resources so that they reach the businesses that do not have a technology focus and consequently likely do not seek operations advice online. This group may well represent the greatest opportunity for risk reduction as they would be the most likely to benefit from low-cost changes to their operations. In particular we would recommend a focus on distributing the following resources to businesses while also implementing evidence-based alterations and improvements to the current resources:

3.3.3.1.1 The Ransomware Playbook

The effectiveness of the ransomware Playbook resource might be limited due to its lack of distribution, resulting in small business owners not being adequately reached. To address this issue, we propose that the CCCS takes proactive steps to directly send these materials to small business owners via email or mail, with special attention given to those with fewer than 10 employees who may lack dedicated IT staff and cybersecurity practices. Furthermore, the CCCS should focus on distributing an annually updated resource package to small businesses, offering concise and practical advice on preventing and mitigating the impacts of ransomware.

In order to drive change in the workplace effectively, the CCCS must convince business owners that adopting best practices to protect against ransomware is not only in their best interest but also essential for the survival of their businesses. While recent data from the government of Canada shows that many businesses have taken steps to prevent ransomware, there

Case study: The WannaCry Ransomware Attack:

The WannaCry ransomware wreaked havoc in May 2017, infecting over 200,000 computers across 150 countries and targeting various institutions, including government agencies, hospitals, businesses, and educational institutions. This widespread attack caused an estimated $4 billion in damages worldwide. The WannaCry ransomware infected computers via phishing emails that contained malicious attachments or links. The emails were designed to look like legitimate messages from trusted sources, such as banks or government agencies, and often included a sense of urgency to encourage users to open the attachment or click on the link. Once the user clicked on the attachment or link, the ransomware was downloaded and executed on the user's computer, encrypting their files and demanding a ransom payment in exchange for the decryption key. This case highlights the incredible risk that momentary error in a business setting can have devastating impacts on an entire enterprise (Herrera Silva , Barona López, Valdivieso Caraguay, & Hernández-Álvarez, 2019).

is still a need to encourage and support small and under-equipped enterprises to embrace a more cyber-aware workplace. Some findings shed light on flawed thinking that may be prevalent in small businesses:

Research indicates that business owners may overrate their ability to detect and respond to cyber threats, making them more vulnerable to ransomware attacks. Studies conducted in the Netherlands suggest that entrepreneurs do not perceive their businesses to be at high risk of victimization, an optimistic bias that hampers the implementation of self-protective behaviours and a proper understanding of ransomware risks. Additionally, entrepreneurs may overestimate the effectiveness of their current security measures and their own ability to safeguard their companies. This overconfidence bias creates a false sense of security and prevents them from identifying gaps in their cybersecurity measures (Bekkers et al., 2023).

Similar findings in research on individuals (i.e., not just business owners) indicates that those who are overly optimistic about their online safety are less likely to take proactive measures to protect themselves and are more prone to engaging in risky online behaviour (De Kimpe et al., 2022). These insights underscore the need for better education on the risks of online threats, particularly ransomware, and emphasize the importance of business owners critically evaluating their own biases and awareness of cybercrime, as well as the biases of their employees. Therefore, as the CCCS addresses the growing risks of ransomware for small businesses, it is vital to consider and address potentially flawed risk perceptions among owners and employees and enhance their cyber threat awareness.

3.3.3.1.2 Get Cyber Safe

The Canada Center for Cyber Security Website offers valuable resources aimed at educating both business owners and citizens about common cybersecurity issues. Of particular relevance to ransomware, they provide information on recognizing the red flags of phishing, social engineering, malware, and unsafe websites (Get Cyber Safe, n.d).

Based on the academic literature surrounding phishing training, the Get Cyber Safe delivery method exhibits several clear strengths, along with room for improvement. One notable strength is the use of graphics and clear language, which is a highly effective way of delivering information (Bullee & Junger, 2020). However, while the Get Cyber Safe training materials offer a comprehensive explanation of common cyber risks, they may not be as robust as designed for training small business employees, as indicated by extensive academic assessments of SETA. To enhance this resource, we recommend implementing the following improvements:

3.3.3.2 Develop phishing detection training games

We strongly recommend that the government develop a comprehensive range of educational materials for cybersecurity training, integrating gamification elements such as games and brief tests. Research has shown that incorporating gamification into phishing training can reduce vulnerability and enhance the effectiveness of the training compared to traditional text-based or imagery-based methods (Bullee & Junger, 2020).

Interactive games and quizzes that assess users' ability to detect phishing, followed by immediate feedback on their performance, can be highly effective. Users who receive feedback on their phishing detection skills can better reflect on their mistakes and improve their understanding of potential threats. Such interactive programs tend to yield stronger results compared to passive training methods where users are not actively engaged in the learning process.

In the context of gamification, it is important that the training games include real-life examples of phishing attempts, allowing users to practice their skills in realistic scenarios. Additionally, training involving the execution of tasks with interactive questions and answers ensuring active participation can aid in knowledge retention. The inclusion of informative feedback and explanations for incorrect answers further enhances the learning experience and reinforces users' understanding of phishing tactics.

3.3.3.3 Distribute Booster trainings on a frequent basis

Research emphasizes the significance of recurrent training sessions in reducing the likelihood of falling victim to cyber attacks. While the ideal frequency for administering booster sessions may lack consensus, the research community generally agrees that multiple training sessions over time are more effective than a one-time training event. Jampen et al. (2020) present a common pitfall in SETA implementation being training programs as single occurrences, leading to infrequent exposure to simulated phishing emails and educational materials This lack of recurring training could result in employee complacency and a false sense of security, rendering them more susceptible to phishing attacks (Reinheimer, Aldag, Mayer, & Mossano, 2020). By providing booster training materials to small organizations, it serves as a regular reminder of the constant threat of ransomware victimization and strengthens cyber threat awareness.

3.3.3.4 Continuously Improve Security Education and training awareness (SETA) to combat spear phishing with Evidence Based Practices in mind.

With the threat landscape of ransomware constantly evolving, Get Cyber Safe bears the responsibility of continuously updating their training practices to ensure businesses and their employees have an up-to-date understanding of novel ransomware attack techniques. We strongly urge Get Cyber Safe to develop a wider selection of training materials, with a particular focus on combating spear-phishing—an effective technique where attackers tailor phishing emails for each victim based on acquired information. Spear-phishing can be challenging to identify as the content is often extremely realistic and perfectly tailored to the recipient's experience. Research by Jampen et al. (2020) emphasizes the need for training programs to include examples that are highly relevant to the specific organizations, as spear-phishing attacks can differ significantly depending on the targeted industry.

To improve the effectiveness of "Get Cyber Safe" materials for small businesses it could include industry-specific examples of spear-phishing. Tailoring the training content to address the unique challenges and vulnerabilities faced by different industries will help employees relate

better to the scenarios presented and learn how to detect and respond to spear-phishing attempts that are relevant to their roles.

To ensure the quality and effectiveness of the training materials a stronger connection with scientific researchers and evidence-based research is essential. Integrating findings from academic studies and incorporating best practices documented in research will enhance the training modules and provide businesses with the most effective tools to defend against ransomware and other cyber threats (Jampen et al., 2020; Ransomware Playbook, 2021; Bullee & Junger, 2020).

In summation, a tripartite strategy that focuses on spear-phishing, industry specific materials and evidence-based continual improvement could assist GetCyberSafe in assisting Canadian Small businesses. Spear-phishing remains a highly effective technique, exploiting individuals' vulnerabilities with tailored emails. By targeting this specific method, we address a pervasive and challenging threat for organizations across different industries. Tailoring training content to industry-specific challenges enhances the effectiveness of learning and response. Incorporating evidence-based research strengthens the quality of "Get Cyber Safe" materials, equipping businesses with more effective tools to defend against ransomware and other cyber threats. This proactive approach fortifies cyber resilience within small businesses, creating a more secure digital environment.

3.3.4 Moving Beyond Formal Regulation

Many departments of the federal government are concerned about cybersecurity in small businesses. (Government of Canada, 2021) The federal government is collaborating with provinces, territories, and the private sector to increase cybersecurity in Canada under the National Cyber Security Strategy.

While both hard law and soft law to increase cyber resilience exist on different levels, there appears to be a disconnect between recommended best practices for small businesses and their actual practices. Hard law, enforced through fines, could be an option to increase compliance with recommended best practices but it does raise questions of who would regulate and who would be regulated. While a universally high level of cybersecurity throughout Canada must be the goal, provinces and territories, as the entity closer to individuals and businesses, generally have jurisdiction for formally regulating industries within their limits. Where federal regulation is possible, small businesses might nevertheless struggle to fulfil regulatory requirements. With limited financial and personal resources and without legal department, keeping ahead of laws and compliance is understandably a difficult task.

Where formal regulatory approaches are not effective, other modes of regulation could come in. Besides law and government-issued guidelines, small businesses are also impacted by informal "regulation" (Lessig, 2006). Lessig identified three non-law systems that regulate the behaviour of an individual or business: norms, digital and physical infrastructure and the market. Behaviour shaped through norms might result from personal or social values. Infrastructure plays its part by enabling or restricting behaviours, such as the ease or difficulty of using an encryption pro-

gram Finally the market can influence behaviour through differentially valuing the goods or services offered and shaping prices. These three non-law systems regulate on their own. However, Governments can influence them to indirectly address a behaviour (Lessig, 2006). For example, an advertisement campaign could influence social norms, ultimately leading to a change in behaviour. On the infrastructure side, the configuration of software could encourage, discourage, or make technically impossible certain behaviour. The government can also impact the market through taxes, subsidies, and quality standards and thereby create certain expectations among market participants (Lessig, 2006). Many assume we must treat norms, digital and physical infrastructure, and the market constraints as a given. However, governments and businesses (and to certain extent the individual) can influence these informal "regulators" to achieve a higher goal (Lessig, 2006).

3.3.5 Particularities in Small Business's Decision-Making

As small businesses are all participants in various market, secure practices can be incentivized through those markets. At the core of the markets power to influence change is the regulating power of price (Levi-Faur, 2011). Among two similar products, the consumer will often choose the cheaper option. Consumers with a heightened awareness of cybersecurity that consequently place great value on that security could prefer those services or products that present cybersecurity as a part of the product, such as through a cybersecurity certification. In this way, customer preferences could incentivize secure practices in small businesses. However, it also appears that not every industry is equally affected by consumer awareness. For example, a customer be less likely to decide on a flower shop based on their cybersecurity but based on their bouquet variety and quality. However, small businesses operate in multiple markets and their profitability is dependent on the goods and services they purchase as well. Some of these services are insurance and banks. It is hard to imagine a legitimate small (or large) business without a formal bank account or without an insurance advisor.

Decision-making in small businesses is often centered around the owner or managers, (Alahmari & Duncan, 2020). Especially in small and family businesses, the founder and owner has large influence on all levels of the business. Their views and experience will impact the decisions they take, and once they set their mind on something, they might not easily be changed in their assumptions (Schein, 1995). Naturally, the initial owner who starts a business is highly interested and skilled in the services the business specializes in. However, unless they are operating a cybersecurity business, increasing their knowledge about secure and resilient practices is likely not their primary interest. For example, a baker who is passionate about providing the best-tasting breads and cakes will likely have more interest in spending their working hours baking bread and cake, researching hygiene best practices, and developing new recipes. Even if the business is relying on online orders, email communication, and online banking, it is, understandably, not the primary concern of the bakery business. As a business owner, they already need to engage in support activities such as managing the business's utilities

contracts, overseeing payments and financial liquidity, and preparing tax declarations. As such, the owner usually already holds several positions within the small business (Alahmari & Duncan, 2020), managing cyber resilience on top of these roles might simply not be feasible for them. If an employee, skilled in cybersecurity, explains about the importance of secure practices, this might very well not reach the owner. However, owners must realize that certain partners are irreplaceable, such as their insurance provider. In this case, their views (or at least actual practices) about cybersecurity might be impacted based on insurance requirements or conditions. While not all owners would be motivated through their investment in insurance, there may well be other partners that could provide such motivation by means of a similar mechanism. The following sections therefore suggest that Cyber Risk Insurance can be used as a blueprint for conditions by other partners of small businesses.

