

“The pull to do nothing would be strong”: limitations & opportunities in reporting insider threats

Heather Holden, Victor Munro, Lina Tsakiris & Alex Wilner

To cite this article: Heather Holden, Victor Munro, Lina Tsakiris & Alex Wilner (2025) “The pull to do nothing would be strong”: limitations & opportunities in reporting insider threats, Information Security Journal: A Global Perspective, 34:1, 63-78, DOI: [10.1080/19393555.2024.2387347](https://doi.org/10.1080/19393555.2024.2387347)

To link to this article: <https://doi.org/10.1080/19393555.2024.2387347>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 10 Aug 2024.



Submit your article to this journal [↗](#)



Article views: 1166



View related articles [↗](#)



View Crossmark data [↗](#)

“The pull to do nothing would be strong”: limitations & opportunities in reporting insider threats

Heather Holden ^a, Victor Munro ^b, Lina Tsakiris^a, and Alex Wilner ^b

^aInfrastructure Protection and International Security program, Carleton University, Ottawa, Canada; ^bNorman Paterson School of International Affairs, Carleton University, Ottawa, Canada

ABSTRACT

Though a reporting mechanism, in which employees report suspicious and/or potentially malicious coworker behavior, is thought to be important to tackling insider risk, the literature on the subject is sparse and unconvincing. Empirical evidence of the actual use and utility of this type of detection mechanism is slim. Our article explores the propensity of employees to report a coworker's concerning behavior suspected to be related to insider activity that would negatively impact an organization. This study uses an inductive approach and qualitative analysis of original interview data collected from 16 financial services organizations to explore attitudes and opinions about reporting a coworker's concerning behavior, providing lessons on countering insider threats useful across industries and national security domains. The results show that there is confusion, uncertainty, and cognitive dissonance surrounding institutional reporting mechanisms, with some participants expressing both affirmative and negative opinions about their personal likelihood of reporting. Employees do want to report concerning coworker behavior that suggests an insider threat, but not at their own expense. These results are consistent with those from other studies and sectors. Our study will assist organizations in refining their assumptions around workforce attitudes regarding the reporting of coworkers.

KEYWORDS



Detection; employee reporting mechanisms; insider risk; insider threat; security-conscious culture

1. Insider threat reporting: a primer

To manage insider risks a range of national security and intelligence organizations recommend the use of reporting mechanisms to encourage employees to report the concerning behavior of their coworkers. Often the process is pitched as an *early warning detection tool* that helps “engage the workforce” (CERT National Insider Threat Task Force, 2016), facilitates an “upward flow of insider-relevant information from the workforce” (National Counterintelligence and Security Center NCSC, 2021), and enables a “people as sensors” approach to countering insider threats (Cybersecurity and Infrastructure Security Agency CISA, 2020). The early warning provided by employees via reporting mechanisms is expected to help detect and identify current and future insider threats, lessen the consequences of related malicious events by shortening the duration of the unwanted activity, and provide

elements of general deterrence (CERT National Insider Threat Center, 2018).

Unfortunately, empirical evidence of the actual use and utility of this type of detection mechanism is slim. The international literature that does exist paints an inconclusive picture. For instance, in a 2018 study published by the Conference Board of Canada, when asked whether employees would report an insider threat, only 38% of Canadian executives from the private, public, and not-for-profit sectors said that “most would report” malicious or suspicious behavior. That figure was down significantly from 66% answering the same question during a similar 2012 study (Conference Board of Canada CBC, 2018). The decrease in certainty about whether employees would report a potential insider threat caused the Conference Board of Canada to conclude that their findings merit closer and repeated investigation; in particular, they ask whether organizations lack clear reporting mechanisms and/or whether employees receive sufficient ongoing training about how to

CONTACT Alex Wilner  alex.wilner@carleton.ca  Norman Paterson School of International Affairs, Carleton University, 5306 Richcraft Hall, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

recognize concerning behavior suggestive of insider threats. In the UK, Alison Bell and colleagues investigated the likelihood that employees at a British energy company would report a coworker's change in behavior related to insider threat and, drawing on insights from the bystander effect, conducted an online survey for which they received 55 responses to questions based on four scenarios (Bell et al., 2019). Their 2019 British study reached a similar conclusion as the Conference Board of Canada: employees are unlikely to report a change in behavior of a potential insider threat unless they held an undefined amount of sufficient evidence. And in the United States, Randazzo and colleagues examined cases of insider-initiated incidents and conducted interviews asking about detection of the incident and identification of the insider; the authors concluded that incidents were detected by various methods, with little consistency found as to who or how exactly insiders were detected (Randazzo et al., 2005).

With so few empirical studies exploring the subject of insider risk reporting, our study aims to analyze and assess individual *intentions* to report a colleague's or coworker's concerning behavior with regards to insider threats. Our study uses a sample drawn from Canada's financial institutions as a backdrop. Canada's six largest banks have all adopted reporting mechanisms following the guidance of the Financial Consumer Agency of Canada. The scope of these reporting programs is broad and encourages reporting of activity in conflict with the firms' Codes of Conduct, which include but go well beyond the theft or misuse of sensitive information. While the scope of these reporting programs thus include more than just insider risk and information security, Canadian financial institutions are relying on their employees to use reporting mechanisms to help report concerning behavior *indicative* of current or future insider risk. Our empirical approach is explorative: we analyze data from 19 interviews conducted with 16 different financial services organizations, exploring attitudes and opinions about reporting a coworker's concerning or suspicious behavior. The results of our study shed light on how organizations might refine their assumptions around workforce attitudes regarding the reporting of coworkers.

Our paper is structured in four sections. Section one provides a concise summary of the literature

on insider risk reporting, followed by a synopsis of our study's methodology and data collection. In section two we provide a detailed summary of our results, broken down into four subsections grouped according to whether and under what conditions respondents would report a colleague's suspected misbehavior. Section three provides an interpretation of our empirical findings and a discussion of the specific recommendations some interviewees voluntarily provided based on their worldviews and experiences. The final section proposes next steps for the study of reporting insider threats, with a focus on developing theory and conceptual frameworks and producing empirically relevant findings.

