BEHAVIOURAL INDICATORS OF INSIDER THREAT

*Acknowledging the contributions of the student participants from Carleton University, Norman Paterson School of International Affairs

Table of Contents

Executive Summary

In January 2023, Carleton University's Capstone in Canadian Security Policy partnered with VigilantCS to support further research into staff-level conduct and insider threat to improve oversight of individuals in positions of trust, such as financial services, law enforcement, government agencies and other professionals. The purpose of this report is to provide research in support of the development of a behavioural algorithm. The authors of this report, as part of the partnership, reviewed academic research on behavioural factors that had a strong correlation to the insider threat and built a data dictionary to align conduct risk and insider threat factors.[1] This partnership had the goal of providing research support to VigilantCS to support the creation of a "digital platform that cost-effectively manages and monitors conduct risk and staff-level compliance."[2]

A narrative literature review was conducted to explore the existing literature on insider threats in the workplace, particularly in the financial services and public security sector. A review of the existing literature demonstrated that the terms *insider risk*, *insider threat* and *conduct risk* were often used interchangeably, despite several key conceptual differences. These initial findings led us to conclude that each term needed to be explicitly defined and theoretical explored.

The authors adopted the *Carnegie Mellon Common Sense Guide to Mitigating Insider Threats* (the guide) definition of insider threat, which stipulates that the term refers to "the potential for an individual who has, or had, authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."[3] Although the guide discusses insider risk and insider threat as separate, but related terms, other academic articles frequently conflated the two terms with the same definition. Therefore, the authors utilized the guide to define insider risk, which, for the purposes of this research project, referred to "the impact or likelihood associated with the realization of an insider threat"[4]. The authors also reviewed academic literature relating to conduct risk. Unlike insider threat and insider risk, conduct risk is a term that is heavily and predominantly used by the financial sector. In order to identify a definition for conduct risk that aligned with the research project's public security scope, the research team drew upon several sources for conduct risk and created a unique definition. Throughout this document, conduct risk will refer to "the risk of inappropriate, unethical, or unlawful behaviour on the part of an organization's management or employees or those with access to organizational assets that lead to negative organizational costs."[5]

Following the establishment of clear-cut definitions for each term, the authors conducted a secondary literature review to identify the behaviours that are associated with each insider threat type, lumped into four broad fields: cybersecurity, workplace violence, fraud and extortion. Throughout each field, case studies exhibited that no single behavioural characteristic was

[1] Wilner, Alex, "INAF 5254 – Capstone in Canadian Security Policy Course Outline," *Brightspace* (accessed 29 April 2023), 1, https://brightspace.carleton.ca/d2l/le/content/132851/Home

[2] "About Us," *Vigilant CS* (accessed 26 April 2023), VigilantCS, https://vigilantcs.com/about/

[3] "Common Sense Guide to Mitigating Insider Threats, Seventh Edition," *Carnegie Mellon University Software Engineering Institute* (2022), iv, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=886874

[4] Ibid.

[5] Carleton University-NPSIA Student and al., 2023

indicative of an insider threat. Instead, insiders displayed a combination of several indicators, over a prolonged period of time, that turned them from 'regular' employees to individuals who posed a threat to colleagues and organizational assets. Furthermore, research illustrated the various different points organizations could collect data from in order to develop an accurate assessment of an organization's and individual's risk profile. For example, organizations could accurately assess levels of disgruntlement and stress through various data points, including human resources records, email and chat logs. For other issues such as substance abuse, background checks could be conducted against several employees to check for records on impaired driving, assault, and substance abuse.

After establishing a set of salient behavioural indicators for insider threats, the authors synthesized the data and presented it in a single table [See Table below]. The measurements represented in this table highlighted the overarching benefit of internal monitoring based on technological indicators. These include, among other things, the number of bytes of downloads on company systems, bytes uploaded to external websites or programs, the number of attempts to access blocked files, databases or websites, and suspicious internet searches. Aside from technological monitoring, our research indicated that sentiment analysis through assessment of keywords found in emails and chat channels, human resources complaints, sizeable and unexplained changes in credit ratings also represented potential data points for which companies could use to measure an employee's overall risk profile.

Our research led us to conclude that there were six cross-cutting indicators that were indicative of insider threats *for all types*. The primary indicators of insider threat were a decline in job performance, as well as working odd hours, whereas secondary cross-cutting indicators included substance abuse, misuse, absenteeism, disgruntlement and stress. Substance abuse, notably, seemed to be on the rise among employees, therefore organizations needed to explore alternative corporate social programs that would support employees facing issues relating to substance abuse.

Finally, it is important to identify and consider certain gaps that we encountered while conducting our research. First, the data on indicators associated with insider threats is heavily biased towards those of white male employees, thereby limiting the veracity of conclusions drawn from this data. Second, although there are several data points which organizations can collect from, the disaggregation of the same data makes it difficult to reliably interpret certain and/or specific data points. Furthermore, the collection of certain types of data, such as health information for substance abuse, is legally protected by law, therefore companies may experience significant hurdles in collecting such data. Lastly, the ethics of behavioural monitoring must be considered when proposing an insider risk management framework. Ultimately, this framework involves the (potentially surreptitious) surveillance of employees and drawing inferences and conclusions based on observable, but not conclusive, indicators. Therefore data points should be carefully considered for their privacy implications, and how their use may affect employees who do not necessarily fit the mold of a "regular employee."

Introduction

Insider threats are a complex and dynamic risk that have had profound impacts on both the public and private sectors. According to the US Cybersecurity and Infrastructure Security Agency (CISA), an insider is "any person who has, or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems."[6] Insider threats are particularly dangerous because of the individual's position as trusted agents of a company, or government agency.[7] Insiders can be difficult to detect, as they are presumably aware of internal controls within an organization and utilize that knowledge to conduct unauthorized activities.[8] The Ponemon Institute's *2022 Cost of Insider Threats Global Report* notes that insider threat incidents have risen by 44% over the past two years.[9] The cost to enterprise, per incident, is approximately USD $15.4 million, representing an increase of more than one-third since 2020.[10] The average time taken to respond to insider threats also increased from 77 days to 85 days, which demonstrates a need across different industries to be acutely aware of insider threats and responses.[11]

The issue of the insider threat to private companies and government agencies is often seen as a problem associated with 'a few bad apples' and tends to be abridged to an issue with individual employees. Recent trends have shown that this approach is flawed and that a more systematic study of the behavioural indicators of insider threats is needed to better understand and appreciate the complexities of this issue. Moreover, insider threat mitigation practitioners emphasized the need for risk mitigation programs that not only govern the conduct of employees, but also the regular, day-to-day practices of businesses and government agencies. This reflects an important shift in the academic discourse surrounding the insider threat. Companies and government agencies have a certain degree of control over how they address the insider threat within their respective organizations. A strong workplace culture that incentivizes ethical conduct, professionalism and strong internal controls can significantly degrade an insider's ability to inflict damage to or harm organizational assets. Ultimately, an effective insider risk management program will mitigate the insider threat emanating from employees, by governing and managing the risk accrued through employee conduct.

This paper aims to provide a systematic review of the behavioural indicators that have a strong correlation to insider threats. It will provide insight into the academic debates around the concepts of insider threat, insider risk and conduct risk, and will further explore the conceptual linkages between each term. Subsequently, it will examine salient behavioural indicators in four key fields

[6] "Defining Insider Threats." *United States Cybersecurity and Infrastructure Security Agency* (accessed 29 April 2023). https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[7] "What Are Insider Threats?" *International Business Machines* (accessed 28 April 2023). https://www.ibm.com/topics/insider-threats?utm_content=SRCWW&p1=Search&p4=43700067188221065&p5=e&gclid=CjwKCAjwo7iiBhAEEiwAsIxQEa_yoUGM8zx_IWIanTB-wkiEjpUnW0GnYtcBJw36rHeNAgvJIH1llxoC8F0QAvD_BwE&gclsrc=aw.ds

[8] Froehlich, Andrew. "What Is An Insider Threat?" *TechTarget* (accessed 29 April 2023). https://www.techtarget.com/searchsecurity/definition/insider-threat

[9] Ibid.

[10] Ibid.

[11] Ibid.

in which the insider threat materializes: cybersecurity, workplace violence, insider fraud and extortion.

Literature Review

Historically, the academic literature paid considerable attention to external threats posed towards organizational data, particularly due to their visibility to researchers, as well as the ease of remedial action. Clive Blackwell (2009) pointed out that although the proportion of attacks originating from insiders was questionable, it was still a significant marker, and that the insider threat phenomenon needed to be studied due to the significance of damage they could cause to an organization.[12] In his study, Blackwell acknowledged that the insider threat does not just emanate from malicious activities or intent.[13] Insider weaknesses that are exposed by unsafe activities and lack of internal controls could lead to accidental failures or exploitation by outsiders at significant cost to the enterprise.[14]

Building on Blackwell's conceptualization of the insider threat, Eleanor Thompson (2019) delineated the insider threat to four main categories: the virtuous insider, the wicked insider, the vengeful insider and the malicious insider.[15] The virtuous insider is seen as a well-intended, good employee whose risky behaviour may impose (unintentional) costs on the organization.[16] The wicked insider is someone who knowingly bends the rules to support the organization's mission, albeit with significant disregard, or to pursue self-interest.[17] The malicious insider is someone who engages in deliberately destructive behaviour to disrupt an organization's mission.[18] Lastly, a vengeful insider is someone who willfully acts out against their supervisor or co-workers, yet who still believes in and supports the mission of the organization itself.[19]

The studies of Blackwell (2009) and Thompson (2019) serve as a useful starting point for our study of the behavioural indicators associated with insider threats. Both authors correctly hint that the insider threat is not a 'black-and-white' phenomenon. Insider threats can emanate from 'good' employees who do not necessarily understand the consequences of their actions. However, up to this point, the literature had not differentiated between the different types of insider threat. Its focus on the insider threat phenomenon was confined to individual-level attributes that incentivize an employee to commit a malicious act. For practitioners in insider threat mitigation, this could prove to be problematic. Detecting an individual insider threat, as well as acting to remove or mitigate the threat, is a difficult endeavour and can potentially open an organization up to litigation if not executed properly. Furthermore, organizations that have not built robust corporate processes in place to mitigate insider risks may find it difficult to retain employees and by extension, business knowledge.

[12] Blackwell, Clive, "The Insider Threat: Combatting the Enemy Within," *IT Governance Publishing* (2009): 8
[13] Ibid.
[14] Ibid.
[15] Thompson, Eleanor E, "The Insider Threat: Assessment and Mitigation of Risks (1st ed.)," *Auerbach Publications*: 14-15
[16] Ibid, 15
[17] Ibid.
[18] Ibid.
[19] Ibid.

Recently, Carnegie Mellon University's *Common Sense Guide to Mitigating Insider Threats: Seventh Edition* (2022) has emerged as the most up-to-date, seminal source for knowledge on insider threat detection and insider risk mitigation. The guide acknowledges the definitional differences between insider threat and insider risk. They define insider *threat* as "the potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally in a way that could negatively affect the organization."[20] Furthermore, Carnegie Mellon defines insider *risk* as "the impact and likelihood associated with the realization of an insider threat."[21] In both an academic and practical context, these definitional variations are important to acknowledge, as organizational responses towards insider threats and insider risk often differ. Due to the individual nature of the insider threat, an organization's response towards a perceived insider threat may be limited to administrative recourse, such as disciplinary action, additional training or job termination. However, the macro-level nature of insider risk allows organizations to take on a more proactive approach towards the insider threat phenomenon. Instead of detecting an insider threat late in its life cycle, an organization can adopt a broad-based insider risk management program that aims to reduce and ultimately prevent the threat and consequence posed by insiders.[22]

Since the 2007 financial crisis, the corporate sector has increasingly paid more attention to *conduct risk* management, especially in light of the impact that unethical financial behaviour had in causing the crash in financial markets.[23] The Risk Management Association defines conduct risk as "the risk of loss to an institution, or the harm to an institution's customers or other stakeholders, resulting from any willful act or omission by an institution's employee or independent contractor, or an employee or independent contractor of an institution's affiliate or third party."[24] Deloitte (2016) memorialized the concept of "conduct risk" through the publication of a report titled *The Culture of Risk: The Importance of Managing Conduct Risk and Maintaining an Effective Risk Culture Across the Business*. The report, which was ostensibly written to address the financial services sector, argued that conduct risk in an organization does not emanate from one singular business line.[25] Rather, it can be a product of longstanding business practices, such as improper customer onboarding practices, collusion with market participants, tax avoidance, inaccurate financial disclosures and fraudulent activities.[26] The Securities Industry and Financial Markets Association (SIFMA) reached a similar conclusion as Deloitte, and noted that conduct risk is derived from "wider organizational breakdowns" and implied that a strong "firm culture" could

[20] "Common Sense Guide to Mitigating Insider Threats, Seventh Edition," 3. https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

[21] Ibid.

