INSIDER RISK FOR CANADIAN FINANCIAL INSTITUTIONS

CAPSTONE REPORT

PREPARED BY

ANTHONY HOPE
IVAN BARKAR
HAYLEY OYHENART
DARIAN SCHERBLUK

NORMAN PATERSON SCHOOL OF INTERNATIONAL AFFAIRS

TABLE OF CONTENTS

Executive Summary ..... page 1

Acknowledgements ..... page 4

Introduction ..... page 5

Literature Review ..... page 6

Methodology ..... page 19

Strategic Foresight ..... page 23

Research Findings ..... page 32

Legal ..... page 45

Recommendations ..... page 47

Conclusion ..... page 48

References ..... page 49

Appendix A: Questionnaire ..... page 55

Appendix B: Consultation Questions ..... page 58

EXECUTIVE SUMMARY

INSIDER RISK FOR CANADIAN FINANCIAL INSTITUTIONS

At its broadest level, an insider risk is defined as "the potential for an individual who has or had authorized access to an organization's assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Mellon, 2018, 11). Traditionally, insider risks are perceived to be influenced "by a combination of technical, behavioural, and organizational issues" (Mellon, 2018, 11). Before summarizing the research process and findings for this capstone project regarding the environment of insider risks for Canadian financial institutions, it is important to emphasize why issues revolving around insider risks are important to study and how this project is of great organizational value.

Every organization has the potential to be a victim of an insider risk as employees and third-party vendors all have a certain level of access to the given company's business data and storage infrastructure. Whether these individuals have limited access to general company data or possess the crown jewels of sensitive organizational data, this access is what causes company insiders to be the most significant threat to any given organization. Thus, responding to early indicators of an insider risk enable organizations to proactively address non-compliant policy behaviour while maintaining the privacy of client information and decreasing overall company risk vulnerabilities quickly and appropriately. Essentially, lackluster insider risk programs can have damaging long term effects on an organization financially and reputationally.

The main purpose of this capstone project was to build upon existing research and relevant debates in the field of insider risks through primary research. Over the span of four months, surveys and consultations with field experts of insider risks, security and compliance were conducted in order to unpack the current industry understanding of how insider risks may be mitigated. Furthermore, forecasting exercises such as horizon scans and future wheels were completed to assist in anticipating what the future of insider risk mitigation strategies need to address and how companies can adapt their insider risk programs in an ever evolving Canadian work landscape.

This report takes a forwarding looking approach to the challenges of insider risks and organizational mitigation strategies. The following questions are addressed throughout the research report: 1. How are insider risks defined and understood? 2. What motivates inside risk events? 3. What are the components of a good insider risk program? 4. What gaps currently exist within the insider threat environment, and how can they be effectively addressed? 5. What forward looking insider risk trends can be identified? 6. What lessons, recommendations, and counter measures might serve Canadian financial interests?

This study begins by examining the academic and practitioner literature in the field of insider risk to gain a greater understanding around the complexities of insider risks, comparative approaches of

mitigating potential insider risks, emerging consideration and common practices used in the field. Major trends highlighted by insider risk academic literature included the importance of organizational and holistic approaches to mitigate insider risk occurrences. More specifically, many academic pieces emphasized the need for significant corporate buy-in. In addition, behavioural and social human factors were considered for insider risk motivators. Cyber and technological implications were also often discussed as tools for insider threat mitigation while legal implications of all above elements in preventing insider risk were sparsely included. Furthermore, practitioner literature informs that insider risks are primarily sector-agnostic and costly and that they can originate from employees and at third party vendors at every level of an organization. A concern found in the practitioner pieces was the lack of forward-looking perspective as they did not account for future trends regarding insider risks. Finally, the case studies reviewed discussed the broad nature of insider risks, as well as, cross-sectionality of the insider risk environment. An important takeaway from the case studies were their discussion around work from home implications on the insider risks landscape.

Following the literature review, this report maps out the research design used to investigate contemporary understandings of insider risk in the private and public sectors. Additionally, strategic foresight methodologies are outlined regarding how they may forecast future trends and themes of insider risk mitigation strategies.

In the next section of the research report, results from the strategic foresight practices, expert consultations and questionnaire are discussed. Insights from the horizon scanning regarding insider risks include work from home challenges, emphasis on personnel safety and satisfaction, global and political attitudes on security, and the implications of new technology in detecting and monitoring strategies for insider risks. Conclusions from the future wheels suggest that new technologies implicated in insider risk detection will affect workplace culture and the bottom line. In addition, the polarization of global political attitudes on security is predicted to negatively affect workplace culture and insider risks.

The questionnaire and consultations findings had overlapping similarities when it came to identifying motivations behind insider risks. Overwhelmingly, respondents identified no primary motivation for insider risks as they were perceived to be mainly unintentional due to negligent behavior. For the rare case of malicious insider risks the primary motivation highlighted was employee dissatisfaction with a negative work culture that is often coupled with secondary risk factors, such as financial gain or ideological differences.

Findings from questionnaire and consultations diverged when describing the characteristics of a good insider risk program. Questionnaire responses focused on an insider risk program's ability to protect client confidentiality, company data from insider attacks, and to detect insider risk events and compromised assets. Survey respondents focused more on the end results of asset protection rather than proactive prevention measures that can be implemented to make a good insider risk program which was highlighted in many of the consultations. Consults continuously emphasized that insider risk programs need to be people-focused and empathy driven. Employee workplace

culture was seen as critical in mitigating insider risks as employees need to feel respected and have dignity in their work. Significant executive buy-in for insider risk programs and regular security awareness training were also discussed in most of the consultations.

There was an overlap in the findings from the questionnaire and consultation responses when it came to recognizing current gaps within insider risk programs. Surprisingly, a majority of individuals that participated in the study did not have formal insider risk programs at their organization. In addition, many companies have focused on building a “security perimeter” which are not inward focused. A lack of executive buy-in was a major concern along with the fact that when technology is used to mitigate insider risks, relevant data sources were not usually centralized. Finally, there was hesitation to include physical security as part of insider risks as the scope of the insider risk landscape was feared as becoming too broad.

When discussing the topic of emerging insider risks, responses from the questionnaire and consultations once again overlapped. The most overwhelming trend identified was the introduction of new security vulnerabilities because a majority of individuals are forced to work from home because of the COVID 19 pandemic . There were future concerns around employee mental health, the impacts of large-scale layoffs, technology and data integrity preservation, as well as, move to the cloud in terms of concentrating company data. Following the analysis of these questionnaire and consultations findings, legal considerations in the Canadian context are summarized to allow for an understanding of the limitations of insider risk programs and mitigation strategies.

The literature review, strategic forecasting practices, as well as the questionnaire and consultations result all ultimately contributed to industry best practice recommendations which are highlighted in the final section of the report. The recommendations are four-fold, first being that organizations must build insider risk programs that are people-focused and that respect the dignity and privacy of all employees. Second , company executives and management must work towards a positive workplace culture that is empathetic, diverse and transparent. Third , organizations must use technology to supplement insider risk programs through monitoring and detection of anomalous behaviour based on preset baselines and in a transparent way, while also being conscious of Personal Information Protection and Electronic Documents Act (PIPEDA) constraints. Fourth and finally, companies must increase training opportunities that encompass security and information technology vulnerability awareness, workplace violence, and empathetic leadership.

Overall, this research report analyzes insider risk issues from multiple insightful perspectives to form a comprehensive and objective end-product. There is also great potential for the research and findings detailed in this report to be expanded upon in future projects. Upon conclusion of this research process, it is safe to say that the landscape of insider risks is constantly evolving and has extremely complex nuances that need to be understood. Therefore, it is crucial for organizations to continue prioritizing research into the development of insider risk programs, education, and mitigation strategies.

ACKNOLWEDGEMENTS

We are grateful to all the individuals who helped plan, facilitate and participate in our research and who made this report possible and wish to recognize all who have positively contributed to this report. As graduate students at Carleton University's Norman Patterson School of International Affairs (NPSIA), we would like to express our gratitude to Lina Tsakiris and Victor Munro, PhD candidate at NPSIA, for all the resources and input they have provided us. The meetings and conversations we had were vital in inspiring our research approach to insider risk, enabling us to look at this issue from multiple perspectives to form a comprehensive and objective report. We hope that this is the beginning of a long partnership and that we can continue to expand on our insider risk research outlined in this report.

In addition, we would like to thank our supervising professor, Dr. Alex Wilner, for providing guidance and feedback throughout this capstone project. Professor Wilner's insights and knowledge helped steer us through this research journey from beginning to end.

Finally, we would like to thank all the research participants who completed the insider risks questionnaire or participated in one of our consultations. Each individual's experiences and perspectives helped shape the findings of our research. Without the direction provided, Professor Wilner's academic guidance, or the participation of insider risk field experts we would have not been able successfully complete a research report that is true forward looking that can provide added organizational value.

INTRODUCTION

The threat of the insider poses a novel risk to all organizations, especially financial institutions as they provide critical services to all Canadians. Traditionally, organizations have sought to build a sophisticated security perimeter. But, what protects an organization from an elevated risk existing within the perimeter walls? With the evolving nature of the work environment, the threat of an insider incident must be considered and corresponding programs must be developed to mitigate emerging risks. This report will investigate what motivates an insider to become a risk to the organization and what the main components are of a good insider risk program. Furthermore, the gaps that currently exist within established insider risk mitigation strategies will be explored in addition to what the future trends of insider risk may be.

Through consultations with industry experts and questionnaire responses from practitioners in the field of security, risk and compliance in both the private and public sectors, this report will unpack current understanding of how insider risks may be mitigated. Additionally, this study will include methods of strategic foresight, which will assist in forecasting what challenges may exist for the future of insider risk mitigation strategies.

This study will begin by examining the academic and practitioner literature in the field of insider risk, providing readers with a greater understanding of the current landscape of insider risks. Next, we will outline the research design used to investigate contemporary understandings of insider risk in the private and public sectors. Additionally, strategic foresight methodologies will be outlined, illustrating how organizations may anticipate future trends and themes of insider risk mitigation strategies. The results of the foresight process, expert consultations and questionnaire will then be synthesized, and will ultimately contribute to industry best practice recommendations. Additionally, legal considerations will also be summarized to allow for an understanding of the limitations of insider risk programs and mitigation strategies.

LITERATURE REVIEW

This literature review was conducted to provide a survey of current knowledge as it relates to insider risk. Literature from both the academic and practitioner perspective will be discussed. For the purposes of this study, the literature examined was restricted to sources primarily from Canada, the United States and Western Europe. As such, this paper cannot make claims on the generalizability of insider risk programming beyond these jurisdictions.

ACADEMIC LITERATURE

During our examination of the academic literature we noticed that the insider risk landscape was understood and structured in a fairly particular manner. The literature that has been consulted describes insider risk as originating from human and social factors – whether this is employee behaviour, corporate attitudes and culture, personal and psychological variation in employees, as well as their own personal background. A large portion of the literature classifies these variables in multiple taxonomies in order to predict the likelihood of insider risk events. This section will outline these variables, how the existing academic literature presented them, and what some of the gaps were. Furthermore, it will touch on some of the implications of these gaps for our research and for further work.

Behavioural, Cultural, and Moral Indicators of Insider Risk

The first observable trend in the academic literature is that there are numerous behavioural, cultural and moral indicators that can lead to insider risk incidents. The first such indicator discussed in the literature relates to the psychological and behavioural tenets of employees; the way an employee thinks and acts is going to be one of the most prominent indicators of whether or not they are going to exhibit a risk to the organization. The academic literature points to a number of stressors that affect these indicators and outline how each stressor can interchange, blend or exacerbate each other. It also generally discusses the interconnected nature of these psychological stressors and points to the fact that this cannot be understated – that the behaviours and psychology of employees, their habits, actions, and mental state is likely going to predict their likelihood of risk. Another important indicator discussed is the employee's background and culture – this includes things like upbringing, heritage, past experiences, as well social circles and can understandably affect other indicators and spur issues in others. The last behavioural indicator that the literature review discusses is the managerial and social culture within any organization and how their actions and attitudes will ultimately shape a large portion of how employees view the organization and how they behave. These elements of the broader trend will be broken down below.

One of the indicators most commonly observed in the academic literature are the psychological and behavioural factors that could spur insider risk events (Kont et al., 2018; Elifoglu et al., 2018). These can vary from pre-existing conditions to developing or newly developed psychological factors that may or may not be triggered by the work environment. It is important to note that the literature discusses that a consistent and prolonged interaction with employees is necessary, as these factors may develop at any time and can be produced from a variety of external causes unrelated to the workplace.

These could also take the form of impersonal corporate attitudes – such as not feeling a sense of attachment to the corporation. Similarly, disenfranchisement or loss of morale of an employee based on either personal psychological reasons or some sort of workplace event could increase the chance of an inside risk event (Lorrimer, 2020). Lacking a sense of purpose, financial difficulties, or personal traumatic events such as divorce and separations or loss of a loved one, as well as a variety of other strenuous psychological shocks, could contribute to an employee being susceptible to becoming an insider risk (Kont et al., 2018). The literature likewise points to indicators like depression, bi-polar disorder as well as feelings of inadequacy that can all heighten various different forms of insider risks. It is important to note that the literature differentiates between indicators, and outlines which kind of threats – fraud, sabotage, espionage, theft or unintentional negligence - can occur and as a result of which indicator. For instance, certain negative emotions, stressors, and conflicts that individuals exhibit are more likely to be associated with insider incidents of fraud, espionage, and sabotage. These detectable psychological behaviours can be used to flag and prevent potential insider risks, as well as by monitoring the friendliness, disengagement, self-centeredness and attitude towards authority among employees (Kont et al., 2018). The literature posits that tracking the psychological behavioural patterns of employees can be useful for organizations to detect the potential for different types of threats. An example of such a breakdown can be seen in the following figure from the NATO Cooperative Cyber Defence Centre (Kont et al., 2018).

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial Obligations	Low	High	High	Medium	Low
Address change	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

Figure 1: NATO Cooperative Cyber Defence Centre: Insider Threat Detection Study

These psychological and behavioural factors are also discussed in the context of the ongoing COVID-19 pandemic. For instance, the socio-environmental impacts of an online workplace are discussed in the more recent literature. These demonstrate how morale and mental health could become an issue for employees or potentially exacerbate existing mental health issues (Lorrimer, 2020). Moreover, depending on the work or the employer-employee relationship, tensions or hostilities could be worsened by employers having unrealistic expectations of their employees during their time working from home. Similarly employers may lack sensitivity to their employee's personal situations and limitations. These are only some of the causal factors that the academic literature reveals as at risk of occurring in the new workplace environments. Beside hostilities, this new environment could produce resentment, dissatisfaction, as well as other passive detrimental strains for employees that the organization should also be mindful of – much of these being akin to mental health issues previously discussed.