2. Methodology – data collection: attitudes towards reporting co-workers

Insider risk is traditionally understood as malicious activity that negatively impacts the confidentiality, integrity, or availability of critical assets, including client information, by people considered to be insiders due to current or previous employment within the organization. Insider risk is expensive with respect to reputational, legal, and financial liability and damage (Jacqueline et al., 2016) and is likely to be more prevalent and common than generally assumed (Conference Board of Canada [CBC], 2018; Cybersecurity and Infrastructure Security Agency [CISA], 2020; Fortinet, 2019; Ponemon, 2020; Ponemon Institute and DTEX, 2021, 2021; Verizon, 2019, 2021).

Insider risk controls are usually complex in nature, and are approached from an interdisciplinary perspective that crosses traditional academic domains and fields, from social science and psychology to criminology, security studies, business management, computer science, cybersecurity, and network design (e.g., Bunn & Sagan, 2014; CISA, 2020; Hunker & Probst, 2008; Moore et al., 2015; Pereira & Santos, 2015; Pfleeger & Caputo, 2012; Prabhu & Thompson, 2022; Stubben & Welch, 2020). Within this diversity of response, a consistently recommended insider risk control approach includes the use of reporting mechanisms that encourages and incents employees to confidentially report the concerning or suspicious behavior of their coworkers. When used as an early

warning mechanism of insider risk, information provided by employees is thought to lessen the consequences of an insider risk event by shortening the duration of the damaging activity or by deterring suspicious behavior that could function as a precursor or gateway to an eventual and more meaningful insider risk event (CISA, 2020).

Functionally, reporting is a crucial mitigation component to countering insider threats that is largely based on and driven by behavioral indicators, which feature prominently within the literature and have been studied extensively across various insider threat types. Different types of insider risk behavior that have been the subject of academic study include the role of addiction (Maasbert and Beebe 2020), poor and/or declining job performance (Maasberg et al., 2020, trustworthiness (Ho et al., 2018), stress (Whitty, 2021), and interpersonal conflicts in the workplace (Maasberg et al., 2020). Different theories, frameworks, and methods, borrowed from a variety of academic disciplines (e.g., psychology, social-psychology, criminology, political science), have likewise been applied to help explore and explain these behavioral indicators of insider risk. The results include the generation of different typologies, like the “dark triad” of personality traits (including Machiavellianism, narcissism, and psychopathy) (Maasberg & Beebe, 2014); addiction theory in relation to risk taking (Maasberg & Beebe, 2014); signals detection theory in personal decision making under conditions of uncertainty (Mills et al., 2018); inductive criminal profiling based on probabilistic knowledge (Maasberg et al., 2020); and the bystander effect, which helps explain why colleagues and friends of a potential insider threat may be altogether less inclined to report suspicious activity (Bell et al., 2019).

Other organizational or bureaucratic approaches tap into the role strong personal bonds or security and protocol awareness have in determining the propensity of workers to report potentially malicious behavior. For illustration, in South Africa, Safa et al. (2018) conducted a study of active employees in the finance sector who were familiar with the importance of information security, that looked at organizational policy compliance based on situational crime prevention and social bond theories. The results of the study displayed that

increased commitment to one’s employment position or to the organization itself, reduced the likelihood of an adverse intention toward the organization. Moreover, involvement in information security activities (i.e., better security awareness), and a personal belief that information security misbehavior was negative and unacceptable, also significantly reduced the likelihood of potential insider threat intentions. These findings support a general premise that a reduction of the bystander effect and increased reporting of suspected insider threats, could result with enhanced organization bond and security awareness initiatives between the employer and employee.

Our study’s core objective is to empirically assess attitudes on insider risk reporting, as informed by the nascent literature on the subject. Based on detailed qualitative interview data, we gather the opinions and attitudes about the use and utility of reporting mechanisms for insider threat identification from a range of professionals working in Canada’s financial services sector. We conducted one-on-one, open-ended interviews with professionals with a range of seniority, experience level, and areas of expertise from several interrelated fields and departments, including information technology, compliance, legal, investment/brokerage, financial planning, security, and risk management. The perspectives of our interviewees are derived from personal experiences in the private and public sector, among large and small organizations. Interviewee responses will continue to be confidential and anonymous with no reference to name, institution, geography, or job title, as per a written Statement of Consent. Ethics approval was sought and received from Carleton University Research Ethics Board-A (CUREB-A), Project # 115552, Spring 2022.

Nineteen people from 16 Canadian institutions were interviewed individually throughout July and August of 2022. Interviews were conducted over the phone with one researcher; hand-written notes were taken. Each interview lasted approximately 30 minutes and consistently began with the interviewer providing a short overview of the project scope and baseline research question, which each interviewee had been previously introduced to in identical invitation letters. The structure then allowed each interviewee time to share thoughts,

scenarios, experiences, and generally allow their own ideas and memories to develop over the remaining time left on the interview call.

The qualitative analysis in this study completes the first three of the typical four stages of continual Grounded Theory Analysis, which can be understood as:

- (1) Create a general overarching research question about the population (*Do employees report a co-worker's concerning activity at Canadian financial institutions?*)
- (2) Interview a small sample of the population to understand their attitudes and opinions on the research question.
- (3) Analyze the data collected with an open mind to let the data speak for itself and to see if hypotheses emerge.
- (4) Conduct future studies based on different population samples, sizes, and methodologies to test whether hypotheses hold true; as the process continues, the theory develops.

With the premise that interviewees have informed and thoughtful ideas to share on this complex topic, interview questions were open-ended, probing, and conversational. A limitation of this approach is that interviews did not follow a consistent structure. To mitigate this potential problem, several core questions were consistently asked to anchor the interviews to one another; a consistent introduction was likewise provided to set the context. Another limitation relates to our relatively small sample size; opinions may not be representative of the population from which they were sampled. Our population was likewise sampled using practical methods, including personal connections, networking, and referrals. While these connections did provide us with better access to interviewees, thus broadening our sample size, they might have otherwise introduced selection bias into the study based on the very existence of those personal connections (e.g., shared educational, socioeconomic, and other identity-related factors). Finally, given the sensitive nature of the discussion, some interviewees might have avoided expressing opinions and attitudes during the interview process; to provide assurance as to the protection of information

and identities, as per our institutional ethics review and approval, interviewees remained anonymous, interview data were not recorded other than through handwritten notes, and there was no attribution to institution, geography, role, or field of expertise.