[22] Ibid.

[23] Cole, Ben, and Francesca Sales. "What Is Conduct Risk?: Definition from TechTarget." *TechTarget* (published on 21 December 2016), https://www.techtarget.com/searchcio/definition/conduct-risk.

[24] Devlin, Frank, "Mitigating Conduct Risk To Preserve and Improve Reputation." *The RMA Journal* 101 (8) (2019): 2.

[25] "The Culture of Risk: The Importance of Managing Conduct Risk and Maintaining An Effective Risk Culture Across The Business." *Deloitte* (2016): 3. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-conduct-risk-pov-noexp.pdf

[26] Ibid.

foster the creation of strong norms and expected behaviours that would guide ethical behaviour on the part of a firm and its employees.[27]

Private industry has also weighed on the discussion of insider threat and the extent to which it causes problems, particularly in the field of cybersecurity. McKinsey and Company (2018) rightly points out that oftentimes, organizations struggle to define the insider threat and as a result, deploy inadequate solutions to detect and mitigate them.[28] In particular, a typical approach to insider threat management is prone to mass collection of employee data, detection of false-positives due to malicious activity being built into a 'baseline' behaviour, and discovering breaches after they have occurred.[29] The McKinsey assessment underscores a key gap in the existing literature among both academia and private industry. A lack of a clear definition and delineation among these terms can lead to misguided approaches that will be counterproductive towards an organization's insider risk management framework. Ultimately, it is important for practitioners in the field to recognize these conceptual differences and operationalize these findings into their respective risk management frameworks.

Similarities and Differences

Although insider threat, insider risk and conduct risk conceptually differ in many respects, they also tend to overlap with each other. Ultimately, frameworks to manage insider risk, insider threat and conduct risk centre around human behaviour. From an individual standpoint, employees that find themselves in difficult personal circumstances, and possess certain behavioural predispositions, are seen as more likely to act in ways that are detrimental to an organization's reputation, culture and bottom-line. By nature of their role in the company, potential perpetrators, which may include current or past employees, third party vendors, contractors, suppliers, and partners, may have access to important organizational assets and may misuse such privileges to inflict considerable damage to an organization. However, as previously mentioned, organizational approaches cannot reduce the issue to a few 'problematic' employees. The way that an organization manages insider risk will often inform the frequency of insiders posing legitimate threats to an organization. For example, an organization can maintain a robust security policy that accounts for the types of information handled by the enterprise, along with the risk posed to such information if handled by individuals with certain predispositions. Furthermore, business practices that centre around ethical conduct can significantly reduce an organization's risk profile, and by extension, the threat posed by insiders.

It is, however, important to underscore the nuances between insider risk, insider threat and conduct risk. First, organizations respond in different ways to each phenomenon. As statedabove, the typical organizational response to an insider threat is through disciplinary, administrative, or labour-related measures. Such actions are aimed at mitigating, or removing the threat posed by an individual employee towards the organization. Second, organizations must recognize that insider

[27] "MB-3: New: Conduct Risk Management and Ethical Culture." *Securities and Financial Markets Association* (accessed on 27 April 2023): 3. https://www.sifma.org/wp-content/uploads/2020/03/MB3-NEW-Conduct-Risk-Management-and-Ethical-Culture.pdf:

[28] Bailey, Tucker et al., "Insider Threat: The Human Element of Cyberrisk." *McKinsey & Company* (published on 24 September 2018), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk.

[29] Ibid.

risk *informs* the insider threat. A typical organizational response to insider risk happens on a larger scale and is likely to change how an organization handles its business practices, IT access privileges and its workplace culture. It would recognize the role that the nature of the business plays in shaping the organization's risk profile and would aim to incentivize behaviours that mitigate and reduce the likelihood of an insider threat. Lastly, although conduct risk has historically been associated with the financial services sector, it can be applied across organizations and sectors, including the public security sector. Separately, conduct risk is also narrowly applied in the sense that it only pertains to 'bad' behaviour or misconduct. Many industry experts have suggested that organizations should not limit themselves to problematic behaviour, and should instead prioritize more data collection to accurately assess baseline behaviours.

A Note on Data Sources

An organization's insider risk management strategy will vary depending on its industry, activities, size, and capabilities. An effective insider threat and conduct risk mitigation program will collect and analyze information from several data sources across the organization. As organizations expand the number of data sources used to assess their risk profile, they subsequently improve their ability to produce accurate alerts and make decisions about individual insider threats, or organization-wide insider risk mitigation programs that are informed by reliable evidence and data.[30] **Figure 1** in **Appendix A** provides an illustration of recommended data sources, both technical and non-technical data sources, to be included for insider threat detection, prevention, and response.[31]

The data sources illustrated in **Appendix A** do not entirely reflect all data points that can be used to prevent or detect all insider threats within every organization. According to the Computer Emergency Response Teams (CERT) at the Software Engineering Institute of Carnegie Mellon University, "some organizations might not collect all the listed data, and some organizations have different data sources available that provide additional information about workforce members and critical assets."[32] Furthermore, incorporating these technical and non-technical data sources into an analytic capability is extremely challenging. Therefore, an organization must acknowledge its limited resources and better understand what types of critical assets it has and how such assets could be misused by insiders.[33] Furthermore, organizations should choose data points based on their applicability to the organization's risk profile. Across organizations, similar technical and non-technical data sources can be used in insider risk mitigation such as, email logs, electronic communications, organization's mobile devices, employee-related information (background and credit checks, access card logs, attendance), violation records (racial, gender, or sexual harassment, use of inappropriate language), and telephone logs.[34]

[30] "Common Sense Guide to Mitigating Insider Threats, Seventh Edition," 98. https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf
[31] Ibid.
[32] Ibid, 86
[33] Ibid.
[34] Koshy, Sunita et al., "Conduct Risk Management and Ethical Culture." *SIFMA Compliance and Legal Conference* (2020), 5, https://www.sifma.org/wp-content/uploads/2020/03/MB3-NEW-Conduct-Risk-Management-and-Ethical-Culture.pdf

Sign post could be used here: The next two sections turn to a brief overview of this project's methodology, detailing x, y, z, and a discussion of behaviour indicators.

Methodology

The purpose of this project is to review and validate academic research on behaviour factors that have a strong correlation to insider threats. As such, we decided that the most effective way to achieve this task was via a two-step literature review. First, a literature review was conducted to gain foundational knowledge of our various terms, insider risk, insider threat and conduct risk. Throughout this phase of research, the commonalities and differences of these terms was also reviewed and considered. Second, a narrative literature review was used to identify the common and widely agreed upon behaviours that are associated with the different types of insider threat. These insider threats include fraud, workplace violence, theft of trade secrets or customer information, and IP theft. Throughout this project we will consider each of these types of insiders separately and pinpoint behaviours that are unique to each. This information will allow us to establish a data dictionary that captures key problem behaviours and provide an explanation of how they may appear in physical and technological scenarios.

Behavioural Indicators

Behavioural science studies (psychology, sociology, or anthropology) provide important insights that help insider risk management practitioners understand perpetrators' motivations, behaviours, and mindsets. A crucial element in these studies is acknowledging human behaviour when designing, building, and using technical controls for mitigating insider threats.[35] Research suggests that the insider threat typically materializes through certain psychological and behavioural indicators that are usually informed by events occurring **after** an employee has been pre-screened into an organization.[36] These indicators are often exhibited by employees through concerning behaviours prior to an insider attack:[37] "Randazzo et al. reported that eighty percent of insider cases in their study raised official attention for concerning behaviors such as tardiness, truancy, arguments with coworkers, and poor job performance; and in 97% of those cases, supervisors, coworkers, and subordinates were aware of these issues."[38] This important detail is often lost when organizations are formulating controls to mitigate insider and conduct risks. One limitation for insider threat research is the lack of real-life data of known incidents. Organizations are reluctant to disclose that information due to privacy concerns and reputational damages[39]. Most of the time these incidents are solved internally.

[35] Pfleeger, Shari Lawrence and Deanna D. Caputo., *"Leveraging Behavioral Science to Mitigate Cyber Security Risk," Computers & Security* 31 (2012): 597

[36] Bell, Alison J.C. et al., "The Insider Threat: Behavioral Indicators and Factors Influencing Likelihood of Intervention." *International Journal for Critical Infrastructure Protection* 24 (2019): 167

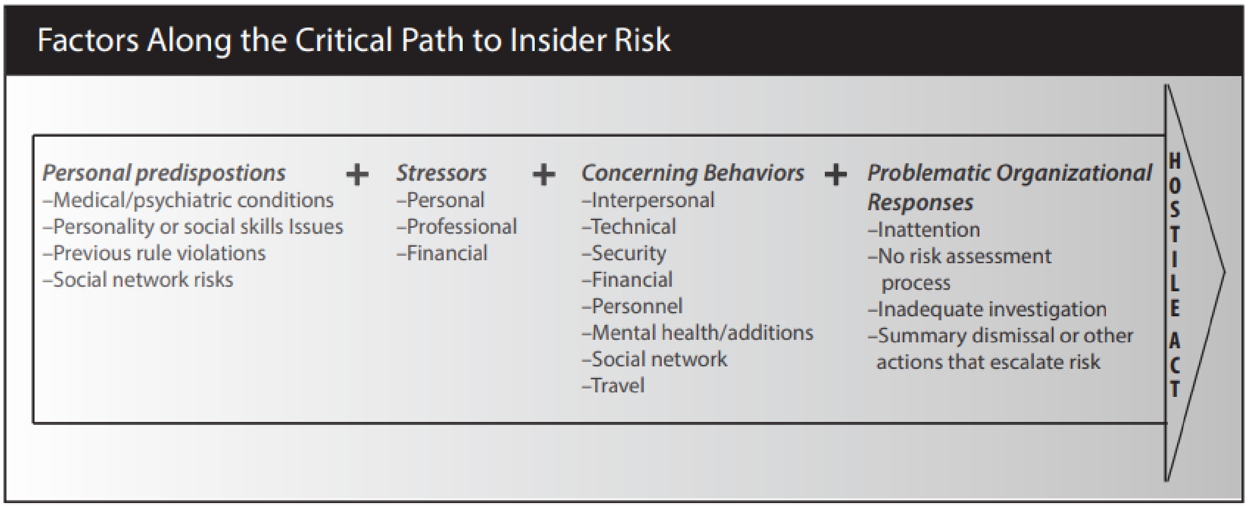
[37] Shaw, Eric and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks," *Studies in Intelligence* 59 (2) (2015): 3 https://nationalinsiderthreatsig.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf

[38] Greitzer, Frank L. et al., "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis," *E-Service Journal* 9 (1) (2013): 109

[39] Gheyas, Iffat A. and Ali E. Abdallah., "Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis." *Big Data Analytics* 1 (1) (2016): 1

