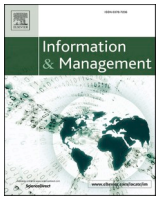
Information & Management 61 (2024) 103877

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im



VISTA: An inclusive insider threat taxonomy, with mitigation strategies

Karen Renaud [a,b,c,f,*], Merrill Warkentin [d], Ganna Pogrebna [e,g,h], Karl van der Schyff [f]

[a] University of Strathclyde, Glasgow, UK
[b] University of South Africa, Pretoria, South Africa
[c] Rhodes University, Grahamstown, South Africa
[d] Mississippi State University, Mississippi State, USA
[e] Charles Sturt University, Bathurst, Australia
[f] Abertay University, Dundee, UK
[g] The Alan Turing Institute, London, United Kingdom
[h] The University of Sydney Business School, Darlington, Australia

ARTICLE INFO

Keywords:
Insider threats
Taxonomy
Mitigations
Cybersecurity

ABSTRACT

Insiders have the potential to do a great deal of damage, given their legitimate access to organisational assets and the trust they enjoy. Organisations can only mitigate insider threats if they understand what the different kinds of insider threats are, and what tailored measures can be used to mitigate the threat posed by each of them. Here, we derive VISTA (*inclusi**V**e In**S**ider **T**hreat t**A**xonomy*) based on an extensive literature review and a survey with C-suite executives to ensure that the VISTA taxonomy is not only scientifically grounded, but also meets the needs of organisations and their executives. To this end, we map each VISTA category of insider threat to tailored mitigations that can be deployed to reduce the threat.

1. Introduction

Employees can cause security breaches, compromising the CIA properties of an organisation's information (confidentiality, integrity, availability), either accidentally or deliberately. This is why they are commonly referred to as 'insider threats' [1,2]. The threats constituted by insiders are increasing, challenging to detect, and difficult to mitigate [3]: a so-called 'hard problem' [4]. Bitglass [5] discovered, in 2020, that 61 % of companies they surveyed had suffered an insider threat event in the previous 12 months. Moreover, Kaspersky found that while cyber-attacks caused 23 % of data leakages, employees caused 22 % [6].

'Insider threats', especially those emanating from insiders who set out deliberately to harm the organisation, have existed since the beginning of organised societies. There have always been individuals willing to betray their group's trust, driven by a variety of motivations. One of the earliest documented examples of an insider threat in a political context is the story of Ephialtes of Trachis, described by Herodotus in his 'Histories'. Ephialtes was a Greek who betrayed his country during the Battle of Thermopylae in 480 BC by showing the Persian army, led by King Xerxes, a secret mountain path that allowed them to outflank the Greek forces led by King Leonidas of Sparta. As a consequence, the Greeks suffered a significant defeat, and Ephialtes' actions had a major impact on the course of the Greco-Persian Wars. While Ephialtes wasn't an 'employee' in the modern sense; his betrayal can be considered an early example of an insider threat because he used his knowledge of the local terrain to undermine his own people's defence.

In the Middle Ages, when the concepts of 'employee' and 'employer' became more pronounced towards the Renaissance and the Age of Discovery period, 'insider threat' events were documented more frequently. For example, Finney [7] highlights one of the oldest insider threat events, in 1456, when a man called Gutenberg had the deeds of his innovative printing business stolen by an insider, one Peter Schöffer, so that Peter's father-in-law could claim the company. Many centuries later, in the cyber era, the insider threat poses a headache to those trying to secure organisational information and systems [8–10]. As Hayden [11] put it in 1999, "*Today's Information Systems (IS) provide enormous leverage and access to vast amounts of sensitive, unclassified, and classified mission critical data. The potential for abuse is obvious*" (p.4).

Insiders have all the requisite knowledge about internal systems and their topology, and also have legitimate access to sensitive and valuable information assets [12,13]. As such, they are able to do far more damage than outsiders [14,15]. In 2023, Rosenthal [16] estimates the average cost of an insider threat incident to be $11.45 million, up from $8.76 million in 2018. Organisations are justifiably concerned about this

* Corresponding author at: University of Strathclyde, Glasgow, UK.
E-mail address: karen.renaud@strath.ac.uk (K. Renaud).

https://doi.org/10.1016/j.im.2023.103877
Received 8 December 2022; Received in revised form 12 October 2023; Accepted 18 October 2023
Available online 21 October 2023

threat [17], because insiders can threaten their survival.

In formulating the most effective mitigations to the insider threat, it behoves us to consider what other domains do. For example, the field of education advocates tailored instruction to meet the specific needs of each learner [18]. Medicine, too, aims to predict, prevent, and treat illnesses *according to the individual's needs* [19]. Heathrow airport has experienced great success by tailoring their cybersecurity training to the needs of individual staff members [20]. Matching effective insider threat mitigations to the characteristics and motivations of the insider seems equally advisable. As such, we should aim to apply the *most effective* intervention, to target each *particular* insider threat type, at the *right* time. To achieve this, an inclusive taxonomy of insider threats enables cognizance of the full range of insider threats, what motivates and causes them, and how each different threat type can be mitigated. This empowers organisations in formulating tailored prevention and response strategies [21].