Our approach to data analysis was built on the foundation of qualitative data coding, which maximizes the likelihood that analysis is done systematically, such that others can review and replicate the study's general approach (Auerbach & Silverstein, 2003). Coding is the process of creating and assigning labels to categorize qualitative data whereby codes are used to organize themes and patterns for subsequent and further analysis (Given, 2008). While *deductive* coding begins with a set of pre-established codes to apply to a dataset, *inductive* coding – the basis for this study – begins the coding process with a blank slate allowing a set of codes to be created passively based on the data itself. Here the codes emerge from the data. Inductive coding is appropriate for open-ended interview questions, such as in this study, where there is uncertainty regarding the direction conversations will flow (Auerbach & Silverstein, 2003). The approach minimizes the likelihood that valuable insights might be missed by relying solely on preestablished codes. Inductive coding is also appropriate when exploring a subject that is not yet well understood, or when investigating attitudes, or creating new theories. All these considerations apply to this study.

One challenge of inductive coding is ultimately deciding on the particular codes to use; there are so many ways to read and interpret any given statement from any given interviewee. To maximize the depth of our exploratory analysis, three coding methods were applied in our analysis, including:

- *In vivo coding*, which makes use of the interviewees' own words rather than an interpretation of the data – a method especially useful when data is derived from participants from different areas of expertise and professions (Given, 2008). The *in vivo* coding step consisted of extracting key language from the interview data, while maintaining strict anonymity to individual speakers.

- *Descriptive coding*, which summarizes *in vivo* extracts using a phrase that encapsulates the general idea in a condensed manner – a method especially useful for organizing the data into topic areas for future studies (Given, 2008). The descriptive coding step consisted of categorizing *in vivo* material into bundles of similar or related themes to help organize and enrich the data so that connections and differences became apparent (Auerbach & Silverstein, 2003). Our goal was to evaluate patterns within the content of the interview responses and examine the frequency with which similar ideas were shared. Thematic conflicts, patterns, and similarities were identified to help derive meaning and guide the development of hypotheses following our grounded theory methodology.
- *Indicative worldview coding*, which focuses on interview excerpts that provide insight regarding the values, attitudes, and beliefs of the participants – a method useful for exploring the interpersonal experiences of interviewees (Given, 2008). The worldview coding step consisted of identifying themes of opinions held by interviewees.

What follows next is a detailed description of our interviewee data and *in vivo*, descriptive, and worldview coding.

3. Empirical results: the rhetoric of reporting vs. the reality of inaction

The aim of this study is to explore the propensity of employees (from within Canadian financial institutions) to report concerning coworker behavior that potentially indicates insider threat. The motivation is to gain an understanding of the degree to which reporting mechanisms effectively provide an early warning detection tool to manage insider risk. What follows below are the results of our interviews using *in vivo* comments. This section is organized into three parts.

The first two parts describe the two dominant *in vivo* codes that emerged during our analysis. The first code is called “*Yes, but ... if ...*”; the second code is called “*No, because ...*”. The “*Yes, but ... if ...*” code captures comments that support the

notion that people do, in fact, report their coworkers, but in each case the *in vivo* comments include a qualifying condition or a dependency. The “*No, because ...*” code captures comments that support the notion that people do not report their coworkers; it includes interviewee *in vivo* opinions about the contributing factors that stop people from reporting.

The third part of this section presents the results of the worldview coding process where *in vivo* comments were thematically grouped around the reasons interviewees gave as to why people do or do not report their colleagues. The purpose of this additional coding step is to investigate the overlaps in the suggested conditions explaining why people do or do not report. Four themes emerged through the worldview coding – policy, training, programs, incentives – that help interpret what employees are really saying (e.g., what values and beliefs are behind their statements) as captured in the *in vivo* comments. Several interviewees volunteered specific suggestions for ways to strengthen organizational insider risk programs as informed by their own worldviews and experiences.

3.1. Part 1. “*Yes, but ... if ...*” *in vivo* coding results

Of the 19 interview participants, 14 (74%) made *in vivo* comments in support of the notion that people do report concerns about coworkers that may indicate insider threat. Seven descriptive codes emerged from this qualitative examination of the *in vivo* comments.

- (1) *Yes, but ... it depends on my own risk assessment.*
 - “If it was a big and obvious risk with evidence, I’d go to compliance”
 - “Whether I’d report depends on the level of the crime and the overall broader impact”
 - “Yes, I do think we report, but this would be applicable to a person who understands the consequences”
- (2) *Yes, but ... I have reservations about the process*
 - “Maybe by going to the next level up, but I’d likely just quit, especially if

- I brought it to someone's attention and nothing was done"
- "I would remove myself from the situation if I was concerned – if I brought it to my supervisor's attention but they didn't do anything"
 - "I would go to the CEO and if the CEO didn't want to act, I would probably choose to prioritize my own career and find another job because I would feel unequipped to fight the fight"
- (3) *Yes, but . . . I would talk to the person first*
- "I would talk to the advisor directly, then report to Anti-Money Laundering"
 - "If it was a close colleague, I might take them out for coffee and ask them what's going on in their life. I'd talk to them first and if the concerning behavior kept going on then I'd report it"
 - "I would pull the person aside directly and talk to them about the behavior observed"
- (4) *Yes, but . . . only if there are trustworthy reporting options*
- "If the culture encourages the idea of reporting and if managers get training to provide psychological safety, then people will report, but there's going to be a subset of people who won't stick their neck out therefore you need to provide an option for anonymous reporting – you need multiple options for people"
 - "I'd make sure I'm really certain about something before I report a senior peer, so I'd wait longer, I'd want more evidence and I'd go the confidential reporting route"
 - "I think that I would report anonymously because I would feel protected"
- (5) *Yes, but . . . I'm not sure how I would report*
- "I don't actually know how to report in my firm – internally, we only have a compliance department – if I didn't know the person, I'd report to compliance"
 - "I would do something like find someone to share the information with – someone I trust or a mentor – I don't know if my first instinct would be formal reporting – I would likely seek informal counsel"
- (6) *Yes, if . . . the reporting employee is loyal to the organization*

- "Loyalty that comes with longevity makes it more likely that they'd report – how do you address the fact that we likely won't report as a workforce? Good hiring practices good culture with happy employees who are proud to work there"
 - "If you're running your organization with a high degree of integrity with respect to clients probably the same internally"
- (7) *Yes, if . . . the reporting employee has self-confidence*
- "Reporting requires self-confidence – that comes with age, and I have it, but others don't always"
 - "If there was something I observed, I would note it in some way, but for me to report using a formal path, it would depend on my self-assurance, self-doubt about if it's reportable"