Eric Shaw and Laura Sellers developed the *Critical Path to Evaluate Insider Risks* as a means of determining a common set of attributes and behavioural pattern for offensive and defensive counterintelligence purposes. The critical path is a framework that describes "useful categories for assessing if a given person of concern might be on a destructive path." It is geared towards technical professionals (e.g., cyber security specialists and data analysts), as they assess the data, to remind them of the multiple human factors that may influence an individual's decision to commit IT sabotage. The four elements of the framework are the following: personal predispositions, stressors, concerning behaviours, and problematic organizational responses.[40]

Figure 2: Critical Path to Evaluate Insider Risks


Factors Along the Critical Path to Insider Risk
Personal predispostions
–Medical/psychiatric conditions
–Personality or social skills Issues
–Previous rule violations
–Social network risks
+
Stressors
–Personal
–Professional
–Financial
+
Concerning Behaviors
–Interpersonal
–Technical
–Security
–Financial
–Personnel
–Mental health/additions
–Social network
–Travel
+
Problematic Organizational Responses
–Inattention
–No risk assessment process
–Inadequate investigation
–Summary dismissal or other actions that escalate risk
HOSTILE ACT

Source: Eric Shaw and Laura Sellers, 2015

Individuals experiencing a stable life rarely commit unlawful acts. However, negative personal or work-related events can occur anytime throughout an employee's career, which influences an insider to conduct an attack.[41] However, individuals with certain personal predispositions, or characteristics that enhances an individual's risk profile, may exhibit certain behaviours leading to misconduct and insider threats.[42] Moreover, individuals may experience certain stressors, which refers to positive or negative events that occur in people's lives that have an effect on their personal, professional and/or financial situations.[43] "While everyone experiences stress in life," Shaw and Sellers argue further, "research indicates that stressors especially place pressure on those who possess vulnerable predispositions and can lead them down the next step of the critical path."[44]

[40] Shaw, Eric and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks," 3. https://nationalinsiderthreatsig.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf

[41] Bell et al. "Insider Threat: Behavioural Indicators and Factors," 167

[42] Shaw, Eric and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks," 3. https://nationalinsiderthreatsig.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf

[43] Ibid, 4.

[44] Ibid.

Concerning or problematic behaviours include policy violations and standard procedure, professional misconduct, and others that management and coworkers observed over time.[45] It is important to caution, once again, that not all individuals who struggle with these particular issues (personal predispositions, stressors, and problematic behaviour) are potential insider threats. Finally, problematic organizational responses refer to how organizations respond to troubling behaviour. An organization's involvement can have an impact in an individual's movement down the critical path.[46] Research has noted that "the likelihood, or risk, that individuals will commit hostile acts against their organizations increases with the accumulation of factors acting on them over a period of time."[47] Furthermore, organizations need to take into account that "the number of employees who can be said to have exhibited or been affected by all of the factors represents a very small proportion of any organization's population."[48] It should be noted that one limitation for insider threat research is the lack of real-life data of known incidents. Organizations are reluctant to disclose that information due to privacy concerns and reputational damages.[49] The following section will examine behavioural indicators for cybersecurity, workplace violence, fraud and extortion that have a strong correlation with insider threat.

Cybersecurity

Cybersecurity is a broad field that encompasses various systems, processes and technologies used to detect, prevent, and respond to malicious attacks against devices, data, and networks.[50] For the purpose of this report, we define cybersecurity as a violation/misuse of an organization's information security policy or attacking the organization's IT systems and assets.[51] Computers and information technology are an integral part of our lives and businesses. Individuals and organizations use IT to process transactions and information, store data, analyze and access information, and much more. With the growing threat of cyber-attacks and complex information systems, information security has become increasingly critical to businesses, organizations, and individuals.

Unfortunately, organizations have invested greatly on enhancing technological safeguards while neglecting the human behaviour informing security incidents.[52] Technical controls, such as firewalls, antivirus, identification, authentication, and intrusion detection systems, provide round-

[45] Ibid, 4-5
[46] Center for Development of Security Excellence (CDSE), "Behavioral Science and Insider Threat" (accessed 29 April 2023): https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Behavioral-Science-and-Insider-Threat.pdf
[47] Shaw, Eric and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks," 2
[48] Ibid, 3
[49] Gheyas, Iffat A. and Ali E. Abdallah. "Detection and Prediction of Insider Threats to Cyber Security," 5
[50] "Is CyberSecurity A Promising Career?" *University of Tulsa* (published on 7 February 2022), https://cybersecurityonline.utulsa.edu/blog/is-cybersecurity-a-promising-career/#:~:text=The%20crux%20of%20the%20matter,against%20%20devices%2C%20data%20and%20networks
[51] Carleton University-NPSIA Student and al., 2023
[52] Briney, Andy, "2001 Information Security Industry Survey," *Information Security Magazine* (published October 2001), 34 http://lfca.net/Reference%20Documents/2001%20Information%20Security%20Survey.pdf

the-clock protection to IT systems and applications.[53] Although research on technical controls for mitigating cybersecurity insider threats is abundant, Silaule et al. (2022) argue that "there is a necessity to have a full view and interdisciplinary approach that considers the technological aspect of cybersecurity insider threats along with the human or insider element, which is difficult for organizations to detect, prevent or reduce."[54] Simply put, if organizations increasingly focus on technical controls, they may lose sight of behavioural indicators, which are crucial in preventing and deterring insider threats. The fictitious scenario that follows below highlights some behavioural indicators found in insider threat incidents related to cybersecurity.

Case Study: Disgruntled Employee

Tom Jerry works at SellersOne Inc. as a support technician. Tom became extremely dissatisfied with his day-to-day job, which consisted of installing software and hardware on SellersOne' computers, resolving network issues, as well as providing technical support to employees. Over the past few months, Tom was late to work and often left early. He even took longer lunch breaks than allowed and called in sick multiple times to avoid being physically in the office. One day Tom emailed his manager, Olivier Jenkins, indicating that he was dissatisfied with the job and that he will produce low quality.

Hi Olivier,

I am emailing you to discuss my assigned task. I do not plan on taking any ownership of modem troubleshooting. If you insist that I must complete the task, I can 100% assure you that the job at hand will be completed with little to no effort, and no attention to detail. I've been working overtime for the past 8 months to help reduce the backlog, and haven't received any support nor recognition for my work. I am exhausted.

Thanks,

Tom

Tom also shared his frustrations regarding his work and manager with a co-worker via a shared company chat service expressing the following:

James, man I really hate Olivier. Yet again he's asking me to do more troubleshooting. The deadline is TOMORROW. Is he insane? Like you know there are other employees in the Team he can ask to complete the task. I don't even know why he's the manager at this point. He has little technical knowledge and always asks me to complete HIS TASKS, which are mostly complex, so that he looks good in front of his boss. GIVE ME A BREAK. Fuuuuuuuuck this. I am over it James, I really am. I hope Olivier is not coming to Chantelle's farewell lunch tomorrow. If I see his face, I might end up punching him. I can't wait to go home.

[53] Wilson, Mark et al., "Information Technology Security Training Requirements: A Role and Performance-Based Model, Special Publication (NIST SP)," *National Institute of Standards and Technology* (1998), 25. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151633

[54] Silaule, Carol B. et al., "A Model to Reduce Insider Cybersecurity Threats in a South African Telecommunications Compay," *South African Journal of Information Management* 24 (1) (2022), 1

Eventually, Tom's job dissatisfaction led to his resignation. Despite his negative comments and communications, Michael Hall, the owner of SellersOne Inc., let Tom retain email access as a paying customer following his resignation. Several weeks after Tom's resignation, he used fake accounts that he had created to modify all the company's administrative passwords, changed the computer's registry, deleted the company billing system, as well as three internal databases. Prior to these attacks, Tom used the SellersOne computers to express his intent to harm the company via emails and social media to his relatives and a former co-worker.

I love the scenario. But what is it's purpose? Does it link to Concerning Beahviours, below. If so, tell us why in the first sentence or two that follows. If not, explain here what it's purpose is in relation to the previous section on Cybersec. If not that either, explain why the scenario is positions here, or move it to where it will be used to highlight whatever it is meant to highlight.

Concerning Behaviours

The below table contains a list of salient indicators that are associated with insider cybersecurity threats, as highlighted by the above vignette. It is important to note that these indicators, on their own, may not be indicative of insider cybersecurity threats. If these indicators are observed as part of a pattern of behavior, then practitioners may have reasonable concern of insider cyber security threats taking place.

Indicators	**Description**	**Observable Behaviours**	**Data sources**
Substance Abuse and Misuse	Use of or involvement with alcohol, illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants	Changes in hygiene or professional appearance (wearing dirty clothes and smelly odor). Employees' eyes might be watery, bloodshot, or glassy. Employees might act hostile, angry, paranoid, or fearful for no reason. Employees' speech sounds slurred or incoherent[55].	HR Records Monitor badge records for tardiness, absences during the day, and missed work[56] Background Check (substance related arrests (i.e., DUI)[57])

[55] McGuinness, Elly. "6 Signs Your Employees May Be Abusing Drugs," *SureHire Occupational Testing* (published 31 May 2022), https://www.surehire.com/6-signs-your-employees-may-be-abusing-drugs/

[56] Cassidy, Tracy and the CERT Insider Threat Center. "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," *Carnegie Mellon University Software Engineering Institute Blog* (published 12 April 2018), https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

[57] Ibid.

Rule Violation	Unwillingness to comply with rules and regulations, or to cooperate with security requirements. Employees feel above the rules or that they only apply to others.[58]	Recurrent mishandling of classified information (e.g., attempts to take classified documents home from work)	Virtual Private Network Log Printer/Scanner/Copier/Fax Logs Authentication Logs[59]
Disgruntlement	Employees observed to be dissatisfied in their current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with their current job.[60]	Difficulty collaborating with colleagues and/or lashing out verbally or electronically to management and/or coworkers.	Email logs Chat logs[61]
Aggressive or Violent Behavior	Employees exhibit argumentative or aggressive behavior or are involved in bullying or intimidation.	Shouting and swearing at coworkers, as well as hitting, kicking, biting, and pushing	HR Records
Absenteeism	Employee has exhibited chronic unexplained absenteeism.	Frequent absences or unexplained disappearances from a desk[62] (ie: excessive breaks and vacations/travel, late starts, long lunch breaks[63])	HR Records Travel reporting Monitor badge records for tardiness, absences during the day, and

[58] Crespo, Conrado. "Insider Threats: Five Indicators of Risk and What To Do," *CounterCraft* (accessed 29 April 2023), https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

[59] Ogonji, Mark Mbock. "A Modeling and Simulating Insider Cyber Security Threats Using Psychosocial Factors," *University of Nairobi School of Computing and Informatics* (2013), 9-10, http://erepository.uonbi.ac.ke/bitstream/handle/11295/63350/Ogonji_Cyber%20security%20threats.pdf?sequence=3&isAllowed=y%20(all%20the%20way%20to%20absence)

[60] Ogonji, "Modeling and Simulating Insider Cyber Security Threats," 25

[61] United States Department of Defense, "Insider Threat Indicators," *National Insider Threat Special Interest Group* (accessed 29 April 2023), https://www.nationalinsiderthreatsig.org/itrmresources/Behavioral%20Indicators%20Of%20Concern%20For%20Insider%20Threat%20Programs%20-%20Part%201.pdf

[62] Weast, Eric, "Disgruntled Employee Suddenly Quits South Florida Business," *ECW Network and IT Solutions* (accessed 29 April 2023), https://www.ecwcomputers.com/disgruntled-employee/

[63] "How To Recognize And Handle A Disgruntled Employee | 10 Steps," *GetSling* (accessed 29 April 2023), https://getsling.com/blog/disgruntled-employee/

			missed work[64]
Working Odd Hours	Accessing the premises outside of normal hours with or without justified authorization[65]	User with a high number of system logins during unusual hours such as midnight or during weekends without any specific work related reasons[66]	Monitor Badge Records VPN Remote Access
Decline in job performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.	Frequent mistakes, not following a job through, unable to cope with instructions given. Inability to cope with a reasonable volume of work and to meet deadlines	Employee performance management system/Performance Evaluation

Workplace Violence

Workplace violence is reported to be on the rise in Canada, the US, and elsewhere. For the purpose of this report, we use the *Occupational Safety and Health Administration's* definition of workplace violence as "any physical assault, threatening behaviour, or verbal abuse occurring in the work setting[67]." Workplace violence incidents include, but are not limited to, threats, assault, verbal abuse, harassment, stabbings, shootings and suicides. It should be noted that it is hard to determine if an individual is a threat to themselves, others or a combination.