It is often recommended that awareness about cyber resilience must be increased among those who access company information systems and especially among decision-makers in businesses (Alahmari & Duncan, 2020). But things aren't as easy as putting business owners' back into the classroom to learn about cyber resilience. They might not have enough resources to participate in training or to give on their skills to their employees. A constant requirement for more training can also lead to training fatigue.

As in all areas of life, however, the decisions by business owners and managers in small businesses are not uninfluenced by the outside world. While some obvious influence can be traced to direct advice by lawyers or tax advisors, other influence is more indirect. Their decisions can be influenced indirectly, among other aspects, by practices and requirements of their competitors, wholesale sellers, customers, and insurance companies. When a new practice is employed by a competitor, say, extended opening hours, increases their profit or publicity, a small business might be inclined to extend opening hours as well. Similarly, when the long-term wholesale seller a business owner is relying on changes to only accept a certain type of payment, the business owner might be inclined to start using this type of payment. And when, for example, auto insurance promises beneficial rates to those with formal driving lessons, a young business owner might be incentivized to participate in such formal lessons.

3.3.5.1 Possible Measures to Influence Small Business's Cybersecurity Decisions

This section suggests two ways forward, one involving Cyber insurance and the other involving Small Business financing. The processes and services related to Cyber Risk Insurance such as risk assessments and hotlines, such services can increase their clients' awareness of best practices and enhance their resilience.

Similarly, a cyber threat risk assessment could be included as part of the process for loans and financing options for small businesses. Beside improved cybersecurity practices among business clients, this approach might further decrease the risk of defaulting on a loan due to the impacts of a ransomware attack. Here, the federal government could include such risk assessments and other resources into the Canadian Small Business Fi-

nancing Program.

3.3.5.1.1 Cyber Risk Insurance

Lawrence Lessig (2006) presents regulation through the analougous case of the options by which the government can increase the number of car passengers wearing seatbelts. Apart from threatening punishment and public education campaigns, the more traditional way of regulation, governments could require cars to be built with automatic seatbelts, targeting the car technology, or "subsidize insurance companies to offer reduced rates to seatbelt wearers (law regulating the market as a way of regulating behaviour)." While subsidies are not always feasible, this example highlights how insurance policies can impact, or *regulat*e behaviour in insured persons.

According to Statistics Canada, 16% of Canadian businesses have a Cyber Risk Insurance policy. These insurances are seen as part of ransomware risk management as they frequently cover direct losses, data restoration expenses, and losses due to business interruption. Of those businesses impacted by a ransomware attack, 13% directly worked with their Cyber Risk Insurance provider to resolve the attack (Statistics Canada, 2022). Insurance providers can be an important "first responder" in ransomware cases, bundling resources and directing clients to reliable service providers or the police — similar to how auto insurers might have recommended repair workshops (CAA, n.d.) and pet insurers might offer a 24/7 emergency hotline (CAA, n.d.).

Apart from bundling resources, Cyber Risk Insurance policies usually require certain security standards to be met. Cyber resilience assessments are a component of Cyber-Risk Insurance Policies which involves asking businesses about the types of security measures in place to protect facilities and systems (Communications Security Establishment, 2022) Through risk assessments, Cyber Risk Insurance policies might be able to raise awareness about ransomware mitigation among small businesses. Specific conditions could directly encourage a business owner to implement security measures. For example, a policy might require backups of important office files every 30 days. In this case, a business owner can either implement such backup measures, or try to find a different insurance provider.

Cyber Risk Insurance are clearly not primarily concerned with paying ransom money; they can include "guidance on effective cyber security practices, free or discounted technical solutions, as well as post-breach remediation". (Mott et al., 2023, p2) As such, the process of getting a Cyber-Risk Insurance policy and adhering to the contractual agreements might act as a prevention method for ransomware, which, of course, is in the interest of the insurance company. Through pre-attack and post-attack services, the likelihood of an attack and the severity of it might be alleviated. Regardless, there are fears about attacks targeted at those businesses with Cyber-Risk Insurance Policies and, among the increase of ransomware attacks and interest in Cyber-Risk Insurance, many businesses might not be able to find an insurer willing to offer them insurance (Mott et al., 2023). Insurers might also struggle with the dynamics and potential chain reaction along interconnected digital service providers posed by ransomware attacks (Mott et al., 2023).

While insurance policies covering pre-attack

mitigation measures and supporting a client in data recovery after an attack are surely helpful, in certain cases the payment of ransom money is surely the "cheaper option" from a purely financial viewpoint. The clients of insurers known to pay more easily might be at risk of more frequent or more severe attacks. An interview with an anonymous member of a ransomware group suggested that targeting an insurer, retrieving their customer data, and then targeting their customers is especially appealing (Smilyanets, 2021). When a business owner expects to be targeted specifically because they have a Cyber Risk Insurance policy, their confidence in this insurance as a valid method of risk mitigation can be expected to decrease.

More broadly, however, it must be asked whether insurers paying ransom money in some cases counteracts the call by law enforcement agencies across the globe, including in Canada, to not pay the ransom money((Royal Canadian Mounted Police, 2021; Europol, n.d.; United States, National Cyber Investigative Joint Taskforce, n.d.). With this advice, law enforcement is trying to prevent ransomware from being a lucrative "business". Without incoming ransom payments, criminal organizations have a harder time attracting developers to design new ransomware. To not counteract this law enforcement strategy, Cyber Risk Insurance which regularly pays the ransom should not be officially recommended.

Cyber Risk Insurance could focus on covering the costs of recovery after an attack without ever paying any ransom money, such as covering costs for security specialists to attempt to retrieve encrypted data or to mitigate reputation loss. An insurer could provide the insured with the benefits of mitigating disruptive ransomware attacks and providing a support network without interfering with law enforcement's guidance. The option to rely on the knowledge of a professional Cyber Risk Insurer can help to take financial and administrative stress especially from small businesses which do not have many resources at hand and for who cyber incidents are often disproportionately more expensive compared to their business size (Mott et al., 2023), as well as preventing decision fatigue resulting from an overabundance of differing security guidance and checklists. However, the option of a safety net through an insurance could encourage a business to seek out that insurance instead of implementing secure practices (Westbrook, 2021) . A business owner might decide to get a Cyber Risk Insurance *instead* of implementing secure practices, thinking that the insurance will cover any negative consequences of an attack anyways.

Overall, the question whether to support Cyber Risk Insurance appears to be a complex one. Not all questions have yet been answered and many fears and hopes might eventually turn out to not be accurate. As such fast-evolving field, defining best practices for (cyber) insurance providers could work to prevent expected negative effects of Cyber Risk Insurance, be it payment of ransom money or an unintended incentivization of a *laisser-faire* attitude.

Based on these considerations, the government of Canada should consider:

- Leveraging existing forums to further increase cooperation across all levels of government to ensure the option of high quality of Cyber Risk Insurance for all Canadian busi-

nesses. All businesses, regardless of location, should have the option to incorporate reliable Cyber Risk Insurance as a part of their risk management. Insurance policies across Canada should ensure cooperation between the insured, insurers, and law enforcement, particularly regarding ransom payments.

- Further examining potential soft or hard regulations for Cyber Risk Insurance for incidents in federally regulated sectors and the effects of Cyber Risk Insurance on diversified risk management. This could consequentially shape the insurance landscape in other sectors, for example towards a focus on data recovery and reputation loss mitigation instead of ransom payments.

- Further researching options to create guidelines and provide educational information regarding Cyber Risk Insurance, both for insurers and customers considering insurance. This could include guidelines targeted at small business clients about what policy conditions to look for in a good Cyber Risk Insurance policy to be optimally prepared for mitigating a ransomware attack, potentially similar to the Credit Card Comparison Tool (Financial Consumer Agency of Canada, 2017).

3.3.5.1.2 Loans and Financing Options for Small Businesses

Cyber Risk Insurance might not be attractive to some small businesses as the risk of being target of ransomware might be perceived as low. Alternatively, Cyber Risk Insurance might be an expense a small business is not willing or able to afford. Consequently, an alternative mechanism is required to ensure that these business owners are reached and incentivized to implement ransomware resilient cybersecurity practices in their business.

Banks are already involved in educating customers about certain measures of cybersecurity (Get Cyber Safe, 2022) and protect customers in case of payment card fraud (Canadian Bankers Association, n.d.). Banks therefore could be said to already play a role in reducing the risk from cybersecurity threats to their customers and society in general. This is important as most businesses have a partnership with a bank, in that the bank provides them with financial services such as business accounts, and very often business loans.

For small businesses, loans have a large impact on the future of the business (Fracassi et al., 2012). Pu simply, without loans or financing options, some business plans are not feasible. On the other hand, where different loan conditions exist, the more beneficial conditions are likely more attractive to businesses. If a better interest rate or repayment plan can be offered when the business meets certain requirements, there is an incentive to meet those requirements where possible. These incentives can be designed to incentivize behaviours that are in the benefit of society or the long-term benefit of the applicant. For example, certain beneficial loan conditions are offered for financing the purchase or electric and hybrid vehicles (National Bank of Canada, n.d.), incentivizing the purchase of these vehicles over combustion engine cars.

A successful business generates and captures value to the benefit of the loan provider, as they are less likely to default on the loan. (Fracassi et al., 2012). Loan providers naturally have an interest in clients whose business is suc-

cessful and are disinterested in clients who have unsuccessful businesses. Unsurprisingly, businesses must meet certain conditions to be eligible for a loan, partially to ensure a low default risk. For example, a sound business plan is usually necessary for a start-up to receive funding (Desjardin, n.d.). Ransomware attacks can impact a business's financial well-being and future existence, thereby potentially causing a business to default on loans or even face bankruptcy. (Yuryna Connolly et al., 2020). As paying a ransom does not guarantee the restoration of normal business function (Bezanson et al., 2022)Therefore, robust risk mitigation strategies are essential to a business's financial well-being in case of an attack. As an example, loan conditions could include an incentive to have, a cyber incident response plan in place, which can reduce the degree of harm resulting from an attack.

Apart from private banks, the federal government is also involved in providing financing options for small businesses through the Canada Small Business Financing Program and "makes it easier for small businesses to get loans from financial institutions by sharing the risk with lenders." (Government of Canada, 2023). This program would allow the government to design and test cybersecurity incentivization strategies as a part of this financing. For example, Tech start-ups and those wishing to finance upgraded technological equipment could be incentivized to purchase secure technologies over less secure alternatives through information shared through loan process and beneficial conditions if secure technologies and practices are implemented. As the Canada Small Business Financing Program is implemented in partnership with private financing institutions, it would ensure that there is public-private coordination.

Mitigating the risks of ransomware attacks is similarly in the interest of small businesses and their financing partners. With small businesses being highly heterogeneous, some operating their own servers while others run entirely on free third-party email account, financing options must be available to all kinds of business types. A balance must be struck between high levels of cybersecurity and the feasibility of such measures in a variety of highly diverse businesses. Similar to formal laws, a federal approach in financing might not be able to reflect this diversity. However, given the importance of prevention and mitigation of ransomware at all levels within the Canadian society, some guiding action might be required. An approach of incentives, for example through beneficial interest rates, repayment plans, or other benefits depending on the business client's size and industry, could be an option.

Based on these considerations, private sector partners should consider:

- Providing incentives within their financing schemes for clients that already have a higher level of ransomware resilience, for example regarding backups. A higher level of resilience could potentially decrease the financial impact a ransomware attack has on the client, thereby increasing their financial well-being. However, consideration must be given to the heterogeneity among small business clients and between their industries.

- Providing attractive financing options specifically targeted at financing secure tech-

nology, similar to incentives to purchase an electric or hybrid vehicle over a combustion engine vehicle.

Similarly, the government of Canada should consider:

- Cooperating with the private sector to include base levels of cybersecurity as part of the Canada Small Business Financing Program and to consider federal financial incentives for improving ransomware resilience in small businesses.

- Further researching how ransomware attacks impact the financial well-being and continuing existence for businesses with differing levels of cybersecurity.

3.3.6 EU regulations for cybersecurity

3.3.6.1 Introduction

The European Union has long history of providing regulation and guidelines for cybercrime and cybersecurity. It prioritized ransomware in its efforts to reduce the harms from malicious uses of the internet. This section chronologically examines some of the efforts of the European Union to regulate cybercrime and cybersecurity over the past decade.