Notably, there is a multifactorial and overlapping nature to such indicators. The indicators are not mutually exclusive, and could work in combination - or one prominent factor - that is responsible for a insider threat event within a organization. This strengthens the notion that employers and stakeholders should consider every employee as an individual with their own unique portfolio of behaviours, stressors and motivations.

An employee's background and culture are also important factors to consider. Many pieces of literature (Kont et al., 2018; Bell et al., 2019; Elifoglu et al., 2018) recognize that every individual's personal moral and psychological profile has a part to play in how they act and behave, and whether or not they pose – or may pose – an inside risk. However, we have found that there is no clear consensus regarding archetypes and that typically perpetrators did not share a common profile. The majority of insider risk profiles were scattered across a variety of demographics as well as a variety of sectors and job functions. Nevertheless, in highly securitized positions, it is recommended that employers be mindful of an employee's background as well as reliability, mental health and moral character.

Managerial and social culture within an organization is also discussed within the insider risk context, specifically on how to bridge human resources processes with personnel culture, and how to effectively implement this bridging in order for employees to reflect the organization's priorities in regards to corporate security (PA Consulting & CPNI, 2012; Elifoglu et al., 2018). Doing so will also help employees feel included and satisfied with their organization and management. The way that management interacts and behaves, and the standard that they set within an organization, is seen to be important for the way that employees will behave and act and this must also be given consideration when trying to analyze employee attitudes and minimize likelihood of threat or risk events.

Finally there is an effort within the literature to find solutions to insider risk activity. This is a trend encompassing communications and how monitoring employee's communication is a useful tool in predicting how they will behave. Whether there be a change in regular patterns or new communication activities, these are observable behaviours that are useful for detection and

prevention of insider risks. Some of these include monitoring frequency of communication between employee pairs, analyzing contents of employee's communication, and the practice of organizational information sharing. Other techniques that can be used to flag and prevent potential insider risks include tracking employee conversations through emails, messaging and other predictive technical methods (Greitzer & Hohimer, 2011). This trend becomes even more pertinent in light of the work from home dynamics of the COVID-19 pandemic, with many employee interactions being digital, from personal - often unsecured – spaces and potentially occurring in a less-formal online setting; a setting which may be susceptible to anonymity, disenfranchisement and other setbacks of having to have the majority of interactions through an impersonal online medium (Lorrimer, 2020) The negative implications of this must be kept in mind by employers and mitigated through appropriate checks and balances, which according to the analyzed readings are mainly technologically based.

Holistic Organizational Approach to Insider Risk

Another broader trend within the academic literature is the perspective that there should be a holistic organizational approach to mitigating insider risks. Much of the literature points out that it is difficult to gauge the success of effective insider risk programs due to not being explicitly aware when threats are deterred. Because there is no way to predict which direction a threat will come from when an event occurs one of the ways an organization can learn from it and adapt is to be able to have a flexible enough insider risk program to analyze and adapt the mitigation strategy. That is to say an organization must learn from cases and use them to inform and improve the tools used to deter future insider risk (PA Consulting & CPNI, 2012). Having such a "looping" and flexible approach allows organizations to make the most of a risk event. Moreover, looking at insider risks as a whole is beneficial in informing your entire organization on the signs associated with it, and helps maintain the appropriate security culture in the organization (Healey, 2016).

A primary way the literature advises on mitigating inside risk is to emphasize a holistic view of insider risks at every level of management within the organization. The literature reaffirms that insider risks can occur at every level and that sophisticated technical skills are not required to produce a risk from an insider (Carnegie Mellon, 2018; Kowalski et al., 2008). By the same token threats can be mitigated at every level provided management instills the correct security culture within the organization. Notably, in the academic literature the prescription on how to do so is largely to increase "awareness" and promote education of employees through integration of personnel with human resources cultures more effectively. Additionally, an emphasis is placed on technology and investing in cyber systems that monitor and detect behaviours.

There are also a number of more minor general takeaways pertaining to the workplace that are important to be aware of for insider risk that the academic literature underlines. Firstly, perpetrators most often - approximately 80% - planned their actions. This is indicative that there is often pre-meditated activity that can be observed, and possibly interrupted. Secondly, insider threats were detected by a variety of methods and people – scattered across the organization. Moreover, someone close to the insider often had full or partial knowledge of the insiders'

intentions. This emphasizes that insider risk can happen at all levels and that interpersonal relationships are crucial in insider risk prevention. Thirdly, financial gain motivated most perpetrators and victim organizations often suffered financial loss. This point to the fact that financial considerations and incentives are top of mind for both the perpetrators and the organizations. Lastly, perpetrators committed acts while on the job. This indicates that monitoring and managing employees at work, as well as having effective mechanisms for insider threat prevention in the physical workplace is still an important tenet of ITP (Randazzo, 2005). Takeaways from these points show that examining people at every level holistically on the job is extremely important.

Emphasis on proactive measures versus simply hardening targets is another key suggestion within the work we consulted. This can be achieved as discussed through awareness and monitoring technology solutions. However, some literature urges companies and organizations to shift their focus from a protective or defensive outlook towards one that is more flexible and creative, examining how threats can be deterred or preventive as opposed to simply how much protection an organization can apply to what they value. Importantly, this is an under explored and under-represented theme in the articles we have covered.

In addition to literature related to the organizational and human centred approach to insider risk programs, a significant portion of the literature pertains to technology solutions integrated into insider risk programs. Over the past and current decade, the insider risk environment has and will continue to undergo significant transformations as a result of unprecedented technological innovation. Upon completing a review of existing academic literature within the field of insider risks, two specific patterns stood out in the scope of utilizing rapidly evolving technological advancements to detect and prevent insider risks. These areas include tracking employee behaviour through their everyday cyber activity on their work computers and continual recognition of employee identification through the use of biometrics. With new creations and significant improvements made to employee recognition technology, this section of the academic literature review will explain what behavioural cyber and biometric technologies are and how they have impacted the insider risk environment.

Technological Horizons: Cyber Behaviour

Cyber behaviour can be defined as an activity that targets or uses a computer, a computer's network, hardware or software, or an internet networked device (Jang-Jaccard & Nepal, 2014, 973-974). As outlined in various pieces of academic literature, employee's cyber behaviours can be continually analyzed to detect insider threats through computer printing records, login patterns, internet searching and systems browsing history, as well as, uploading and downloading behaviours. In turn an individual's cyber behaviours can be regularly recorded and overtime abnormal patterns can be flagged for further examination as possibly malicious acts. In this light, tracking cyber behavioural patterns can be extremely useful tools for organizations to detect internal information data theft or unauthorized information modification and access to mitigate the possibility of an insider risk attack (Ko et al., 2016, 4). This narrative of tracking cyber activity in the workforce as a

method of flagging potential behaviour that can lead to data breaches, theft or unauthorized modification has been echoed in various academic texts which will now be discussed.

In Bulpett's article, Safeguarding against the insider threat, the author highlights a drastic twenty six percent increase in data breaches and information threats since 2015 in which forty eight percent of attacks were a result of insider risks (Bulpett, 2020, 14). Bulpett goes on to conclude three main reasons to explain a significant increase of insider data breaches including increasingly vulnerable work environments of companies conducting digital remote working, a changing workforce with more job hopping, and an evolving employee identity in the "cloud" (Bulpett, 2020, 14-16). To combat organizational vulnerabilities of insider risk, the author suggests reducing and more strictly monitoring access points to classified information within cyber networks (Bulpett, 2020, 16). In this article, monitoring employee's cyber behavior for 24/7 risk assessment is ultimately proposed as a main solution to mitigate insider risks for data breaches.

Furthermore, Probst et al. chapter nine, Monitoring Technologies for Mitigating Insider Threats in their textbook Insider Threats in Cyber Security, similarly emphasizes a recent influx in cyber data breaches correlated to insider risk incidents (Probst et al., 2010, 197-198). Throughout the chapter, the authors outlined a large-scale automated deceptive cyber decoy system which would deploy fake ordinary looking classified documents to detect the presence of insider activity within an organization. In response to an unauthorized opening of decoy documents, a SONAR alert-management system would collect the triggers and alert the appropriate parties (Probst et al., 2010, 208). By using cyber decoys and in-depth network monitoring, this book chapter exemplifies how utilizing multiple cyber detection technologies can maximize the likelihood of detecting insider risks of information theft or unauthorized access to information.

Moreover, Greitzer's and Hohimer's article, Modeling Human Behavior to Anticipate Insider Attacks, reinforces the significant cyber security challenges that threaten government and organizations across all different kinds of industries. The authors attempt to establish a predictive threat assessment approach that provides automated support for the detection of high-risk behavioral triggers to prevent data leakage, and sabotage caused by insider risks. The text discusses a predictive modeling framework that integrates cyber data sources and motivational factors that enable malicious insider exploits (Greitzer & Hohimer, 2011, 27-28), Greitzer and Hohimer outline the monitoring of network-based data in the forms of file permissions, network print logs, search engine queries, access to account and much more that are relevant to insider risk detection threshold practices (Greitzer & Hohimer, 2011, 31). Essentially, the authors stress the need to create a predictive approach to detecting insider risks rather than relying on reactive practices of dealing with data leakages and information sabotage after they occur.

Overall, the themes illustrated in the three texts discussed were reflected in a majority of the reviewed academic articles that discussed cyber behavior in relation to insider risks. A main point established throughout the review of academic literature pertains to the unfeasibility of completely eliminating the risks posed by insider risks in cyber security. Nevertheless, the probability of data

breaches and organizational damages from insider risks can be greatly reduced by prioritizing the implementation of strict cyber monitoring of employees by using emerging technologies (Balakrishnan, 2015, 6-7). The need to rapidly analyze internal events, generate quality insights and reduce monitoring workloads by accelerating cyber automation is necessary to create faster real time responses to insider risks.

Technological Horizons: Biometric Behavior

Biometric and cyber behaviors are inherently linked to one another as both technologies monitor and track the unique aspects of an individual's character. However, cyber behavior monitors computer-based activities to detect potential insider risk activity but cannot identify the specific individual behind the threat (Ko et al., 2016, 4). Whereas biometrics monitors human characteristics and can define the individual that has committed an act flagged as a potential insider risk liability.

Biometrics are essentially the scanning of a person's physical or behavioral attributes for digital identification purposes to grant access to specific systems, devices or data (Li & Jain, 2015). Biometrics include recognition of kinesthetics body movements, vocal patterns, physiological features, and device-based gestures to define and differentiate specific individuals. Biometric behavior that can be monitored and detected for irregularities include cursor movements, keyboard strokes, mobile interactions, vocal patterns, eye-color, face recognition, fingerprints, eye movement, and body proportions. (Ko et al., 2016, 3-4). By tracking and recording each employee's biometric behavior and testing for inconsistencies over certain periods of time, biometrics can be extremely useful tools for organizations to detect fraudulent behavior from employees that use another coworker's identity to carry out dangerous and threatening activities. Fraudsters often obtained access to their victim's account through password hacking and sophisticated cyber attacks using backdoor accounts (Ko et al., 2016, 4). This narrative of monitoring employee biometrics in the workforce for continuous identity validation to reduce the likelihood of insider fraud risks has been echoed in various academic texts which will now be discussed.

Eberz's et al. article, Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics, discusses the use of biometrics based on distinctive eye movement patterns to detect and prevent insider risks. With an experiment the authors show that eye movement biometrics support reliable and stable continuous authentication of users preventing unauthorized access to information during everyday tasks (Eberz et al. 2016, 24-25). Through reading, writing, browsing, and video tasks, the eye movement biometrics technology was able to distinguish familiar and unfamiliar users by analyzing eye movements and eye gaze. The authors concluded that this technology can be effective in limiting insider risks who are trying to access unauthorized unfamiliar information sources, being an extra security measure for organizations at a relatively inexpensive cost (Eberz et al., 2016, 29).

Moreover, Fridman's et al. article Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location collects and analyzes behavioral biometrics

data from Android mobile device for continuously verifying the identity of a person. The areas of focus for authenticating identity included text entered via soft keyboard, mobile applications used, and physical location of the device as determined from GPS or public Wi-Fi (Fridman's et al., 2017, 515). After thoroughly testing the authentication system, it achieved a successful detection rate of ninety five percent after one minute and ninety nine percent after thirty minutes of user interaction with the device (Fridman's et al., 2017, 520). By fusing multiple mobile identification tools such as fingerprints and face recognition along with device-based gesture biometrics, the authors claim to have addressed the problem of active authentication for vulnerable information storage systems like phones. In turn, this technology can help prevent insider risks of fraud by quickly identifying foreign users of a particular mobile device.

Furthermore, in Locke's article, IBM adds behavioural biometrics to banking fraud solution, discusses how IBM financial organization has incorporated behavioral biometric technology to its online banking with the goal of further preventing banking fraud on a large scale. This biometric technology incorporates machine learning to track how users interact with banking websites by establishing patterns of mouse movements and voice authentication to continuously confirm an individual's identity (Locke, 2016, 1). These biometric identification tools had a ninety nine percent success rate in actively confirming the appropriate users identity. In the end, the inclusion of biometric machine learning in everyday banking activity has not yet fully reached its potential maximum benefit and the next steps will be to further implement these biometrics tools on the employee side of the banking sector to combat insider risks.

The main themes outlined in the three articles discussed in relation to biometrics were similarly echoed in various reviewed academic articles. An overlapping theme has been biometric technologies' ability to transform the practices in which an organization can protect their business, employees and customers from insider risks caused by fraudulent activity. Biometrics has been proven in various texts to expose new patterns of human actions that can lead to improving the indication of potential fraud (Hu et al., 2019, 2), encouraging best practices of insider risk mitigation are being followed (Nicolaou, 2020, 2-3) and most importantly is one of the strongest tools for continuous identification of users (Fridman's et al., 2017, 520). However, these new biometric technologies require significant amounts of data to be collected from employees and customers which could arguably be deemed as intrusive of privacy. Throughout the academic literature review there was no specific mention of how the utilization of these emerging technologies corresponding to Canadian privacy and security laws. Simply altering employee or customer privacy consent policies will likely not suffice. Therefore, this issue needs to be addressed before the practical application of cyber and biometric technologies can be commonly used to monitoring and detect insider risks within Canadian organizations.