According to the Ottawa Police Service 2019 Annual Report, 61 complaints of disrespectful behaviour and five concerns of workplace violence were brought forward[68]. These incidences of misconduct included inappropriate behaviour, gossip, rumors, bullying, intimidation, yelling, swearing and conflict. A study conducted by researchers from the Canadian Labour Congress, University of Toronto and Western University suggest that workplace violence continues to be rampant in Canada. The researchers examine several workplaces across Canada, such as corporations, service sectors, hospitality, private sectors, and blue-collar jobs, and found that over 70 percent "of survey respondents experienced at least one form of harassment and violence or

[64] Cassidy et al., "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

[65] Crespo, "Insider Threats: Five Indicators of Risk & What To Do," https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

[66] Mills, Jennifer U. et al., "Predict Insider Threats Using Human Behaviors," *IEEE Engineering Management Review* 45 (1) (2017), 40

[67] Cassidy, Tracy et al., "Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies," *Carnegie Mellon University Software Engineering Institute* (2018), 2, https://apps.dtic.mil/sti/pdfs/AD1090846.pdf

[68] Chief of Police, Ottawa Police Service, "Positive Workplace: 2020 Annual Report," *Ottawa Police Services Board*, (2021), 5, https://pub-ottawa.escribemeetings.com/filestream.ashx?documentid=21298

sexual harassment and violence, in the two years prior to completing the survey[69].” Moreover, in the United States, the Federal Bureau of Investigation (FBI) reported that between 2000 and 2013, 80 percent of active shooters occurred at work. In fact, out of “those active-shooter incidents cited in the report, more than 46 percent were perpetrated by employees or former employees and 11 percent involved employees who had been terminated that day.”[70]

Despite organizations’ interest in thwarting violence in the workplace, some lack basic technical controls and/or capabilities designed to prevent, detect and mitigate potential risks of workplace violence. Traditional technical controls, such as User Activity Monitoring (UAM) and User-Entity Behavioural Analytics (UEBA/UBA) are used to mitigate insider IT sabotage, unauthorized disclosures, espionage, fraud and other technical insider threats[71]. Nevertheless, even with the large amount of data the above-mentioned tools collect, “most insider threat monitoring solution stacks are still in their infancy in terms of utilizing behavioral or non-traditional technical data sources such as human resource records.”[72] The case study below highlights some behavioural indicators found in insider workplace violence incidents.

Case Study: Viciously Attacking a Co-Worker

Elizabeth Jane has been working at ATC Telecommunications for eight years. She was in a romantic relationship with Ian Bailey, a male co-worker, which lasted for three years. Elizabeth recently broke off the relationship, however, Ian would not leave her alone. Ian kept calling her several times a week (during and outside of work hours). He shows up wherever she goes on the weekends, and stares at her from a distance. He often parks his car next to hers at work. Ian would also message Elizabeth via email and social media (Facebook & Instagram) threatening to hurt himself if they do not get back together. Elizabeth felt uncomfortable and blocked him on social media.

A few days later, while Ian went on vacation for two weeks, Elizabeth reported his behaviour to the Human Resources (HR) department. She provided text messages and emails as evidence of Ian’s misconduct in the workplace. The HR department assured Elizabeth that they would conduct an investigation to gather and examine all the relevant facts regarding the issue.

Later, Elizabeth received a text message from an unknown number:

“Hey Liz, it’s Ian.

[69] Berlingieri, Adriana et al., “Harassment and Violence in Canadian Workplaces: It’s [Not] Part of the Job,” *Centre for Research and Education on Violence Against Women and Children* (2022), 6, https://documents.clcctc.ca/human-rights/Respect-at-Work-Report-EN.pdf

[70] Cassidy, Tracy et al., “Technical Detection of Intended Violence: Workplace Violence as an Insider Threat,” *Carnegie Mellon University Software Engineering Institute* (2017), https://insights.sei.cmu.edu/blog/technical-detection-of-intended-violence-workplace-violence-as-an-insider-threat/?_gl=1*1573q87*_ga*MzU0NTMyOTIx%20LjE2NzcxMDMyMTc.*_ga_87WECW6HCS*MTY3NzEwMzIxNi4xLjEuMTY3NzEwMzI5MS4wLjAuMA; Rugala, Eugene A. et al., “Workplace Violence Issues in Response,” *Critical Incident Response Group National Center For The Analysis of Violent Crime* (accessed 29 April 2023), https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view

[71] Cassidy, Tracy et al., “Analyzing Incidents of Workplace Violence To Inform Incident Planning and Mitigation Strategies,” 2

[72] Ibid.

I cannot stop thinking about you Liz. I don't know what went wrong with us, but I would like to get back together. I will do whatever it takes to gain your love back."

Elizabeth did not respond to the text message and blocked the number.

Upon returning to the office, Ian received an email from Elizabeth stating the following:

"Ian, we already talked about it. I do not want to be in a relationship with you. You need to stop stalking me wherever I go. It's very weird. Let's go our separate ways and please leave me alone."

Ian becomes furious. He wanted to hurt her so that she could feel his pain. Ian lost control and entered Elizabeth's cubicle. He stood there for a second and then punched her in the stomach. Screaming, Elizabeth is flung from her chair. Ian departs the office on foot. . Alerted by the commotion coworkers call the police.

Concerning Behaviours

The below table contains a list of salient indicators that are associated with workplace violence. It is important to note that these indicators, on their own, may not be indicative of workplace violence. If these indicators are observed as part of a pattern of behavior, then practitioners may have reasonable concern of workplace violence taking place.

Indicators	**Description**	**Observables**	**Data source**
Stress	Employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.	Struggling to complete daily task/panic attacks	HR Records
Disgruntlement	Employees observed to be dissatisfied in their current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with their current job.[73]	Difficulty collaborating with colleagues and/or lashing out verbally or electronically to management and/or coworkers.	Email logs Chat logs[74] HR Records
Substance Abuse and Misuse	Use of or involvement with illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants	Changes in hygiene or professional appearance (wearing dirty clothes and smelly odor). Employees' eyes	HR Records Monitor badge records for

[73] Ogonji, "Modeling and Simulating Insider Cyber Security Threats," 25

[74] United States Department of Defense, "Insider Threat Indicators - Behaviors of Concern," https://www.nationalinsiderthreatsig.org/itrmresources/Behavioral%20Indicators%20Of%20Concern%20For%20Insider%20Threat%20Programs%20-%20Part%201.pdf

		might be watery, bloodshot, or glassy. Employees might act hostile, angry, paranoid, or fearful for no reason. Employees' speech sounds slurred or incoherent[75].	tardiness, absences during the day, and missed work[76] Background Check (substance related arrests (i.e., DUI)[77])
Aggressive or Violent Behavior	Employees exhibit argumentative or aggressive behavior or are involved in bullying or intimidation.	Shouting and swearing at coworkers, as well as hitting, kicking, biting, and pushing	HR Records Disciplinary Records
History of Violence	Employee has a repeated history of violence inside and outside the workplace	Battery/assault arrest records[78]	Criminal Records Check
Decline in job performance	Employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance	Frequent mistakes, not following a job through, unable to cope with instructions given. Inability to cope with a reasonable volume of work and to meet deadlines	Employee performance management system/Performance Evaluation HR Records
Absenteeism	Employee has exhibited chronic unexplained absenteeism.	Frequent absences or unexplained disappearances from a desk[79] (e.i. excessive breaks and vacations/travel, late starts, long lunch breaks[80])	HR Records Travel reporting Monitor badge records for tardiness,

[75] McGuinness, Elly, "6 Signs Your Employees May Be Abusing Drugs," https://www.surehire.com/6-signs-your-employees-may-be-abusing-drugs/

[76] Cassidy et al., "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

[77] Ibid.

[78] Cassidy et al., "Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies," 6, https://apps.dtic.mil/sti/pdfs/AD1090846.pdf

[79] Weast, "Disgruntled Employee Suddenly Quits South Florida Business How to Protect Your Company from Insider Threats," https://www.ecwcomputers.com/disgruntled-employee/

[80] "How To Recognize And Handle A Disgruntled Employee | 10 Steps," *GetSling*, https://getsling.com/blog/disgruntled-employee/

			absences[81] during the day, and missed work
Working Odd Hours	Accessing the premises outside of normal hours with or without justified authorization[82]	User with a high number of system logins during unusual hours such as midnight or during weekends without any specific work related reasons[83]	Monitor Badge Records VPN Remote Access
Concerning Web searches	Employee is accessing blocked Websites	Visiting restricted Websites and darknet sites[84]	Web Proxy Logs

Fraud

Fraud refers to the wrongful or criminal deception of individuals or organizations that is intended to result in personal or financial gain for the perpetrator. Conceptually, this term can apply to several activities across industries. For the purposes of this report, we will focus on occupational fraud, which is perpetrated by individuals against the organizations that employ them.[85] Occupational, or insider fraud, is one of the most costly and common forms of crime and has significant impacts across industries ranging from the financial services sector to the public security sector in government.[86] Insider fraud often takes place over a longer period of time, as opposed to insider IT sabotage or intellectual property theft, because internal enterprise monitoring systems either do not monitor behavioural red flags associated with fraud, or simply lack sufficient business processes to do so.[87] Insider fraud can be triggered through several means. From an individual standpoint, employees may commit fraud for their own personal or financial gain, ranging from a job promotion to advancing one's reputation across the enterprise.[88] Individuals may also seek employment in a specific company or agency for the deliberate and sole purpose of

[81] Cassidy et al., "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

[82] Crespo, "Insider Threats: Five Indicators of Risk & What To Do," https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

[83] Mills et al., "Predict Insider Threats Using Human Behaviors," 40

[84] Cassidy et al., "Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies," 6, https://apps.dtic.mil/sti/pdfs/AD1090846.pdf

[85] "Occupational Fraud 2022: A Report to the Nations." *Assocation of Certified Fraud Examiners* (accessed 26 April 2023), https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

[86] Ibid.

[87] Sullivan, Peter. "How Insider Fraud Can Be Detected and Avoided in the Enterprise." *TechTarget*, September 2018. https://www.techtarget.com/searchsecurity/tip/How-insider-fraud-can-be-detected-and-avoided-in-the-enterprise

[88] "Introduction to Fraud Indicators," *Fraud Advisory Panel* (published on 14 November 2011), 1 https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-14B-Fraud-Indicators-Nov11.pdf

gathering intellectual property and misusing data to fit their own purposes.[89] Fraud can also be perpetrated through enterprise-wide conduct, in which upper management may appear to condone unethical, or even criminal practices to improve the enterprise's bottom line.[90] This can often be influenced by a corporate culture that prioritizes meeting performance benchmarks at all costs, rather than a balanced approach that emphasizes the role of ethical behaviour in the workplace.

To understand the factors that cause an individual or entity to commit fraud, Donald Cressey (1973) introduced the fraud triangle, which was built on the premise that fraud is likely to result from a combination of motive, opportunity, and rationalization.[91] First, an individual requires a motivation or incentive to commit a fraudulent act. Usually, an individual's motivation to commit fraud results from a perceived pressure on a person, such as a desire to meet performance benchmarks, financial distress, and a change in working conditions. Second, an individual has an opportunity to commit fraud. If an organization lacks sufficient internal oversight and business processes to detect and prevent fraud, then the individual may proceed with committing the fraudulent act. Depending on the nature of an enterprise's operations, it may be more difficult to detect such acts due to lack of monitoring, or the ease of circumventing internal controls. Third, an individual may be capable of rationalizing fraudulent acts as being in keeping with their ethical inclinations. They may *rationalize* their actions out of spite towards a particular manager or employer, believing that their action serves as 'payback' against a perceived (or real) slight or injustice. Conversely, an individual may rationalize their actions due to a lack of leadership by upper management, by implying that the organization's leadership condoned their actions.