3.3.6.2 NIS

In 2013, the EU implemented legislation called the EU Cybersecurity Strategy, which included the EU Network and Information Security Directive or NIS Directive (European Union Agency for Cybersecurity, n.d.). According to this directive, EU member states must build a security culture across critical infrastructure sectors including: energy, transport, water, banking, financial markets, healthcare, and digital infrastructure. The NIS directive describes these sectors as drivers of essential services; therefore, it requires them to adopt steps to manage security risks and to report cyber-attacks to the corresponding national authorities. Additionally, it defines a digital service as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." (Directive (EU) 2015/1535 of the European Parliament, 2015) This definition includes cloud services, providers, and online marketplaces. The required security measures are to be taken or implemented according to the proportion to the risks presented on a case-by-case basis. They should include technical and organizational measures that are fitting and proportionate to the risk, ensure the security of the network and information, and prevent and minimize the impact of incidents on the IT systems used by the services (European Union Agency for Cybersecurity, n.d.).

Although the Directive highlighted that EU states should increase their awareness of cyber-attacks, it did not specify a framework for tackling ransomware attacks.

3.3.6.3 The Cyber diplomacy toolbox

By 2017, The EU established a framework for a joint EU Diplomatic Response to Malicious Cyber Activities called the "Cyber Diplomacy toolbox." This framework "is expected to encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term" (European Council, 2019). This initiative incorporates all measures, including

sanctions, in a joint response to malicious cyber-attacks. It highlights the importance of cooperation of all member states in all cyberattack responses. It concludes that the response must be proportionate to the scope, scale, duration, intensity, complexity, sophistication, and impact of the cyber activity (European Council, 2019).

According to the toolbox, cyber-attacks that may cripple a member state's banking system or energy network are comparable to military attacks. Therefore, the member states agree that international law applies to cyberspace (Moret & Pawlak, 2017). It sets guidelines for countering malicious cyber activity, which include preventative measures, including awareness raising of EU cyber policy; cooperative measures in the form of diplomatic dialogue among member states; stability measures such as official statements by EU leaders; restrictive measures (sanctions); and EU support for member states when being the target and victim of an attack (Lațici, 2020). In this context, this initiative allows states to take necessary measures, which include the response to ransomware in the form of sanctions.

Additionally, the cyber diplomacy toolbox emphasizes "situational awareness," which asserts that while each member state is free to make political decisions concerning offensive cyber activities, collective assessment and action are necessary for an effective response. Furthermore, the EU Cyber diplomacy cooperates with multiple global cybersecurity projects and partnerships (e.g., CyberEat, EUDigital, OCWAR-C, YAKSHA).

3.3.6.4 NIS2

The NIS2 Directive (2022) builds on the prior National Information Systems (NIS) directive providing legal measures that increase the level of cybersecurity. This directive requires that EU member states be equipped to respond to cybersecurity threats, such as by having a Computer Security Incident Response Team (CSIRT) and an adequate national Network information authority (NIS). Additionally, it sets out harmonized sanctions across the EU for potential offenders. The NIS2 obliges member states to measures to protect the information systems, which include:

"(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management, disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use

of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate." (NIS, n.d.):

The European Union acknowledges that ransomware is a global problem which requires cooperation with international partners. Accordingly, the EU signed a joint EU-US statement to address ransomware cooperation. The statement highlights that law enforcement, raising public awareness on protecting networks and the risks associated with paying cyber-criminals, are necessary steps to protect against ransomware (European Council, 2021).

3.3.6.5 Counter Ransomware Initiative (CRI)

The Counter Ransomware Initiative is the international cooperation commitment between the European Union, the US, Eastern European states, The United Arab Emirates, Korea, Israel, Japan, Kenya, Ireland, the United Kingdom, South Africa and Nigeria to counter ransomware (Council of the EU, 2021). These states specifically commit to cultivating resilience, disrupting ransomware, pursuing offenders, fighting illicit finance that supports ransomware, and working with the private sector toward the same objective. To achieve these goals, CRI members established five working groups: Resilience, Diplomacy, Disruption, Countering Illicit Financing, and Public-Private Partnerships. In practice, member states commit to:

- Hold ransomware offenders accountable and deny them safe haven
- Implementing measures against money laundering and the financing of terrorism. These include know-your-customer rules (KYC).
- Bringing offenders to justice under each member's applicable laws, and
- Collaborating to address ransomware. (The White House, 2022)

3.3.6.6 GDPR The General Data Protection Regulation

In 2016, the EU agreed upon the GDPR as the primary law to protect citizen data. It imposes regulations for all organizations that collect data related to EU citizens (GDPR, n.d.). The requirements of the GDPR include a set of principles upon which corporations or companies should process people's data. These principles include lawfulness, which enforces fair and transparent processing; purpose limitation, which enforces that processing data is only for the purposes specified when collected; data minimization, which requires the minimal collection of the data for the specific purpose of that process; accuracy; storage limitation, which limits the length of data storage; integrity and confidentiality; and accountability. In practice, the GDPR generally requires the private sector to obtain consent for processing people's data, anonymizing that data, and putting in place security when transferring data across borders. Those who fail to comply with these principles cane be subject to fines.

3.3.6.7 Challenges with regulations in the EU

Concerns with the current EU approach to cybersecurity, including measures to address ransomware, point to the challenging aspects of working with the private sector, negotiating with offenders and the prevalence of ransomware despite measures and regulations.

A European Union Agency for Cybersecurity (ENISA) report highlights that the total number of ransomware attacks is more significant than what is publicly available, as the private sector does not report all incidents to the authorities (European Union Agency for Cybersecurity, 2022). Companies may attempt to deal with the attacks internally to avoid negative publicity. In this manner, cultivating a sense of cooperation between the private and public sectors to map all attacks and enforce the law on offenders has become a difficult task.

While ENISA may "strongly recommend" sharing and reporting the ransomware incidents, as long as there is a reputational or business continuity risk associated with reporting, the private sector may continue to handle incidents privately.

Additional challenges are raise by considering the variation in the what cybersecurity represents to stakeholders in different sectors (Fischer-Hübner et al., 2021). In the context of banking, the cybersecurity threats they face are increasingly more professional which combined with the consumer demands for near real-time services create limit the ability of the banks to react effectively to prevent disruptions.

It is also important to note that even with the cooperative agreements and toolbox, the member states maintain their sovereignty within their national borders. As a result, the processes for cooperation between law enforcement agencies include additional levels of translation, validation and verification that slows the pace of investigations.

3.3.6.8 Considerations Before Adopting Regulations

Based on presented EU context, the following recommendations are relevant in an age of ransomware:

- Regulations should take into consideration the legislative context in which they are enforced: regulation relies on the local context and cannot simply be transferred to a different context;

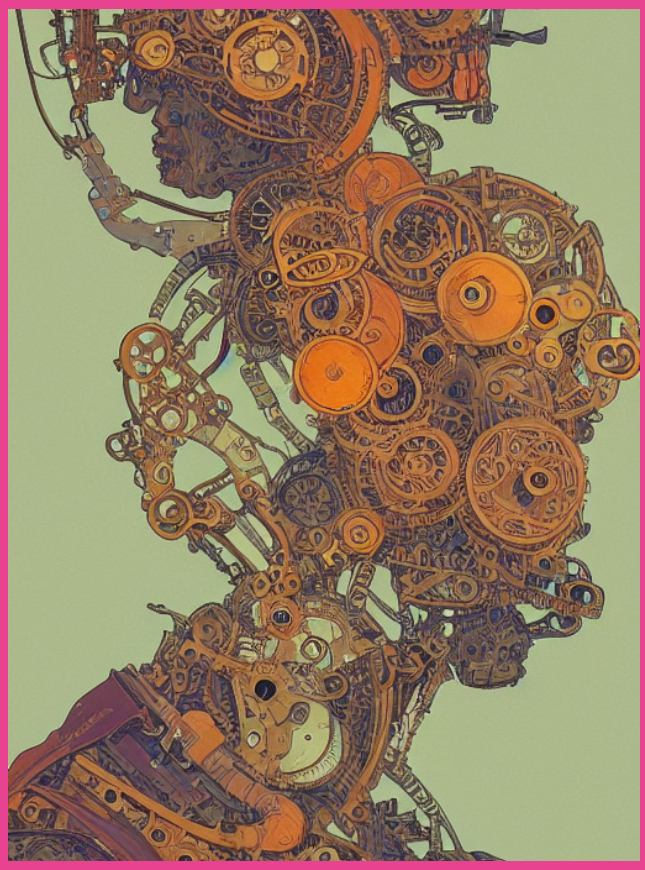
- Efforts should include cooperation with the private sector. Regulation that does not reflect the realities of a specific industry or for a particular business size might discourage trust in regulators;

- The rationale of regulations should be defined clearly to determine whether their objective is to "coerce targets, to change their behaviour, constrain their activities or access to resources" (Moret & Pawlak 2017). Regulatory instruments should be tailored to specific outcomes while maintaining a balance so as not to unnecessarily increase the complexity of the legal landscape;

- Due to the global nature of cybercrime and ransomware, regulations should permit situational awareness. The complexities of attribution in multi-jurisdictional investigations

across cyberspace can require delicate and consider approach so as to strike a balance between operational and political considerations; and

- Finally, the international nature of the cyber law should be considered when drafting regulations. While different states have different priorities and approaches to regulation there is a need for a general coherence in order to ensure a minimum level of efficacy. For example, the introduction of a new encryption standard that is not compatible with the standards of other nations could result in a negative response.



Behaviour

4 Behaviour

4.1 Behavioural System Model

The many different players and interactions that are that make up the cybersecurity ecosystem result in a very complex and chaotic environment. The practice of concept modelling allows for such systems to be represented in a manner that enables a greater understanding of their important aspects. Concept modelling is a common technique within the field of information systems. Consequently, the representation of cybersecurity systems that include the human in this manner provides the additional benefit of allowing the communication of social concepts in a language that is native to computer engineers. This section will explain this

model and its importance for this paper.

4.1.1 Information System Model

The Information System Security Risk Management (ISSRM) Domain Model is an established model that is used to describe the key concepts and relationships in information system security (Matulevičius & Abasi-Amefon Affia, 2018). This model separates information system concepts into three categories: asset-related concepts, risk-related concepts, and risk treatment-related concepts. Asset-related concepts refer to the assets in the system that need to be protected with respect to the security needs of the system, risk-related concepts refer to security risks in the system that exist due to vulnerabilities in the system, and risk treatment-related concepts refer to decisions that will attempt to mitigate risk in the system.

One of the main takeaways from the ISSRM domain model is that vulnerabilities in a system give rise to threats, and that the realization of a threat is an attack. In short, in a perfect world, if there are no vulnerabilities in a system, there cannot be any threats, and therefore no attacks can occur. It is important to note that in the ISSRM domain model a threat is seen as a potential of an attack, and it does not necessarily mean that there exists an actor with desire to make an attack. An attack in the domain model is simply seen as an actualization of the treat.