PRACTITIONER LITERATURE

The following section will examine the existing literature being used in practice by private firms and government entities. It is important to draw a distinction between these sources and the previously examined academic sources to understand the thinking behind insider risk programs and their practical application beyond the theoretical plane.

Defining the Problem

A defining characteristic of the literature is the common consensus among what an inside risk is. However, the language used to describe and define the term is done so at a high-level that permits refinement by an organizational entity to suit their specific context. Broadly speaking, the literature reveals that an inside risk relates to people working within an organization who have access to information and whose actions, be they inadvertent, negligent or malicious, cause harm to the organization. While the specific phrasing may differ, government departmental publications regarding insider risk in the defence, security and intelligence communities of Canada, the U.S. and the U.K. concurred on the meaning of inside risk. This definition is an adequate starting point, but requires further operationalization by any organization tracking or responding to inside risk. For example, more needs to be said on the means by which one may commit an inside risk, and elucidate the motivation behind inside risk beyond a surface-level categorization of inadvertent, negligent or malicious. Before delving deeper into means and motivations, it would be worthwhile to further consider the definition of insider risk at a broad level.

People working within an organization: the nomenclature of 'insider risk' is quite clear – the risk is one that comes from within an organization. Therefore, it includes employees, students (also known as interns), as well as contractors working with an organization. Therefore, hackers unassociated with the organization seeking to cause financial or reputational damage to the organization, while a significant risk, are not within the scope of insider risk. Excluded too are state actors seeking to commit corporate or government espionage, unless they use an existing person within the organization as a conduit to execute their attack. With the scope of the problem limited to individuals working with an organization, the inside risk programming response is also limited in scope. Recognition of this, in tandem with the findings of our study, will inform robust recommendations for mitigating inside risks through insider risk programs.

Access to information: this part of the insider risk definition is vague, and purposely so. The domain of insider risk activity is broad and can encompass both physical and technological risk – to be elaborated on further on in the discussion of insider risk means – and so practitioners who deal with insider risk programming view information in the broadest sense. Information about the physical security features of a work site may introduce risks to physical safety as an insider works to overcome security measures. More common in practice, however, information is likened to data. Data is any information about the organization's proprietary information that – if disclosed, altered or destroyed – could cause reputational or financial damage. In practice, inside risk programs are designed around the CIA model – that is, they ensure data remains confidential, integrity of the data is maintained, and available when needed (Walkowski, 2019).

Inadvertent, negligent or malicious: multiple sources concur that the overwhelming majority of insider risk cases are inadvertent. They are the result of accidental, unintentional actions by an individual often caused by a lack of training (PA Consulting Group, 2012). Negligent, on the other hand, refers to when individuals constitute an inside risk by purposely disregarding or attempting

to go around the rules, not to harm the organization, but to get their work done quicker or without the need to go through policy channels. These two instances make up the majority of insider risk cases, but they are often low impact. Malicious insider risks – those actions that are intentionally committed to harm an organization – are relatively rare occurrences but have a large impact. For example, Raytheon found that the average financial cost of an inside risk by a manager was USD $1.5 million, and the average cost for a non-manager was USD $288,000 (Raytheon, 2015). Much of these costs are avoidable with an adequate insider risk program.

Harm: harm is vaguely phrased here, and allows for refinement by organizations to fit their specific context. Harm to an organization would often include reputational harm, financial losses, loss of prestige or, in rare circumstances, harm to individuals within the organization.

The means for insider risk activity differ depending on the broad level motivation. For inadvertent inside risk activity, actions commonly taken include clicking on a phishing or other spam type of links; for negligent risk activity, it's finding a workaround of the rules to get things done quicker or easier, such as installing a third-party unverified software against corporate IT guidance; for malicious risk activity, activities can range from purposeful theft of information via printing or saving data on an external memory device to committing physical violence.

Scope

The practitioner literature also makes clear that inside risk activity is relatively sector agnostic, meaning that where proprietary information exists, opportunities for its exploitation abound. The data type most sought – and most financially valuable – is personally identifiable information (PII), such as log in credentials, social insurance and date of birth information, or credit card details. It is estimated that PII is sought and exfiltrated by an insider in about 1/3 of all inside risk cases (Raytheon, 2015).

While sector agnostic, IBM has estimated that the financial services sector is the most impacted when it comes to inside risks (IBM, 2020). The report found the median cost of a cyber insider risk – that is, an inside risk involving the use of corporate networks to disrupt the availability of information, alter and disrupt the integrity of information, or to expose it to unauthorized individuals – was USD $4.5 million and took an average of 314 days to identify and contain. The estimated cost includes the financial loss that can be directly attributed to an insider, as well as the cost of investigation and recovery after the fact. While the costs are substantial, the practitioner literature is unified in asserting that the majority of these events can be detected and mitigated before becoming successful. The literature advocates for robust insider risk programs that are developed and tested well before an event may occur. An inside risk program should build in monitoring and detection activities at every stage of a potential inside attack.

Figure 2: Stages of an Insider Risk Attack (Balikrishnan, 2015)

The stages of a potential insider risk attack, according to the SANS Institute, are as follows (Balikrishnan, 2015):

1. **Grievance and Ideation:** in this phase, an insider feels a real or perceived grievance that leads to job dissatisfaction and could be a motivator for wanting to commit an inside attack. Mitigation steps at this step may include creating a culture of respect in a workplace, managing employees with empathy and understanding of their unique circumstances and modifying work to meet employer and employee needs, or having a formal and robust grievance process.
2. **Preparation:** the potential inside risk would begin to think of potential ways to "get back" at the organization or how they could benefit financially. They begin to develop a plan and devote time to gathering requisite knowledge, tools, materials, etc. Mitigation steps at this stage may include internet usage / productivity monitoring.
3. **Exploration:** the potential inside risk would continue to explore ways to execute an attack, and confirm their resolve to do so. This is typically the tipping point for deciding whether to go forward or not. Network monitoring is again beneficial at this stage to detect anomalous behaviour and begin an investigation to affirm whether or not an inside risk event may occur.
4. **Experimentation:** at this stage, the inside risk resolves to commit an attack. They begin to experiment with and prepare how to conduct an attack, including testing viable options. The insider likely may be unproductive with work tasks or secretive about their activities, which colleagues may be able to detect when adequately trained.
5. **Execution:** At this point, the inside risk executes their attack against the organization. If not immediately detected and stopped, damage is likely to occur to the organization.
6. **Escape**: The inside risk will try to cover their tracks to avoid detection. This could involve network manipulation, or exiting the company altogether. By this point, the damage has been done and the organization will need to adequately respond after-the-fact. Best practice would suggest an investigation would need to occur to determine how the inside risk was able to execute an attack and a review of security and insider risk programs and policies is warranted to avoid future similar attacks.

The practitioner literature is focused on sharing knowledge and best practices to organizations to build a robust insider risk program from scratch. In general, the pathway to developing an appropriate program was encompassed within three overarching themes (Public Safety Canada 2019):

Holistic Approach to Security

The literature emphasizes the importance of establishing an organizational culture of security founded on robust policies that are transparent and communicated regularly to employees at all levels. However, in order to establish a culture of security, leadership needs to buy-in to corporate security initiatives and model compliance. Further, it is important to designate an executive as the champion for inside risk and security culture. This person should be aided by a working group with representation from areas across the organization, including the following key departments: human resources, legal services, information technology services, and corporate security.

A part of a holistic approach to security also entails building security measures and expectations into service agreements with third-party vendors and service providers who have access to company proprietary information. Service providers should be vetted to the same standard as employers, and trust should be established and maintained throughout the service period. A best practice for maintaining trust is to create long-term relationships with the same service provider.

Know and Empower People

People working for or with an organization are both the organizations greatest assets, but when it comes to inside risks, they can also be great liabilities. The literature therefore recommends implementing personnel screening that is commensurate with job risk classifications. Individuals who will have access to sensitive data should be rigorously vetted via criminal record, credit and reference checks prior to onboarding. Security screening updates should occur at periodic intervals to detect changes in personal circumstances that may indicate higher likelihood of risky activity. When employees leave an organization, they should undergo an exit interview and their accesses should be swiftly deactivated.

Employees also should be provided with adequate security awareness training to decrease the risk of unintended security infractions. Specifically, employees should know how to spot phishing attempts, understand corporate password integrity guidelines, and learn the signs of social engineering. It is also helpful to foster a “see something, say something” culture.

Protect Infrastructure

The third and final category of inside risk mitigation techniques is to identify critical assets and infrastructure and develop resources and policies to protect them. This includes leveraging technology to monitor employee network behaviour for signs of anomalous or unusual activity. Monitoring techniques may include tracking remote access, network data flow, and removeable media such as USB sticks. All organizations should also have updated business continuity plans to be able to flexibly and efficiently respond to unexpected events while maintaining the integrity, security and confidentiality of information.

LITERATURE REVIEW SUMMARY

This literature review encompasses sources from both academic and practitioner streams. This has allowed for a holistic survey of the current field of insider risk, as scholarly work may differentiate from practitioner application of information. In the academic literature, it was found that human and social influences may be a source of insider risk. The COVID-19 pandemic and changing workforce trends serve to compound the human aspects of insider risk, and may elevate the risk profile of certain employees.

Furthermore, there is a bifurcation in the academic literature between people focused insider risk programs and technology based insider risk programs. While the people focused insider risk mitigation strategies attempt to be proactive in preventing employees from mobilizing to become an insider threat, technology based insider risk programs tend to be reactive to detect indicators of employee behaviour. For example, some insider risk programs may monitor employees' cyber behaviours or biometrics to detect indicators of insider risk. However, technology focussed literature emphasizes that one cannot completely eliminate the risks posed by insiders, but the risk can be greatly reduced through robust monitoring systems. Canadian financial institutions must contend with the divergent insider risk mitigation strategies in academic literature, and may consider incorporating aspects of both streams.

There is a general consensus on the definition of insider risk, and a common understanding that the risk must be taken seriously. A majority of the literature is predicated on protecting the confidentiality, integrity and availability of proprietary data. Unfortunately, the literature is not forward-looking. It does not account for changing workforce trends, such as the general move and increased flexibility for work-from-home arrangements. While the COVID-19 pandemic has exacerbated the speed of this development, this trend has been occurring from well-before the pandemic. The literature is also more focused on building inside risk norms than on how to implement inside risk programs. For example, in the practitioner literature, many sources recommend building a "see something, say something" culture where employees can report suspicious behaviour or suspected non-compliance. There is no mention of how to achieve this type of culture, nor any discussion on the potential negative externalities like potential increased employee dissatisfaction at having to report or being reported by colleagues.

METHDOLOGY

The initial stages of this research entailed undertaking an extensive literature review. The purpose of the literature review in the broad scheme of the project was to gain an understanding of existing research and relevant debates in the field of insider threats. As researchers with minimal prior knowledge of the insider threats landscape, the literature review helped build the baseline of understanding in the field of insider threats. The analysis of existing literature provided a great understanding of how complex insider risks are, difference between United States and Canadian approaches, emerging consideration and specific terminology used in the field. In turn the literature review insights helped contextualize the findings from the questionnaire, consultation and foresight exercises that were completed. The literature review was divided into three separate sections including academic literature, practitioner literature and Canadian case studies all examining the overarching scope of insider threats. The review of the existing literature established what areas of insider threats have been focused on by others and what the common trends in existing literature findings were. In addition, the literature review highlighted what gaps in the insider threat environment have been identified, what recommendations authors had for further research and outlined predictions for the future of insider threats. The information uncovered in the literature heavily shaped the research design of the questionnaire and the strategic forecasting process.

The questionnaire and consultation designs for this research were created with the intention to understand professional participants' insights on the current and future landscape of insider threats, as well as the efficacy of prevention and detection measures in place today. The concepts covered in the questions for both primary data extraction tools were designed to include many of the major areas of focus for this research project. The questionnaire and consultations were targeted towards professionals working both in the private sector and government in various countries that are involved in security, risk and compliance. The questionnaire and consultations were also constructed in a way for participants to analyze the changing work practices caused in part by the COVID-19 pandemic, in addition to pre-COVID trends such as a move towards an informal "gig economy". This was done to help understand insights and predictions about potential gaps in insider threat prevention and detection programs moving forward and recommendations to address those gaps. With the support of field experts' perspectives, this capstone project can be to be truly forward looking with the collected primary research used to complement existing literature to highlight future policy recommendations and strategic stressors regarding insider threats.

The number one priority when designing the insider threat questionnaire was to ensure it would meet the research objectives of compiling information on practitioners' understanding and experience of insider threat programs. These responses would then be used in comparison to the findings from the literature review to provide a holistic analysis of the insider threat landscape in the report.

The questionnaire was designed with the intention of probing relevant insider threats issues. Major topics covered included motivating factors that cause insider threat incident, identifying organizational insider threat program objectives, indicators and monitoring methods, as well as, future trends and risks within the insider threat environment. These topics were covered in mostly qualitative questions and responses throughout the survey so that it was easy for respondents to provide their opinions and experiences without much constraint. The questionnaire also included a series of questions in which responders specified their level of agreement to a statement on five-point Likert scales to provide some information for quantitative analysis. The survey language was designed to be easily understandable while also following a logical arrangement increasing in specificity with each question. Overall, questions were particularly worded to encourage respondents to provide accurate, unbiased, and complete information.

Furthermore, the survey avoided any personal or directly identifying questions intending to be as anonymous as possible. The number of questions asked were also limited to twelve so that participants could easily and quickly complete the survey. The first two questions were used as controls to exclude non-desired respondents via qualifiers determining whether participants work in security, risk or compliance positions and that their organization has an insider threat program. As a caveat, the two control questions assumed respondent honesty in qualifying their answers. Finally, at the end of the survey there was an option for respondents to request a follow-up consultation to discuss their responses to insider threat topics in more detail.

In terms of distributing the questionnaire, a voluntary and convenience approach was taken. The questionnaire was completely voluntary as there were public posts made by the researchers on their LinkedIn profiles advertising the survey with a direct link to complete it on a google form for interested individuals. To generate more traffic for the questionnaire, field experts reshared the survey with their LinkedIn network and cold-messaging relevant professionals on LinkedIn was completed by the researchers. In addition, members of capstone project conveniently circulated the questionnaire within their professional networks, sampling pre-identified respondents known to the researchers.