Case Study: The Wells Fargo Cross-Selling Scandal

In 2016, an American financial services company Wells Fargo was forced to pay a $3 billion settlement to the U.S Department of Justice and the Security and Exchange Commission, following long-running criminal and civil investigations into company-wide fraudulent sales practices, such as cross-selling.[92] Cross-selling, at the time, was seen as a key performance metric for employees and awarded additional pay to employees based on a ranking system that measured several different types of sales tactics. [93] According to Forbes, Wells Fargo's issues emanated from executives at Wells Fargo who pressured frontline bank employees to aggressively cross-sell products by implementing sales quotas in an effort to improve sales and revenue.[94] If branch

[89] Ibid.

[90] Ibid.

[91] Huang, Shaio Yan et al., "Fraud Detection Using Fraud Triangle Risk Factors," *Information Systems Frontiers* 19 (2017), 1344 https://doi-org.proxy.library.carleton.ca/10.1007/s10796-016-9647-9

[92] Kelly, Jack. "Wells Fargo Forced to Pay $3 Billion For The Bank's Fake Account Scandal." *Forbes* (2020). https://www.forbes.com/sites/jackkelly/2020/02/24/wells-fargo-forced-to-pay-3-billion-for-the-banks-fake-account-scandal/?sh=557d30c042d2

[93] Tayan, Brian. "The Wells Fargo Cross-Selling Scandal." *Harvard Law School Forum on Corporate Governance* (2019). https://corpgov.law.harvard.edu/2019/02/06/the-wells-fargo-cross-selling-scandal-2/

[94] Kelly, "Wells Fargo Forced to Pay $3 Billion For The Bank's Fake Account Scandal," https://www.forbes.com/sites/jackkelly/2020/02/24/wells-fargo-forced-to-pay-3-billion-for-the-banks-fake-account-scandal/?sh=4467030542d2

managers did not meet sales quotas one day, a shortfall was added to the next day's goals, which incentivized branch managers to meet daily targets.[95]

An independent investigation concluded that the company's practices created excessive pressure on employees to sell unwanted or unneeded products to customers.[96] Employees feared retribution for failing to meet the goals of upper management, even if such goals were unreasonably high.[97] In order to meet these goals, employees resorted to opening new accounts and issuing debit or credit cards without customer knowledge.[98] In some cases, bank associates even forged signatures in order to meet certain targets.[99] Such pressure was enough to force employees to ignore and circumvent internal protections, such as Wells Fargo's ethics program, reporting line for conflicts of interest and whistleblower hotline.[100] Furthermore, the investigation concluded that Wells Fargo's organizational structure enabled the proliferation of unethical behaviour. The decentralized nature of decision-making in Wells Fargo exposed the bank to significant risk, and the bank's internal controls were woefully insufficient in addressing the issues brought about by the fraud.[101]

The Wells Fargo case represents a strong operationalization of the fraud triangle model. Employees, on a wide scale, faced pressure from upper management to meet sales targets, saw an opportunity to take advantage of lax internal controls and de-centralized decisionmaking to commit fraudulent acts, and presumably rationalized their behaviour through the financial benefits accrued from such acts, or by their continued employment with Wells Fargo. Not only did this case represent the concept of the 'insider threat' well, but it also illustrates how each concept relates to each other. A strong insider risk culture can prevent insider threats from harming organizations, or can mitigate their impacts, by promoting conduct that minimizes risks to an organization's reputation and bottom-line.

Concerning Behaviours

The below table contains a list of salient indicators that are associated with insider fraud. It is important to note that these indicators, on their own, may not be indicative of fraud. If these indicators are observed as part of a pattern of behavior, then practitioners may have reasonable concern of fraud taking place.

Indicators	Description	Observables	Data Sources
Sudden, unexplained change in financial circumstances	Employee appears to demonstrate an unexplained, substantial improvement in their lifestyle beyond what their current job salary can afford.	Living beyond one's financial means or	Background Checks Credit Inquiries

[95] Tayan, "The Wells Fargo Cross-Selling Scandal," https://corpgov.law.harvard.edu/2019/02/06/the-wells-fargo-cross-selling-scandal-2/
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid.

		suffering from acute financial distress.[102]	
Abuse of access privileges	Employee observed trying to circumvent internal IT controls to gain unauthorized access to specific files.	Attempt to coerce colleagues with appropriate access privileges to access files on employee's behalf.[103]	Employee Badge Records HR Records Internal IT Records Email and Chat Logs
Unusually close association with clients or partners[104]	Employee observed to be unusually close to external clients, vendors or partners.	Demonstrates irritability and defensiveness among colleagues, continuous engagement with clients or partners beyond professional expectations.[105]	Email and Chat Logs Job Satisfaction Surveys From Clients
Stress	Employee appears to be under physical, mental, emotional strain or tension that he/she has difficulty handling.	Struggling to complete daily tasks, experiencing repeated panic attacks.	HR Records
Disgruntlement	Employees observed to be dissatisfied in their current position; chronic indications of discontent, such as strong, negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with their current job.	Difficulty collaborating with colleagues, demonstrates irritability and defensiveness with management and co-workers.	Email Logs Chat Logs HR Records
Suspiciousness[106]	Employee observed to be constantly apprehensive of inquiries from colleagues or management.	Maintaining strict secrecy over projects, controlling demeanor, refusal to take vacations	Performance Evaluations HR Records

[102] No Author. "2020 Global Study on Occupational Fraud and Abuse." *Association of Certified Fraud Examiners* (2020). https://legacy.acfe.com/report-to-the-nations/2020/docs/infographic-pdfs/Behavioral%20Red%20Flags%20of%20Fraud.pdf

[103] Agrafiotis, Ioannis et al., "Identifying Attack Patterns for Insider Threat Detection," *Computer Fraud and Security* 2015 (7) (2015), 10

[104] "2020 Global Study on Occupational Fraud and Abuse," *Association of Certified Fraud Examiners,* 1-2, https://legacy.acfe.com/report-to-the-nations/2020/docs/infographic-pdfs/Behavioral%20Red%20Flags%20of%20Fraud.pdf

[105] Ibid.

[106] Ibid.

		out of fear of being caught.	Email and Chat Logs

Extortion

The Criminal Code of Canada stipulates that "everyone commits extortion who, without reasonable justification or excuse and with intent to obtain anything, by threats, accusations, menaces or violence induces or attempts to induce any person" to commit a specific act.[107] Unlike other insider threats presented in this report that are generally more straightforward in nature, extortion-like behaviours are often referred to in different ways in the literature, but rarely explicitly as extortion. As a result, extortion in the workplace must be explored through a more abstract lens that draws upon a variety insider threat types. This approach is appropriate given that, in a Canadian context, extortion in the workplace appears to be more frequently called workplace harassment, coercion or psychological violence.[108] This is likely because extortion typically involves at least the threat of violence, be it psychological, physical, or emotional.[109]

In addition, it is also essential when considering this type of insider threat that the insider can be either the driving extortionist or the one being extorted. In cases where an employee is committing extortion, they may demonstrate behavioural indicators specific to this type of insider. Such behaviours may include downloading external software onto company systems, or an increase in workplace devices.[110] [111] Additional behaviours could include changing of network access credentials, accessing files that are not required for job completion, moving, and deleting documents[112]. Additional behavioural indicators include proximity or intimate knowledge of a crime being committed against their business.

Conversely, an employee may be extorted by an outside entity to engage in similar activity on behalf of that outside entity. This is increasingly becoming a concern for businesses. Given the availability of access to personal information, such as the names and contact information of

[107] Criminal Code of Canada, "Extortion," *Justice Laws Website* (accessed 28 April 2023), https://laws-lois.justice.gc.ca/eng/acts/c-46/section-346.html

[108] Government of Canada, *"Is It Harassment? A Tool to Guide Employees,"* Government of Canada, 2015; Shonna Waters, "Feeling Uneasy? Here's What Workplace Coercion Looks Like," *BetterUp* (2021), https://www.linkedin.com/pulse/employee-blackmail-c-j-westrick-sphr/?trk=pulse-article_more-articles_related-content-card.; Government of Quebec, "Forms of Violence," (accessed 10 April 2023), https://www.quebec.ca/en/family-and-support-for-individuals/violence/forms-violence.

[109] PricewaterhouseCoopers and Microsoft, *"Starting an Insider Risk Management Program,"* (accessed 25 April 2023). https://download.microsoft.com/download/b/2/0/b208282a-2482-4986-ba07-15a9b9286df0/pwc-starting-an-insider-risk-management-program-with-pwc-and-microsoft.pdf

[110] Mott, Nathaniel, "Former Ubiquiti Dev Arrested for Orchestrating Data Breach, Trying To Extort $2M," *PC Magazine* (published 2 December 2021), https://www.pcmag.com/news/former-ubiquiti-dev-arrested-for-orchestrating-data-breach-trying-to-extort.

[111] Boso, Ariel, "Thinking Beyond Spies at Twitter: Insider Threats Are A Growing Danger – And Can Come From Anyone," *CPO Magazine* (accessed 29 August 2022), https://www.cpomagazine.com/cyber-security/thinking-beyond-spies-at-twitter-insider-threats-are-a-growing-danger-and-can-come-from-anyone/

[112] "How to Mitigate Insider Threats: Strategies for Small Businesses," Crowdstrike (published on 26 October 2022), https://www.crowdstrike.com/solutions/small-business/mitigating-insider-threats/

company employees, there are increased opportunities for criminal organizations to seek out 'weak links' within companies to undertake extortion on their behalf.[113] In particular, criminal organizations will likely target individuals that are susceptible to blackmail and also have a large quantity of personal information available via social media. An example of this phenomenon occurred when the group Lapsus$, which had previously attacked Microsoft, Cisco, Nvidia and online authentication company Okta, relied on the recruitment of company insiders, to offer money to employees and key personnel who divulge credentials or other information needed to carry out attacks or breaches."[114]

Case Study: Extorting Employer

Lillian Stephens has been working as an administrative coordinator at Nails Inc. for the past ten years. Lillian has begun to feel that her commitment to the company is underappreciated. She is also going through an acrimonious divorce from her partner. In addition, in her role as administrative coordinator Lillian has access to her employer's email inbox. She chances by an email discussing her future with the company. Realizing that she will likely be let go in the coming weeks Lillian begins to more frequently access and manipulate her company's payroll files which is she is responsible for administering to ensure all staff receives bi-weekly pay. During the next pay period, several members of Nails Inc.'s management do not receive their pay cheques. Lillian is questioned about this and informs her superiors that she has changed the administrative passwords to the payroll software and will not release the weekly pay cheques unless her future at the company is guaranteed or she is given a year and half worth of severance pay.

Case Study: Extorted by Criminals

Matthew Howl has been working in IT security for Buddy's Construction Services, a leading construction company in Chicago, USA, for the last eight years. He is proud of his job and frequently updates his LinkedIn with pictures of his team, office renovations and other personal details. Three weeks ago, Matthew becomes the target of a cybercriminal organization that is seeking to disrupt the American construction supply chain. With the quantity of personal information about Matthew available to the organization, they succeed in pressuring him to grant them entry into Buddy's Construction Services' system.

Matthew begins working unusual hours, often leaving the office much later than any other member of his team. Additionally, he has started suggesting numerous changes to the company's IT security system. Finally, it is clear that Matthew is increasingly stressed about making the proposed IT changes as quickly as possible and demonstrates frustration whenever questioned about them arise. After several weeks of abnormal behaviour, Buddy's Construction Services experiences a distributed denial-of-service attack. Around this time, Matthew's lifestyle seemingly and significantly improves.