Section 2 defines insiders and the insider threat and justifies the derivation of yet another taxonomy, given the existence of others in the research literature. We then explain how the VISTA insider threat taxonomy was derived. Section 3 outlines mitigation options from the research literature that can be used to ameliorate the full range of insider threats. Section 4 discusses the paper's findings, and Section 5 concludes.

The **contributions** of this paper are:

- Justification for a more inclusive taxonomy, based on a survey of C-Suite[1] executives, summarised in Table 1.
- VISTA, an inclusive taxonomy of human insider threats, visualised in Fig. 4.
- Tailored mitigation measures to address each different category of insider threat most effectively (Table 3 explained in Section 3 and demonstrated in Table 4 in Appendix A).

2. Insiders, insider threats & VISTA

2.1. Definitions

"Insiders" are defined by the Cybersecurity & Infrastructure Agency (CISA) [22] as: "*any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems*". The 'insider threat' is defined by CISA as: "*the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems*". While comprehensive, this definition is perhaps not nuanced enough to help organisations to understand all the different kinds of insiders, and the mitigations that will reduce each threat.

Insider threats, and their causes, are heterogeneous. It is to be expected that effective threat reduction mitigations for one kind of insider would be less than effective in mitigating another kind. For example, if the threat is rooted in ignorance of security practices, the mitigation is better training. If the threat is rooted in noncompliance or negligence, interventions need to be designed to improve compliance, but these same mitigations are unlikely to sway malicious insiders. Whistleblowers, by contrast, do not cause harm either accidentally or maliciously. They act based on an inner commitment to society and feeling they need to expose unethical practice. Whistleblower-tailored mitigations should address the issues within their organisation that might cause a whistleblower to act.

[1] Corporate officers who have "chief" in their job titles: e.g.,chief executive officer, chief operating officer, or chief financial officer.

Table 1
Overall topic mapping emerging from C-suite professionals survey.

Topic #	Description	Topic summary	Top 5 keywords
Topic 1	Limitations of Current Taxonomies	This topic discusses the *shortcomings* and *limitations* of existing taxonomies in capturing the full range and complexity of insider threats. It **emphasizes the need for improvement** in addressing **unintentional** insider threats, errors, oversights, and the **multifaceted nature of insider behaviors.**	shortcomings limitations capturing complexity threats
Topic 2	Unintentional Insider Threats	This topic focuses on the category of insider threats that arise from **unintentional actions, mistakes, lack of training, or negligence**. It highlights incidents such as employees unknowingly compromising security, falling victim to scams, mishandling sensitive data, or making errors due to inadequate cybersecurity awareness.	unintentional mistakes training negligence cybersecurity
Topic 3	Incomplete Coverage of Insider Behaviors	This topic addresses the incomplete representation of insider behaviors in current taxonomies. It **suggests the inclusion of insiders who act out of personal convictions, ideological reasons, convenience, or to save effort**. It also highlights the importance of considering insiders who intentionally or inadvertently bypass security measures, compromise systems, or exploit vulnerabilities.	personal motivations vulnerabilities exploit behaviors
Topic 4	Need for Comprehensive & Adaptive Approaches	This topic emphasizes the need for comprehensive and adaptive approaches to insider threat management. It discusses the **evolving nature of threats**, the importance of adapting strategies to changing risk factors, and the need for customization based on individual organizations' threats and security needs.	comprehensive adaptive evolving customization organizations
Topic 5	Insider Threats from Ex-Employees	This topic specifically focuses on the risks posed by ex-employees who **exploit their past affiliations and insider knowledge to cause harm or compromise security**. It highlights the importance of considering this category of insiders in threat assessments and response strategies.	ex-employees affiliations knowledge harm security
Topic 6	Insider Threats due to Poor Security Awareness and Training	This topic emphasizes the significance of insufficient security awareness and training in contributing to insider threats. It suggests the inclusion of insiders who unintentionally or unknowingly compromise security due to a **lack of knowledge, awareness, or**	security awareness knowledge awareness cybersecurity protocols

(*continued on next page*)

Table 1 (*continued*)

Topic #	Description	Topic summary	Top 5 keywords
		understanding of cybersecurity protocols.	
Topic 7	Insiders Misusing Privileges and Access	This topic addresses the category of insiders who misuse their privileges or access for **personal gain or to compromise systems**. It highlights the need to consider insiders who knowingly disregard cybersecurity practices, intentionally exploit vulnerabilities, or assert control over systems.	misusing privileges access gain compromise
Topic 8	Overcoming Simplification & Reductionism	This topic discusses the **oversimplification and reductionism observed in current taxonomies.** It emphasizes the importance of capturing the full complexity and nuances of insider threats, such as the diverse motivations, behaviors, and actions of insiders.	Over-simplification reductionism complexity nuances motivations

2.2. Insider threat examples

Sometimes, people infiltrate an organisation specifically to carry out industrial espionage [23,24] or to engage in sabotage [13], so these insiders pose a threat from the outset. Other insiders are threats due to a number of psychological indicators, which have previously been implicated in malicious insider behaviours of this kind [25–28]. For example, Aldrich Ames, the KGB double agent who was convicted of espionage, was said to have suffered from narcissistic personality disorder and Robert Hanssen, ex-FBI agent who spied for Soviet and Russian intelligence services, was said to lack a conscience [29]. Spotting these can help an organisation to detect insider threats [30].