Finally, the insider threat questionnaire was approved for distribution and use by Carleton University Research Ethics Board-A. Each of the researchers were required to complete Carleton's research ethics training. In addition, all of the survey questions were thoroughly vetted by Carleton's Research Ethics Board so that they operated in compliance with Tri-Council's policy regarding ethical conduct for research involving humans. In the end, the ethics approval clears the way for making use of the research more comprehensively.

Moreover, the sampling and distribution technique used for the questionnaire could potentially cause bias results because not everyone in the population that is qualified to answer the survey was given an equal chance to participate. In essence it is impossible to comprehensively know how well represented the population of insider threat experts are in the survey. Nevertheless, a non-random voluntary convenience sampling approach was taken because it is the most practical method to use within the time and resource constraints of this three-month project.

The overall goal of the consultations is to understand potential nuances in insider threat program creation, review, and revision. In addition, consultations were intended to qualify survey results with personal experiences from experts who have taken on varying roles in the insider threat environment. Essentially, the consultations would further illustrate the current and future scope of the insider threat environment through the perspective of field experts.

The consultations were designed to build upon the insider risk topics discussed in the survey. Similar to the survey, consultations questions were designed to go from asking participants about general knowledge and as the consultation progressed questions became more specific. This structure was adopted to reduce potential bias of influencing participants into providing certain types of responses for the current or future questions in the consultation. For example, participants were asked what makes for a good insider threat program generally, then asked to rate specific insider threat program elements on a Likert scale. Like the questionnaire, both qualitative and quantitative questions were used in the consultation. Topics covered in the consultations elaborated in more depth on topics such as insider threat motivating factors, insider threat program objectives, gaps, indicators and monitoring methods, as well as, future workplace trends in the post-COVID environment related to insider risk.

Furthermore, to conduct the consultations with the utmost confidentiality none of them were recorded. Rather one of the researchers would ask the questions while the others would be taking notes on the responses. To ensure the accuracy and authenticity of responses, the note takers tried to transcribe as best as possible the word for word responses of the participants. At the start of each interview there was also a reminder to participants that their identity would remain completely anonymous and that the amount of information participants shared for each question is completely voluntary at their discretion.

The same non-random voluntary convenience sampling approach used in the questionnaire was implemented when completing the insider threat consultations with field experts for timing and practicality reasons previously mentioned. In addition, one of the advisors for this project helped identify a handful of relevant insider risk subject matter experts to consult with. The researchers also contacted members from their professional network to secure additional consultations. The professional domains of consultation participants vastly differed from private sector and public sector employees spanning across various countries. These participants had different strengths in knowledge and experience surrounding technological, legal, physical, social, psychological, cultural, political, and administrative aspects of the insider threat environment. In turn, the diversity of participants' backgrounds enabled the collection of varying perspectives and insights to consider in the findings and recommendation portion of this report.

In addition to the industry consultation and questionnaire sampling method, this study also adopts methods of strategic foresight to anticipate changes in the landscape of insider risk that may occur in the future. Strategic foresight methodologies do not aim to predict the future, rather they seek to forecast what may be possible in the future. This forward-looking research approach begins by conducting a horizons scan, wherein a broad range of media sources and non-traditional

sources are examined to detect weak signals, which are indicators of change in the security environment. Weak signals are then analysed to identify higher level sights — the main themes derived from the horizons scan. These insights are then utilized for the purposes of conducting two forecasting exercises using futures wheels.

The futures wheels outlined in this report provide a forecast of the consequences of the selected higher level insight. The diagrams are organized such that the higher level insight is placed in the middle, and the first circle represents the first order consequences of the stated future trend in the insider risk security environment. The second circle represents the second order consequences of the insight, and the third circle represents the third order consequences. These consequences are situated in chronological order - expanding away from the initial insight. The diagrams produced from these exercises will contribute to a greater understanding of the future of insider risk and to the industry best practices recommendations.

As discussed prior in the methodologies section, the horizon scan is used to provide a forward looking outlook for the project and help inform the consultations. We began this process by scanning multiple media outlets, non-traditional media and sources, as well as fringe sources that could provide indicators for future drivers of change. By looking at non-traditional sources this methodology allows for a non-restrictive and candid view of the insider risk landscape all the while taking into consideration broad political factors that may contribute to the future of insider risk.

During our scanning process we identified over thirty weak signals that could indicate change within the insider threat landscape. Interestingly, these signals group well into similar categories that have been identified in the literature review. That is, signals based on personal and human factors, those based on technological and cyber elements and lastly, on more broad political factors. These three classifications of human, technological, and broader political factors are thus the three main avenues through which we can expect change in the insider risk landscape according to the horizon scan methodology.

Human Focused Change

First, there are several weak signals that underline the new realities of the COVID-19 pandemic, specifically in regards to its effect on employees and people. Since pandemic issues are top of mind for most organizations along with the work from home dynamic it is expected to also see them across a variety of media sources. Notably, this is important for our research because these novel realities are unobservable through an analysis of the existing insider risk academic literature; likewise the past case studies examined are not reflective of the pandemic.

Signals found in this human-focused trend emphasized a wide variety of ideas all of which focused on employees and people as the principle factor in insider risk. First, the effects of mental health, general employee wellness, and other personal stressors on company attitudes in a work-from-home environment were discussed (Nextgov, 2020). Second, the need to take a 'people-centric' approach when creating solutions to circumvent modern insider risk is emphasized - especially having adequate awareness of suspicious or malicious behaviours (SCMagazine, 2021). Furthermore, the emergence of a new physical security environment during a work from home posture, and the need for organizations to adapt to this through appropriate technological and systemic means is discussed (BanklessTimes, 2021). This can usually take place through increased employee management or monitoring as discussed in the cyber and tech sections.

Lastly signals mention that all these factors can amount to potential risk, negligence and alienation of employees. All of these tendencies have certain behavioral or personal pre-existing traits that if observed - or insulated appropriately through awareness and technology - could prevent and circumvent insider risk (SCMagazine, 2021).

Ultimately the weak signals observed here indicate that people are the principle driver of insider risk. Thus despite newfound technologies as well as broader trends, focusing on employee behaviours and their attitudes – through monitoring, awareness and development of a healthy corporate culture - is still front and center for preventing insider risk. This is especially the case when considering the ongoing global pandemic.

IT & Technology Focused Change

This second category is by far the most diverse and extensive containing a number of different technologies and concepts that may potentially play a role in the future of insider risk. The principal issue with this category is that with the abundance of evolving new technology it is hard to predict which of these concepts will play a role in insider risk. Many novel technologies have implications across a wide variety of industries and could be misused or distorted to produce detrimental effects on a company despite the inventors' best intentions. Likewise, with new technologies, their full capacities or implications are not well known yet – or fully developed - and require further research or field testing in order to deduce any meaningful prognosis. Nevertheless some standouts are especially pertinent to the banking and corporate security field and will be discussed as follows.

First, it is difficult to discuss the future of the financial sector and not discuss blockchain technologies as well as de-centralized currency. With the advent of cryptocurrency, financial institutions worldwide have contrasting opinions on this concept, some not deeming it a serious risk, others outright banning the medium (Huxley, 2020). Regardless of a bank's or nation's stance the reality is that there is significant tangible value to be made from cryptocurrency and thus it will be here to stay, as well as the potential risks posed by its technology. The implications of having a de-centralized currency are numerous but particularly interesting is that blockchain technology lends itself to other kinds of de-centralized items. Among these items are components such as decentralized passes or digital IDs, non-fungible tokens, passwords, web-spaces or other domains or virtual assets. The idea is that instead of having a physical ID someone could have a encrypted digital token that confirms their identification and that is stored on a decentralized platform – across a variety of servers - thus having someone's credentials 'decentralized' and not on any one location (Wired, 2021). Keeping up with this particular technology would be invaluable to all industries especially when aiming to augment security or better understand how to better encrypt technology against insider risks.

Another field of technology that is pertinent to the insider threat landscape – and that was prominent among our scanning – was monitoring and detection technologies. This includes facial detection technology, movement and eye scanning technologies, as well as different kinds of neural

networks and AI designed to recognize patterns of employee behaviors and predict decisions (BBC, 2019., Venturebeat, 2020). Although these new monitoring, surveillance and behavioral recognition technologies can be especially pertinent for mitigating insider risk there are also a number of privacy concerns that arise with them. These are important to make note of especially if using said technology to monitor or observe employees. Considering the often lagging nature of legal context with new technology it is imperative to be aware of where the two intersect and how this may be actioned within an organization.

Breaking down each of these individual technologies and their implications may perhaps be beyond the scope of this report. But, their importance to insider risk programs can be distilled to the notion that having an understanding of the rapidly evolving technology landscape, and practicing the adequate corresponding cyber-hygiene, is essential when it comes to minimizing insider risks as well as fostering an effective corporate security culture.

Political and Global Change

Lastly, there were a number of broader signals in the global, political and security sphere – not specific to insider risk – that could potentially play a significant role for an organization. This becomes ever more pertinent when contextualized with the finding that corporate buy-in, as well government buy-in - for state run organizations - is necessary for adequate management of insider risk. Global security events that increase threats in general could potentially increase insider risk, and hallmark threat events that occur internationally within an industry will likewise raise domestic concerns. Moreover, international security events such as foreign interference within critical industry will undoubtedly have a significant impact on the manner in which –and to what extent- domestic organizations will have to securitize their industries.

Some examples of such events can be observed through the increase in international incidents pertaining to national hacking and interference (Wired, 2021). There have also been an increase in incidents targeting private companies specifically with more profound and advanced hacks that have taken place cross-industry and exposed numerous sectors simultaneously, such as the SolarWinds hack (Wired, 2021). In addition to overt hacks there exists a massive flow of companies constantly reporting - and patching - data breaches within their organizations. Furthermore, politically motivated interference and hacking is increasing surrounding public health critical industry from Chinese actors as well as other intellectual property (IP) theft (ZDNet, 2021). This is being brought to light by not only allied governments but is also highlighted by our own domestic agencies (CSIS, 2020). These trends present a need for policy change and attention by decision makers and stakeholders to take national digital IP security more seriously. Especially in light of growing tensions with Russia and China – the usual suspects in foreign interference - it is extremely likely that espionage and foreign interference, particularly in the cyberspace, will be given serious attention by governments. Stakeholders in Canadian critical industries such as the financial sector should be in-tune with this and make use of the novel securitization of the space – using the current climate to raise awareness and build capacity to deter insider risks more broadly as well as from foreign rivals simultaneously. This can be accomplished with joint efforts with domestic agencies which have recently been increasing critical industry stakeholder engagements.

INSIGHTS

COVID-19 Pandemic & Working From Home

As a result of the COVID-19 pandemic, workplaces were forced to adapt their operations quickly to protect their employees from the harmful virus. However, the quick shift to a work from home environment has increased the potential for an insider risk incident to occur. It is projected that in 2021 there will be an 8% increase in insider risk incidents as a result of the factors of the COVID-19 pandemic (Baksh, 2020). In the COVID-19 era it has been posited that the most prolific insider risk is the compromised insider, whose credentials have been accessed for nefarious purposes (Zerucha, 2021).

Weak signals found in the horizon scan indicate that resulting work from home dynamics brought on by the COVID-19 pandemic have elevated behavioural, technical and organizational risks that Canadian organizations must contend with (Deloitte, 2020). Behavioural risks pertain to how anxiety and stress may increase the risk for an insider event to occur (Deloitte, 2020). With the ongoing financial and emotional hardships of the COVID-19 pandemic, employees may face a lost sense of optimism that can lead to insider activity out of desperation for safety and security (Deloitte, 2020). Additionally, new technical risks have been introduced to workplaces as a result of work from home arrangements, as an organization's equipment is now in employee's homes and not in their offices (Deloitte, 2020). This brings about greater risk that the equipment and information supplied may be misused by others in the household, and employees may become more relaxed in regards to following security protocols (Deloitte, 2020). Finally, new organizational risks have emerged for companies as their operations were forced to adapt a lower risk tolerance to accommodate work from home arrangements (Deloitte, 2020). These new risk tolerances pose a hazard for the future of organizations as the new risk tolerance could become the status quo (Deloitte, 2020).

Emphasis on personnel safety and satisfaction

The second insight offered by the horizon scanning recommends that organizations prioritize the safety and satisfaction of their personnel in order to prevent insider risk. Employees are the backbone of any organization and signals show that they are taking the brunt of the burden during the pandemic. Mental health, stressors as well as pre-existing grievances may only be worsened during this time. Organizations should seek to maintain and build a personal connection with their employees in order to foster a sense of community and understanding between employees at every tier of the organization. By emphasizing such a connection, employees are more likely to feel loyalty, community ties and a sense of purpose towards their workplace. This will lead them to be more mindful, maintain security awareness and abide by company policies more closely. A special focus on personnel, reinforced with IT strategies, is paramount for mitigating contemporary insider risk events.

Global and Political Attitudes on Security

As discussed in the prior section these are turbulent times when considering international security, hacking and foreign interference (Wired, 2021., CBC, 2021). This broader spurious and competitive landscape between nations, state run companies, and private stakeholders is an ongoing struggle to maintain the upper hand in political and economic power. These larger trends will undoubtedly play a role in the domestic insider threat landscape, evolving the definition as well as the understandings and expectations surrounding security within Canadian critical industries. Institutions and stakeholders should be mindful of the climate within which they are operating, which foreign partners they are interacting with, what is being conducted and how proprietary information is being shared within international partnerships. Similarly institutions should keep close contact with domestic public safety institutions in order to raise awareness, build effective policy and promote deterrence against insider threat events from foreign actors as well as effectively securitize the space within the appropriate federal guidelines. Ultimately international politics and events will color corporate and government buy-in for the future of insider risk, as well as the institutional standards, expectations and initiatives.

Case Study: General Electric

Two former GE employees charged with economic espionage and theft of trade secrets in the USA for stealing proprietary files to start a wind turbine corporation to benefit the People's Republic of China. (Department of Justice, 2019)

New Technologies

Lastly, new technologies will be heavily implicated in the way insider risk is parameterized, executed and deterred. Whether this is new monitoring and detecting technologies, de-centralized technology or artificial intelligence, these developing technologies will accrue significant advancements within the next ten to fifteen years. Monitoring and detection technology will likely be the most influential, particularly in the short term post-pandemic landscape, providing employers with new tools to monitor and detect behaviors and negligence by employees. Notably, these technologies will have serious ethical implications when it comes to privacy and legality of monitoring. Inversely decentralized technology will likely impact the physical aspect of security and preventing insider risk. These technologies have the potential to change the rules of the game entirely with new physical security mechanisms and possibilities. Likewise this new technology could have implications that have not been accounted for yet and thus merit future research and attention, especially within the space of insider risk. Notwithstanding, new technology will certainly have a significant role to play in how insider risk is seen and mitigated. Thus, promoting cyber-hygiene as well as educating and raising awareness to new technologies as they occur is paramount to insider risk and corporate security within every critical industry.