[113] Boso, "Thinking Beyond Spies at Twitter: Insider Threats Are a Growing Danger — And Can Come From Anyone," https://www.cpomagazine.com/cyber-security/thinking-beyond-spies-at-twitter-insider-threats-are-a-growing-danger-and-can-come-from-anyone/
[114] Ibid.

Indicators	Description	Observables	Data Sources
Stress	Employee appears to be under physical, mental or emotional strain or tension that he/she has difficulty handling.	Struggling to complete daily tasks / panic attacks.	HR Records
Abnormal/unnecessary software downloads	Employee appears to be downloading video conferencing services that are not used by the team or demonstrates a strong desire or disdain towards updating existing computer software.	Spending increased time on laptop, restarting computer numerous times a day due to downloads.	Web Proxy Logs VPN Remote Access
Increased manipulation of data	Employee is spending more time moving, changing, or deleting company files and documents.	Spending an increased time period on laptop or computer.	Web Proxy Logs.
Working odd hours	Employee is spending more time moving, changing, or deleting company files and documents.	Spending an increased time period on laptop or computer.	Web Proxy Logs
Criminal Record	Battery/assault records	Battery/assault records	HR Records Criminal Record Background Check
Decline in Job Performance	Employee has received corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance	Frequent mistakes, not following a job through, unable to cope with instructions given. Inability to cope with a reasonable volume of work and to meet deadlines.	Employee performance management system/Performance Evaluation HR Records

Measurements and Findings

It is crucial to quantify the behavioural indicators to identify potential insider threats. Organizations may utilize the measurements describe in **Table 1** to issue alerts of cases that merit further attention.[115] Moreover, organizations should determine their threshold in identifying behaviours or incidents that are deemed abnormal or statistical outliers. It is important to note that having a baseline comparing normal user behaviours against unusual behaviours enables organizations to effectively predict and identify potential insider threats[116]. One potential challenge in creating a baseline is the lack of data of known incidents[117].

TABLE 1: Measurements for Behavioural Indicators

Insider Type	# of bytes of downloads on company assets	# of bytes uploaded to external websites or programs	# of attempts to access blocked files, database or websites	Increase in downloading or uploading large volumes of data	Sizeable and unexplained change in credit rating	# of unexplained absence, Internet Web surfing and HR complaints	# of times access card and/or VPN are used outside work hours	Key words found in emails and internal chat channels
Cyber	✓	✓	✓	✓		✓	✓	✓
Violence	✓	✓	✓	✓		✓	✓	✓
Fraud	✓	✓	✓	✓	✓	✓	✓	✓
Extortion	✓	✓	✓	✓			✓	

Overall Findings

Overall, our research of specific insider threats demonstrated some cross-cutting behavioural indicators and measures that can be of value to VigilantCS' framework. The only indicators that were present in all the insider threat types *was declining performance* and *working odd hours*. Secondary cross-cutting indicators noted in at least three of the insider threat types includes: *substance abuse/misuse*, *absenteeism*, *disgruntlement*, and *stress*.

[115] Brown, David P. et al., "Improving Insider Threat Detection Through Multi-Modelling/Data Fusion," *Procedia Computer Science* 153 (2019), 100-107; Bishop, Matt et al., "AZALIA: An A to Z Assessment of the Likelihood of Insider Attack," *IEEE Conference on Technologies for Homeland Security* (2009), 385-392

[116] Mills et al., "Predict Insider Threats Using Human Behaviors," 40

[117] Roy Sarkar, Kuheli, "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures," *Information Security Technical Report* 15 (3) (2010), 113

TABLE 2: Cross Cutting Behavioural Indicators

Insider Type	Decline in job performance	Working odd hours	Substance abuse/misuse	Absenteeism	Disgruntlement	Stress
Cyber	✓	✓	✓	✓	✓	
Violence	✓	✓	✓	✓	✓	✓
Fraud	✓	✓	✓	✓	✓	✓
Extortion	✓	✓				✓

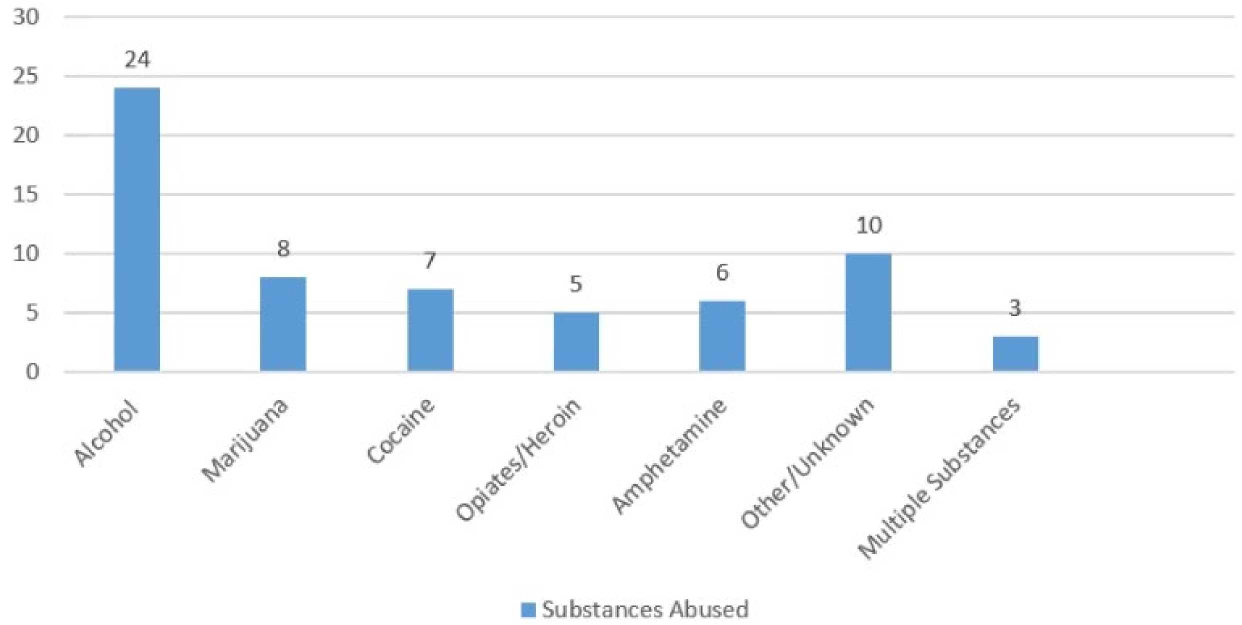
The human resources information system serves as an important data source to help detect, prevent and mitigate potential insider threats. The system collects, maintains and reports employees' background investigations, personal references, requests for personal, medical, and other leaves, education level, life events, attendance records, performance evaluations, legal issues (i.e., garnished wages), disciplinary issues, complaints by or against the employee and employment applications (includes background check, references, education and work history)."[118]

One notable finding of our research is that the utilization and abuse of substances, such as alcohol and drugs by insiders has risen since 2010. As per the CERT National Insider Threat Center's Insider Corpus, "there has been an increase from 1.1 insider cases involving substance abuse per year in the 20 years leading up to 2009 to an average of 4.4 cases per year from 2010 to 2016."[119] As seen below, **Figure 3** shows the prevalence of substance use or abuse from 1996 to 2016.

[118] Bishop, Matt et al., "AZALIA: An A to Z Assessment of the Likelihood of Insider Attack," *IEEE Conference on Technologies for Homeland Security* (2009), 389

[119] Cassidy et al., "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

Figure 3: Substances Used or Abused (Insider Incidents 1999-2016)



Source: Tracy Cassidy and CERT Insider Threat Center, 2018

The finding demonstrates that organizations should explore alternative corporate social programs that would support employees facing issues relating to substance abuse, which are not captured in network monitoring systems or IT solutions. Some alternative solutions, which are outlined in the CERT Common Sense Guide for Mitigating Insider Threats Fifth Edition,[120] include utilizing employee assistance programs (EAPs), educating employees on recognizing substance use and abuse disorders, and providing a supportive work environment to those suffering from substance abuse issues to aid in their recovery process.

Further Considerations

The key gaps and limitations of this research project include: representation, data disaggregation and the ethics associated with privacy of employees.

Representation

Throughout the literature review, it was evident that the vast majority of sources that discussed insider threats and their related behaviours were predominantly from the financial service sector. As a result, there are limitations in the existing available research. Since the individuals surveyed in the existing research were primarily employed in the financial services sector, existing data was biased towards explaining the behaviours of one demographic, namely white male employees.

[120] Carnegie Mellon University Software Engineering Institute, "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," *CERT National Insider Threat Center* (2016), 38, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Conversely, however, the Canadian Banking Association reported that in 2021, between 39.5% and 48.6% of senior and middle management positions, respectively, in the banking industry were held by women.[121] Additionally, visible minorities held 22.5% of all senior management positions, 37.7% held middle management jobs, and 43% held all professional positions.[122] This bias in the data significantly limits the scope of the conclusions that can be drawn from existing data and further studies must account for the demographic differences that make up each respective sector in which insider threats are actively being studied on, especially the public security sector.

Data Disaggregation

A second limitation of this research project is that many of the proposed behavioural indicators of an insider risk can go unnoticed due to data disaggregation in the workplace. Our research has demonstrated a wide variety of data points to assess an enterprise's overall risk profile, however many of these sources contain information that is not easily obtained. Bureaucratic hurdles will almost certainly block the sharing of certain types of information about an employee's behavioural changes between human resources and an individual's own team. These types of highly private information could include health and medical information related to an employee. For example, if HR is aware that an employee is required to change their hours due to ongoing cancer treatments they are receiving, HR may not be allowed disclose this private information without the consent of the employee. In this scenario, privileged personal information is rightfully protected by law, as is the employee. However, in an alternative scenario, human resources could be informed by an employee that they are experiencing substance abuse problems and are struggling to complete their daily work commitments. In this scenario, the employee is demonstrating behaviours that could be or become indicative of an insider threat. Yet, human resources is also legally obligated to protect this individual's health information in this case, too, and would be unable to act based on knowledge of potentially problematic behaviour.

Alternatively, information of a potential insider simply may not be proactively shared by employees with management for a variety of reasons. These reasons could include colleagues fearing reputational harm among their peers reporting inappropriate behaviour or even uncertainty related to the extent to which a behaviour is a problem. As such, many employees could be aware of the threat of an insider and simply never raise the alarm.

Ethics

Finally, several ethical considerations must be considered when proposing an insider risk management framework which, for all intents and purposes, engages in monitoring or surveillance of employees on the job.

Notably the behaviours indicative of an insider threat can also be demonstrated by employees for a myriad of other reasons. While an employee's odd behaviours may be similar to that of an insider threat, it is also possible that they are exhibiting the behaviour for other reasons, such as a change

[121] "Focus: Representation of Women at Banks in Canada," *Canadian Bankers Association* (published 7 March 2023), https://cba.ca/representation-of-women-at-banks-in-canada

[122] "Focus: Banks as Employers," *Canadian Bankers Association* (published 13 March 2023), https://cba.ca/banks-as-employers-in-canada

in medication, new personal preferences, or new job responsibilities. Given the evolving professional accommodations being granted to employees in light of the COVID-19 pandemic and remote work, employees may experience difficult adjustments period or may be simply receiving a workplan better suited to their needs. These scenarios are ambiguous in nature, therefore individual employees need to be awarded a fair and due process to explain their actions. Furthermore, individual privacy would be breached if an individual is unnecessarily or unjustly monitored by their employer in order to ensure that they are not or will not become an insider threat. Alternatively, it is possible that the individual is demonstrating behaviours that resemble insider threat behaviour but hold no malicious intent. For example, if an individual has become disgruntled, they may act out in the workplace without ever crossing the threshold of becoming an insider threat. The extent to which initial problematic behaviour warrant monitoring continues to remain ambiguous and unclear to this day.

Finally, some individuals may simply express or conduct themselves in a manner that some would think is consistent with an insider threat. Conventional notions of personal conduct are, at times subjective, therefore human resources and insider risk management practitioners should be aware that people can still behave in "unusual ways", yet still be employed as productive, ethical members of a company or government agency.