3.2. Part 2. "No, because . . ." *in vivo* coding results

The second *in vivo* code captures the reverse tendency, that employees do not or are hesitant to report a colleague's suspicious behavior. Of the 19 interview participants, 18 (95%) made *in vivo* comments suggesting that people do not report concerns about coworkers that could be related to insider threat. Some participants made both "Yes, but . . . if . . ." comments and "No, because" comments. Seven descriptive codes emerged from this qualitative examination of the *in vivo* comments

- (1) *No, because . . . people don't know what to report*
- "We usually don't 'know,' and we don't report just 'concerns' – we need clear evidence"
 - "The day-to-day workforce probably doesn't know their reporting options and nor do they know how to identify concerning behavior"
 - Because of a lack of knowledge, they wouldn't know what to report
 - "There's a lack of knowledge about what insider risk is"
 - "There is a polarity between insider threat and a desire to accept it as part of inclusivity and diversity"

- (2) *No, because . . . people fear negative impact for themselves*
- “We have a fear of backlash”
 - “If there’s reputational damage to yourself or no appropriate channel to report, then the fear of being known as the whistleblower would stop me”
 - “Nobody wants to be that person – there is a hesitancy to report even though we’re all aware of the channels”
 - “The elephant in the room is the fact that we’re willing to be naïve about insider risk, in some cases because of the personal and professional benefits the exposure to risks brings”
- (3) *No, because . . . people don’t trust the process*
- “I’m not aware of a single investigation that resulted in finding or proving wrongdoing”
 - “I wouldn’t have trusted that the manager would do it right so maybe I don’t trust the process”
 - “The whistleblower program is in place to protect the firm’s reputation by giving the appearance of a willingness to investigate”
 - “I don’t think there’s enough trust and awareness, so even if we see something, we likely ignore it”
 - “Not really having any insight into how the system works and what I’m opening up . . . this leads to hesitancy, doubt, uncertainty”
- (4) *No, because . . . security culture and leadership are lacking*
- “If we want to use reporting as an insider risk control, it will need to be mandatory that the banks report on those reports; only this would incentivize banks to make to their employees report on their coworkers”
 - “It’s a huge challenge to overcome differences in opinions between Security and Human Resources professionals about things like tracking, enforcement policies, interviews for investigations”
 - “We have annual training, but not a lot of attention is given to the whistleblower program therefore I feel like it’s not the
- first place I’d go, and I feel like that’s common amongst my peers”
- “I’m not convinced that all organizations have a strong security culture – the culture of the company has to be one where everyone realizes how security enables the business”
- (5) *No, because . . . people just want to do their job; they can’t be bothered*
- “We don’t want to bother, don’t need the headache”
 - “Staff don’t read policies and although they do have training, I’m not sure people are paying attention”
 - “People tend to not want to get into conflict situations, they don’t want to disrupt their day-to-day life; they think about the investigation and the time involved and people just don’t want to bother”
 - “They don’t know what, how, or when to report, they see something and then they forget, they think it’s too complicated – all these things make them conclude they just want get their work done”
 - “I think the pull to do nothing would be strong”
- (6) *No, because . . . people lack self-confidence, especially with power imbalance*
- “Self-confidence is required to speak up. . . I know they don’t have the confidence to confront their advisors”
 - “We all know the advisor has all the power”
 - “Do they have a blind respect for hierarchy, inhibiting their propensity to report? We are more reserved in Canada – quiet and polite and maybe less likely to report”
 - “It depends on who – if it’s a very senior person, I don’t think anyone would say anything”
 - “There are lot of people who have been here a long time and I have the sense that people won’t question a person who’s been here a long time”
- (7) *No, because . . . people fear negative impact for colleagues*

- “The vast majority would look the other way because we don’t like telling on other people”
- “People are willing to turn a blind eye. . . no one wants to be responsible for someone losing their job”
- “People don’t want to throw anyone under the bus and get it wrong, they’re apprehensive about reporting someone, especially if they like that person”
- “Culturally I’m not sure about the level of comfort around the idea of reporting someone you work with . . . this is a contributing factor, in the background”

3.3. Part 3. *Worldview coding results*

The results presented above began with identifying each interviewee’s dominant opinion about the propensity to report and then expanded into a detailed categorization of quotes to identify common attitudes and opinions based on *in vivo* coding. Now, in Part 3, regardless of the interviewee’s dominant opinion about the propensity to report, worldview themes that emerged about conditions or variables that might influence or help determine decision-making in either circumstance are presented. As noted above, the rationale behind this third coding process is to develop high-level themes that help explain why employees do or do not report concerning behavior.

In developing these worldview themes, consideration was given to the meaning behind the interviewee’s comment: what is it interviewees are trying to convey; what are they requesting; who are they speaking about; what do they think people need from their employers? Four worldview codes were developed. Once the worldview codes were established, representative *in vivo* quotes were extracted for general and specific recommendations for insider risk practitioners to consider as appropriate for their circumstances regarding what to do, how to do it, and why to strengthen their programs. Readers will take from this short list of recommendations from interviewees elements that are appropriate for their current program weaknesses and

opportunities, leadership personalities, budget priorities, and so forth.

3.3.1. *People view their worlds as lacking policy leadership*

All 19 interviewees mentioned something about leadership, whether they were lamenting hiring practices that promote managers without appropriate training or lamenting policies that lack enforcement abilities. The fact that many of the *in vivo* quotes indicating this worldview are vague and do not include specific actionable recommendations reveals the enormous challenge of addressing what many refer to as the security culture of the organization. For example:

How can we start to think about the insider risk problem as a change management problem rather than a security problem because it’s bigger than that and requires broader thinking?

How do I influence a culture of openness and sharing so people accept risk controls and we don’t end up with a problem that we can’t recruit or retain people?

It’s a huge challenge to overcome differences in opinions between Security and Human Resources professionals about things like tracking, enforcement policies, interviews for investigations.

Banks don’t have an incentive to report; more likely to take the loss.

You need a strong and realistic cyber security policy with teeth to be able to dismiss repeat offenders.

If we want to use reporting as an insider risk control, it would need to be mandatory that the banks report on those reports; only this would incentivize banks to make their employees report their co-workers. Public agencies have the power to expose the problem and be the bad guy so no one bank risks reputational damage or loss of employees since the rules would apply to all banks and require that banks report their insider risk events.