FUTURE OF TECHNOLOGY FOR INSIDER RISK PROGRAMS

Figure 3: Technology & Insider Risk Programs Futures Wheel

- Centre circle represents the driver of change in the future
- First circle represents first order consequences of stated change
- Second circle represents second order consequences
- Third circle represents third order consequences

This futures wheel outlines the potential futures and consequences of the institution of new technologies used to detect and monitor insider risks. Using strategic forecasting methods, this exercise will establish the cultural, technical, and organizational risks posed by the imposition of advanced technologies within insider risk mitigation strategies.

New technologies for the detection of insider risks will usher in a new security culture for the organization, which will pose a set of risks to the existing workplace culture. Employees may feel as though they are being constantly monitored, and will therefore trust the organization less. The breakdown in organizational trust between the organization and employees may lead to elevated motivations to commit an insider risk event. Furthermore, a more fearful workplace culture may lead to a higher rate of employee turnover and brain drain from the organization. Additionally, if employees grow fearful of the constant surveillance, they may fail to innovate which will contribute to a lack of business advancement.

New technical risks posed by novel insider risk detection technologies may impact an organization through creating unnecessary dependencies on third party service providers. For instance, data collected to be analysed for indicators of insider risks may be vulnerable if stored and managed by a third party outside of the organizational structure. Through contracting out security services more people will have access to an organization's information, and may therefore add more risk of an insider incident. In addition to risks posed by managed service providers, new technologies to detect insider risks may increase security complexity to such a degree that they will impact the organization's response time to threats of an insider incident.

Finally, new organizational risks may be posed through the implementation of novel insider risk detection technologies. These advancements in technologies may replace previously human occupied jobs in security and compliance, and instead require that organizations hire professionals to maintain the insider risk software. Furthermore, novel insider risk detection technologies present a high opportunity cost to organizations, as they may fail to invest in other insider risk mitigation strategies that have potential to provide better protection to the organization. For instance, investment in employee aftercare programs may reduce the motivation to commit an insider incident, and stop the risk before it mobilizes.

SHIFTING GLOBAL POLITICAL ATTITUDES FOR INSIDER RISK PROGRAMS

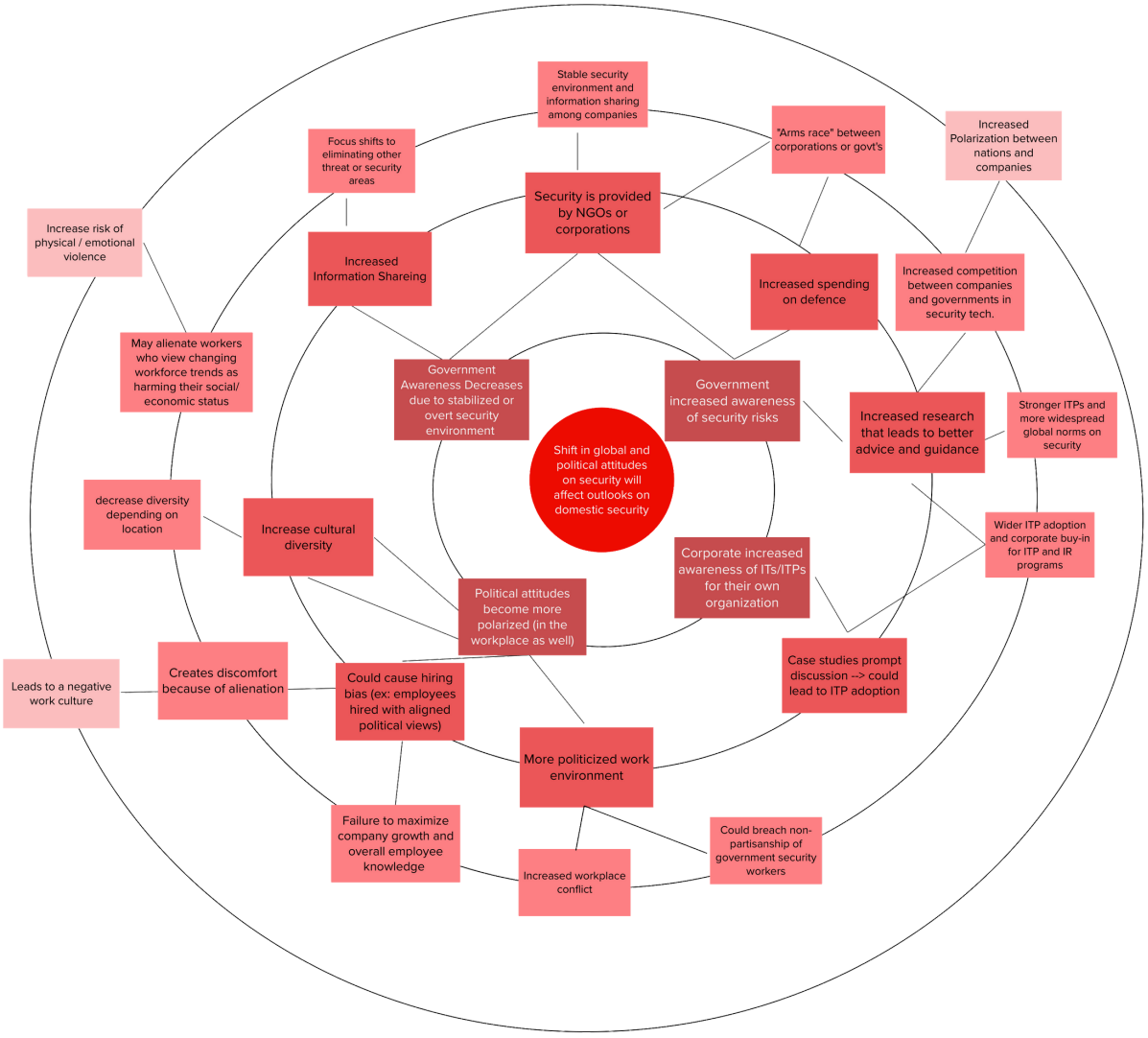

Figure 4: Global Political Attitudes & Insider Risk Programs Futures Wheel

The second futures wheel addresses our third insight of how shifting global political attitudes may affect insider risk within institutions – as well as domestic security considerations within individual nations. Using our strategic forecasting methods, this exercise will outline some of the forward looking implications, consequences, and nuances of this insight that we have extrapolated over time. Considering the broad scope of this trend the implications outlined in the chart are not conclusive and only encompass some of the more pertinent political, social and cultural consequences that we have detected.

Firstly, it is important in this insight that global and political attitudes may shift in either direction. There is likely to be a securitization of national assets as well as critical industry. Inversely, over the long-term there may be cooperative international factors that trigger a détente in security attitudes and lead to nation's cooperating instead of competing in security. Both of these can occur, although only the former was thoroughly considered in this exercise as evidence points to increased securitization and continued polarization of the international security environment.

Some consequences and trickledown effects of polarization of the international security environment could pertain to the heightening of political attitudes within the workplace as well; this could take the form of different agendas by certain organizations or government departments or simply disagreement between employees on certain issues. This in turn could lead to a hostile work environment, tensions, as well as increased workplace conflict. This may cultivate a negative workplace culture, leading to employee alienation or resentment that could result in an insider risk event. This in turn would lead to a failure to produce desired company growth and could lead to a respective variety of negative consequences for the institution.

Another first order consequence of a shift in global attitudes could be the increase of corporate or government awareness and buy-in for security risks more generally. Specifically this could lead to an increase of interest in insider threat programs (ITPs) which in turn may lead to increased research, investments in security, and a heightened securitization of the insider risk environment. Although on the surface beneficial, heightened securitization in an already polarized environment is likely to lead adversaries or competitors in the similar direction further raising tensions. Thus the effects of this insight are for the most part ambiguous. Although these effects do point to the fact that some form of polarization is likely, and that the long term consequences of a shift in political attitudes will likely have a generally detrimental effect on insider risk as well as on workplace environment and culture. Whether this be implicit or explicit, this negative trend of securitization and polarization of the international security environment is something to be mindful of for decision makers within the context of the next ten to fifteen years.

RESEARCH FINDINGS

In the following pages, we will begin to examine the findings we obtained from our industry consultations and questionnaire. We will start out by briefly outlining the data we collected with some important caveats to keep in mind. Then, we will go through what our research tells us about the following four areas related to insider risk:

1. Who is likely to commit an inside risk?
2. What are the current best practices for insider risk programs?
3. What gaps currently exist within inside risk programs?
4. What are the forward-looking trends and how will industry have to adjust to mitigate inside risk in the near future?

After answering these four vital questions, we will begin to compare and contrast our research with what we had previously found throughout the literature. We will also examine our findings in light of our foresight exercises to identify areas of convergence areas of incongruency that may require attention to bridge potential gaps. The end-goal of our findings will be to provide recommendations to ensure insider risk programming is more in line with a forward-looking threat landscape.

Data

Questionnaire

Our questionnaire was launched in early-March, and was originally posted on LinkedIn. The goal behind posting it via this social network was to promote it to industry insiders who would be best positioned to provide meaningful insights on insider risk. While the survey was posted on the researchers' personal accounts, the questionnaire was amplified by individuals with existing networks related to inside risk, security and compliance. By the close of the survey date on April 1, we collected a total of 19 responses. Unfortunately, five responses were screened out because the individuals answering the survey indicated they were not working or had not worked in positions related to security, risk and compliance within their respective organizations. Therefore, we kept 14 responses and used these as the basis for our analysis with respect to the questionnaire.

Overall, we did not receive as many responses to our survey as we had planned. Nevertheless, the results of the questionnaire combined with the industry consultations we conducted provide important insights into the current and future landscape of inside risk. The reason the

questionnaire was constrained to a small sample size was due to logistical reasons of time and resources. Another cause for the small sample size was participant concerns around the privacy and anonymity of their identity, as the platform we used to collect responses - Google Forms - collects IP addresses. While we endeavoured to ensure participants that this information could not be seen by the researchers, some participants nevertheless did not want to continue.

We also encountered some difficulty with individuals in the intelligence, security and defence sector who were worried that sharing any information could give away their security methods. This may explain why no government sector employees completed the survey. In spite of this, the fourteen participants who completed the questionnaire were representatives from other key sectors of the workforce including private corporations, private risk and consulting, education, and the financial sector. As a result, other than the government sector, the results from the questionnaire include representation from a majority of occupational sectors that directly deal with the insider risk environment.

Finally, in terms of questionnaire design, our literature review led us to predict that integrating technology into insider risk programs would be prevalent in our findings. As a result, we designed our questionnaire mainly around technological interventions that could be used (see Appendix A for a full copy of the questionnaire). By focusing on technology, we neglected to include other components of insider risk programs that our consultations demonstrate are critically important – namely creating a positive work culture. Therefore, our findings for our questionnaire are skewed towards favouring technological interventions. To mitigate this, we adapted our consultation questions to help fill in any gaps in knowledge from the questionnaire findings (see Appendix B).

Consultations

We began our consultations simultaneously with the launch of our questionnaire in early-March. Initially, we consulted with an individual connected to other individuals working in security, risk and compliance fields to help us recruit our first respondents. We also leveraged our personal networks, and sent messages to individuals we had identified as potentially relevant via LinkedIn messaging. While we initially expected the consultations to be solely supplemental to the questionnaire, we were able to consult with more individuals than we had initially predicted and gain critical insights into inside risk and inside risk programs. In total, we spoke with 11 individuals throughout March. Five of these individuals were government employees, while three each were from the financial services sector and the non-financial services private sector. The individuals we spoke with came from both large institutions and small boutique businesses. All had experience in the realm of security, risk or compliance.

When recruiting individuals to join us for a consultation, we informed them that the platform used would be Zoom. However, to encourage an open-ended and candid conversation, we informed each participant that we would not be recording their video or audio and that no personally identifiable information would be collected. The only demographic information we collected was the industry they worked in, which we classified into the following three sectors: government, financial

services or non-financial services private sector. Each session was scheduled for 15 minutes, but the majority of sessions lasted between 30 and 45 minutes in total.

We guided our consults through a series of questions linked to our four primary research questions (see Appendix B for a list of our consultation questions). Most of our questions were open-ended, to encourage respondents to tell us in their own words what they thought of inside risk and how to combat it. Only one question asked respondents to rate components of inside risk programs on a Likert Scale. This enabled us to quantify common elements of inside risk programs. Unlike the questionnaire, we adapted our consultations to encompass what we were learning along the way. Therefore, our consults guided us as researchers away from technological interventions to inquiring more about the importance of workplace culture and employee satisfaction as critical elements of mitigating inside risk. Further details on this will be provided later on.

Who is an Inside Risk?

Time and again, our research found that employees are simultaneously an organization's greatest asset and their largest liability when it comes to inside risk. When asked what the biggest driver behind motivating an individual to be a threat to the organization is, our respondents surprised us with their answer. Almost unanimously, they agreed that the biggest driver was **no** driver at all. Rather, the overwhelming majority of inside risk cases were the result of accidental or non-malicious negligent behaviour. Accidental or negligent breaches of company security policies are voluminous, but they are often low impact. Examples of accidental inside risk vary, and they encompass mistakes relating to use of technology and also mistakes relating to physical access to data. An example of the former would occur when an employee unknowingly installs a virus, malware, spyware, trojan or other computer vulnerability that has the potential to monitor the network or exfiltrate data via a phishing email or other spam link. An example of the latter may entail not locking a computer when leaving the workstation, creating an environment where it would be possible for an unauthorized individual to be exposed to proprietary information. In both these examples, employees don't intend to cause the organization harm. Rather, a lack of training to detect fraudulent or phishing/spam emails may have caused the employee to click the link, while a lax security culture or environment may make an employee think it is acceptable to leave their workstation unattended for a short period of time.

Unfortunately, this means that any employee is capable of constituting an inside risk. Therefore, it is critically important to have robust measures in place to prevent accidents from happening. This could include having good organizational cyber security hygiene that leverages technology to detect viruses and other malware in combination with appropriate and regular employee training on security awareness. As many inside risks are accidental, it is important to communicate clearly to employees what to do in terms of reporting if they have or believe they have accidentally acted in a way that may violate the confidentiality, integrity or availability of proprietary company assets. As part of this process, it is critical to ensure employees will not feel threatened with derogatory notations on their file or otherwise receive negative actions against them by the security department or their management. Rather, employees should feel comfortable and respected

during the reporting process to encourage full disclosure of the steps they took that resulted in the inside risk event. It is also important to recognize that any employee – regardless if they are a senior executive or a working level contributor – be subject to the same standards outlined in corporate security policies. An accidental inside threat can happen anywhere in the hierarchy of a corporate structure.