Our very humanity could also make us an 'insider threat'. On the other hand, some insiders engage in effort minimisation [31,13] with adverse consequences. For example, the UK's National Health Service was fined in 2012 when some of their discarded drives were sold on eBay with patient information on them [32], pointing to a lack of care in ensuring that the drives were wiped before discarding them.

On the other hand, employees can also 'flip' from being benign to being an insider threat [33], sometimes as a result of their perception of managerial actions toward them [13,34], but also as a result of organisational behaviour that they consider unethical or unlawful [35,36]. Organisations could behave contrary to ethical and legal norms and this might lead to an external whistleblowing event [37–40]. Examples are: Snowden (NSA) [35], Jackson (Ventavia) [41], Haugen (Facebook) [42], and Peter Rost (Pfizer) [43].

The organisation's culture, atmosphere, or management style could also cause people to become insider threats. Employees could feel burnt out by overwork or aggrieved at organisational injustice [9,29,33,44–47] Disgruntlement is one of the biggest insider threat triggers [10,13,48–54]. For example, EnerVest IT Administrator Ricky Joe Mitchell heard that he was going to be fired. He reset the company's servers to their original factory settings, disabled cooling equipment for EnerVest's IT systems and deleted PBX system info [55] essentially halting organisational functioning. Some insiders perpetrate acts for personal gain, some out of a desire to harm the organisation. Some harms are deliberately inflicted; others are incidental (occurring as a consequence of the insider behaviour, but not being the primary goal of the person's actions).

These examples demonstrate that insider threats differ fundamentally in terms of knowledge, compliance motivation, intention, volition, and goal. As such, it makes sense to derive an attribute-based taxonomy of insider threats so that we can formulate tailored mitigation strategies to address all the different kinds of insiders to maximise effectiveness of organisational efforts in this respect. In the next section, we elaborate.

Note that the term "taxonomy" (from the Greek "taxis" (arrangement) and "nomia" (method)) is recognized for its use in biology, where it is the method for classifying organisms that share characteristics (called genus and species) but is also widely applied to the classification of discreet instances of other conceptualized entities. Typology, on the other hand, is the study of types and may refer to classifications in linguistics, psychology, statistics, and many other disciplines. It could easily be applied to our framework as well, as it refers generally to putting things into types. Ontology, another related term, refers to a set of categories within a domain that shows their properties and the relations between them, but we do not explicate in detail any such relationships. Doty and Glick [56] suggest that typologies represent conceptual classifications, whereas taxonomies are classification schemas based on observable characteristics. We choose here to adopt the widely-recognised and widely-used term "taxonomy" to label our framework to provide greater clarity and contribution.

2.3. Why yet another taxonomy?

Glass and Vessey [57] explain that taxonomies help to organise and structure knowledge within a field. This, in turn, enables researchers to appreciate and investigate relationships between concepts. In other domains, taxonomies are successively refined as new insights are gained. For example, for many years, primate taxonomies did not include Bonobos, but when primatologists realised that they were not 'small chimpanzees', a new taxonomy was developed to acknowledge this [58]. One area with a prolific number of taxonomies is the behavioural change field [59]. Michie et al. [60], in justifying their new taxonomy, argues that it '*extends the scope and improves the reliability*' of a previously-published behaviour-change technique taxonomy by Abraham and Michie [61]. Hence, it is common for taxonomies to evolve as new insights are gained and it is likely that insider threat taxonomies will continue to evolve.

When we contemplate insider threats, a number of taxonomies and typologies have been formulated (for reviews, see Salem et al. [62], Hunker and Probst [63], Azaria *et al.* [64], Abdallah et al. [65], Sanzgiri and Dasgupta [66], Ophoff et al. [67], Homoliak et al. [2]). These offer insights into the domain of interest but may not address emerging threats and other perspectives due to a number of factors, including the following:

Factor 1: Inadequate (Uni-dimensional) classification: While some recent attempts have been made to propose a topological framework with more than one dimension (see, e.g., [68]), the majority of traditional taxonomies categorise insider threats as either malicious (e.g., [25,50,62,69–71]) or non-malicious/ unintentional (e.g., Greitzer et al. [72], Wall [73], Reason [74]). These two categories are insufficiently fine grained to address the full spectrum of insider threats. Our taxonomy thus applies a multi-dimensional approach to understanding insider threats, which helps us better understand and mitigate these threats.

Factor 2: Evolving technologies: The rapid advancement of technologies, such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT), has created new opportunities for insider threats (e.g., Shi et al. [75]). These technologies, while beneficial, can also be exploited by malicious actors to compromise systems and steal valuable data. VISTA, proposed in this paper, addresses the potential vulnerabilities that these technologies present and the methods insiders use to exploit them. Previous taxonomies were formulated before the advent of generative AI tools e.g.,

ChatGPT. However, as Renaud, Warkentin and Westerman [76] point out, these tools signal a significant shift in the kinds and sophistication of future exploits when used by cyber criminals. What this means for the defenders and for organisations across the globe is that traditional ways of preventing cyber attacks and training insiders to act securely should change too. Insider threat taxonomies need to reflect this new reality.