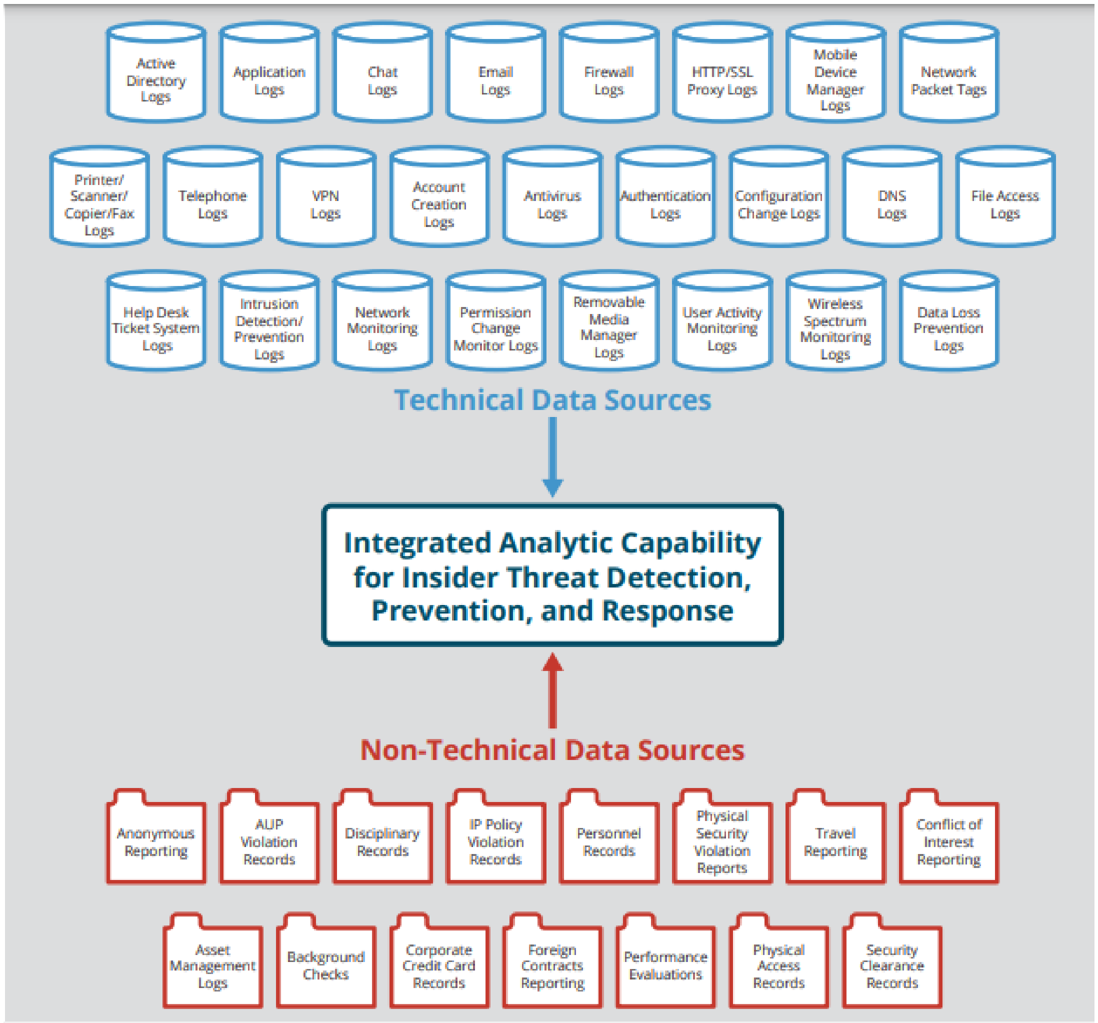
These ethical concerns present an opportunity for future thinking and consideration by VigilantCS to ensure that insiders are proactively identified while respecting privacy and differences.

Conclusion

In summary, this research paper sought to support VigilantCS in their development of a behavioural algorithm to proactively assess insider threat. As such, a literature review was conducted by the research team to identify behavioural indicators that have a strong correlation to insider threat, particularly cybersecurity, workplace violence, fraud and extortion. The literature showed that perpetrators share similar patterns of insider threat behaviours, and insider attacks can be triggered by stressors (personal, professional and financial issues). The research paper highlighted five cross cutting behavioural indicators, namely decline in job performance, working odd hours, substance abuse/misuse, absenteeism, disgruntlement and stress. A data dictionary was created to capture key behavioural indicators associated with different types of insiders. However, there are some gaps worth noting such as the representation in data, the possibility of data disaggregation and the ethical dilemma of employee monitoring.

Appendix

Figure 1: Recommended Data Sources for Insider Threats Analysis


Active Directory Logs
Application Logs
Chat Logs
Email Logs
Firewall Logs
HTTP/SSL Proxy Logs
Mobile Device Manager Logs
Network Packet Tags
Printer/ Scanner/ Copier/Fax Logs
Telephone Logs
VPN Logs
Account Creation Logs
Antivirus Logs
Authentication Logs
Configuration Change Logs
DNS Logs
File Access Logs
Help Desk Ticket System Logs
Intrusion Detection/ Prevention Logs
Network Monitoring Logs
Permission Change Monitor Logs
Removable Media Manager Logs
User Activity Monitoring Logs
Wireless Spectrum Monitoring Logs
Data Loss Prevention Logs
Technical Data Sources
Integrated Analytic Capability for Insider Threat Detection, Prevention, and Response
Non-Technical Data Sources
Anonymous Reporting
AUP Violation Records
Disciplinary Records
IP Policy Violation Records
Personnel Records
Physical Security Violation Reports
Travel Reporting
Conflict of Interest Reporting
Asset Management Logs
Background Checks
Corporate Credit Card Records
Foreign Contracts Reporting
Performance Evaluations
Physical Access Records
Security Clearance Records

Source: Carnegie Mellon Common Sense Guide 7th Edition, 2022

Figure 2: Data Dictionary

Indicators	Description	Observable Behaviours	Data sources
Substance Abuse and Misuse	Use of or involvement with alcohol, illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants	Changes in hygiene or professional appearance (wearing dirty clothes and smelly odor). Employees' eyes might be watery, bloodshot, or glassy. Employees might act	HR Records Monitor badge records for tardiness, absences during

		hostile, angry, paranoid, or fearful for no reason. Employees’ speech sounds slurred or incoherent[123].	the day, and missed work[124] Background Check (substance related arrests (i.e., DUI)[125])
Rule Violation	Unwillingness to comply with rules and regulations, or to cooperate with security requirements. Employees feel above the rules or that they only apply to others.[126]	Recurrent mishandling of classified information (e.g., attempts to take classified documents home from work)	Virtual Private Network Log Printer/Scanner/ Copier/Fax Logs Authentication Logs[127]
Disgruntlement	Employees observed to be dissatisfied in their current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with their current job.[128]	Difficulty collaborating with colleagues and/or lashing out verbally or electronically to management and/or coworkers.	Email logs Chat logs[129]
Aggressive or Violent	Employees exhibit argumentative or aggressive behavior or are involved	Shouting and swearing at coworkers, as well as hitting,	HR Records

[123] McGuinness, “6 Signs Your Employees May Be Abusing Drugs.” https://www.surehire.com/6-signs-your-employees-may-be-abusing-drugs/

[124] Cassidy, “Substance Use and Abuse: Potential Insider Threat Implications for Organizations,” https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organization

[125] Ibid.

[126] Crespo, “Insider Threats: Five Indicators of Risk & What to Do,” https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

[127] Ogonji, “Modeling and Simulating Insider Cyber Security Threats,” 10 http://erepository.uonbi.ac.ke/bitstream/handle/11295/63350/Ogonji_Cyber%20security%20threats.pdf?sequence=3&isAllowed=y%20(all%20the%20way%20to%20absence)

[128] Ogonji, “Modeling and Simulating Insider Cyber Security Threats,” 25 http://erepository.uonbi.ac.ke/bitstream/handle/11295/63350/Ogonji_Cyber%20security%20threats.pdf?sequence=3&isAllowed=y%20(all%20the%20way%20to%20absence)

[129] United States Department of Defense, *“Insider Threat Indicators - Behaviors of Concern,”* https://www.nationalinsiderthreatsig.org/itrmresources/Behavioral%20Indicators%20Of%20Concern%20For%20Insider%20Threat%20Programs%20-%20Part%201.pdf

Behavior	in bullying or intimidation.	kicking, biting, and pushing	
Absenteeism	Employee has exhibited chronic unexplained absenteeism.	Frequent absences or unexplained disappearances from a desk[130] (e.i. excessive breaks and vacations/travel, late starts, long lunch breaks[131])	HR Records Travel reporting Monitor badge records for tardiness, absences during the day, and missed work[132]
Working Odd Hours	Accessing the premises outside of normal hours with or without justified authorization[133]	User with a high number of system logins during unusual hours such as midnight or during weekends without any specific work related reasons[134]	Monitor Badge Records VPN Remote Access
Decline in job performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.	Frequent mistakes, not following a job through, unable to cope with instructions given. Inability to cope with a reasonable volume of work and to meet deadlines	Employee performance management system/Performance Evaluation
Sudden, unexplained change in financial circumstances	Employee appears to demonstrate an unexplained, substantial improvement in their lifestyle beyond what their current job salary can afford.	Living beyond one's financial means or suffering from acute financial distress.[135]	Background Checks Credit Inquiries

[130] Weast, "Disgruntled Employee Suddenly Quits South Florida Business How to Protect Your Company from Insider Threats," https://www.ecwcomputers.com/disgruntled-employee/

[131] *"How To Recognize And Handle A Disgruntled Employee | 10 Steps,"* SLING, https://getsling.com/blog/disgruntled-employee/

[132] Cassidy et al., *"Substance Use and Abuse: Potential Insider Threat Implications for Organizations,"* https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organization

[133] Crespo, "Insider Threats: Five Indicators of Risk & What to Do," https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

[134] Mills, "Predict Insider Threats Using Behaviors," 40

[135] *"2020 Global Study on Occupational Fraud and Abuse."* Association of Certified Fraud Examiners, 1-2, https://legacy.acfe.com/report-to-the-nations/2020/docs/infographic-pdfs/Behavioral%20Red%20Flags%20of%20Fraud.pdf

Abuse of access privileges	Employee observed trying to circumvent internal IT controls to gain unauthorized access to specific files.	Attempt to coerce colleagues with appropriate access privileges to access files on employee's behalf.	Employee Badge Records HR Records Internal IT Records Email and Chat Logs
Unusually close association with clients or partners[136]	Employee observed to be unusually close to external clients, vendors or partners.	Demonstrates irritability and defensiveness among colleagues, continuous engagement with clients or partners beyond professional expectations.[137]	Email and Chat Logs Job Satisfaction Surveys From Clients
Suspiciousness[138]	Employee observed to be constantly apprehensive of inquiries from colleagues or management.	Maintaining strict secrecy over projects, controlling demeanour, refusal to take vacations out of fear of being caught.	Performance Evaluations HR Records Email and Chat Logs
Stress	Employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.	Struggling to complete daily task/panic attacks	HR Records
History of Violence	Employee has a repeated history of violence inside and outside the workplace	Battery/assault arrest records[139]	Criminal Records Check
Concerning Web searches	Employee is accessing blocked Websites	Visiting restricted Websites and darknet sites[140]	Web Proxy Logs

[136] Ibid.
[137] Ibid.
[138] Ibid.
[139] Cassidy et al., "Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies," 6, https://apps.dtic.mil/sti/pdfs/AD1090846.pdf
[140] Ibid.