While the majority of inside risk cases are the result of accidents or negligence, malicious intent does occur that could result in significant losses to the company. When characterizing inside threat activity, many respondents acknowledged that malicious intent was low volume, but had a very high impact. One respondent specifically noted that inside threat activity can generally "hurt, maim or kill" an organization. The respondent was most concerned with inside risk events that have the potential to "kill," suggesting that more resources should be put into detecting and preventing malicious cases of inside risk. With respect to what motivates malicious inside risk activity, the number one response provided via the consultations and questionnaire was general employee dissatisfaction and a perceived negative work culture. However, when given the opportunity to expand on their thinking via the consultations, respondents clarified dissatisfaction wasn't necessarily sufficient to push someone over the edge from being a disgruntled employee to constituting an inside risk. Rather, there was often a secondary motivation acting in conjunction with feelings of revenge or retribution against the organization that lead to an insider being a threat to the organization. Financial benefit was most often mentioned as a secondary motive, but ideological differences were also mentioned as a potential secondary driver.

Interestingly, only six out of fourteen valid survey responses indicated financial benefit as the primary motive for inside risk activity. This number was even lower during the consults, with only two of eleven respondents identifying financial benefit as the primary motive. When asked to elaborate on why respondents did not indicate financial benefit as the primary motive in their response as we and the literature had predicted, many respondents pointed to the fact that most employees and indeed most individuals endeavour to act ethically and in accordance with personal values that would be opposed to personal financial benefit as a primary means for constituting an inside risk.

In our questionnaire, we additionally asked why organizations set-up an inside risk program and what their primary goal is to help us further understand what motives industry insiders are looking for. The questionnaire responses laid out some of the key objectives of organizational insider risk programs. Feedback on this topic was quite expansive with answers ranging from disrupting insider threat events, to educating employees on insider risks, to creating centralized insider risk framework and to ensuring the overall safety of the work community. However, there were two recurring trends that survey participants pointed out. Six of the fourteen respondents indicated the importance of their insider risk program's ability to protect client confidentiality and company data from insider attacks. In addition, the detection of insider threat events and compromised assets were highlighted by five of the fourteen survey participants as being the main objective of their insider threat program. Responses generally focused more on the end results of asset protection rather than proactive prevention measures that can be implemented to make a good insider risk

program. We do not believe this is a strong rationale for inside risk programs. Focussing on asset protection as opposed to preventive measures leads to the development of a “security perimeter” as opposed to a holistic security culture. We will go further into the risks of taking a perimeter approach to security in the gaps section, but in brief this mentality can lead to misunderstanding employee behaviour that could lead to an inside risk event.

Best Practices for Developing an Insider Risk Program

In addition to understanding what motivates insiders to undertake a risk event, we asked respondents how they managed inside risk (through our questionnaire) and their best practices and tips for mitigating inside risk through insider risk programs (via consultations).

Questionnaire

Findings from the questionnaire portrayed respondent’s thoughts on their organization’s insider risk program’s indicators and monitoring methods. The use of technological means to monitor for possible indicators of insider risk was at a hundred percent response rate with fourteen out of fourteen participants stating their employer used technological monitoring for insider threat detection. Based on the survey responses, monitoring of internet usage and data transmission were the most often means of using technology to monitor for possible indicators of insider risk. Thirteen of fourteen respondents claimed their organization implemented these on an ‘always active’ basis, which helps them set and readjust baseline standards for acceptable usage of company IT infrastructure against unusual or anomalous behaviour that may require further monitoring or investigation for inside threats. As previously stated, this portion of the survey was focused solely on technological responses to insider risk program and did not consider the integration and impacts of human factors into insider risk detection and prevention. As such, the results of the questionnaire were heavily skewed towards technology as a primary means to fight against insider threats and were inconsistent with the general findings of the consultations.

Consultations

In asking about best practices for insider risk programs, we designed our interview questions to encourage open-ended responses for respondents to provide their perspectives without biasing them with pre-identified areas of importance as identified in our literature review. Only after collecting their unprompted responses did we then ask respondents to rank 10 components of insider risk programs. We took the average of their responses and have presented them in graph 1 below at the end of this section.

Overwhelmingly, the first best practice for insider threat programs identified by our respondents was that they need to be people-centred and empathy driven. This finding is consistent with respondent perspectives that intentional and malicious inside risk events are motivated primarily by employee dissatisfaction and a negative workplace culture. When probed on what respondents meant by “people-centred” and “empathy driven,” we were told that it was critically important that

employees feel respected and dignified at all points in the inside risk program process. Respondents mentioned various points for empathy driven leadership that may reduce the risk of an employee constituting an inside risk. Aftercare programs were frequently cited as a best practice, encompassing caring for employees and understanding their needs during their employment ('after' their onboarding) and for a time after their departure from the organization. When employees face hardships – be they financial, work-related or personal – employers should work with employees to reduce potential vulnerabilities in a way that preserves the dignity and privacy of employees and that maintains the respect of their employees. When asked how employers can keep a pulse on employee's personal, work and financial circumstances, respondents mentioned the critical role of management and colleagues in detecting changes in behaviour that may indicate a problem. This, respondents said, can only be done in an environment where trust is built and maintained among colleagues and between employees and their employer.

The second most frequently cited best practice for insider risk programs was to have executive buy-in, a senior executive responsible for championing a positive, comprehensive and transparent security culture, and a governance model that is holistic and robust. Many respondents noted it was extremely difficult today to get senior leadership buy-in for insider risk programs, because the programs are generally seen as value-protective instead of value-creating. Most respondents asserted that it often took a major insider risk incident within an organization or a competitor to warrant executive attention and subsequent buy-in. When executive buy-in is achieved, some respondents told us that maintaining their support was a different challenge because insider threat programs are a "victim of their own success." When they work, there are no successful attacks. This has the effect of reducing visibility and creates a mentality that "attacks do not happen here." Interestingly, our team's initial hypothesis was that technology would be identified as the most important component of an inside threat program, but our results show that when program components are ranked, senior executive buy in and ownership of insider threat programs was ranked the most important attribute, earning a 9.6 / 10 on a 10-point scale (1 = very unimportant, 10 = very important).

In tandem with senior executive buy-in, another attribute of successful insider threat programs is that they must be adequately funded and resourced. While it didn't score as high as we thought, technological interventions that monitor and detect risky behaviour was still identified as important, but costly. Therefore, it was deemed essential that insider threat response programs are adequately funded to ensure they can be as effective as possible.

It is again important to underline that human factors – people-centered program development and empathy driven leadership – were deemed critically important to insider threat programs in our consultations. This also includes proper and adequate employee security awareness training, which would help reduce the prevalence of accidental inside risk events. It was also deemed useful to screen employees and layer their access to resources to ensure no one individual has access to all the "crown jewels" of the organization. When asked to rate the components of inside threat response programs in terms of importance, it was interesting to note that components involving

people, not technology, scored the highest. Executive buy-in was deemed the most important with an average score of 9.6, while creating a “see something, say something” workplace culture received a score of 9.2. Technological interventions and monitoring capabilities all averaged around an 8.0 – 8.5. This reaffirms our finding that ITPs need to be people-focused and people-centred.

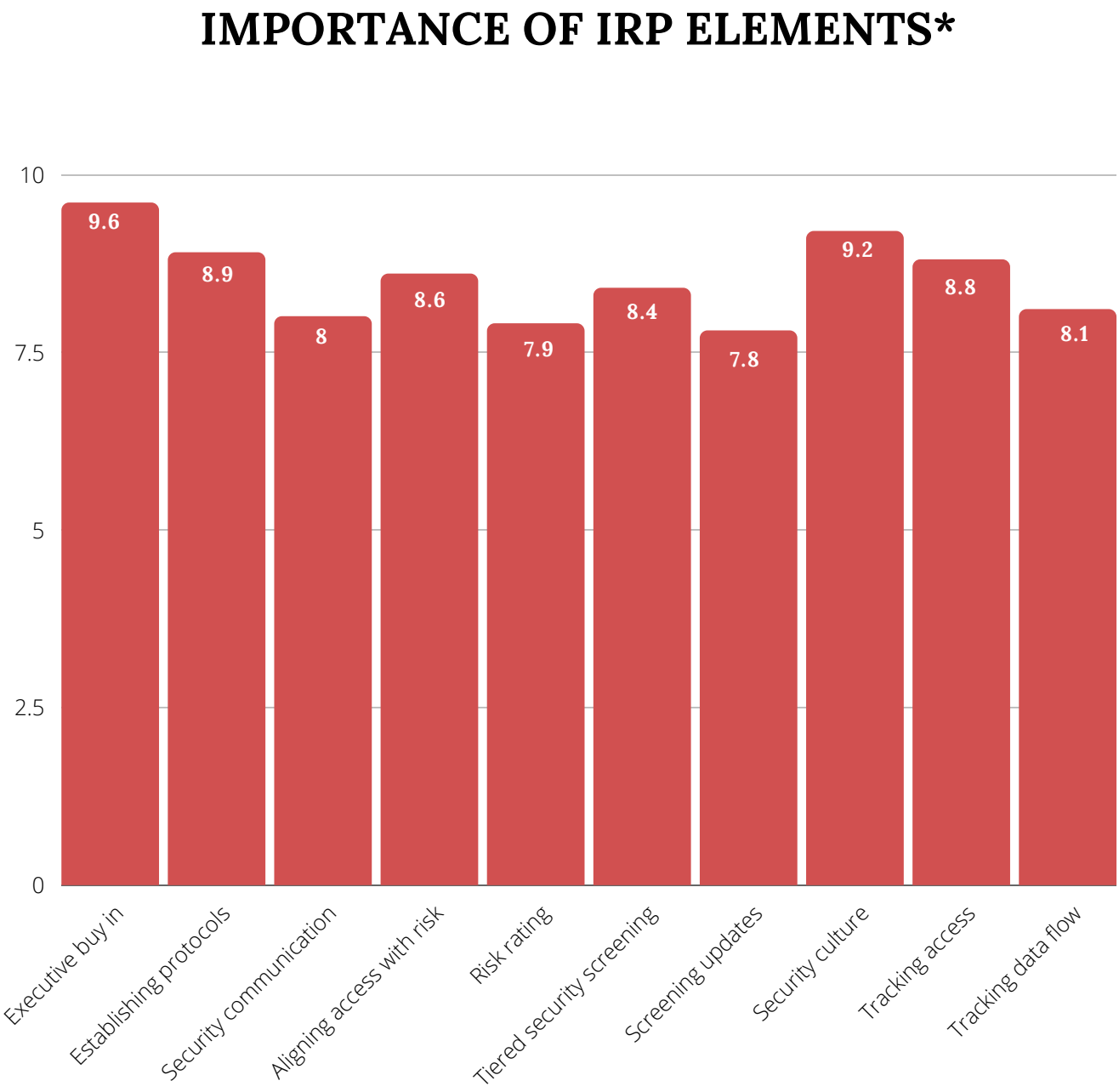

Figure 5: Importance of Insider Risk Program Elements
*please see pg.39 for variable descriptions

Executive buy in: having a senior executive responsible and accountable for overseeing an insider risk program.
Establishing protocols: establish clear security protocols on access and resource management, risk identification and mitigation measures.
Security communication: communicating security protocols to employees upon hiring and refreshing them at regular intervals, at least annually.
Aligning access with risk: align employees access with position risk levels
Risk rating: assign a risk rating to all company assets
Tiered security screening: implement a tiered personnel security screening with more rigorous vetting for those with higher risk positions.
Screening updates: implement periodic personnel security screening updates.
Security culture: foster a 'see something, say something' culture.
Tracking access: track remote access and monitor device endpoints.
Track data flow: track network data flow.

Insider Risk Gaps

We asked respondents how their organization has implemented insider risk programs and whether they foresaw any gaps within their own programs, or within those of others in their industry. Recognizing the sensitive nature of internal security programs, we reminded respondents that their responses – be they provided via a consultation or questionnaire - would not be associated with their identity aside from the general industry they worked in. We hoped this would enable us to have more candid discussions that would be useful for guiding our findings and recommendations.

Surprisingly, many of the respondents who spoke with us indicated their organizations do not have formal insider risk programs. Rather, they responded that their organization engaged in regular cyber security monitoring more akin to building a security perimeter to keep unauthorized individuals out as opposed to monitoring those within the organization. This building of a security perimeter was deemed a significant gap in inside risk programming, and one respondent told us it reenforces the typical security architecture and goal of keeping threats from coming in then protecting against those having originated within the organization. Other respondents of the consultations reported their security programs were mostly housed within IT departments, but some noted that human resources did deal with corporate policy compliance issues, though these were reactive and not necessarily proactive. That is, they dealt with compliance issues when it was brought to their attention, but didn't have formal monitoring mechanisms.

In both the questionnaire and consults, those who indicated they did have an insider risk program told us they leveraged technology such as machine learning to monitor and collate user activity on the network to look for anomalous behaviour or signs of risk. In implementing this technology, respondents noted it was important to set thresholds for user activity beforehand, such as the normal size of data packets being transmitted on a network, printer traffic activity, etc. This

was deemed important so that follow-on investigations were only triggered when something unusual happened and so that they were done in as unbiased a manner as possible. Additionally, to avoid potential privacy issues, one respondent noted it was important to protect privacy and ensure employees didn't feel like they were constantly being monitored which could lead to a negative workplace culture. A best practice – but one the respondent didn't feel was being widely applied in industry – was to mask data until an event arose, which would then require a committee to agree to unmask the identity of the user behind the anomalous data for a follow-on investigation. Related to technology, some smaller organizations we spoke to addressed the resourcing constraints in being able to leverage technology within their firms. Leading edge solutions are massively expensive, and the executive boardroom or security committee had to balance investment in technology with investment in people and training.

A significant gap repeated by many respondents was the difficulty in acquiring executive buy-in for insider threat programs. In one context, a respondent told us the burgeoning insider threat program at their organization was grass roots and working level driven because executives couldn't justify resourcing the program when no major incidents had previously happened. The respondent also recognized that the executives thought the external IT and cybersecurity defences were sufficient to protect company assets.