Factor 3: Remote work environments: The global shift towards remote work has increased the reliance on digital communication and collaboration platforms (e.g., Hartmann and Lussier [77]). This shift has expanded the attack surface for insider threats, as employees have access to sensitive data from various locations and devices. The taxonomy proposed in this paper considers the challenges posed by remote work environments and the unique risks they present.

Factor 4: Holistic approach: A new taxonomy should be operationally viable; hence, we focus not only on the motivations and actions of insiders, but also on the organisational, technical, and environmental factors that contribute to insider threats. By taking a holistic approach, organisations can develop more effective strategies for detecting, preventing, and mitigating insider threats.

Factor 5: Adaptive countermeasures: The proposed taxonomy allows us to provide a framework for developing adaptive countermeasures that can evolve with the threat landscape. This includes continuous monitoring of user behaviour, implementing data loss prevention (DLP) solutions, and using AI and machine learning to detect anomalies in real-time.

Factor 6: Enhanced training and awareness: By developing a new taxonomy, we provide a new platform for organisations to better educate their management about the various forms of insider threats, their potential consequences, and the role they play in preventing such threats. A well-informed management is one of the most effective defences against insider threats.

To complement and test the above reasoning derived from our analysis of the existing literature on insider threats, we conducted a survey with C-suite professionals to explore whether they found current taxonomies helpful and whether a need for taxonomy improvement is justified. To conduct the survey, over 3000 professionals from a wide variety of organizations were approached through the LinkedIn platform, with 154 providing responses. The professionals received a direct message in their LinkedIn inbox and were invited to participate in a survey via Google Forms with 4 questions about insider threats complemented by a brief socio-demographic questionnaire. Participants were informed that their answers were confidential, and the researchers had no opportunity to connect answers to their LinkedIn profiles. In terms of demographics, 83 % of the C-suite professionals approached in the survey were male and 17 % female, which reflects the global shortage of female executives [78]. The average age was 55, with average tenure in post of 5.3 years. The majority of participants (65%) represented large businesses (with over 500 employees); 25 % - businesses with 250 to 500 employees; and 10 % - small businesses of 250 employees or less. The participants occupied the following roles: CEO (Chief Executive Officer), CISO (Chief Information Security Officer), CTO (Chief Technology Officer), COO (Chief Operations Officer), CFO (Chief Financial Officer), and CDO (Chief Data Officer) with CISOs and CTOs forming 57 % of the sample. In terms of geographical composition, 58 % of respondents were from the US, 19 % from the UK, and 23 % from other countries.[2] The survey was conducted in English, provided executives with the brief study background and consent form, proceeding to ask C-suite professionals the following questions:

(a) *Do you utilize insider topologies in your daily work?*

Yes/No question (if the answer was Yes, the participant was asked to provide details in an open-ended format).

(b) *What are the key advantages or benefits of using insider topologies in your work?*

Open-ended question

(c) *What are the main disadvantages or drawbacks associated with insider topologies?*

Open-ended question

(d) *If you had an opportunity to modify existing insider topologies, what changes or improvements would you suggest?*

Open-ended question

Participants were asked to provide brief answers to each question (approximately one sentence or one short paragraph long). Only 23 of 154 C-suite professionals (15%) stated that they used insider topologies. We collated all answers and conducted text analyses of the survey answers using Natural Language Processing (topic modelling) approach. Specifically, we conducted analysis in 2 parts. *First*, we combined all answers and produced topic modelling mapping from the entire corpus of answers using the RoBERTa topic modelling approach. *Second*, we conducted a series of the Latent Dirichlet Allocation (LDA) topic modelling allocations with GPT2 tokenizer for each of the questions (b), (c), and (d) separately. All models were conducted in Python 3.11.3. The output of the RoBERTa topic modelling approach is presented in Table 1.

Our LDA analysis confirms the robustness of the obtained results (detailed code and output from the topic modelling exercise is presented in Appendix B). Note that our earlier (factor) argument based on the review of existing literature and the survey results from the C-suite professionals highlight several similarities, providing a strong justification for a more inclusive taxonomy to cover the full range of insider threats.

The literature-based (factor) argument mentions the limitations of current taxonomies in capturing the full spectrum of insider threats. This aligns with Topic 1 of the survey results, which discusses the shortcomings and limitations of existing taxonomies in capturing the complexity of insider threats. Both emphasize the need for improvement and a more inclusive approach.

The literature-based argument emphasizes the evolving technologies and their impact on insider threats. This corresponds to Topic 2 of the survey results, which focuses on unintentional insider threats arising from the rapid advancement of technologies. Both the argument and the survey results highlight the need for the proposed taxonomy to address the vulnerabilities associated with evolving technologies.

The literature-based argument mentions the challenges posed by remote work environments, expanding the attack surface for insider threats. This aligns with Topic 6 of the survey results, which emphasizes insider threats due to poor security awareness and training, specifically in the context of remote work environments. Both highlight the unique risks and the need to consider them in the new taxonomy.