Acknowledging that insider risk practitioners and organizational leaders will struggle to find realistic actionable recommendations in the above quotes, this worldview theme is one of begging for leadership in everything from lobbying government bodies (public agency setting mandates to report insider risk reports) to human resources policies.

3.3.2. *People view the training they receive as unsophisticated*

A total of 16 interviewees commented specifically on their view that poor training is a major factor in the propensity to report insider risks because it results in people not being able to recognize it when they see it or when they're involved. Some people had specific recommendations, but like the *in vivo* quotes for the above worldview theme, many of the comments were vague and simply revealed a worldview that training is insufficient and requires attention. For example:

The elephant in the room is the fact that we're willing to be naïve about insider risk, in some cases because of the personal and professional benefits the exposure to risks brings.

There is a reluctance to accept the insider risk limitations and controls because there is an unwillingness to accept that there is a risk.

We're engaging our colleagues in marketing and communications to try to re-word and train people better.

Need to do a 'hard sell' on security training.

I am losing sleep over the non-malicious, non-accidental insider threat as a result of wilful blindness or unawareness of the presence of risk in the form of foreign influence as gifts and research benefits.

I don't necessarily feel that there's great information for me as a leader regarding how to identify insider risk. We have training on Diversity and Inclusion, and I feel like people might be struggling with identifying insider anomalies and risk in this context – I think we're getting mixed messaging or a lack of clarity . . . I don't think the training is considering both at once.

Arguably, the worldview that insider risk training is unsophisticated overlaps with the worldview that leadership is lacking because learning and development professionals create corporate training curricula and products based on priorities established by leadership. While interviewees were not asked to provide recommendations, several volunteered specific recommendations such as in the quote above regarding efforts to engage marketing and communications professionals to simply select words to make training more effective. Others shared their thoughts on why better training is required: because people don't have clear and

consistent definitions of reportable concerns, they underestimate or dismiss the likelihood and consequences of potential insider risk incidents.

3.3.3. *People view their worlds through a lens of mistrust, insecurity, and hesitancy and therefore need more assurances of process and protection*

All 19 interviewees made a comment about a lack of trust. Some bluntly discussed their lack of trust that the process would be carried out professionally, thoroughly, and without retaliation. Like the worldview *in vivo* comments above, the following indicate attitudes and opinions about reporting coworkers rather than providing specific actionable recommendations. For example:

I wouldn't rely on the whistleblower program for much.

I'm not aware of a single investigation that resulted in finding/proving wrongdoing.

Organizations need to increase the general awareness of risks, how to identify them, how to report them and work hard to make sure everyone trusts that their reporting remains confidential.

The main fear is retaliation, so you need to take proactive measures to train managers on everything from what counts as retaliation to how to make sure it isn't happening-this is what will encourage people to speak up.

I wouldn't have trusted that the manager would do it right so maybe I don't trust the process.

I don't think there's enough trust and awareness, so even if we see something, we likely ignore it.

It's part not really having any insight into how the system works and what I'm opening up . . . this leads to hesitancy, doubt, uncertainty.

This worldview theme suggests that insider risk practitioners and organizational leaders would benefit from an honest reflection on their processes as well as the assurances they provide to the workforce. It also suggests organizations would benefit from conversations that challenge their assumptions about the degree to which their workforce would benefit from assurances about processes and protection.

3.3.4. *People view reporting as taking away from their potential for success and therefore need incentives to take the time to learn, observe, and report concerns*

Interviewees did not use the word incentive, but the 11 people who shared that they would put themselves and their own career first said things that indicate some form of incentive is required to change behavior. For example:

With all the factors, I would think, what would be the point, what's in it for me?

Maybe by going to the next level up, but I'd likely just quit, especially if I brought it to someone's attention and nothing was done.

We don't want to bother, don't need the headache.

I would probably choose to prioritize his own career and find another job because I would feel unequipped to fight the fight against a corporation.

Get to know your employees . . . Include in performance review key performance indicator such that a manager will drop down one or more performance grades if their direct reports say that they haven't made an effort to get to know them.

People tend to not want to get into conflict situations, they don't want to disrupt their day to day life; they think about the investigation and the time involved and people just don't want to bother.

They don't know what, how or when to report, they see something and then they forget, they think it's too complicated – all these things make them conclude they just want get their work done

4. Analysis & discussion: interpreting what we heard

The purpose of this section is to explore and attempt to explain the meaning of the empirical results presented above with a goal of unpacking the findings and discussing their significance and implication. Our interpretation of the results is informed by the context of the theoretical literature on reporting and the study's inductive methodology and qualitative analysis of the *in vivo* interviewee data. With the aim of exploring attitudes and beliefs individuals hold about whether or not to report a coworker's behavior, the interpretation that follows focuses on the utility of reporting

mechanisms to provide an early warning detection tool alongside the barriers identified by interviewees. The following discussion tracks the three-part structure of the results section.

4.1. *The conditional 'yes' to reporting*

The first of two *in vivo* codes that emerged, “*Yes, but . . . if . . .*,” reveals that under clear-cut conditions participants believe that colleagues would report a coworker. Interviewees shared with us the key conditions that support this process. Two factors stand out: solid evidence of concerning behavior or wrongdoing, and a trustworthy reporting process and mechanism. And yet, because of the open-ended, conversational nature of our interview methodology, participants also had the opportunity to express conflicting or competing views thereafter. A significant number of people (14 of the 19 interviewees, or 74%), for instance, made comments that indicated that while employees would take a first step in reporting a colleague, they would do so on condition of other factors or steps being met.

Two of the descriptive *in vivo* codes, *Yes, but . . . it depends on my own risk assessment* and *. . . I would talk to the person first*, have practical implications for insider risk training, education and awareness efforts that provide clarity and direction on risk assessment and steps for employees to take. While these two descriptive *in vivo* codes indicate an overall awareness of potentially unacceptable behavior existing in-step with a collegial concern for a coworker's well-being, teaching a standard insider risk assessment approach and identifying standard steps to follow when reporting will help remove employee hesitation to report and encourage a consistent response to similar future behaviors. One participant noted, for instance, that “*Society has evolved such that we do report more out of a concern for someone's mental well-being – if they've seen a change in behaviour, for example.*” This theme recurs in our data, indicating that training and awareness efforts within an organization or industry on what to report and how to report it might improve overall reporting frequency, quality, and engagement. This suggests further that an opportunity exists to leverage progress on mental health awareness to refine

guidance on insider risk, providing a workforce more useful information on the preferred steps needed when reporting concerns.