Due to its usual focus on the technical aspects of a system the ISSRM domain model is complicated and contains may technical elements. These technical specifications are unnecessary for our purposes as they direct attention to the technical and reduced the generalizability of the model to non-technical issues. As a consequence, we have created a simplified model based on the ISSRM model is shown in the figure below. This model illustrates the core concept of the ISSRM, that the existence of threats is reliant on the existence of vulnerabilities, and that attacks are the actualization of threats to the system. It is important to note that we define system in this paper as a collection of interacting computer components in the organization, were each component and interaction is prone to having vulnerabilities. This definition of system therefore includes all software and hardware technologies used in the organization, and the technologies of communication used to allow different computing components to interact. In the work done by Matulevičius & Abasi-Amefon Affia, they define system assets as the individual system components that make up a system that support the business assets (i.e., business items) of the organization (Matulevičius & Abasi-Amefon Af-

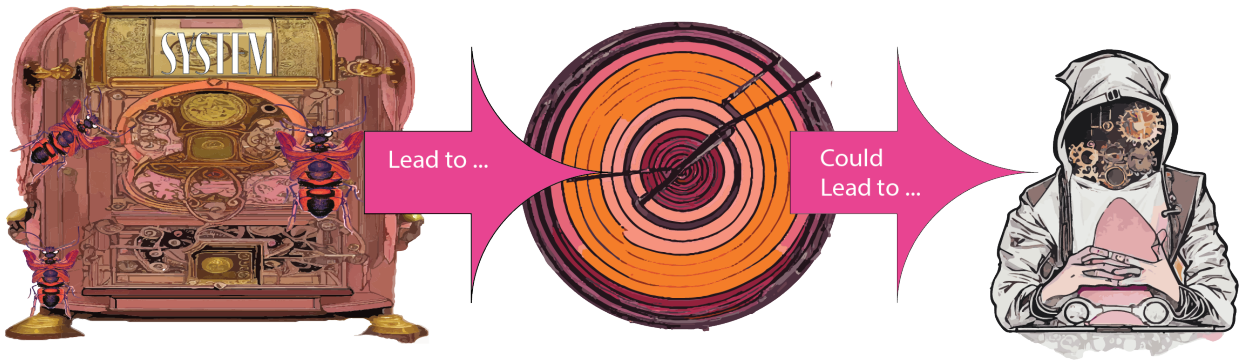


Figure 2 - General system cybersecurity threat model

fia, 2018). Therefore, the proposed definition of a system is based on the idea of having multiple system assets.

4.1.2 Introducing Behavioural Concepts to The System Model

The model presented above can easily be extended to include human behaviours. It is important to remember that attacks are the realization of threats. Which is to say that there are two components to an attack, the threat and the realization. Consequently, we can categorize human behaviours that lead to attacks as being either those that introduce a threat and those that realize an attack. The introduction of a threat to the system, or a vulnerability introducing behaviour, would be actions that give rise to vulnerabilities in the system. As an example, a developer accidentally programming a vulnerability into the system would be categorized as a vulnerability introducing behaviour.

Alternatively, those actions that realize a threat into an attack are considered to be threat realization behaviours. For example, suppose an employee clicks a link by accident and downloads malware to the company server; this would be categorized as a threat actualization behaviour since clicking on the link actualized a threat into an attack on the system.

The General system cybersecurity threat model presented above can be augmented to include these concepts as is shown in the figure below.

4.2 Behavioural Groups

This section will describe in more details about the behavioural groups that will be studied in this chapter.

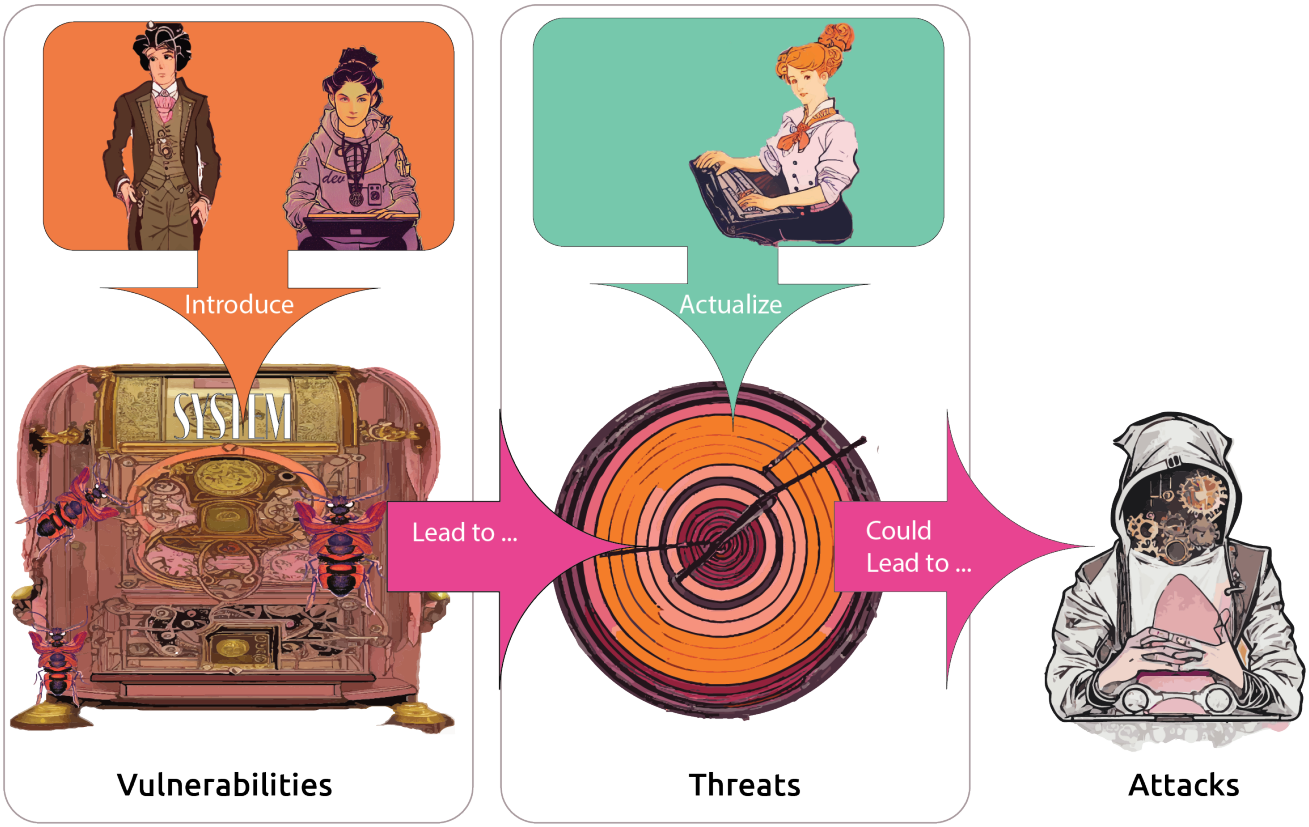


Figure 3 - Cybersecurity System Behavioural Model

4.2.1 Vulnerability Introduction Behavioural Group

Some actions can introduce vulnerabilities in the system. The most obvious behaviours that belong to this group would be those performed by system developers, since the computer and architectural changes made to the system can directly introduce vulnerabilities. However, developer behaviours cannot be seen as the only source of decisions made on the system design as there are many other actors involved in the process of software development. As a consequence, there are other behaviours that indirectly influence a system design that must also be included. For example, a client may request specific features or an employee in risk management can make recommendations that are reflected in the system design, input that could result in system vulnerabilities. As a result of this complex of behaviour that influences the design and implementation of software, the developers cannot be made responsible as if they were the only source of decisions made on the system design. To better understand how a system design was developed with certain vulnerabilities, all behaviours surrounding the decisions on how these vulnerabilities were included must be considered. We note that malicious behaviours in this group (i.e., those of insider threats) will not be examined in this paper. While not much is known about the relative impact of the deliberate introduction of vulnerabilities into software when compared with the accidental vulnerabilities, we would suggest that as with most other human endeavours, accidental causes of harm would be more likely. For example, in 2021, 6.2% (19,257) of deaths in Canada were as the result of an accident (Statistics Canada, 2023), more than 24 times number of deaths by homicide (788) (Statistics Canada, 2022). As the decision-making behind intentional harm and accidental harm could be considered to be significantly different, we will concentrate on accidental causes as it is likely the greatest source of harm.

In this report, the main behaviours we focus on for this group are:

- System developer behaviours
- Risk management behaviours
- Operational behaviours
- Business behaviours

4.2.2 Threat Actualization Behavioural Group

A vulnerability, or threat in the system often requires an action in order to be realized. As a consequence, we could group those behaviours that would cause any threat in the system to be turned into an attack. Both individuals inside and outside the organization could be responsible for these behaviours. Internal actors can therefore accidentally, act on threats that exist in the system due to vulnerabilities and allow the creation of attacks.

However, due to it being difficult for organizations to control the behaviour of external actors, we focus on only the behaviours from internal actors in this paper. Similarly, for the same reason as in the vulnerability introducing behaviours, malicious actors will not be studied in this group. It should be noted that individuals typically belonging to the vulnerability introduction behavioural group, such as software developers or risk managers, can

also belong to this group as any employee can theoretically act on threats that exist in a system. Therefore, if we exclude external actors, we can say that this behavioural group includes the behaviours of all employees in the organization that allow the realization of threats into attacks.

4.3 Vulnerability Introducing Behaviours

Developers, engineers, and technical personnel are at the forefront of software development. People in these positions directly impact the code base and architecture of the products they develop. The decisions and actions these technical personnel make throughout the various stages of development (from proposal to implementation, to testing, to deployment) dictate the security and stability of their products. Therefore, they are immediately responsible for vulnerabilities that appear in a system that can be exploited to execute a successful ransomware attack. However, it is crucial to recognize that these developers did not introduce vulnerabilities intentionally. Investigating and understanding the behaviours and circumstances that led to the introduction of vulnerabilities is not to assign blame, rather it is to address these behaviours and make recommendations to replace the vulnerability introducing behaviours with behaviours that lead to more secure and robust software development and maintenance. This section gives an overview of prominent causes behind behaviours that lead to the introduction of security vulnerabilities in applications and systems. In order to examine a greater range of contributing factors we will expand beyond development-oriented analysis frameworks (i.e., DEVOPS). We also provide recommendations to change these behaviours.

4.3.1 Design Failure

Even the most powerful companies in the world with the most talented developers may introduce security vulnerabilities when designing and developing systems if the design of the system do not adequately consider cybersecurity.

In 2018, Coincheck, one of the biggest cryptocurrency exchanges, was hacked and lost 526,800,010 XEM tokens, which were equivalent to 500M USD at that time (Suga et al., 2020). A root cause for the threat was the use of an inappropriate cryptographic algorithm and corresponding parameters to generate the private key and the public key pair. As a result, the multi-signature scheme, a more secure solution to manage the keys, unable to be implemented (Suga et al., 2020).

If the engineering team used a more secure encryption algorithm at the beginning, this attack would have been avoided. However, security was seen as an afterthought, rather than a fundamental system requirement (Jaskolka, 2020). This seems to indicate that strong security measures were not allocated the importance as the functionality of the system in its design. As this system was a financial system that could be considered as being more likely to be targeted by external actors it could be considered a design failure to have not given a greater priority to security.

4.3.2 Optimism Bias

Decision-making regarding security strategy could be compromised due to optimism bias. Optimism bias plays a problematic role when developers or managers assume their organization or product is not an attractive target for attackers (Assal & Chiasson, 2019; Rhee et al., 2012). This line of thinking poses significant risks as the decision to compromise a system may not be based on its attractiveness. While attackers may target entities that appear more attractive, they can also indiscriminately target vulnerable systems (Hayes & Bodhani, 2013). Regardless of perceived attractiveness, robust security practices should not be disregarded, as the consequences may be severe.

4.3.3 Project Management Constraints

Project management constraints, as known as the project management triangle or project triangle, is a classical model in business management (Van Wyngaard et al., 2012). The project triangle involves three interdependent dimensions: time, scope, and cost. When an organization in any field makes big decisions for the project, they should consider at least one point of these three. In this section, we discuss constraint dimensions and how these constraints can contribute to the introduction of vulnerabilities in a system.

4.3.3.1 Time Constraints

Time plays a significant role when we make decisions. In a normal development work-flow, the product team, engineering team, and quality assurance (QA) team evaluate a proposal or a project and agree on a feasible delivery date. The estimated time is generally based on experience but due to the rapidly changing security requirements for projects, these estimates may be insufficient. Thus, developers may not have adequate time to implement all security requirements. When developers are pressured to deliver code quickly it increases the likelihood that issues and bugs are produced.

Actions and decisions made under time constraints can impact quality assurance initiatives. For example, Heartbleed, a severe security issue in the cryptography library OpenSSL, was found in 2014 (Zhang et al., 2014). On reason behind this issue is that there were only two full-time engineers on this project, and they did not have enough time for testing and code review (Walsh, 2014). Unfortunately, OpenSSL is one of the most widely used libraries to secure the channel between servers and clients. This vulnerability exposed a massive security issue, resulting in sensitive data leakage, unauthorized access, and other threats. This example emphasizes the impact that time constraints may have on systems on a wide scale.