Furthermore, the literature-based argument advocates for a holistic approach, considering organizational, technical, and environmental factors contributing to insider threats. This resonates with Topic 4 of the survey results, which emphasizes the need for comprehensive and adaptive approaches to insider threat management. Both highlight the importance of considering multiple dimensions and factors in the new taxonomy. For example, one executive wrote: "*Current taxonomies have served as a valuable tool in my cybersecurity practice. Despite their usefulness, they frequently neglect unintentional insider threats due to oversights or*

[2] Data from the survey available from: https://github.com/BehaviouralDataScience/insidertopology.

errors. I think the main problem is that we do not have enough dimensions in topologies. They need to incorporate more types and have more angles/ dimensions."

Our earlier argument also emphasizes the need for adaptive countermeasures and enhanced training and awareness. These align with the overall theme of the survey results, which highlight the importance of addressing different categories of insider threats and improving security awareness and training.

2.4. Developing VISTA (inclusiVe InSider Threat tAxonomy)

Built on the foundations of Loch et al. [79], later taxonomies e.g., [13,80] distinguished between internal and external threats and between human and non-human threats, as well as other categories of differentiation. In this paper, we focus only on *human* insider threats. We followed the taxonomy development process outlined by Nickerson [81] to derive VISTA.

Step 1 - Determine meta-characteristic:

We consulted a variety of existing insider threat taxonomies and typologies to identify the dimensions to be used in this taxonomy, starting with a very early taxonomy proposed by Loch et al. [79] and also consulting others [13,82–88]. We categorise insiders on the following dimensions, based on distinctions drawn in the research literature (see Fig. 1):

Dimension 1 (D1): **Knowledge –** *Unaware* vs. *Aware.* knowing what to do [89], or not. This is a pre-requisite for volition and compliance.
Dimension 2 (D2): **Compliance –** *Non-Compliant* vs. *Compliant.* Organisations craft policies and train their employees. As such, employees can choose to comply with policy mandates, or not [13]. There is a large body of research related to this choice e.g., [90–96].
Dimension 3 (D3): **Volition –** *Deliberate* vs. *Incidental Harm*. Insiders often harm organisations [63,97–99]. Insiders can act deliberately in this respect, or harm the organisation incidentally, as collateral damage when they are trying to act for their own benefit carrying out selfish yet non-malevolent actions [30]. The motivation is different, as should the amelioration and organisational response be [22,46,63,100].
Dimension 4 (D4): **Goal –** *For Self; For Society; For Ideals; For Malice*. Schoenherr and Thomson refer to a similar dimension calling it *ethicality* [101]. While organisations want their employees to act for the good of the organisation, insiders can act to satisfy other goals. They can: (a - *for self*) pursue their own goals for personal gain or to cut corners [102], (b - *for society*) act to right wrongs or to reveal an organisation's unethical behaviours, (c - *for ideals*) to act based on a personal ideology, or (d - *for malice*) to settle scores with the organisation [35,63,80,103,104].

Step 2 - Determine ending conditions:

Every dimension is unique, with its own set of features, and the taxonomy is inclusive.

Step 3 - Approach:

Empirical-to-Conceptual

Step 4 - Identify objects:

Within the context of insider threats, the *objects* are insider types who can harm the organisation. To ensure that all different types of insider threats were identified, we carried out a search of the literature: *keywords:* 'insider threat taxonomy' (excluding papers about insider threat detection), *years:* 2013 to present. SCOPUS delivered 623 results and Google Scholar delivered 73 additional results.

After filtering to retain only papers that address different kinds of insider threat types, either in a taxonomy or a list, we were left with 102 papers. Taxonomies or classifications of different kinds of insiders were extracted to arrive at a comprehensive set. The following named insider types were mentioned (semantically similar types merged):

#1 **Oblivious:** poorly trained by the organisation, and thus lacking awareness [11,31,105–107]. Non-compliance is not the causative because they are untrained or inadequately trained. An employee cannot be considered compliant nor non-compliant if they do not know the rules. This type of insider threat is more common than might be anticipated because many companies fail to train their employees adequately, at least in the UK [108].
→ **Also referred to as:** well-intentioned [11].
#2 **Wilfully ignorant:** refuses to take part in training or awareness programmes [109] or ignores training [110]. → ***Also referred to as:*** *non-responders* [111]; *insider hazards* [112]; *wilful recklessness* [103].
#3 **Imperfect:** makes mistakes [100,111,113–115], acting unintentionally or accidentally, perhaps due to forgetfulness [13] or misconceptions [116]. An example is mistakenly sending an email to the wrong person [73,117], physically losing a mobile device [118] or making a disposal error such as selling a mobile device without wiping the hard drive [100]. They might also be deceived by a social engineering attack [73] into taking an ill-advised action. This group exists because we are all *fallible* humans [119], and any employee can make a mistake and cause damage despite their best intentions.
→ **Also referred to as**: inadvertent [120,121]; careless [122]; cyber friendly fire [99,123]; passive non-volitional non-compliant [13]; unintentional [124,125].