Two of the descriptive *in vivo* codes, *Yes, but . . . I have reservations* and *. . . if there are trustworthy reporting options*, expose some shared attitudes regarding the importance of institutional and organizational trust (and mistrust). These attitudes might have been learned through previous or personal experience while reporting concerning behavior or may reflect a third party's experience or a comparable interaction with institutional leadership. Either way, this result indicates that trust is critical to reporting frequency and suggests that organizations must take steps to tackle residual "but . . . if" undertones tucked within in it. Moreover, this finding is likewise linked to employee retention, a practical concern to the financial services sector and beyond. The results suggest that interviewees link reporting misbehavior and institutional trust with continued employment. Some participants noted specifically that they would "quit," "remove" themselves, or "find another job" if they made an insider risk report and nothing came of it. Trust, then, is a responsive mechanism for reporting insider risk: it needs to be bolstered, refined, and earned.

The remaining three descriptive *in vivo* codes – *Yes, but . . . I'm not sure how I would report, . . . if the reporting employee is loyal to the organization*, and *. . . if the employee has self-confidence* – indicate that personality, personal characteristics, self-confidence, and general attitude may play an important role in whether a person decides to report suspicious behavior. Importantly, organizations can take steps to embolden and empower employees to do so. Providing employees with trusted "mentors" or another avenue for discussing sensitive issues or developments related to insider risk management could help build employee confidence and compel reporting. Training and awareness programs might likewise further encourage employees by helping them better understand the reporting pathways and options they have, the protections they will enjoy in reporting insider threats, and the importance of doing so. Growing employee confidence is an iterative and compounding process that organizations can harness and leverage over time.

4.2. The firm 'no' to reporting

The second *in vivo* code, "*No, because . . .*," suggests a paradox of sorts. Even for interviewees whose immediate inclination is to report suspicious coworker behavior, when these individuals actually contemplate and reflect upon how they would personally react, most nonetheless conclude that they (and by extension, other employees) would *not*, in fact, report coworkers. All but one interviewee offered comments indicating that they and others would not report, sharing a variety of rationales and conflicting reasons that are assumed to hold across and beyond the Canadian financial services sector.

For illustration, from the descriptive *No, because . . .* code, the most prevalent rationale for non-reporting rested on a lack of employee understanding of what to report. One participant suggested, for instance, that "*I consider myself the first line of defense and I'm looking for trends [suggestive of insider threat]; but peers in other regions across the country don't do this.*" Another shared that "*. . . there's so much nuance and grey area*" when looking out for misbehavior. All of this suggests that more explicit training in and better description and more-nuanced awareness of insider threat and reporting would benefit organizations. One interviewee concluded, for instance, that their organization was "*. . . engaging with colleagues in marketing and communications to try to re-word and train people better*" to recognize and report suspected malicious behavior. Presentation and communication are front and center.

A second insightful observation relates to the perceived consequences a would-be reportee risks when reporting suspected misbehavior, as captured in the *No, because . . . people fear negative impact for themselves* and *. . . people don't trust the processes* codes. Here, interviewees add a personal perspective to their general skepticism and lack of confidence in an institution's or organization's reporting mechanism. Comments herein even suggest that for employees who have an acute awareness of what to look out for and would know an insider threat when they see it, a variety of personal concerns may nonetheless stop them from reporting. These fears include reputational harm, being known or labeled as a "whistle-blower" [*. . .*

nobody wants to be that person”), an unwillingness to personally test the reporting process, and an unwillingness to forego the possible rewards generated by suspicious or concerning behavior perceived as trickling down from the risks of the concerning behavior. For example of the latter, one interviewee warned that because of “the limited global pool of PhD economists,” Canadian employees were collaborating and sharing information with foreign coauthors “in countries who are at odds with Canada . . . [unaware of] the risks in the foreign coauthor’s gifts and benefits of joint publication.” Another interviewee noted that an “investment associate wouldn’t report suspected trends indicating back-handed deals with an advisor at an offshore firm because they get a piece of the revenue generated.” The bottom line is that reporting concerning behavior may not be costless, and fear of repercussion might tip the balance toward inaction.

A third finding relating to reporting hesitancy touches on a workforce’s disengagement from the process altogether. Two codes stand out: *No, because . . . security culture and leadership are lacking* and *. . . people just want to do their job, can’t be bothered*. The two are intertwined. Employee apathy toward insider threat stems in part from a perceived lack of strategic and corporate leadership in building the necessary “security culture” that would buttress and reinforce a robust reporting mechanism. Instead, some interviewees noted a lack of corporate action or guidance on difficult developments related to managing insider risk, as in the case of a rise in tension between security professional and HR professionals within an organization. Others identified uncertainty over the confidentiality of reporting process. The result is employee indifference when it comes time to report misbehavior: “ . . . don’t need the headache,” “*people just don’t want to bother*,” “[employees] *just want get their work done*.” These and other comments in this descriptive code indicate that genuine efforts by corporate leadership to engage the workforce with consistent conversations about how each person’s security awareness and conscientiousness enables the business to grow could help convince employees that reporting is not only necessary and important, but also worth the effort.

The final two descriptive *in vivo* codes – *No, because . . . people lack self-confidence especially with power imbalance* and *. . . people fear negative impact for colleagues* – relate to workplace relationships. Rank, title, and position matter when thinking about reporting an insider threat. Participants suggested, for instance, that employees would hesitate to report on a superior, executive, or manager – “*if it’s a very senior person, I don’t think anyone would say anything*.” Finding creative ways to even the playing field would help compel employees of all ranks to report misbehavior regardless of position.

4.3. Worldviews regarding conditions and dependencies

In the final stage of our data coding process, we exposed four underlying worldviews that indicate the attitudes and opinions about conditions under which employees would report their colleagues for suspicious behavior. In essence, these worldviews relate to the degree to which employers have implemented consistent reporting (1) policies, (2) training, (3) programs, and (4) incentives, creating a security-conscious ecosystem in which employees conclude that the benefits to their employer outweigh the risks to themselves of reporting a coworker.