4.3.3.2 Scope Constraints

The limitation of scope demands the attention of everyone, no matter their professional background or having work experience or not. If the scope is narrow, certain scenarios may not be covered; if it is wide, unnecessary resource wasting will happen.

When designing and developing security systems, even a small unclear point of scope may bring a disaster. In 2017, Equifax leaked sensitive information of millions of people due to exploitation of the vulnerability of Apache Struts they used (Hough et al., 2020). Apache

Struts is an open-source framework that is widely used to build web applications, and there is a vulnerability that allows remote code injection in some outdated versions. Although security researchers found the vulnerability and Apache released the patch, Equifax failed to install the patch for their vulnerable Apache Struts because the version was not recognized by the system, leading to the data breach (Drenick, 2017). The scope constraints issue of this case was Equifax did not have a robust vulnerability management work-flow.

Equifax is a prominent and dominant organization with sophisticated teams, but their scope constraints can lead to mistakes in ensuring the product directions and decisions in security approaches.

4.3.3.3 Cost Constraints

Cost constraints involve the amount of resources that are dedicated to a project. Where either the client or the developing organization underestimates the security needs of a project reflect this in the amount of resources provided such that the budget allocated, or tender bid submitted may not be sufficient to include the appropriate degree of security.

A development project that does not adequately include security elements within the development and implementation process such as software supply chain assurance, quality assurance, implementation testing or end user training can be more likely to result in security threats for the implementing organization.

4.3.4 Usability and Tooling Challenges

Team members, like software testers, rely on a variety of tools to design and develop systems. It is crucial to ensure these tools provide adequate support in considering the needs of users and security perspectives.

Security-oriented Static Analysis Tools (SATs) detect mishaps in code, such as quality issues and security vulnerabilities. These tools then notify developers of the issues and the possible ways to fix them. However, these tools may have usability issues (Smith et al., 2020). Some issues include missing guidance on how to resolve flagged issues and difficulties accessing and understanding the interface. Further, these issues can affect work-flow continuity.

To work around usability issues, developers may take the liberty of picking useful tools that are more convenient to them without getting approval from management, a phenomenon known as Shadow IT (Raković et al., 2020). For a developer that is incentivized to efficiently finish their work, such a solution can be attractive. However, it can be very problematic as a tool may be incorporated into the security ecosystem of a company without proper security evaluations, leading to the potential of code injection or the leaking of sensitive data (Malkin et al., 2022).

4.3.5 Over-trust in suppliers (e.g., Open-Source SDKs)

Placing too much trust in software component supplier, such as blindly trusting open-source SDKs can include vulnerable components

which can then impact an organization's security when adopted into their own systems.

While best practices dictate that developers should analyze third-party code components prior to their use (Critical Infrastructure Partnership Advisory Council (CIPAC), 2022) this may not happen in practice. For example, developers may be subject to time constraints that preclude the proper procedures for integrating new code or an inappropriate technology stack (combination of development tools) may be proposed due to objective misalignment.

Software supply chains are complicated by the use of open-sourced software components. Within the development ecosystem, there is a certain degree of trust in the institution of open-sourced software and its crowd sourced development community. That is, open-source software is believed to be more reliable as there are thousands of independent developers using and testing the source code and fixing the bugs. Thus, developers may assume the open-source software they are integrating into the system is secure. However, this may not be the case as groups working on these code bases may not be as numerous as assumed or may be subject to the bystander effect. For example, the source code of Diebold voting machines, which had vulnerabilities and the code was readable for every developer, was still published on the Internet in 2003 and widely used in 37 states of USA (ACM, 2009; Schryen & Kadura, 2009; AMCIS, 2009).

4.3.6 Insecure development practices

Developers can themselves introduce security issues into software themselves as a result of not being aware of the security implications of particular practices. As an example, we will examine the practices of embedding credentials into the code of implemented software. Developers sometimes directly code the credentials that are used by systems to authenticate themselves to other systems into software and hardware platforms. Embedding credentials is considered a bad security practice as this effectively allows secrets to be exposed and potentially exploited by attackers to help them gain access to different parts of the system they have infiltrated. As an example, the Mirai Malware 2016 exploited hard coded credentials of IoT devices by scanning the IoT devices in the network and randomly choosing the possible combinations of Username and Password to gain remote access (Singh Verma & Chandavarkar, 2019). Once succeeding, the adversary collected the user's sensitive data and infected devices in the same network. There are many reasons why developers would embed credentials directly into a system. One main reason is to save time for debugging and testing, since developers can skip authentication with other services by embedding their credentials in the tested component. Although it might make testing easier, this is not security-oriented behaviour. In fact, hard-coded credentials have been identified as one of the top 25 most dangerous software weaknesses by Common Weakness Enumeration (Basak et al., 2022).

4.4 Vulnerability Introducing Behaviours: Recommendations

Although some behaviours we mentioned in

this part are hard to avoid (e.g., over-trust in suppliers) and some have existed since this industry was born (e.g., time constraints), there are still methods to mitigate the vulnerabilities. In this section, we will introduce some recommendations based on well-known and practical solutions to ease these threats.

4.4.1 Security by Design

Software development and maintenance teams should change the behaviour of prioritizing functionality first and addressing security later. Instead, they should view security as an integral part of their product and a top priority. Security should be considered from the earliest stages (planning, design, etc.) up until the release and maintenance of their product (deployment, monitoring, etc.) (Assal & Chiasson, 2019). Security should be "baked in" to the process rather than "bolted on" later.

To achieve a secure design, it is important to not overcomplicate a design unnecessarily. The more complex the software design, the higher the likelihood of implementation errors and security vulnerabilities. A simple and clear architecture will be easier to understand, maintain, and audit while reducing the risk of overlooking potential security weak points (Assal & Chiasson, 2018). In addition to simplicity, security policies that determine how the application handles data, access, and interactions securely, should be incorporated into the design (Assal & Chiasson, 2018). These policies can cover authentication, authorization, data handling, encryption, and security principles. As an example, two policies that are security oriented are default deny, where all requests are denied by default unless explicitly granted access, and least privilege where users, applications, and processes are given the minimum access needed to complete their tasks. Together they reduce the attack surface by limiting the exposure of resources.

4.4.2 Use Secure Tools

Using only approved tools that meet industry standards (e.g., those validated by NIST) or organizational policies can help reduce introducing vulnerabilities from third party software. This can be achieved by performing security assessments of third-party tools to ensure the software is trustworthy and would reduce the risk of incorporating vulnerable or insecure components into the application (Assal & Chiasson, 2018). Ideally, it should be understood by all developers that blindly trusting third-party suppliers is not appropriate behaviour. Instead, developers should vet third-party tools to identify and address any vulnerabilities, or weaknesses that might be present.

Lastly, businesses and developers should collaborate on the creation of a list of common and secure tools, as this would reduce the range of tools developers can choose from to complete their work. While this may be limiting from a developer perspective as it constrains the possible functionalities that a developer could introduce in a system, it would offer a greater security for all developers without the expense of each having to do their own validation. To minimize the impact of a restrictive list, it should involve many senior developers in creation, and updated as needed, so that the listed tools provide all that developers need to complete their work.

4.4.3 Integrating Security into Testing

Incorporating security testing into the functional test plans enables organizations to detect and address potential security vulnerabilities at an early stage of development, minimizing the risk of overlooking security flaws. Additionally, this allows for the simultaneous execution of functional and security tests, eliminating redundant efforts and may help detect common vulnerabilities that could be exploited.

Security should be seen as an integral part of the system, and therefore, so should security testing. From a developer's perspective, the behaviour around testing should be changed. To do this, developers should test by analyzing security risks in the system and creating tests around those risks, effectively testing with an attacker's mindset (Potter & McGraw, 2004). Encouraging developers to think about potential attacks while developing can help create better test cases and catch more security vulnerabilities. Management should also be aware of the importance of testing. This is achievable through metrics. In the software world, metrics quantify attributes in software processes, products and projects (Lopes Timóteo et al., n.d.). Providing metrics to measure the security testing in order to measure testing progress and impact can help management understand the importance of security testing (Türpe, 2008). In fact, good metrics will help convey technical information in a non-technical format and can therefore allow upper management to participate in the security testing process. A metric-based approach to testing can therefore change the mentality around testing and highlight its importance to many members within the organization.

4.4.4 Avoiding Optimism Bias

Addressing optimism bias in cybersecurity is not simple. The first step an organization can take is to address the issue head-on by raising awareness and educating employees about the negative impact of overconfidence on security decisions can help (Hewitt & White, 2022; Rhee et al., n.d.). An organization could work towards a shared culture by encouraging regular open discussions about security, which could lead to better decision-making (Buehler et al., 2005). Furthermore, ensuring individuals of all backgrounds, such as technical and non-technical individuals, are included in these discussions can challenge and reduce optimism bias. Lastly, it is important for individuals to be able to report optimism bias in their work environments should it occur. Without this ability, it is impossible for optimism bias to be investigated.

4.5 Threat Actualization Behaviours

Only a single point of access is needed to infiltrate a network to provide an adversary the opportunity to search and acquire data or systems to be held for ransom.

Social engineering techniques, such as phishing emails, are common techniques for tricking people to install ransomware. Through social engineering, people are persuaded to engage in **risky behaviours** like downloading disguised malware (Mouton et al., 2016).

Despite training and education initiatives that

try to help people detect phishing emails and reduce risky behaviours, people continue to engage in actions that can be exploited by ransomware adversaries such as ignoring or dismissing security warnings, pop-ups, and other red flags (Alsharnouby et al., 2015). In this section, we discuss some reasons why risky behaviours continue to persist.

4.5.1 Unclear Behavioural Implications

Without specialized expertise, mental models of security, networks, and other technical aspects can be flawed or incomplete. These limitations may impede people's ability to make connections between ransomware and potential risks caused by their actions like downloading email attachments or clicking on links. Without understanding these connections, people may continuously engage in a risky behaviour without being aware of the potentially detrimental implications (Kang et al., 2015).

In addition, flawed or incomplete mental models of ransomware can lead to the miscalculation of risk. Individuals may not realize that, initially, adversaries are looking for easy ways to access a network before finding sensitive information or integral systems to hold for ransom. Therefore, they may not feel themselves belonging to the category of the "high risk" or vulnerable individuals due to their limited access to important information and systems; they may believe themselves as not extraordinary, a "nobody", who is less attractive to adversaries than a higher up employee like their boss who is privy to sensitive information and wields power within an organization (Stanton et al., 2016).

4.5.2 Low Awareness of Mitigation Strategies

Techniques in detecting and avoiding risks might not be effectively implemented because they are not well known or understood by employees. Many individuals who are victimized by ransomware are unaware of possible mitigating strategies (Shinde et al., 2016).

Similarly, it is also common to observe users not taking basic steps towards security such ensuring that the firewall in the system is working, and that their internet or WiFi settings are secure (Furnell & Thomson, 2009). Many users may prefer to set up passwords that are either easy for them to remember, or they may choose to reuse the same passwords across different computers and/or platforms (Furnell & Thomson, 2009). Without security guidance to challenge these preferences, they may not be aware of the potential implications of exposing their organization to ransomware incidents.

4.5.3 Perceived Cost Outweighs Perceived Benefit

The clarification of secure behaviours or a heightened awareness of mitigation strategies available do not promise the avoidance of risky behaviours. The time, mental capacity, effort, and other resources required to follow security advice is not free. When making cost-benefit calculations, the anticipated costs of implementing protective actions may surpass its benefits; when costs outweigh benefits, security actions may not be taken

(Bhana & Ophoff, 2023; Herley, 2010).

Individuals may stop or refuse to practice security measures simply because they think the measures are useless (Stanton et al., 2016). For example, if from an employee's perspective the future cyber-attacks are going to occur regardless of the implementation and practice of any security measures then exercising these measures would be a waste of effort.

For individuals who felt themselves as the ordinary "no one" working for the organization, they may perceive the amount of energy required to ensure the safety and security of the company as outweighing their personal value and their potential gain in the work environment (Stanton et al., 2016). Once they perceived such increasing demands of the "cost" with little to no return of the "benefits," employees are less likely to spend time and energy to comply with the organizational cyber safety requirements.