#4 **Depleted:** overworked or treated unjustly, and might well become an insider threat due to being stressed and depleted [9,29,33,44–47,126] because they are fatigued or overloaded 59], because they are suffering from techno-stress [127] or because security-related stress leads to information security policy violations

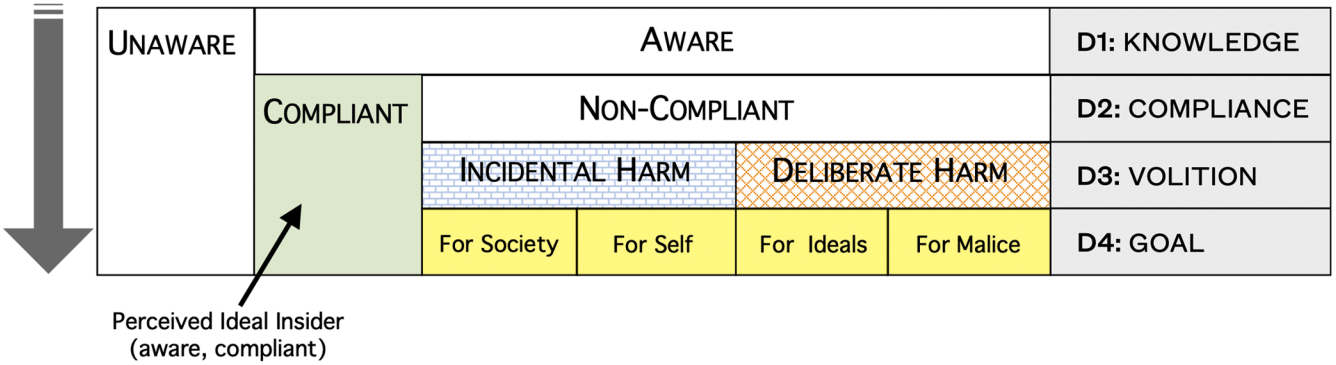


Fig. 1. Dimensions (Di) used by VISTA to classify insider threats.

[128]. These employees are not deliberately malicious but their actions can still harm the organisation.

#5 **Naïve:** does not deliberately act to subvert organisational policies or to harm the organisation, but might be pressured into cutting corners [129], or be too easily fooled by social engineers [72,99,130,131] Sometimes this kind of insider is overambitious and focuses primarily on performance goals set for them by the organisation. This may lead them to ignore security policies. → ***Also referred to as:*** *well-meaning* [73]; *well-intentioned* [53], *Samaritans* [132]; *pawns* [133–135].

#6 **Negligent:** is generally familiar with security and/or IT policies but deliberately choose to ignore them [22,53] [73,136] e.g., failing to log off when leaving a PC, poor password practice [137,13], or looking for an easy life [73]. They generally do not comply with security policies [31,13]. → ***Also referred to as:*** *volitional non-malicious non-compliant* [13]; *goof* [134,135].

#7 **Persistent pilferer:** uses company resources to supplement their income over an extended period of time [106,109]. This might be because they are addicted or have fallen upon hard times [138]. Whitty also points to those who are simply greedy or like to show off with a flamboyant lifestyle [102]. A Gartner report [139] found that 62% of insider threats were in this category. → ***Also referred to as:*** *career thieves* [132]; *fraudulent* [102]; *second-streamer* [140].

#8 **Malevolent:** acts to harm the organisation, often in retaliation for some perceived slight [22,48,53,99,111,141–144]. They might sabotage, steal data, embezzle, defraud or deliberately violate policies or carry out industrial espionage [13,23,24]. Their actions can be triggered by injury to male pride and ego or a sense of personal failure [145], disgruntlement, perceived mistreatment [9,27,45,146–149] anger management issues and ignorance of authority, as well as antisocial, narcissistic or Machiavellian tendencies [27,132,150,151]. → ***Also referred to as:*** *career criminals* [138]; *traitors* [11,21,125]; *lone wolf* [134]; *turncloak* [133]; *intentional malicious non-compliant* [13]. *Machiavellians, avengers* [132], *zealots* [11].

#9 **State sponsored:** identifies targets based on government interests, not personal financial gain [152,153]. They might steal intellectual property for their home country, for example.

→ Also referred to as: moles [133].

#10 **Extremist:** is driven by ideology [104]. Sometimes, the person infiltrates the organisation deliberately in order to harm it. In other cases, they become an extremist due to some trigger event while they are part of the organisation [104]. → ***This group also includes:*** *hacktivists*, who conduct activities for political or principle based reasons [152], and intend to do harm.

#11 **Mischievous:** intentionally misuses their privileges to make their jobs easier by using workarounds or unauthorised applications (not deliberately malicious) [99,115,118] or are bored with their jobs [154]. → ***Also referred to as:*** *underminers* [73]; *dangerous tinkering* [155]; *noseyness* [103]; *explorers* [132]; *browsers* [11]; *clever clogs* [138].

#12 **Colluder:** collaborates with an external threat actor to compromise an organisation [22,121,156], either willingly or because they are being coerced [144]. An insider might be directly recruited to carry out fraud or espionage or steal intellectual property [109,122]. → ***Also referred to as:*** *moles* [111]; *masqueraders* [48]; *insider affiliates* [25]; *collaborator* [135].