Abnormal/unnecessary software downloads	Employee appears to be downloading video conferencing services that are not used by team or demonstrates al strong desire or disdain towards updating existing computer software	Spending increased time on laptop, restarting computer numerous times a day due to downloads	Web Proxy Logs VPN Remote Access

Bibliography

"About Us," *Vigilant CS* (accessed 26 April 2023), VigilantCS, https://vigilantcs.com/about/

Agrafiotis, Ioannis et al., "Identifying Attack Patterns for Insider Threat Detection," *Computer Fraud and Security* 2015 (7) (2015), 10

Bailey, Tucker et al., "Insider Threat: The Human Element of Cyberrisk." *McKinsey & Company* (published on 24 September 2018), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk.

Bell, Alison J.C. et al., "The Insider Threat: Behavioral Indicators and Factors Influencing Likelihood of Intervention." *International Journal for Critical Infrastructure Protection* 24 (2019): 167

Berlingieri, Adriana et al., "Harassment and Violence in Canadian Workplaces: It's [Not] Part of the Job," *Centre for Research and Education on Violence Against Women and Children* (2022), 6, https://documents.clcctc.ca/human-rights/Respect-at-Work-Report-EN.pdf

Bishop, Matt et al., "AZALIA: An A to Z Assessment of the Likelihood of Insider Attack," *IEEE Conference on Technologies for Homeland Security* (2009), 385-392

Blackwell, Clive, "The Insider Threat: Combatting the Enemy Within," *IT Governance Publishing* (2009): 8

Boso, Ariel, "Thinking Beyond Spies at Twitter: Insider Threats Are A Growing Danger – And Can Come From Anyone," *CPO Magazine* (accessed 29 August 2022), https://www.cpomagazine.com/cyber-security/thinking-beyond-spies-at-twitter-insider-threats-are-a-growing-danger-and-can-come-from-anyone/

Briney, Andy, "2001 Information Security Industry Survey," *Information Security Magazine* (published October 2001), http://lfca.net/Reference%20Documents/2001%20Information%20Security%20Survey.pdf

Brown, David P. et al., "Improving Insider Threat Detection Through Multi-Modelling/Data Fusion," *Procedia Computer Science* 153 (2019), 100-107

Carnegie Mellon University Software Engineering Institute, "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," *CERT National Insider Threat Center* (2016), 38, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Cassidy, Tracy and the CERT Insider Threat Center. "Substance Use and Abuse: Potential Insider Threat Implications for Organizations," *Carnegie Mellon University Software Engineering Institute Blog* (published 12 April 2018), https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

Cassidy, Tracy et al., “Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies,” *Carnegie Mellon University Software Engineering Institute* (2018), 2, 6 https://apps.dtic.mil/sti/pdfs/AD1090846.pdf

Cassidy, Tracy et al., “Technical Detection of Intended Violence: Workplace Violence as an Insider Threat,” *Carnegie Mellon University Software Engineering Institute* (2017), https://insights.sei.cmu.edu/blog/technical-detection-of-intended-violence-workplace-violence-as-an-insider-threat/?_gl=1*1573q87*_ga*MzU0NTMyOTIx%20LjE2NzcxMDMyMTc.*_ga_87WECW6HCS*MTY3NzEwMzIxNi4xLjEuMTY3NzEwMzI5MS4wLjAuMA

Chief of Police, Ottawa Police Service, “Positive Workplace: 2020 Annual Report,” *Ottawa Police Services Board*, (2021), 5, https://pub-ottawa.escribemeetings.com/filestream.ashx?documentid=21298

“Common Sense Guide to Mitigating Insider Threats, Seventh Edition,” *Carnegie Mellon University Software Engineering Institute* (2022), iv, 3, 98 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=886874

Cole, Ben, and Francesca Sales. “What Is Conduct Risk?: Definition from TechTarget.” *TechTarget* (published on 21 December 2016), https://www.techtarget.com/searchcio/definition/conduct-risk.

Crespo, Conrado. “Insider Threats: Five Indicators of Risk and What To Do,” *CounterCraft* (accessed 29 April 2023), https://www.countercraftsec.com/blog/insider-threats-five-indicators-of-risk-and-what-to-do/

Criminal Code of Canada, “Extortion,” *Justice Laws Website* (accessed 28 April 2023), https://laws-lois.justice.gc.ca/eng/acts/c-46/section-346.html

“Defining Insider Threats.” *United States Cybersecurity and Infrastructure Security Agency* (accessed 29 April 2023). https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Devlin, Frank, “Mitigating Conduct Risk To Preserve and Improve Reputation.” *The RMA Journal* 101 (8) (2019): 2.

“Focus: Banks as Employers,” *Canadian Bankers Association* (published 13 March 2023), https://cba.ca/banks-as-employers-in-canada

“Focus: Representation of Women at Banks in Canada,” *Canadian Bankers Association* (published 7 March 2023), https://cba.ca/representation-of-women-at-banks-in-canada

Froehlich, Andrew. “What Is An Insider Threat?” *TechTarget* (accessed 29 April 2023). https://www.techtarget.com/searchsecurity/definition/insider-threat

Gheyas, Iffat A. and Ali E. Abdallah., "Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis." *Big Data Analytics* 1 (1) (2016): 1, 5

Government of Canada, *"Is It Harassment? A Tool to Guide Employees,"* Government of Canada, 2015;

Government of Quebec, "Forms of Violence," (accessed 10 April 2023), https://www.quebec.ca/en/family-and-support-for-individuals/violence/forms-violence.

Greitzer, Frank L. et al., "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis," *E-Service Journal* 9 (1) (2013): 109

"How to Mitigate Insider Threats: Strategies for Small Businesses," *Crowdstrike* (published on 26 October 2022), https://www.crowdstrike.com/solutions/small-business/mitigating-insider-threats/

"How To Recognize And Handle A Disgruntled Employee | 10 Steps," *GetSling* (accessed 29 April 2023), https://getsling.com/blog/disgruntled-employee/

Huang, Shaio Yan et al., "Fraud Detection Using Fraud Triangle Risk Factors," *Information Systems Frontiers* 19 (2017), 1344

Is CyberSecurity A Promising Career?" *University of Tulsa* (published on 7 February 2022), https://cybersecurityonline.utulsa.edu/blog/is-cybersecurity-a-promising-career/#:~:text=The%20crux%20of%20the%20matter,against%20%20devices%2C%20data%20and%20networks

"Introduction to Fraud Indicators," *Fraud Advisory Panel* (published on 14 November 2011), 1 https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-14B-Fraud-Indicators-Nov11.pdf

Kelly, Jack. "Wells Fargo Forced to Pay $3 Billion For The Bank's Fake Account Scandal." *Forbes* (2020). https://www.forbes.com/sites/jackkelly/2020/02/24/wells-fargo-forced-to-pay-3-billion-for-the-banks-fake-account-scandal/?sh=557d30c042d2

Koshy, Sunita et al., "Conduct Risk Management and Ethical Culture." *SIFMA Compliance and Legal Conference* (2020), 5, https://www.sifma.org/wp-content/uploads/2020/03/MB3-NEW-Conduct-Risk-Management-and-Ethical-Culture.pdf

"MB-3: New: Conduct Risk Management and Ethical Culture." *Securities and Financial Markets Association* (accessed on 27 April 2023): 3. https://www.sifma.org/wp-content/uploads/2020/03/MB3-NEW-Conduct-Risk-Management-and-Ethical-Culture.pdf:

McGuinness, Elly. “6 Signs Your Employees May Be Abusing Drugs,” *SureHire Occupational Testing* (published 31 May 2022), https://www.surehire.com/6-signs-your-employees-may-be-abusing-drugs/

Mills, Jennifer U. et al., “Predict Insider Threats Using Human Behaviors,” *IEEE Engineering Management Review* 45 (1) (2017), 40

Mott, Nathaniel, “Former Ubiquiti Dev Arrested for Orchestrating Data Breach, Trying To Extort $2M,” *PC Magazine* (published 2 December 2021), https://www.pcmag.com/news/former-ubiquiti-dev-arrested-for-orchestrating-data-breach-trying-to-extort.

“Occupational Fraud 2022: A Report to the Nations.” *Assocation of Certified Fraud Examiners* (accessed 26 April 2023), https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

Ogonji, Mark Mbock. “A Modeling and Simulating Insider Cyber Security Threats Using Psychosocial Factors,” *University of Nairobi School of Computing and Informatics* (2013), 9-10, 25.
http://erepository.uonbi.ac.ke/bitstream/handle/11295/63350/Ogonji_Cyber%20security%20threats.pdf?sequence=3&isAllowed=y%20(all%20the%20way%20to%20absence)

Pfleeger, Shari Lawrence and Deanna D. Caputo., *“*Leveraging Behavioral Science to Mitigate Cyber Security Risk,*” Computers & Security* 31 (2012): 597

PricewaterhouseCoopers and Microsoft, *“Starting an Insider Risk Management Program,”* (accessed 25 April 2023). https://download.microsoft.com/download/b/2/0/b208282a-2482-4986-ba07-15a9b9286df0/pwc-starting-an-insider-risk-management-program-with-pwc-and-microsoft.pdf

Roy Sarkar, Kuheli, “Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures,” *Information Security Technical Report* 15 (3) (2010), 113

Rugala, Eugene A. et al., “Workplace Violence Issues in Response,” *Critical Incident Response Group National Center For The Analysis of Violent Crime* (accessed 29 April 2023), https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view

Carleton University-NPSIA Student and al., 2023

Shaw, Eric and Laura Sellers. “Application of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence* 59 (2) (2015): 2-3
https://nationalinsiderthreatsig.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf

Silaule, Carol B. et al., “A Model to Reduce Insider Cybersecurity Threats in a South African Telecommunications Compay,” *South African Journal of Information Management* 24 (1) (2022), 1

Sullivan, Peter. “How Insider Fraud Can Be Detected and Avoided in the Enterprise.” *TechTarget*, September 2018. https://www.techtarget.com/searchsecurity/tip/How-insider-fraud-can-be-detected-and-avoided-in-the-enterprise

“The Culture of Risk: The Importance of Managing Conduct Risk and Maintaining An Effective Risk Culture Across The Business.” *Deloitte* (2016): 3. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-conduct-risk-pov-noexp.pdf

Tayan, Brian. “The Wells Fargo Cross-Selling Scandal.” *Harvard Law School Forum on Corporate Governance* (2019). https://corpgov.law.harvard.edu/2019/02/06/the-wells-fargo-cross-selling-scandal-2/

Thompson, Eleanor E, “The Insider Threat: Assessment and Mitigation of Risks (1st ed.),” *Auerbach Publications*: 14-15

United States Department of Defense, “Insider Threat Indicators,” *National Insider Threat Special Interest Group* (accessed 29 April 2023), https://www.nationalinsiderthreatsig.org/itrmresources/Behavioral%20Indicators%20Of%20Concern%20For%20Insider%20Threat%20Programs%20-%20Part%201.pdf

“What Are Insider Threats?” *International Business Machines* (accessed 28 April 2023). https://www.ibm.com/topics/insider-threats?utm_content=SRCWW&p1=Search&p4=43700067188221065&p5=e&gclid=CjwKCAjwo7iiBhAEEiwAsIxQEa_yoUGM8zx_IWIanTB-wkiEjpUnW0GnYtcBJw36rHeNAgvJIH1llxoC8F0QAvD_BwE&gclsrc=aw.ds

Waters, Shonna, “Feeling Uneasy? Here’s What Workplace Coercion Looks Like,” *BetterUp* (2021), https://www.linkedin.com/pulse/employee-blackmail-c-j-westrick-sphr/?trk=pulse-article_more-articles_related-content-card

Weast, Eric, “Disgruntled Employee Suddenly Quits South Florida Business,” *ECW Network and IT Solutions* (accessed 29 April 2023), https://www.ecwcomputers.com/disgruntled-employee/

Wilner, Alex, “INAF 5254 – Capstone in Canadian Security Policy Course Outline,” *Brightspace* (accessed 29 April 2023), 1, https://brightspace.carleton.ca/d2l/le/content/132851/Home

Wilson, Mark et al., “Information Technology Security Training Requirements: A Role and Performance-Based Model, Special Publication (NIST SP),” *National Institute of Standards and Technology* (1998), 25, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151633