The first thematic worldview relates to *in vivo* comments about the need for consistently applied policies. For instance, clear and uniformly applicable direction from upper and senior management is needed when devising a useful reporting mechanism. This helps build employee trust of the system and guidance in using it. Employees need to likewise appreciate the larger context within which reporting exists; it is not solely a security problem but rather about “change management” and institutional culture. Employers need to also communicate more clearly with all stakeholders about the nature and consequences of insider threat, perhaps by instituting a “know your colleague” mechanism (building off “know your client or product” mandates) or by illustrating to employees how reporting fits into other approaches used to identify, counter, and deter insider threat. Participants proposed other innovative ideas including making reporting mandatory

for all employees and encouraging government entities to do the same with entire sectors to reduce the reputational cost individual organizations face when reporting insider threat events alone.

The second thematic worldview relates to confusion and frustration that interviewees expressed about poor training. Interviewees suggested that clear communication of the consequences of insider threats to the business, clients, and general society is essential for effective reporting. Critically, employees also must understand what behavior to report. Appreciating the “why” of reporting insider threat is one thing; understanding the “what” is something else altogether. Employees need tailored guidance on what to look out for.

The third thematic worldview indicates that people need assurances about processes and programs. This worldview code represents the expressions of uncertainty and skepticism about protections for everyone once the reporting process is underway. Interviewees expressed a need for clarity on the reporting process itself and assurances on concomitant protections. Employees are looking for a more nuanced understanding of what reporting actually triggers within the organizations and want to feel safe if and when doing so. Managers, then, need training, too, in better protecting their would-be reporting employees; they also need to communicate these protections in advance. As one participant noted, the “*reporting program is as good as what you put into it.*”

The fourth thematic worldview revealed that people need incentives to pay attention and make the effort to report. This worldview represents the expressions shared about the need for clear alignment between organizational and individual interests. Participants suggested organizations find ways to better tie employment, promotional opportunities, and performance reviews and indicators to insider risk mitigation and reporting.

5. Next steps in the study of reporting insider risk

Despite its assumed importance in detecting, defeating, and deterring insider threats, the actual reporting of suspected insider threats by an organization’s workforce faces innumerable challenges.

While our findings suggest that employees share an overarching willingness and desire to report a coworker’s concerning behavior, they nonetheless face various structural, institutional, relational, social, and psychological hurdles in doing so, as various other scholars have suggested and explored (e.g. Ho et al., 2018; Maasberg & Beebe, 2014; Maasberg et al., 2020; Safa et al., 2018; Whitty, 2021). Indeed, workforce confusion and uncertainty surrounds reporting, such that a single employee can logically express both affirmative and negative opinions about their (and other people’s) likelihood of reporting suspicious behavior within the same breath. In the abstract, reporting insider threats seems easy; but in reality, and in practice, however, doing so proves far more complex. The takeaway is that from the perspective of a workforce, the burden of reporting can, at times, be too great, such that inaction and silence become the most likely outcome. “*The pull to do nothing would be strong,*” is how one participant aptly summarized this dilemma,

And yet, not all is lost. On the contrary. From a practical perspective, our research reveals different ways organizations can refurbish and bolster reporting mechanisms. Our study shows that people do want to report, but not at their own expense. Context seems to matter a lot. A way forward on strengthening reporting is captured in our four worldview themes. Reporting of insider threats can be improved upon through (1) consistent application of clear reporting and insider risk management policies, (2) sophisticated implementation of ongoing training, (3) development of and communication about robust reporting programs, and (4) institutional leadership that incorporates incentives for employees to report suspicious behavior and otherwise leads to a security-conscious organizational culture. Simply put, nudging employees to report suspected insider threats with more frequency and certainty will flow from improving reporting policies, training, and programs while cultivating a broader organizational culture that pivots on security awareness.

Our study invites four avenues for further research on reporting of insider threats. First, from an empirical perspective, the data collected as part of our research – as in the case of previous similar projects – was limited in scope to one

country and one industry. An obvious next step is to expand the population sampled to consider either all of Canada's critical infrastructure sectors, and/or to focus on one (or a few) sectors but from an international standpoint, collecting, analyzing, and comparing data on reporting from various jurisdictions. To mitigate potential bias, future studies could also apply a systematic random sampling methodology to data collection. Increasing and diversifying the sample size should help improve the confidence that opinions, statements, and attitudes gathered are representative of a larger population.

Second, from a methodological perspective, future studies should build off and greatly expand upon, the codes we developed. Our approach followed a grounded theory methodology, such that we inductively developed *in vivo* codes that emerged from our data. A next step would be to use elements of our study as the basis of a closed-ended survey using a Likert scale to quantify the degree to which a systematic sample of employees agrees or disagrees with the findings in this study about opinions, attitudes, perceptions, and behaviors related to reporting insider threat. Other future studies might otherwise use our approach to develop and analyze much more detailed case studies of specific reporting events, providing a comparative assessment of the phenomenon. And, of course, with the right kind of data, a quantitative analysis of reporting might likewise be pursued.

Third, from a theoretical perspective, future research based on different population samples, sizes, and methodologies could help in the development of a theory or competing theories of reporting. This process would help mature the study of insider risk and reporting from one of assumptions informed by supposition to one of concepts, frameworks, and causal relations informed by empirical observations. To date, no theoretical framework accurately explains or predicts reporting behavior. Future frameworks would help better elucidate the general role reporting has on managing insider risk and could help shape our collective understanding of why and under what conditions reporting does (or does not) take place across disciplines, industries, and jurisdictions. Moreover, reporting theories could likewise

function as a conceptual bridge to other, preexisting theoretical frameworks stemming from criminology, psychology, political science, sociology and other fields – as detailed above in section two – building crossdisciplinarity lessons useful for understanding insider risk as both Marangione (2019) and Creech (2020) explore, for example. For instance, a robust theory of reporting informed by different disciplines could better explain the link between deterrence, coercion, reporting, and insider threats. Relatedly, these theories could add some much-needed nuance on the relationship between reporting malicious versus reporting unintentional and/or precursor insider risk behavior, building observable causal patterns that help distinguish between criminal intent, negligence, and accidents.