#13 **Outsider-insider** could be a contractor or vendor who has been given access to facilities, systems, networks, or people brought in to complete some assigned task [22,143,153,156,157]. → ***Also referred to as:*** *insider or outsider affiliate* [25].

#14 **Hero:** does not act for personal benefit but rather for the benefit of society as a whole when they believe that their employing organisation is acting unethically [37–40,158] and is a heightened 'digital age' threat [159]. As such, heroes are very different from the other insiders, in that many would actually approve of their actions. Even so, they use their legitimate access to organisational assets contrary to the purpose for which such access is granted. As such, they do indeed violate internal company policies. External whistleblowers' actions are extremely likely to violate the confidentiality of organisational information and lead to reputational harm [160]. They often take organisational secrets with them (leakage specifically mentioned by insider threat taxonomies proposed by [161] and [2]). → ***Also referred to as:*** *data leakers* [73].

#15 **Entitled:** feels technological entitlement, which predicts bad behaviours and this relationship is stronger when organisations impose restrictions on technology usage [132,162]. This could be because they become emotionally attached to systems they support and might even destroy those systems if their control is taken away [163].

#16 **Bird of a Feather:** is part of a tightly-knit group of similar ages and ethnicity, often model employees, who work together to subvert organisational cybersecurity for personal gain [138].

#17 **Ex-Employee:** has been fired or has left a company use their non-terminated credentials to access the organisation's systems to carry out their nefarious purposes [164].

#18 **Violent:** causes physical harm to fellow employees or to equipment [165]. Cetinkaya et al. [166] mention a number of different kinds of workplace violence, including abusive supervision, bullying, social undermining and incivility. Workplace violence can, if not dealt with, lead to acts that can damage the organisation in the long run [165].

#19 **Rule followers:** rigidly follow the security policy rules, which seems to make them the ideal insider. However, policy rules are: "*static, comprehensive limits of freedom of choice, imposed on operators at the sharp end and violations are seen as negative behaviour to be suppressed*" [167] (p. 222) and are only effective when the threats do not evolve. In reality, Generative Artificial Intelligence (GAI) tools used by hackers [168] (e.g., WormGPT) [169] have introduced dynamism into exploits [76]. For example, employees are often instructed to look for inconsistent language and other signs that emails are not legitimate. Yet, if GAI is used, these signs are easily and automatically removed [170] so that this advice is no longer helpful. In one fell swoop, lists of static rules, if dutifully complied with, are unlikely to prevent successful Phishing attacks [171]. Unthinking obedience to rules might, in reality, facilitate sophisticated cyber attacks [172].

Confirming inclusiveness of object list

To confirm this list of insiders, we searched for news reports about insiders who have harmed organisations using digital means, either deliberately or unwittingly. To find industry and news reports, we searched for 'examples' and 'insider' and 'harm or damage' (2019-present). In all, 72 distinct cases were returned by the search. Only one example from each type is mentioned to demonstrate that the taxonomy can accommodate it.

#1 *Oblivious*: An employee fell for a Phishing attack and lost the company thousands of pounds [146]. When the company attempted to sue the employee to recoup their losses, the judge discovered that the employee had not been adequately trained [173] and dismissed the case.

#2 *Wilfully Ignorant*: Germantown Alderman Dean Massey, a city leader of Memphis, Tennessee, refused to do cyber security awareness training. The city's IT director removed his access to email [174].

#3 *Imperfect*: An employee accidentally exposed health data of patients in a misdirected email [175].

#4 *Depleted*: Joshua Adam Schulte was a Central Intelligence Agency (CIA) employee convicted of leaking classified documents to

WikiLeaks [176]. His trial revealed a toxic workplace with widespread bullying and retaliation [177].
#5 *Naïve*: Twitter employees were taken in by a vishing attack and persuaded to give their credentials away [178].
#6 *Negligent*: A Comparitech employee exposed 250 million Microsoft customer records, spanning 14 years, due to not patching their device [144,179].
#7 *Persistent Pilferer*: An employee stole customers' credit card details and used them to pay her bills [180].
#8 *Malevolent*: Elon Musk reported an employee who committed sabotage because he did not get a promotion [181].
#9 *State Sponsored*: Tunggal [111] reports on Greg Chung, a Chinese born American citizen who stole intellectual property for the Chinese government over decades [182].
#10 *Extremist*: Members of animal rights extremist groups gained employment at companies to obtain photos and videos [183].
#11 *Mischievous*: A Boeing employee emailed a confidential spreadsheet to his home email to work on and showed it to his wife [184].
#12 *Colluder*: An employee was bribed by an outsider to introduce malware into their employing organisation's computers [185].
#13 *Outsider Insider*: Reality Winner was a contractor to the USA's NSA, and leaked information to a journal called The Intercept [186].
#14 *Hero*: Edward Snowden stole data from the USA's NSA and gave it to journalists [35], because he felt that the NSA was behaving illegally.
#15 *Entitled*: Terry Childs, an IT administrator, refused to hand over administrative passwords to the city of San Francisco, arguing that he was the only person who could take care of the network properly [187].
#16 *Birds of a Feather*: Four employees of Armstrong Teasdale stole corporate data and left the organisation *en masse* [188].
#17 *Ex-Employee*: A Cisco ex-employee used his non-terminated access credentials to delete 16,000 employee accounts [189].
#18 *Violent*: In 2021, an employee who had been fired accessed his employer's computer systems and destroyed over 21 gigabytes of data in revenge [190].
#19 *Rule Follower*: In 2019, a UK energy firm was scammed out of US$243,000 when criminals used AI to impersonate the CEO's voice to order an employee to transfer funds to a supplier [191], presumably because he/she was accustomed to receiving this kind of verbal instruction from the CEO and he/she was convinced that it was the CEO at the other end of the call due to recognising his voice.