A couple of respondents acknowledged that their industry could be doing a better job at collaborating with other firms to share best practices and learn from each other about the best ways to mitigate insider risk events from occurring. Often times, when an event happens the lessons learned are kept internal to the victimized organization. Increased sharing of knowledge, tools and resources would better help firms protect themselves against an inside risk event.

Emerging Risks

In the final sections of our questionnaire and consultations, we asked respondents about emerging risks they perceived may afflict organizations who seek to combat insider threats. Throughout the responses there was a strong belief that there will be new risks associated with work-from-home postures, with unanimous agreement on this in both the survey and consultations. However, the reasons why the work-from-home posture concerned respondents surprised us. There were two areas of concern: (1) the risk of data leakage or intentional exfiltration from the organization caused by technology, and (2) the impact on mental health and employee satisfaction while working-from-home compounded with the difficulty in being able to keep the pulse of an organization's workforce. Both facets will be dealt with in turn.

Many respondents mentioned that it would be harder for organizations to monitor and detect incidents of inside risk, particularly malicious or intentional inside risk, while employees were working from home. While there are tools out there to monitor remote device endpoints, respondents were concerned about the ability for an employee to use an external device such as a cell phone to capture images of company proprietary information. Another threat vector exists where employees are able to set up their work device to a home printer.

Printing material may be justified, but there is no ability for asset handling or protection protocols to be applied in one's own home. The concern raised by respondents was that an employee could easily hold onto proprietary information they may have printed for a valid purpose beyond the tenure of their employment. For employees who seek to harm a company, they are able to provide data to competitors or other interested parties who should not ordinarily have access to the privileged information. Finally, many respondents raised concerns about an employee's home network set-up. The concern is that an unsecured network would allow hackers easy access to corporate information via hacking into a home network and getting on a device or peripheral connected to the network to exfiltrate data. While this isn't an inside risk concern per se, it can be mitigated by techniques recommended for a good insider risk program. Namely, providing training on how to practice appropriate cyber hygiene within the home environment would be a prudent practice.

Beyond the technology considerations of working from home, respondents were more concerned about the human factors. Their view was that an insider risk program could only go so far at endeavouring to monitor and detect employees for risk indicators within their home using technology. Rather, most respondents thought it would be better and smarter to devote resources to ensure employees felt respected and supported in a work-from-home environment. This is in line with what we learned about suspected motive for inside risk – the number one motive on the pathway to becoming an internal threat is employee dissatisfaction. Employers should recognize that for some employees, working-from-home entails extra stress. Employees may have children at home, pets or other distractions which make it harder to focus on day-to-day work. Therefore, it was deemed critical that in a work-from-home scenario, employers provide support to help their employees build a workspace within their homes with appropriate setup and equipment to make the experience as comfortable as possible. However, employers must also be flexible and understanding that for some, working eight hours consecutively five-days-a-week is not realistic. Therefore, accommodations should be made on a person-to-person basis to ensure that the needs of the business or organization and the needs of the employee are taken into consideration and are being met as fully as possible. An additional concern raised was that it was extremely difficult for management to maintain an idea of the pulse of their workforce. While in an office, it may be easier to tell when an employee is having an off-day or may need some space or accommodation, working virtually makes this much more difficult. Therefore, it is harder to respond and be empathetic in a virtual environment. To mitigate this, trust should be built and maintained at the team level so that employees feel comfortable speaking up when they have work concerns or personal considerations that may impact their ability to do work in the short term.

Mental health was a big concern for our respondents. Working from home breaks down the barrier between work and leisure. It is also difficult for many people to not be surrounded by their colleagues in-person. Poor mental health can lead to unproductivity, dissatisfaction and a negative culture within a team, department or even an entire organization. Therefore, mental health services should be made available to employees. Employees should also be encouraged to take more frequent 5–10-minute relaxation breaks to take their eyes off of a screen, to stretch, walk around or grab

coffee. Platforms should be made available to keep team collaboration consistent even in a virtual environment.

While the work from home posture that many companies have adopted through the COVID-19 pandemic was top-of-mind for our questionnaire and consultation respondents, there were a few other areas of concern mentioned. One respondent was worried about divisive political climates causing entrenched ideological differences to be brought out in the workplace. The concern here, as has been witnessed in the United States of America in the past 5-10 years especially, is that ideological differences can manifest not only in conventional inside risk, but also in physical harm and violence in the workplace. To combat this, our respondent noted it was important to hire a diverse workforce and welcome tolerance and respect for various points of view. Politics itself, however, should be kept out of the workplace. Finally, another area of concern raised by two respondents was the move to a gig-economy. Some individuals in the workforce are turning to freelancing or picking up “gig-jobs” like Uber, DoorDash, Intelcom and other companies. The risk observed is that individuals may pick up employment working for competitors and divulge proprietary information either accidentally or intentionally. When asking other respondents about this risk, many were hesitant to agree as they judged that working-level employees would not generally have the level of access to cause significant harm to an organization.

RESEARCH FINDINGS SUMMARY

Over the course of this research project, several themes have been uncovered about how insider risk programs operate currently, and what risks may emerge in the future that Canadian financial institutions will need to contend with. Through this research, it has been stated that most insider incidents are accidental in nature, and usually have a low impact on an organization. Although insider incidents that have malicious intent are typically less prevalent, they represent the highest impact to an organization and are therefore a cause for concern. For the malicious insider, it has been found that employee dissatisfaction is usually compounded by a secondary motivation acting in conjunction with feelings of revenge against the organization. Additionally, financial benefit was not identified as a main factor to an employee mobilizing to become an insider risk.

This research has also uncovered that in an attempt to create robust insider risk programs, many organizations default to creating a security perimeter instead. Amongst respondents, the primary reason for establishing an insider risk program in their organization was to protect client confidentiality and company data. This indicates that most organizations were focussed on the end result of asset protection, rather than creating a holistic security culture. By focussing on building walls to prevent the malicious outsider, the vengeful insider can simply walk around them.

Case Study: Desjardins

An insider within Desjardin's IT Department leaked the personal information of million of customers. The Desjardin Group has not committed to reimbursing its members for any losses as a result of the data breach. (Nahari, 2019)

This research has also shed light on how technology used in insider risk programs may assist or hinder the progression of insider risk mitigation strategies. In the questionnaire, most respondents identified that monitoring employee internet usage and data transmission was most frequently used. Additionally, forecasting exercises reveal that Canadian financial institutions will need to be conscious of the unintended consequences of the implementation of insider risk monitoring technology. These novel technologies may have potentially harmful impacts on workplace culture, and increase technical and organizational risks. With the skepticism of how monitoring technologies may impact employees, most respondents in the consultation process did not identify technology as being highly important to their insider risk mitigation strategy. Rather, they identified a people centred strategy as integral to the success of their insider risk program.

Through horizon scanning, it has been revealed that insider risk programs that focus on employee satisfaction may be most successful in the future. This has been echoed by respondents in the consultation process. For example, several respondents emphasized the success of aftercare programs in their insider risk mitigation strategies. Aftercare programs seek to understand employees' needs during their employment and after their departure from the organization.

Respondents also emphasized that employees should feel respected in the reporting process, and organizations should ensure that this process is non-confrontational to employees.

This research undertaking has also uncovered organizational challenges that Canadian financial institutions will need to deal with. Respondents in the consultation process emphasized the need to have executive support for insider risk programs, as well as the need for insider risk mitigation strategies to be adequately funded. During follow up questioning, it was found that insider risk programs are considered asset protection and not necessarily value creation, which sheds light on why such programs may receive less funding than others that will build further value.

When looking towards the future of insider risk programs, a key component of consideration relates to how the COVID-19 pandemic has evolved workplace dynamics as many employees are working from home. The horizon scanning process reveals that there is an elevated risk of an insider event occurring as a result of the factors of COVID-19. This concept has been supported through the consultation process, as many respondents identified COVID-19 as being a primary concern for the future of insider risk for organizations. Respondents identified two areas of concern related to insider risk and COVID-19. Firstly, there is an elevated risk of intentional or unintentional data exfiltration from the organization as a result of work from home postures. For example, employees may use external devices to share or record company information. Secondly, respondents identified the impact the pandemic has had on employee mental health and satisfaction while working from home as a cause of concern for potentially elevated insider risk. This is compounded by the organization's difficulty in monitoring employees for behavioural signs, as work from home dynamics typically limits a supervisor's ability to check-in with employees regularly.

This research has uncovered several trends about the current state of insider risk programs, as well as how they may evolve to changing trends in the future. Using strategic foresight methods in conjunction with a questionnaire and consultation process, this project has revealed how insider risk programs can adapt to accommodate employee needs while also protecting the organization from the risk of the insider.

LEGAL

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the main legislation governing private sector organizations' collection of employee information. An employer's need for information must always be balanced against an employee's right to privacy, and PIPEDA outlines ten fair information principles to guide organizations. These principles are vital to consider in the establishment of holistic insider risk programs, as an organization's quest to insider risk mitigation must consider individual employee's privacy rights.

10 FAIR INFORMATION PRINCIPLES

Accountability An employer is accountable for its own compliance with the fair information principles.	**Identifying Purposes** The reason for collecting the information must be identified by the organization before and at the time of collection.	**Consent** The employer must apprise the employee of the information collection and obtain their consent.	**Limiting Collection** Information collected must be limited to what is needed for the purposes identified by the organization.
Individual Access Any employee must be given access to their own data that the employers has collected.	**Accuracy** Personal information must be accurate and complete.	**Safeguards** Personal information must be protected by appropriate security.	**Openness** Employers must detail its policies and practices relating to the management of personal information publicly.
Limiting Use, Disclosure, and Retention Information collected can only be used for the purposes for which it was collected.		**Challenging Compliance** Any employee must be able to challenge their employers compliance with the fair information principles.	

Figure 6: 10 Fair Information Principles (Office of the Privacy Commissioner of Canada, 2019)

In accordance with PIPEDA, an employee must provide consent for their personal information to be collected. However, in certain circumstances, organizations can disclose personal information without the knowledge or consent of the individual. For example, if an organization is investigating a breach of an agreement, contravention of Canadian law, or for the purposes of detecting, suppressing or preventing fraud that is likely to be committed (Office of the Privacy Commissioner of Canada, 2019). This is a vital fair information principle to consider for the future of insider risk mitigation strategies, as it must be determined if the collection of employee information for the purposes of ongoing investigation is a valid circumstance to not require consent under PIPEDA. As Canadian financial institutions begin to implement holistic insider risk programs, they will not only need to contend with their own security culture, but also how employee consent to insider risk programs will operate.

In addition to future concerns around employee consent to insider risk programs, Canadian financial institutions will also need to balance their security needs against PIPEDA's principle of limiting collection. Many insider risk mitigation strategies suggest processing multiple forms of employee data, from human resources reports to network data flow. Organizations will need to explicitly state how they will limit the collection of employee data for insider risk programs in accordance with the fair information principle stating that information collected must be limited to the original purpose of the data collection (Office of the Privacy Commissioner of Canada, 2019).

Canadian organizations will also need to address what safeguards will be enacted to protect the collected information for insider risk mitigation strategies (Office of the Privacy Commissioner of Canada, 2019). As many insider risk programs seek to collect large amounts of employee data, there is an incentive to contract out the data storage and analysis to a third party outside of the corporate structure. Softwares such as machine learning technology that can analyze large data sets to pinpoint an insider risk are popular in the marketplace, and provide an incentive for Canadian organizations to provide individual employee information to managed service providers. However, Canadian financial institutions that use third party security providers will have to contend with the increased risk of allowing actors outside of the corporate structure access to sensitive information. This will lead to greater risk that employee information will not receive the appropriate safeguards.

The fair information principles enacted by PIPEDA will be vital to consider for the future of insider risk mitigation strategies, as the collection of employee information must be lawful and proactive to ensure no breach of an employee's reasonable right to privacy. With an increasingly large data set of employee information to analyze, Canadian financial institutions will need to ensure employees remain conscious of their actions without creating a workplace culture of fear and skepticism.

RECOMMENDATIONS

People Focused Insider Risk Programs

It is recommended that organizations create insider risk programs that are people focused and respect the dignity and privacy of all employees. It is vital for insider risk mitigation strategies to consider employee satisfaction as a high priority, as if employees are satisfied with their workplace they are less likely to become and inside risk. Furthermore, with the implementation of insider risk detection technologies, it is recommended that the privacy of employees be considered and consulted through the program development process.

Cultivating a Positive Workplace Culture

Creating a workplace that is empathetic, diverse and transparent is essential to reducing the risk of an employee causing harm to an organization. If employees feel respected by their organization, they are less likely to become an inside risk as they will take personal care for the prosperity and success of the company. Furthermore, it is recommended that organizations are transparent with employees on insider risk monitoring programs to avoid negatively impacting workplace culture.

Technology to Supplement Insider Risk Programs

Robust technology solutions integrated in insider risk programs are beneficial to detecting anomalous behaviour based on present baselines. However, organizations must be attentive to ensure that technology solutions do not encompass the entirety of their insider risk program, and only serve to supplement the people centred approach. Furthermore, it is recommended that organizations are transparent with employees regarding the continuous monitoring implemented.

Increased Employee Training

It is recommended that organizations ensure that employees receive regular training on security and IT vulnerability awareness, workplace violence, and empathetic leadership. A people centred approach must not solely emanate from the insider risk program, but also the interactions between supervisors and employees. When all members of the organization embody the employee satisfaction approach to insider risk, the threat of an employee causing harm may be reduced.

CONCLUSION

In conclusion, our research has indicated that notwithstanding the ample new technology, or COVID-19 pandemic, working closely with employees on a personal level is essential in fostering a safe and productive workplace environment, while simultaneously reducing insider risk. Raising security awareness, being mindful of emerging technologies, and good cyber-hygiene are also paramount in the long-run, especially considering political realities and broader security trends of a post-pandemic world. This project has allowed our team to examine these ideas in depth and conduct meaningful research over the course of these four months providing a window into what the future may look like and what factors will be at play.

There are however still questions to investigate and more work to be conducted in the future. Whether it is analyzing specific motives for insider risk, putting together more actionable recommendations, supported with quantitative analysis, digging into employee behaviors more in-depth, or giving a closer look to some of the vast new technology that could impact insider risk - all these can still be explored through dedicated long term research. We hope that this project can spur such future research on some of these questions.

To close, besides being an incredible experiential learning experience for us, we have all been able to explore potential future fields of interest, grow personally, and foster a valuable understanding of the private sector through this capstone partnership. This experience has been an enriching one for us as students and we hope that our initial semester-long project can pave the way for future work and research in the space. We would likewise like to thank everyone that have helped guide us on this journey.