4.5.4 Security Fatigue

Security fatigue refers situations in which individuals become tired of the security measures they are expected to practice and the trainings they must go through. Security fatigue can lead to individuals becoming desensitized and eventually stopping the practice of security measures (Stanton et al., 2016). As a result, the more that organizations urge their employees to practice secure online behaviour, to receive security messages, and to follow new policies regarding security and behavioural compliance, the greater the likelihood that these efforts could be counterproductive.

Sometimes, ordinary behaviour such as setting up easy passwords can also be considered as a part of the risky behaviour an employee does to encounter their security fatigue (Furnell & Thomson, 2009). Often, after being demanded by either the system or the IT and management team to set up multiple different passwords, these people may feel overwhelmed by the work they need to do to set up the secure passwords, to remember them, and eventually will give up on practicing such behaviour. The same applies to messages and emails warning employees about practicing safe and secure online behaviour. Those employees who constantly receive cyber-security related messages may often experience heightened levels of anxiety and stress, thus rapidly increasing the possibility of them feeling burned out and eventually conduct risky behaviour (Bhana & Ophoff, 2023).

In occasions, the rapid introduction of new security policies and technological features may add onto employees' load, particularly as many employees are often not tech-savvy and have trouble understanding the mechanism behind these tools (Bhana & Ophoff, 2023). They may be forced to be on the constant learning path of these tools and may often find themselves unable to keep up with the ever-changing technology.

4.5.5 Over-trust in Security Prevention Teams and Software

Many of these individuals who were victimized in corporate settings often consider their systems to be fully safeguarded by security software currently in place (Shinde et al., 2016). Further, individuals may perceive the responsibility of security exclusive to professional

technicians, such as IT personnel or cybersecurity firms. An over reliance on security professional and software can increase the likelihood of risky behaviours and greater chances of exploitation (Butavicius et al., 2020).

An over reliance on security software and security personnel can relate to employees' limited understanding of the implications of their behaviour. As previously mentioned, individuals with flawed or incomplete security mental models may not realize how their actions can negate the security efforts in place (Kang et al., 2015).

4.5.6 Contextual and Socio-demographic Factors

Identity dimensions such as age, gender, race, and socioeconomic status can lead to an increased likelihood to engage in behaviours or susceptibility to attacks (Oliveira et al., 2017). Factors such as stress experienced by individuals during daily life may make individuals unwilling to comply with the security measures during work (Furnell & Thomson, 2009). For example, an individual may be distracted by the enormous stress emerged from work, family, and personal life, resulting in their failure to practice safe behaviour during work.

Although these factors are difficult for organizations to control, they can be important considerations when understanding the reasons why individuals may persistently be unable to implement security advice. A combination of identity dimensions (and all behavioural reasons discussed thus far) could result in an increased likelihood of problematic security behaviour.

4.6 Threat Actualization Behaviours: Recommendations

This section will focus on providing some recommendations to help mitigate the threat actualization behaviours that can lead to ransomware adversaries accessing sensitive information.

4.6.1 Security Advocacy and Awareness

Activities and programs aimed at promoting individuals' awareness of risky behaviour and cyber security may be beneficial for organizations to prevent ransomware attacks (McCoy & Fowler, 2004). There are many free resources that can support people in avoiding ransomware attacks, including those from the Get Cyber Safe program by the Government of Canada (Government of Canada, 2020).

Educational initiatives advocating for safe online behaviours and safe practices in work environments are often recommended. For example, programs teaching non-tech savvy employees basic knowledge about security and the importance to seek expert help when experiencing technical difficulties, can often help increase employees' understanding of cyber security and the importance of practicing these security measures (Reeder et al., 2017). Tailored phishing campaigns aiming at increasing employees' mindfulness regarding suspicious content should also be introduced by organization's administration teams. Further, initiatives providing knowledge about device security and safety, such as explaining

why individuals should only be doing sensitive tasks on dedicated devices, can also be introduced (Reeder et al., 2017). Through these campaigns advocating for security and safety, employees working in the corporate environment may be more aware of the consequences and risks of their behaviour, thus less likely to conduct them.

As employees are more likely to engage in risky online behaviour due to misunderstandings and an over-reliance on IT personnel, it is therefore important to recommend organization's employees to increase the frequency and quality of communication between security personnel and non-tech employees (Shinde et al., 2016). For non-tech employees, their communication with technical personnel would provide opportunities to understand the technical reasonings of the safety measures, as well as the importance of enforcing such measures. For technical personnel, holding discussions with non-technical employees will allow them to understand the needs from employees. The collective understanding and bonding between the two groups may help the organization to reach its' security goals and objectives more effectively (Johnston et al., 2019).

4.6.2 Customized Ransomware Training

Additionally, an effective training mechanism that could be used to better prepare employees for real-life ransomware attacks is to create role-based tabletop exercises (TTXs) and fire drills, as shown in the Table below. TTXs are simulated incident scenarios that are meant to evaluate managerial capability and team responses (Pearlson et al., 2021). On the other

Target Audience	Type and Objective of TTX	Motivation
Board of directors	TTX: Education and awareness	Boards should be knowledgeable on how to act in the event of a security incident
C-suite	TTX: Crisis management	Helps test the crisis management plans of executives
Organization Employee	Fire drill: test and practice incident response and business continuity plans	Regular drills help build organizational confidence and tests whether the employees can respond quickly and effectively to an incident.
Technical Team	Fire drill: technical response planning	Testing technological teams regularly ensures the technology is working as intended and the support team knows how to operate it

Table 2 - List of recommended training, per employee type (Pearlson et al., 2021)

hand, fire drills help ensure people, processes and technologies respond correctly to an incident (Pearlson et al., 2021). TXXs should be done occasionally while fire drills should be done regularly (Pearlson et al., 2021). Since there are many different roles in an organization, one way to create effective TTXs and fire drills is to derive them based on the roles of individuals within the organization. In this approach, the training would be geared to specific individuals within the organization.

The table above describes recommendations for tailoring training according to the role of individual employees. These considerations are helpful to effectively train teams against ransomware incidents as they involve many combinations of roles in an organization (Boyce et al., 2011). Organizational needs for adequate ransomware training may require the development of TTXs or fire drills targeting many different roles. For example, in an organization where C-suite executives and technical teams work closely together during incident responses, it may be more suitable to create TTXs which require the collaboration of C-suite executives and technical teams. Evidently, the roles in the table above are very generic and can include many different types of people. In practice, an organization should identify key roles within the organization and create TTXs and fire drills around the interactions of these groups.

The training above can be tailored to specific individuals within the organization depending on their specific experience and roles. For instance, a highly technical and mature employee would require much more advanced training than a newly hired employee with moderate technical knowledge. The Advanced Distributed Learning (ADL) initiative under the United States government have developed a training and learning architecture (TLA) that highlights the main points required for tailored user training (Nicholson et al., 2016). The TLA can be seen in the figure below.

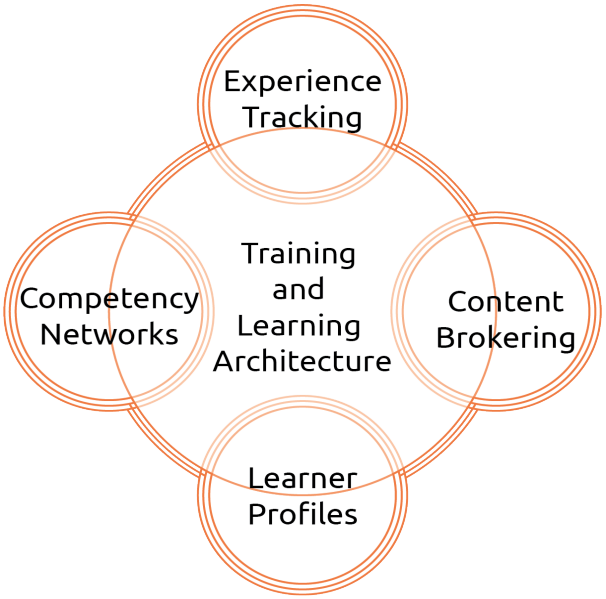


Figure 4 - Training and Learning Architecture, adapted from (Nicholson et al., 2016)

There are four main points in the TLA (Nicholson et al., 2016). The first is learner profiles which has to do with understanding the set of competencies and learning style of the employees. The second is content brokering, which involves setting the training content to accomplish certain training goals based on individual's learner profile. The third is experience tracking which involves updating the learner profile as the employees are trained. The last point is competency network which is considered as the set of learning content that could be used for content brokering (Nicholson et al., 2016). The idea behind this approach is make training learner specific and unique to each individual.

As an example, it is reasonable to assume that an organization TLA could be very effective for phishing training. Rather than sending generic and identical mock phishing emails to employees, it would be more effective to send mock phishing emails of varying difficulties. Therefore, more experienced employees would receive difficult mock phishing emails while less experienced employees would receive easier ones. This allows both experience and less experienced employees to learn at their own levels of experience. This is evidently harder to accomplish in large organizations due to the large number of employees but could be a suitable approach to learning for small and medium organizations.

4.6.3 Cultural Shift and Intrinsic Security Motivations

A major way to improve an organization's cybersecurity posture is through a cultural change that emphasizes security as a core part of everyone's responsibilities. The shift should start from day one of employment, with cybersecurity being ingrained into the onboarding process of every new employee. Each individual's role will be tailored to their specific responsibilities to ensure a comprehensive approach to cybersecurity. For instance, nurses should be well-versed in protecting patient data and maintaining confidentiality, while accountants should be encrypting financial transactions. System administrators would play a vital role by monitoring suspicious activity and maintaining secure network infrastructure.

Organizations should try to establish intrinsic motivations for cybersecurity behaviours among their employees. By increasing employees' interest in security and facilitating opportunities for self-determined motivation, or intrinsic desire, to protect an organization can increase the likelihood that they will adopt secure behaviours (Kam et al., 2022). Moreover, embedding security thoughtfulness into the organization's culture and promoting the idea that security is a collective responsibility and that protecting the organization is a shared goal.

Fostering a sense of belonging and ownership can also encourage employees to take cybersecurity seriously. When employees feel invested in the organization's security, they are more likely to adopt secure behaviours voluntarily.

Additionally, organizations should reward security champions (Ryan et al., 2021) and incentivize more employees among technical personnel to try to become champions themselves. By recognizing and incentivizing employees who demonstrate exceptional commitment to security, organizations can create a culture of cybersecurity excellence and encourage others to follow.

4.6.4 Shift security responsibilities from non-experts

There are several protective actions to mitigate threats that can be exploited by a ransomware attack. Some common examples include avoiding emails sent from unknown address, avoiding attachment downloads, and having general mindfulness when clicking on links (Reeder et al., 2017).

Often, the onus of implementing security strategies is put on end-users. Yet, these strategies may fail as users flow through systems focused

on their goals rather than security practices. As we mentioned previously, users who do prioritize security can become fatigued over time.

We recommend that system administrators or decision makers design systems with safety in mind to mitigate the amount of security responsibility assigned to end-users. Some examples of this strategy may include limiting system access rights, fail-safe defaults, enforcing network-wide software updates, and implementing spam filters to reject or flag suspicious email.

Furthermore, it is important for administrative personnel within the organization to reconsider the amount of work and responsibility they assign to their employees and avoid blaming the employees when risky behaviours are observed. The reduction of victim blaming behaviours within the organization will not only help to avoid the possibilities for poorly implemented security strategies or fatigue, but also help with the creation of a caring environment where employees can practice collective security efficacy (Johnston et al., 2019; Strawser & Joy, 2015).

4.6.5 Build Safe Environments for Information Sharing

Information relating to ransomware attacks (ransomware intelligence) can be used to strengthen mitigation strategies. For example, discussion and sharing of technical details about the techniques, tactics and procedures of ransomware among organizations can benefit prevention and remediation efforts. Other helpful ransomware intelligence can include data about the attack vectors that were uncovered, successful techniques in mitigating the damage, and other characteristics and patterns of the malware. Further, data about ransomware attacks that is shared with the government can inform relating policies and regulations aimed to prevent future ransomware incidents (Gordon et al., 2015).