From a practical perspective, developing and testing robust theories of reporting should ultimately inform and improve the use of reporting. Here theory meets practice. Future research should fulfill a use-and-utility function in countering insider threat, helping to build better approaches to reporting across organizations, industries, and countries. In an ideal scenario, industry and public policy leaders should be able to use research results to prioritize investments of time, training, and money in ways that improve the likelihood that employees will use reporting mechanisms to provide early identification of potential insider threats. In this particular example, improvements in empiricism, methodology, and theory would lead to real-world advancements in reporting suspicious behavior and countering insider threats.

While the above follow-up studies are ongoing, practitioners will want to focus on the interviewees' *in vivo* comments admitting inaction around the reporting of concerning behavior. Practitioners will want to be aware of false thinking that employees will readily report concerning behavior in the workplace. This is material learning for practitioners who may put too much emphasis on reporting expectations without understanding that organizations are likely underreporting. The results of this study provide what's needed first: the awareness of greater than expected inaction. Only with awareness can practitioners start to think about how to solve for the false thinking that employees

will report concerning behavior observed in the workplace, which will have its own share of complexity.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Heather Holden  <http://orcid.org/0000-0002-3420-8710>

Victor Munro  <http://orcid.org/0000-0003-3775-7421>

Alex Wilner  <http://orcid.org/0000-0003-2087-252X>

References

- Auerbach, C., & Silverstein, L. (2003). *Qualitative data: An introduction to coding and analysis*. New York University Press.
- Bell, A., Rogers, B., & Pearce, J. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, 24, 166–176. <https://doi.org/10.1016/j.ijcip.2018.12.001>
- Bunn, M., & Sagan, S. D. (2014). *A worst practices guide to insider threats: Lessons from past mistakes*. American Academy of Arts and Sciences.
- CERT National Insider Threat Center. (2018). *Common sense guide to mitigating insider threat*. Software Engineering Institute, Carnegie Mellon University (additional reference information: TECHNICAL REPORT CMU/SEI-2018-TR-010).
- CERT National Insider Threat Task Force. (2016). *Protect your organization from the inside out: Government best practices*. Software Engineering Institute, Carnegie Mellon University. CMU/SEI REPORT NUMBER: CMU/SEI-2016-TR-015. <https://doi.org/10.1184/R1/12890918.v1>
- Conference Board of Canada. (2018). *Updating our knowledge of the insider threat*. The Conference Board of Canada.
- Creech, G. (2020). Real insider threat: Toxic workplace behavior in the intelligence community. *International Journal of Intelligence & CounterIntelligence*, 33(4), 682–708. <https://doi.org/10.1080/08850607.2020.1789934>
- Cybersecurity and Infrastructure Security Agency. (2020). *Threat mitigation guide*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.
- Fortinet. (2019). *2019 Insider threat report*, 1–37.
- Given, L. (2008). *The SAGE encyclopedia of qualitative research methods*. SAGE Publications.
- Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science and Technology*, 69(2), 271–280. <https://doi.org/10.1002/asi.23938>
- Hunker, J., & Probst, C. (2008). Insiders and insider threats an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks*, 2(1), 4–27.
- Jacqueline, E., Agrafiotis, I., & Nurse, J. R. (2016). Insider threat response and recovery strategies in financial services firms. *Computer Fraud & Security*, (11), 12–19. [https://doi.org/10.1016/S1361-3723\(16\)30091-4](https://doi.org/10.1016/S1361-3723(16)30091-4)
- Maasberg, M., & Beebe, N. (2014). The enemy within the insider: Detecting the insider threat through addiction theory. *Journal of Information Privacy and Security*, 10(2), 59–70. <https://doi.org/10.1080/15536548.2014.924807>
- Maasberg, M., Zhang, X., Ko, M., Miller, S., & Beebe, N. L. (2020). An analysis of motive and observable behavioural indicators associated with insider cyber-sabotage and other attacks. *IEEE Engineering Management Review*, 48(2), 151–165. <https://doi.org/10.1109/EMR.2020.2989108>
- Maasberg, M., Zhang, X., Ko, M., Miller, S. R., & Beebe, N. L. (2020). An analysis of motive and observable behavioral indicators associated with insider cyber-sabotage and other attacks. *IEEE Engineering Management Review*, 48(2), 151–165. <https://doi.org/10.1109/EMR.2020.2989108>
- Marangione, M. (2019). Millennials: Truth-tellers or threats? *International Journal of Intelligence & CounterIntelligence*, 32(2), 354–378. <https://doi.org/10.1080/08850607.2019.1565276>
- Mills, J., Dever, J., & Stuban, S. (2018). Using regression to predict potential insider threats. *Defense AR Journal*, 25(2), 122–157. <https://doi.org/10.22594/dau.16-771.25.02>
- Moore, A. P., Novak, W. E., Collins, M. L., Trzeciak, R. F., & Theis, M. C. (2015). *Effective insider threat programs: Understanding and avoiding potential pitfalls*. www.sei.cmu.edu
- National Counterintelligence and Security Center. (2021). “Insider threat mitigation for U.S. Critical Infrastructure Entities”.
- Pereira, T., & Santos, H. (2015). Insider threats: The major challenge to security risk management. In T. Tryfonas, & I. Askoxylakis (Eds.), *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 9190, pp. 654–663). Springer Verlag. https://doi.org/10.1007/978-3-319-20376-8_58
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597–611. <https://doi.org/10.1016/j.cose.2011.12.010>
- Ponemon. (2020). *2020 cost of insider threat report*, 1–31.
- Ponemon Institute and DTEX. (2021). *The state of insider threats 2021_Behavioural awareness and visibility remain elusive*. Ponemon Institute LLC Publication.

- Prabhu, S., & Thompson, N. (2022). A primer on insider threats in cybersecurity. *Information Security Journal: A Global Perspective*, 31(5), 602–611. <https://doi.org/10.1080/19393555.2021.1971802>
- Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Carnegie Mellon Software Engineering Institute.
- Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security & Applications*, 40, 247–257. <https://doi.org/10.1016/j.jisa.2017.11.001>
- Stubben, S. R., & Welch, K. T. (2020). Evidence on the use and efficacy of internal whistleblowing systems. *Journal of Accounting Research*, 58(2), 473–518. <https://doi.org/10.1111/1475-679X.12303>
- Verizon. (2019). *Insider threat report: Out of sight should never Be out of mind*. Verizon.
- Verizon. (2021). *2021 data breach investigations report*.
- Whitty, M. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization*, 27(5), 911–929. <https://doi.org/10.1017/jmo.2018.57>