REFERENCES

Abedi, M. (2019, July 30). Capital One data breach: Morneau calls for investigation into hack affecting Canadians. Global News. https://globalnews.ca/news/5703501/capital-one-data-breach-bill-morneau/

Baksh, M. (2020, October 26). Report Heralds Perfect Storm for Insider Threats in 2021. Nextgov. https://www.nextgov.com/cybersecurity/2020/10/report-heralds-perfect-storm-insider-threats-2021/169555/

Balakrishnan, B. (2015). Insider Threat Mitigation Guidance, System Admin, Audit, Network, and Security (SANS) Institute, 1-41.

Balakrishnan, B. (2015, October 6). Insider Threat Mitigation Guidance. https://www.sans.org/reading-room/whitepapers/monitoring/insider-risk-mitigation-guidance-36307

Barnette, M. (2021, March 2). How to Increase Workplace Safety and Resource Efficiency. Security Info Watch. https://www.securityinfowatch.com/security-executives/article/21209129/how-to-increase-workplace-safety-and-resource-efficiency

Bell, A., Rogers, M., & Pearce, J. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. International Journal of Critical Infrastructure Protection, 24, 166–176. https://doi.org/10.1016/j.ijcip.2018.12.001

Bulpett, B. (2020). Safeguarding against the insider threat. Network Security, 2020(6), 14–17.

Cheney, K., & Ferris, S. (2021, March 8). Lawmakers confront their own workplace safety after Capitol security review. Politico. https://www.politico.com/news/2021/03/08/security-review-capitol-building-recommendations-474335

Cohron, M. (2021, March 9). Enabling Your Workforce for the Digital Workplace. InformationWeek. https://www.informationweek.com/strategic-cio/digital-business/enabling-your-workforce-for-the-digital-workplace/a/d-id/1340277?

Deloitte. (2020, April). Managing Potential Insider Threat During COVID-19. Deloitte. https://www2.deloitte.com/us/en/pages/public-sector/articles/managing-potential-insider-threat-during-covid-19.html

Denson, B. (2020, September 25). Addressing Insider Threats with Event Triggers. Nextgov. https://www.nextgov.com/ideas/2020/09/addressing-insider-threats-event-triggers/168648/

Department of Justice. (2019, April 23). Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets. The United States Department of Justice. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

Eberz, S., Rasmussen, K., Lenders, V., & Martinovic, I. (2016). Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics. ACM Transactions on Privacy and Security, 19(1), 1–31.

EC-Council. (2021, March 9). What is the Role of a Threat Intelligence Platform in a Successful SOC? Ec-Council Blog. https://blog.eccouncil.org/what-is-the-role-of-a-threat-intelligence-platform-in-a-successful-soc/

Elifoglu, I., Abel, I., & Tasseven, O. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. Review of Business, 38(2), 61–73.

Fiel, P. V. (2021, February 23). Are businesses prepared for an active shooter? Security Magazine. https://www.securitymagazine.com/articles/94658-are-businesses-prepared-for-an-active-shooter

Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2017). Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. IEEE Systems Journal, 11(2), 513–521

Gagliordi, N. (2020, July 21). DOJ indicts two Chinese hackers for attempted IP theft of COVID-19 research. ZD Net. https://www.zdnet.com/article/doj-indicts-two-chinese-hackers-for-ip-theft-of-covid-19-research/

Gilroy, J., & Payne, J. (Hosts). (2021, February 8). Innovative ways to protect data from insider threats [Audio podcast episode]. In Federal Tech Talk. Federal News Network. https://federalnewsnetwork.com/federal-tech-talk/2021/02/innovative-ways-to-protect-data-from-insider-threats/

Greenberg, A. (2021, March 8). 'Retaliation' For Russia's SolarWinds Spying Isn't the Answer. Wired. https://www.wired.com/story/us-solarwinds-russia-retaliation-cyber-policy/Greitzer, F. L., & Hohimer, R. E. (2011). Modeling Human Behavior to Anticipate Insider Attacks. Journal of Strategic Security, 4(2), 25-48.

Grossman, G. (2020, July 18). Work-at-home AI surveillance is a move in the wrong direction. Venture Beat. https://venturebeat.com/2020/07/18/work-at-home-ai-surveillance-is-a-move-in-the-wrong-direction/

Harber, J. (2009). Unconventional Spies: The Counterintelligence Threat from Non-State Actors. International Journal of Intelligence and Counterintelligence, 22(2), 221–236. https://doi.org/10.1080/08850600802698200

Healey, A. (2016). The insider threat to nuclear safety and security. Security Journal, 29(1), 23–38. https://doi.org/10.1057/sj.2015.42

Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., & Liu, Y. (2019). An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning. Security and Communication Networks, 2019, 1–12.

Huxley. (n.d.). How are cryptocurrencies going to affect the banking landscape? Huxley. https://www.huxley.com/en-GB/blog/2018/05/how-are-cryptocurrencies-going-to-affect-the-banking-landscape/

IBM. (2020). Cost of a Data Breach Report 2020. https://www.ibm.com/security/data-breach

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993.

Jasper, M. (2021, February 19). Marine Corps Looks for Insider Threat Monitoring Capability. Nextgov. https://www.nextgov.com/cybersecurity/2021/02/marine-corps-looks-insider-threat-monitoring-capability/172167/

Kelion, L. (2019, December 12). Emotion-detecting tech should be restricted by law - AI Now. BBC News. https://www.bbc.com/news/technology-50761116

Ko, L., Divakaran, D., Liau, M., Liau, Y., & Thing, V. (2016). Insider Threat Detection and its Future Directions." International Journal of Security and Networks, 12(3), 1-19.

Kohen, I. (2021, March 8). Cybersecurity, Compliance And Productivity: Three Critical Priorities When Launching A New Company In Uncertain Times. Forbes. https://www.forbes.com/sites/theyec/2021/03/08/cybersecurity-compliance-and-productivity-three-critical-priorities-when-launching-a-new-company-in-uncertain-times/?sh=398e5712696e

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2018). Insider Threat Detection Study. NATO Cooperative Cuber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Kowalski, E., Cappelli, D., & Moore, A. (2008, January). Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52257

Kowalski, E., Conway, T., Keverline, S., Williams, M., Cappelli, D., Willke, B., & Moore, A. (2008, January). Insider Threat Study: Illicit Cyber Activity in the Government Sector. Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52247.pdf

Li, S., & Jain, A. (2015). Encyclopedia of Biometrics (2nd ed. 2015.). Springer US.

Ljunggren, D. (2021, February 9). China poses serious strategic threat to Canada, says Canadian spy agency head. Reuters. https://www.reuters.com/article/us-china-canada-idUSKBN2A92VH

Locke, C. IBM adds behavioural biometrics to banking fraud solution. (2016). Biometric Technology Today, 2016(11), 1.

Lorrimer, D. (2020, July 7). How Covid-19 has added to 'insider threat' risks. Personnel Today. https://www.personneltoday.com/hr/how-covid-19-has-added-to-insider-threat-risks/

Mellon, C. (2018). Common Sense Guide to Mitigating Insider Threats (6th ed.). Carnegie Mellon University. 1-168.

Milica, L. (2021, March 12). Mitigate insider threats by focusing on people, process and technology. SC Magazine. https://www.scmagazine.com/perspectives/mitigate-insider-threats-by-focusing-on-people-process-and-technology/

Mitrou, L., & Karyda, M. (2006). Employees' privacy vs. employers' security: Can they be balanced? Telematics and Informatics, 23(3), 164–178. https://doi.org/10.1016/j.tele.2005.07.003

Nahari, S. (2019, June 21). Data Breach at Desjardins Bank Caused by Malicious Insider. CyberArk. https://www.cyberark.com/resources/blog/data-breach-at-desjardins-bank-caused-by-malicious-insider

Newman, L. H. (2021, March 2). Microsoft's Dream of Decentralized IDs Enters the Real World. Wired. https://www.wired.com/story/microsoft-decentralized-id-blockchain/

Newman, L. H. (2021, March 8). The Accellion Breach Keeps Getting Worse - and More Expensive. Wired. https://www.wired.com/story/accellion-breach-victims-extortion/

Nicolaou, S. (2020). Mitigating Insider Threats Using Bio-Inspired Models. Applied Sciences, 10(15), 5046

O'Donnell, L. (2019, June 4). A New Approach for Combating Insider Threats. Threat Post. https://threatpost.com/a-new-approach-for-combating-insider-threats/145311/

Office of the Privacy Commissioner of Canada. (2019, May). PIPEDA in brief. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

PA Consulting Group. (2012). Holistic Management of Employee Risk (HoMER). Centre for the Protection of National Infrastructure. file:///Users/hayleyoyhenart/Downloads/Holistic-Management-of-Employee-Risk-HoMER-Executive-summary.pdf

Public Safety Canada. (2019). Enhancing Canada's Critical Infrastructure Resilience to Insider Risk. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004, August). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50287

Raytheon. (2015). The Financial Industry and the Insider Threat: Total Awareness Leads to Secured Enterprise. https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_244836.pdf

Shah, P. (2021, March 11). Machine Learning-Based Real-Time Threat Detection for Banks. Datanami. https://www.datanami.com/2021/03/11/machine-learning-based-real-time-threat-detection-for-banks/

Sharma, R. (2021, March 8). Non-Fungible Token (NFT) Definition. Investopedia. https://www.investopedia.com/non-fungible-tokens-nft-5115211

Strickland, D. (2021, February 19). Employee Internet Management—How to Manage Workplace Internet Abuse. Business 2 Community. https://www.business2community.com/human-resources/employee-internet-management-how-to-manage-workplace-internet-abuse-02387589

Tarun, R. (2021, March 5). What Zero Trust Can Bring to the Financial Sector. Banking Exchange. https://www.bankingexchange.com/news-feed/item/8591-what-zero-trust-can-bring-to-the-financial-sector

Tucker, P. (2014, July 15). Could a Brain Scan Protect U.S. Troops from Insider Attacks? Defense One. https://www.defenseone.com/technology/2014/07/could-brain-scan-protect-us-troops-insider-attacks/88801/

Tucker, P. (2021, February 4). New AI Can Detect Emotion With Radio Waves. Defense One. https://www.defenseone.com/technology/2021/02/new-ai-can-detect-emotion-radio-waves/171863/

Walkowski, D. (2019, July 9). What Is the CIA Triad? F5 Labs: Application Threat Intelligence. https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Week, R. (2021, February 24). How MSPs can help businesses identify insider threats. Channel Pro. https://www.channelpro.co.uk/opinion/12071/how-msps-can-help-businesses-identify-insider-threats

Zerucha, T. (2021, March 2). Insider threats rapidly evolving during pandemic. Bankless Times. https://www.banklesstimes.com/2021/03/02/insider-threats-rapidly-evolving-during-pandemic/

APPENDIX A: QUESTIONNAIRE

Preamble:

We are conducting research on behalf of a Canadian financial institution to understand the landscape of insider threat activity and mitigation techniques. We are looking to survey professionals involved in security, risk and compliance – both private and in government – to understand their thoughts on the current threat landscape and the efficacy of prevention and detection measures in place today.

Recognizing the changing work practices caused in part by COVID-19 – in addition to pre-COVID trends such as a move towards an informal "gig economy" – we are also interested in insights and predictions about potential gaps in insider threat prevention and detection programs moving forward and recommendations to address those gaps.

This survey is anonymous and none of your responses will be mapped back to you individually.

Should you have any questions or concerns about this survey, please contact the student researchers via email:

Anthony Hope - anthonyhope3@cmail.carleton.ca
Darian Scherbluk - darianscherbluk@cmail.carleton.ca
Supervising professor:
Dr. Alex Wilner - AlexWilner@cunet.carleton.ca

Part 1: Questionnaire

1. Does your organization have a formal insider threat prevention and/or detection program?

Yes (go to Q2)
No (go to Q2)

2. Do you work in security, risk or compliance of your organization?

Yes (go to Q3)
No (exit)

3. What motivations for malicious insider threats are you most concerned about today?

a) Employee dissatisfaction (including revenge or retribution)
b) Monetary gain (including fraud)
c) Espionage (for the purposes of benefitting a 3rd party)
d) Other (specify:)

4. How effective do you believe this program to be today?

1 – Not at all effective
2 –
3 –
4 –
5 – Very effective

5. Does your organization use technological means to monitor for possible indicators of insider risk?

Yes
No

6. What measures does your organization employ?

a) Monitor printing usage
b) Monitor removeable media usage (such as a USB)
c) Monitor internet usage (i.e. types of websites visited)
d) Monitor employee productivity (i.e. excessive time spent on the internet, social media, etc.)
e) Monitor geolocation indicators
f) Monitor technological identifiers (i.e. key stroke patterns)
g) Monitor data transmission (i.e. size of data packets to detect anomalous behaviour)
h) Review access management (i.e. for signs of an employee trying to access a resource they are restricted from seeing)
i) Other (specify):

7. Thinking ahead, do you anticipate any new risks associated with work-from-home postures or other changing workforce patterns?

Yes
No

8. What new risks do you anticipate, and how can companies work to address them?

9. What industry do you work in (please do not specify the specific employer for purposes of anonymity)?

a) Government
b) Financial sector
c) Other private corporation
d) Other:

10. Do you have any other comments?

APPENDIX B: CONSULTATION QUESTIONS

1. In your organization's security program, what and who are you most concerned about as it relates to insider risk?

2. What are the attributes of a good insider threat program?

3. On a scale of 1-10, how important are the following for insider threat risk reduction:

a) Having a senior executive responsible and accountable for overseeing an insider risk program
b) Establish clear security protocols on access and resource management, risk identification and mitigation measures
c) Communicating security protocols to employees upon hiring and refreshing them at regular intervals, at least annually.
d) Align employees access with position risk levels
e) Assign a risk rating to all company assets
f) Implement a tiered personnel security screening with more rigorous vetting for those with higher risk positions
g) Implement periodic personnel security screening updates
h) Foster a "see something, say something" culture
i) Track remote access and monitor device endpoints
j) Track network data flow
k) Anything else:

4. How does your organization structure and implement insider threat programs (broadly speaking)?

5. Are there any gaps you can identify – broadly speaking – with insider threat programs today?

6. How often do you review or update your insider risk program?

7. COVID-19 has changed the work patterns for many workers across the world. With more people expected to continue to work from home after the pandemic, do you think security programs are going to have to adapt? What will the challenges be? Proposed solutions?