It can be difficult to motivate organizations to share intelligence. Due to the benefits of intelligence sharing, we recommend that efforts should be made to foster an environment for the open exchange of information relating to ransomware attacks. Organizations and individuals who feel protected from potential repercussions of sharing ransomware information, such as negative impacts on reputation or livelihood, may be motivated to participate in information sharing initiatives. Strong moral judgements, such as displaying negative attitudes toward risky behaviours and victim blaming, should be discouraged and avoided to foster a more understanding and encouraging environment for reporting and information sharing (Strawser & Joy, 2015). Subsequently, this sense of safety may further encourage trust between organizations and lead to a higher likelihood of mutually beneficial collaboration within and between organizations.

Techniques to help facilitate safe environments for sharing ransomware information may vary according to the needs of the organizations involved and the severity of the incidents being discussed. For example, in extremely sensitive incidents involving internal threats that have compromised critical infrastructure which may lead to fatal con-

sequences, sharing parties may require full or partial anonymization, non-disclosure agreements, and legal immunity to be motivated to share information that can be helpful to mitigate and prevent further damage caused by ransomware.

4.6.6 Prepare for Security Failure

Due to the ever-changing nature of ransomware, there may be times when even the best prevention strategies fail. Therefore, organizations should shift some resources from prevention efforts to crisis management efforts that will mitigate the consequences of attacks and prevent successful attacks in the future (Dupont, 2019)frequency and severity of cyber-attacks targeting financial sector institutions highlight their inevitability and the impossibility of completely protecting the integrity of critical computer systems. In this context, cyber-resilience offers an attractive complementary alternative to the existing cybersecurity paradigm. Cyber-resilience is defined in this article as the capacity to withstand, recover from and adapt to the external shocks caused by cyber risks. Resilience has a long and rich history in a number of scientific disciplines, including in engineering and disaster management. One of its main benefits is that it enables complex organizations to prepare for adverse events and to keep operating under very challenging circumstances. This article seeks to explore the significance of this concept and its applicability to the online security of financial institutions. The first section examines the need for cyber-resilience in the financial sector, highlighting the different types of threats that target financial systems and the various measures of their adverse impact. This section concludes that the "prevent and protect" paradigm that has prevailed so far is inadequate, and that a cyber-resilience orientation should be added to the risk managers' toolbox. The second section briefly traces the scientific history of the concept and outlines the five core dimensions of organizational resilience, which is dynamic, networked, practiced, adaptive, and contested. Finally, the third section analyses three types of institutional approaches that are used to foster cyber-resilience in the financial sector (and beyond.

Organizations that are prepared to deal with the consequences of a successful ransomware attacks may be able to easily develop beneficial collaborations between departments across the organization and quickly respond to a developing ransomware crisis. These organizations are more cyber-resilient, and resiliency can lead to opportunities to learn from their experiences and adapt their strategies for dealing with ransomware (Dupont, 2019).

Organizations that make emergency action plans to better prepare themselves for future ransomware attacks, can use strategies such as (Ofir & Koren, 2023)

- Identifying affected systems and the scope of damage caused by the attack.
- Implementing the use of alternative communication channels at time of the attack.
- Getting prepared and familiarized with offline alternatives when digital devices are unusable.

To further strengthen preparedness initiatives, organizations could also consider keeping of-

fline physical copies of personnel contact information (i.e., human resources, IT, general managers, etc.) to prepare for circumstances where online communication methods were unavailable during attacks.

Organizations could also consider communication of an organization's cyber resiliency. This will include communicating crisis response efforts with staff across the organization and to external stakeholders, like clients, media, and shareholders, that will benefit from understanding the organization's cyber resiliency (Knight & Nurse, 2020).

5 References

Abrams, L. (2021, May). Canada Post hit by data breach after supplier ransomware attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/

Achten, N. (2021). La cybersécurité dans le secteur de la santé. In Politique de sécurité: Analyses du CSS (p. 296).

Achten, N. (2022). Rançongiciels: Approches nationales de protection. In Politique de sécurité: Analyses du CSS (p. 297).

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. 82, 69–82.

Assal, H., & Chiasson, S. (2018a). Motivations and Amotivations for Software Security.

Assal, H., & Chiasson, S. (2018b). Security in the Software Development Lifecycle.

Assal, H., & Chiasson, S. (2019). "Think secure from the beginning": A Survey with Software Developers. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3290605.3300519

Bajpai, P., & Enbody, R. (2020). Preparing smart cities for ransomware attacks. 2020 3rd International Conference on Data Intelligence and Security (ICDIS, 127–133.

Basak, S. K., Neil, L., Reaves, B., & Williams, L. (2022). What are the Practices for Secret Management in Software Artifacts? 2022 IEEE Secure Development Conference (SecDev), 69–76. https://doi.org/10.1109/SecDev53368.2022.00026

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 111, 102490.

Bekkers, L., Van 'T Hoff-de Goede, S., Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting

your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security, 127, 103099. https://doi.org/10.1016/j.cose.2023.103099

Bezanson, P. J., Cohen, J. G., Ellis, C. E., Justice, B. E., & Cahoon, C. E. (2022, January 21). Company Data Protection from Ransomware. Ransomware: An Enterprise Risk for the Unprepared. https://www.natlawreview.com/article/ransomware-enterprise-risk-unprepared

Bhana, A., & Ophoff, J. (2023). Risk homeostasis and security fatigue: A case study of data specialists. Information & Computer Security, 31(3), 267–280. https://doi.org/10.1108/ICS-11-2022-0172

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human Performance in Cybersecurity: A Research Agenda. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 55(1), 1115–1119. https://doi.org/10.1177/1071181311551233

Buehler, R., Messervey, D., & Griffin, D. (2005). Collaborative planning and prediction: Does group discussion affect optimistic biases in time estimation? Organizational Behavior and Human Decision Processes, 97(1), 47–63. https://doi.org/10.1016/j.obhdp.2005.02.004

Bullee, J.-W., & Junger, M. (2020). How effective are social engineering interventions? A meta-analysis. Information & Computer Security, 28(5), 801–830. https://doi.org/10.1108/ICS-07-2019-0078

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. Computers & Security, 98.

CAA. (n.d.-a). Auto Body Shops Recommended by CAA - Car Repair Near You—CAA South Central Ontario. Retrieved July 28, 2023, from https://www.caasco.com/insurance/auto/recommended-body-shops

CAA. (n.d.-b). CAA Pet Insurance—CAA South Central Ontario. Retrieved July 28, 2023, from https://www.caasco.com/insurance/pet

Canada, G. (2022). Rapid Response Mechanism Canada: Global Affairs Canada (p. 3 2). https://www.international.gc.ca/

transparency-transparence/rapid-response-mechanism-

Canada, J. (2022). Charter statement Bill C-26: An act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts. https://justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html

Canada, P. S. (2022a). Fundamentals of Cyber Security for Canada's CI Community. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx#a03

Canada, P. S. (2023). Critical Infrastructure. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Canada, P. S. (2018, December 21). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s53

Canada, P. S. (2022b, June 27). National Cyber Security Strategy 2019-2024: Report on the Mid-term Review. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx

Canadian Bankers Association. (n.d.). Learn more about how banks are protecting Canadians from fraud | Learn more about how banks are protecting Canadians from fraud. Retrieved July 28, 2023, from https://cba.ca/protecting-canadians-from-fraud?l=en-us

Canadian Centre for Cyber, C. C. for C. (2019, September 24). Ransomware: How to prevent and recover (ITSAP.00.099). Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099

Canadian Centre for Cyber Security. (2021, October 18). Ransomware playbook (ITSM.00.099). Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

Canadian Centre for Cybersecurity. (n.d.). Tips for Backing up your Information. Retrieved October 10, 2023, from https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsap40002-e.pdf

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In Ethical hacking techniques

and countermeasures for cybercrime prevention (pp. 19–31). IGI Global.

Council, E. (2019). Cyber attacks: EU ready to respond with a range of measures, including sanctions. https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Cybersecurity, E. U. (XXXX). Supporting the implementation of Union policy and law regarding cybersecurity. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Cybersecurity, E. U. A. (2022). Ransomware: Publicly Reported Incidents are only the tip of the iceberg. https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg

Dupont, B. (2019a). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Dupont, B. (2019b). The ecology of cybercrime. In R. Leukfeldt & T. Holt (Eds.), The human factor in cybercrime, Routledge, Londres (pp. 389–407).

Dupont, B., Stevens, Y., Westermann, H., & Joyce, M. (2018). Artificial Intelligence in the Context of Crime and Criminal justice.

EU, C. (2021). Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting. https://www.consilium.europa.eu/en/press/press-releases/2021/06/22/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/

Europol. (n.d.). Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files. Europol. Retrieved July 28, 2023, from https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files

Evans, P. (2018, May 29). “How could this happen?” victim asks as banks reveal hack of up to 90,000 accounts | CBC News. CBC. https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018

Fiore, B., Ha, K., Huynh, L., Falcon, J., Vendiola, R., & Li, Y. (2023). Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky (pp. 285–294).

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Marketos, E.,

& Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. Journal of Information Security and Applications.

Fracassi, C., Garmaise, M. J., Kogan, S., & Natividad, G. (2012). How Much Does Credit Matter for Entrepreneurial Success in the United States? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2157707

Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing 'security fatigue.' Computer Fraud & Security, 2009(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

G.D.P.R. (n.d.). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

Get Cyber Safe. (2022, October 4). Phish, vish, smish – how banks are helping Canadians spot digital fraud. Get Cyber Safe. https://www.getcybersafe.gc.ca/en/phish-vish-smish-how-banks-are-helping-canadians-spot-digital-fraud

Giri, B. N., Jyoti, N., & Avert, M. (2006). The emergence of ransomware. AVAR.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Government of Canada. (2020a). Ransomware 101: How to stay cyber secure. https://www.getcybersafe.gc.ca/en

Government of Canada, I. (2023, October 10). Canada Small Business Financing Program—Home [Home page; Landing Pages]. Innovation, Science and Economic Development Canada. https://ised-isde.canada.ca/site/canada-small-business-financing-program/en/canada-small-business-financing-program

Government of Canada, R. C. M. P. (2020b, August 20). National Cybercrime Coordination Unit | Royal Canadian Mounted Police. https://www.rcmp-grc.gc.ca/en/national-cybercrime-coordination-unit

Government of Canada, S. C. (2022, October 18). The Daily—Impact of cybercrime on Canadian businesses, 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-eng.htm

Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. Journal of Information

Security and Applications, 40, 44–51.

Herley, C. (2010). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice.

Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 11(10), 1168. https://doi.org/10.3390/rs11101168

Hewitt, B., & White, G. L. (2022). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. Journal of Computer Information Systems, 62(1), 50–60. https://doi.org/10.1080/08874417.2019.1697860

Hough, K., Welearegai, G., Hammer, C., & Bell, J. (2020). Revealing injection vulnerabilities by leveraging existing tests. Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, 284–296. https://doi.org/10.1145/3377811.3380326

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal, 22(1), 105–117.

Hutton, C. (2023). North Korean hackers behind $100 million crypto theft, FBI says. The Washington Examiner. https://www.washingtonexaminer.com/policy/technology/fbi-north-korean-hackers-100-million-crypto-theft

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. Human-Centric Computing and Information Sciences, 10(1), 33. https://doi.org/10.1186/s13673-020-00237-7

Jaskolka, J. (2020). Recommendations for Effective Security Assurance of Software-Dependent Systems. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), Intelligent Computing (Vol. 1230, pp. 511–531). Springer International Publishing. https://doi.org/10.1007/978-3-030-52243-8_37

Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. Journal of the Association for Information Systems, 186–212. https://doi.org/10.17705/1jais.00533

Justice, U. S. D. (2018). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber

Attacks and Intrusions. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Kam, H., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self?determination in organisational cybersecurity training. Information Systems Journal, 32(4), 888–926. https://doi.org/10.1111/isj.12374

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). ``My Data Just Goes Everywhere:'' User Mental Models of the Internet and Implications for Privacy and Security. Symposium on Usable Privacy and Security (SOUPS), Ottawa.

Kara, I., & Aydos, M. (2019). The Ghost in the System: Technical Analysis of Remote Access Trojan. 11, 73–84.

Kelly, H. (2021). Ransomware attacks are closing schools, delaying chemotherapy and derailing everyday life. The Washington Post. https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/

Kerns, Q., Payne, B., & Abegaz, T. (2022). Double-extortion ransomware: A technical analysis of maze ransomware (pp. 82–94).

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kosseff, J. (2017). Defining cybersecurity law. Iowa L. Rev., 103, 985.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122.

Lațici, T. (2020). Understanding the EU's approach to cyber diplomacy and cyber defence. European Parliament.

Lessig, L. (2006). Code: And Other Laws of Cyberspace, Version 2.0. Basic Books. https://books.google.ca/books?id=CnGR-Ca9y4RcC

Levi-Faur, D. (2011). Handbook on the Politics of Regulation. Edward Elgar Publishing.

Li, Z., & Liao, Q. (2022). Preventive portfolio against data-selling ransomware—A game theory of encryption and deception. Computers & Security, 116, 102644. https://doi.org/10.1016/j.cose.2022.102644

Lopes Timóteo, A., Álvaro, A., Santana de Almeida,

E., & Romero de Lemos Meira, S. (n.d.). Software Metrics: A Survey. CiteSeerX.

Malecki, F. (2021a). Now is the time to move past traditional 3-2-1 back-ups. Network Security, 2021(1), 18–19. https://doi.org/10.1016/S1353-4858(21)00010-6

Malecki, F. (2021b). Now is the time to move past traditional 3-2-1 back-ups. Network Security, 2021(1), 18–19. https://doi.org/10.1016/S1353-4858(21)00010-6

Malkin, N., Wagner, D., & Egelman, S. (2022). Runtime Permissions for Privacy in Proactive Intelligent Assistants. 633–651. https://www.usenix.org/conference/soups2022/presentation/malkin

Matulevičius, R. & Abasi-Amefon Affia. (2018). Security Risk Management of E-commerce Systems. https://doi.org/10.13140/RG.2.2.35505.53604

McCoy, C., & Fowler, R. T. (2004). "You are the key to security": Establishing a successful security awareness program. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services, 346–349. https://doi.org/10.1145/1027802.1027882

McLaren, P. (2022). Some thoughts on Canada's 'Freedom Convoy' and the settler colonial state. Educational Philosophy and Theory, 54(7), 867–870.

Mehrotra, K. (2020). Hacks on Louisiana parishes hint at nightmare election scenario—BNN Bloomberg. https://www.bnnbloomberg.ca/hacks-on-louisiana-parishes-hint-at-nightmare-election-scenario-1.1388349

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, 101762.

Moret, E., & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: Towards a cyber sanctions regime? European Institute for Security Studies.

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. Computers & Security, 128, 103162. https://doi.org/10.1016/j.cose.2023.103162

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59.

Nadeem, A., & Javed, M. Y. (2005). A Performance Comparison of Data Encryption Algo-

rithms. 2005 International Conference on Information and Communication Technologies, 84–89. https://doi.org/10.1109/ICICT.2005.1598556

National Bank of Canada. (n.d.). Car Loans, Apply Online! | National Bank. Car Loans. Retrieved October 10, 2023, from https://www.nbc.ca/personal/borrowing/car.html

Nershi, K., & Grossman, S. (2023). Assessing the Political Motivations Behind Ransomware Attacks.

Nicholson, D., Massey, L., Ortiz, E., & O'Grady, R. (2016). Tailored Cybersecurity training in LVC environments. MODSIM World.

N.I.S. (n.d.). The NIS 2 Directive. https://www.nis-2-directive.com/

Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. HOLISTICA – Journal of Business and Public Administration, 13(1), 49–72.

Ofir, A., & Koren, R. (2023). Cyber-shock and "digital withdrawal": Organizational lLeadership and Crisis Management During a Hospital-wide Computer Shutdown Following a Ransomware Attack. Prehospital and Disaster Medicine, 38(S1), s98–s98. https://doi.org/10.1017/S1049023X23002728

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017, May). Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. CHI'17, Denver, Colorado.

Orenstein, M. (2022). Russia's use of cyberattacks: Lessons from the second Ukraine War. Foreign Policy Research Institute. https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. ACM Computing Surveys (CSUR, 54(11s), 1–37.

Page, C. (2022). North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies.

Payne, B., & Mienie, E. (2021). Multiple-extortion ransomware: The case for active cyber threat intelligence. ECCWS 2021 20th European Conference on Cyber Warfare and Security, 331.

Pearlson, K., Thorson, B., madnick, stuart, & Coden, M. (2021). Cyberattacks Are Inevitable. Is Your Company Prepared? https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared

Perot, T. (2019, January 10). Adding an Air Gap to the 3-2-1 Backup Rule. Global Data Vault. https://www.globaldatavault.com/blog/air-gapped-backup-rule/

Porcedda, M. G., & Wall, D. S. (2019). Cascade and chain effects in big data cybercrime: Lessons from the TalkTalk hack. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW, 443–452.

Poremba, S. (2021). How to protect against deepfake attacks and extortion. Security Intelligence. https://securityintelligence.com/articles/how-protect-against-deepfake-attacks-extortion/

Potter, B., & McGraw, G. (2004). Software security testing. IEEE Security & Privacy, 2(5), 81–85. https://doi.org/10.1109/MSP.2004.84

Poudyal, S., & Dasgupta, D. (2020). AI-powered ransomware detection framework. 2020 IEEE Symposium Series on Computational Intelligence (SSCI, 1154–1161.

Raković, L., Marton Sakal, Matković, P., & Marić, M. (2020). Shadow IT – Systematic Literature Review. Information Technology and Control, 49(1), Article 1. https://doi.org/10.5755/j01.itc.49.1.23801

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C., & Assi, C. (2023). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access.

Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. IEEE Security & Privacy, 15(5), 55–64. https://doi.org/10.1109/MSP.2017.3681050

Reinheimer, B., Aldag, L., Mayer, P., & Mossano, M. (n.d.). An investigation of phishing awareness and education over time: When and how to best remind users.

Rhee, H.-S., Ryu, Y., & Kim, C.-T. (n.d.). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.

Robinson, A., Corcoran, C., & Waldo, J. (2022). New risks in ransomware: Supply chain attacks and cryptocurrency. Science, Technology, and Public Policy Program Reports.

Royal Canadian Mounted Police. (2021, September 14). Prevent ransomware. https://www.rcmp-grc.gc.ca/en/prevent-ransomware

Ryan, I., Roedig, U., & Stol, K.-J. (2021). Understanding Developer Security Archetypes. 37–40. https://doi.org/10.1109/EnCyCriS52570.2021.00013

Saylors, K. (2019). Cyber attack costs Woodstock more than $660K [Report.]. https://www.woodstocksentinelreview.com/news/local-news/cyber-attack-costs-woodstock-more-than-660k-report

Schein, E. H. (1995). The Role of the Founder in Creating Organizational Culture. Family Business Review, 8(3), 221–238. https://doi.org/10.1111/j.1741-6248.1995.00221.x

Schryen, G., & Kadura, R. (2009). Open source vs. closed source software: Towards measuring security. Proceedings of the 2009 ACM Symposium on Applied Computing, 2016–2023. https://doi.org/10.1145/1529282.1529731

Shinde, R., Van Der Veeken, P., Van Schooten, S., & Van Den Berg, J. (2016). Ransomware: Studying transfer and mitigation. 2016 International Conference on Computing, Analytics and Security Trends (CAST), 90–95. https://doi.org/10.1109/CAST.2016.7914946

Singh Verma, R., & Chandavarkar, B. R. (2019). Hard-coded Credentials and Web Service in IoT: Issues and Challenges (SSRN Scholarly Paper 3358283). https://papers.ssrn.com/abstract=3358283

Smilyanets, D. (2021, March 15). I scrounged through the trash heaps… Now I'm a millionaire:' An interview with REvil\'s Unknown. https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown

Smith, J., Do, L. N. Q., & Murphy-Hill, E. (2020). Why Can't Johnny Fix Vulnerabilities: A Usability Evaluation of Static Analysis Tools for Security. Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. IT Professional, 18(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Statistics Canada. (2022a). Impact of cybercrime on Canadian businesses, 2021. 11.

Statistics Canada. (2023, August 28). The Daily—Deaths, 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/230828/dq230828b-eng.htm

Statistics Canada, S. C. (2022b, November 21). Homicide in Canada, 2021. https://www150.statcan.gc.ca/n1/pub/85-002-x/2022001/article/00015-eng.htm

Strawser, B. J., & Joy, D. J. (2015). Cyber Security and User Responsibility: Surprising Normative Differences. Procedia Manufacturing, 3, 1101–1108. https://doi.org/10.1016/j.promfg.2015.07.183

Strong, W. (2020). NTPC confirms “cyber attack” from unknown source on Thursday. RCMP Investigating | CBC News. CBCnews. https://www.cbc.ca/news/canada/north/ntpc-apparent-ransomware-attack-1.5551603

Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing Cryptocurrency Exchange: Building up Standard from Huge Failures. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Eds.), Financial Cryptography and Data Security (pp. 254–270). Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_19

TELUS Business. (n.d.). Canadian Ransomware Study. Retrieved July 20, 2023, from https://www.telus.com/en/bc/business/ransomware-study?cmp=KNC_sGGL_ccbsec_cdToFu-Ransomware-EN_bTBS_kw=ransomware&SEM_CID=20365088606&SEM_AG=153741111520&SEM_KW=ransomware&SEM_MT=p&inv=1&gclid=CjwKCAjwtuOlBhBREiwA7agf1gd8aXokCBr8YMcl9AcZVk8pbr3VLiPAMQkHBiy2apx2HWxfxde_5hoC1_YQAvD_BwE&gclsrc=aw.ds

Türpe, S. (2008). Security Testing: Turning Practice into Theory. 2008 IEEE International Conference on Software Testing Verification and Validation Workshop.

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications, 101, 18–54. https://doi.org/10.1016/j.

jnca.2017.10.016

United States, National Cyber Investigative Joint Taskforce. (n.d.). Ransomware Fact Sheet. Retrieved July 28, 2023, from https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

Van Wyngaard, C. J., Pretorius, J. H. C., & Pretorius, L. (2012). Theory of the triple constraint—A conceptual review. 2012 IEEE International Conference on Industrial Engineering and Engineering Management, 1991–1997. https://doi.org/10.1109/IEEM.2012.6838095

Wang, J., Liu, L., Lyu, S., Wang, Z., Zheng, M., Lin, F., Chen, Z., Yin, L., Wu, X., & Ling, C. (2021). Quantum-safe cryptography: Crossroads of coding theory and cryptography. Science China Information Sciences, 65(1), 111301. https://doi.org/10.1007/s11432-021-3354-7

Warikoo, A. (2023). Perspective Chapter: Ransomware.

Westbrook, A. D. (2021). A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security. New York University Journal of Law and Business, 18(2), 391–470.

Whitwam, R. (2019, December 19). Ransomware Groups Now Threatening to Release Stolen Data If Businesses Don't Pay. ExtremeTech. https://www.extremetech.com/internet/303697-ransomware-groups-now-threatening-to-release-stolen-data-if-businesses-dont-pay

Wilkie, C. (2021). Colonial pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate. CNBC. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html#: :text=WASHINGTON%20%E2%80%94%20Colonial%20Pipeline's%20CEO%20told,Joseph%20Blount%20Jr

Wilner, A., Jeffery, A., Lalor, J., Matthews, K., Robinson, K., Rosolska, A., & Yorgoro, C. (2019). On.

Yuryna Connolly, A., & Borrion, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. Computers & Security, 119, 102760. https://doi.org/10.1016/j.cose.2022.102760

Zajc, K. (2016). Hard Law. Encyclopedia of Law and Economics.

Zhang, L., Choffnes, D., Levin, D., Dumitraş, T., Mislove, A., Schulman, A., & Wilson, C. (2014). Analysis of SSL certificate re-

issues and revocations in the wake of heartbleed. Proceedings of the 2014 Conference on Internet Measurement Conference, 489–502. https://doi.org/10.1145/2663716.2663758

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., & Chiasson, S. (2018). The aftermath of a crypto-ransomware attack at a large academic institution. 27th USENIX Security Symposium (USENIX Security 18, 1061–1078.

Detailed Table of Contents

Human-Centric
Cybersecurity
Partnership