Step 5 - Identify common characteristics:

During this step, insiders were grouped into categories, as shown in Fig. 2. In Fig. 3, we show how each of the insider threat categories map to the overview diagram in Fig. 1. The interesting part of this diagram could be expressed as "Compliance is not enough" – there are a number of insiders who are indeed compliant, but who still become insider threats, albeit unintentionally.

Step 6 - Group into categories:

Grouping insider threat types into categories sharing the same characteristics, we arrive at the following insider threat categories based on shared characteristics (#i refers to the Object number in the previous list of insiders):

Category 1 (C1). **Untrained – doesn't know rules** (#1 *Oblivious*) — unaware or poorly trained so that they do not know what actions they need to take or how to carry them out. As such, they are neither compliant nor non-compliant but rather blissfully oblivious.
(D1: Unaware)
Category 2 (C2). **Fallible – breaks rules accidentally** (#3: *Imperfect*, #4: *Depleted*, #5: *Naïve*) — aware of actions to take (trained) but make mistakes that hurt the organisation, perhaps due to a lack of technological savvy [154], due to wanting to meet organisational

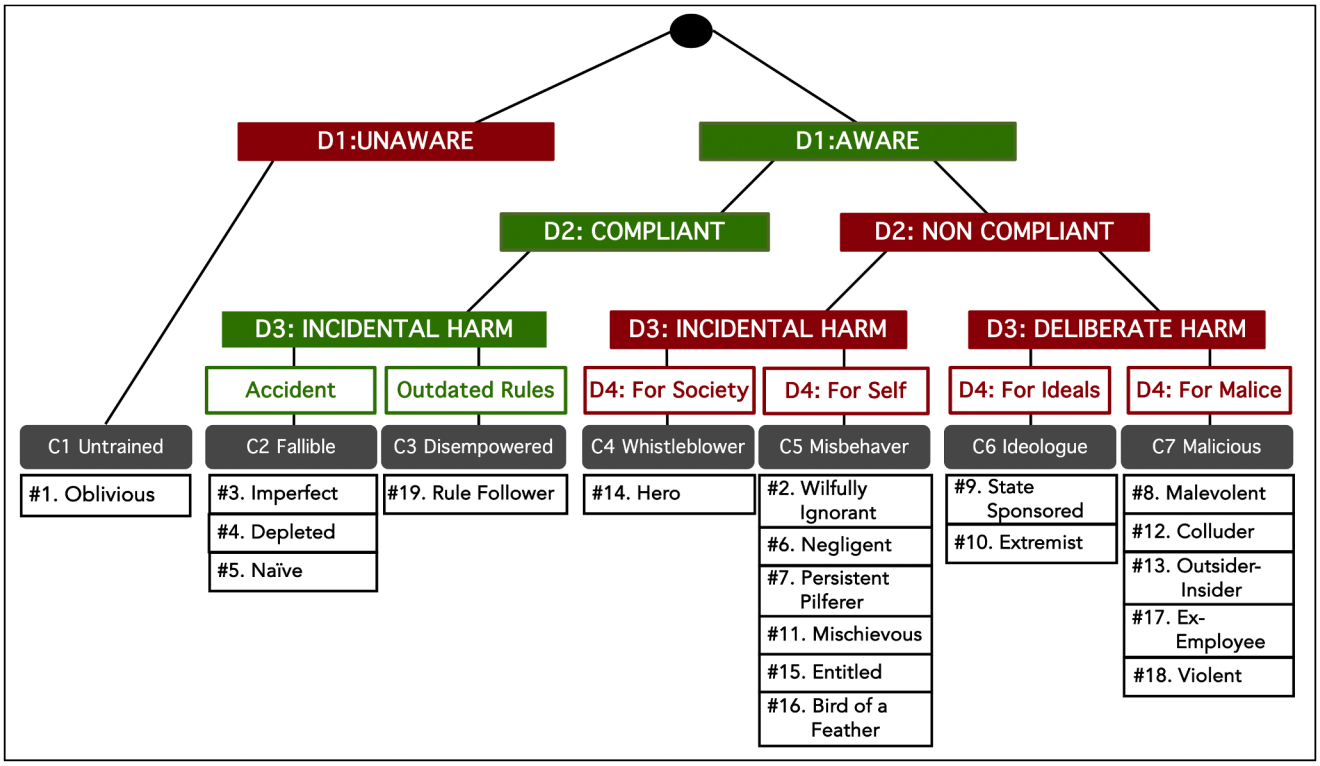


Fig. 2. Grouping insider threats according to dimensions (Di from Fig. 1) to categories (Ci) of insider types (#i).

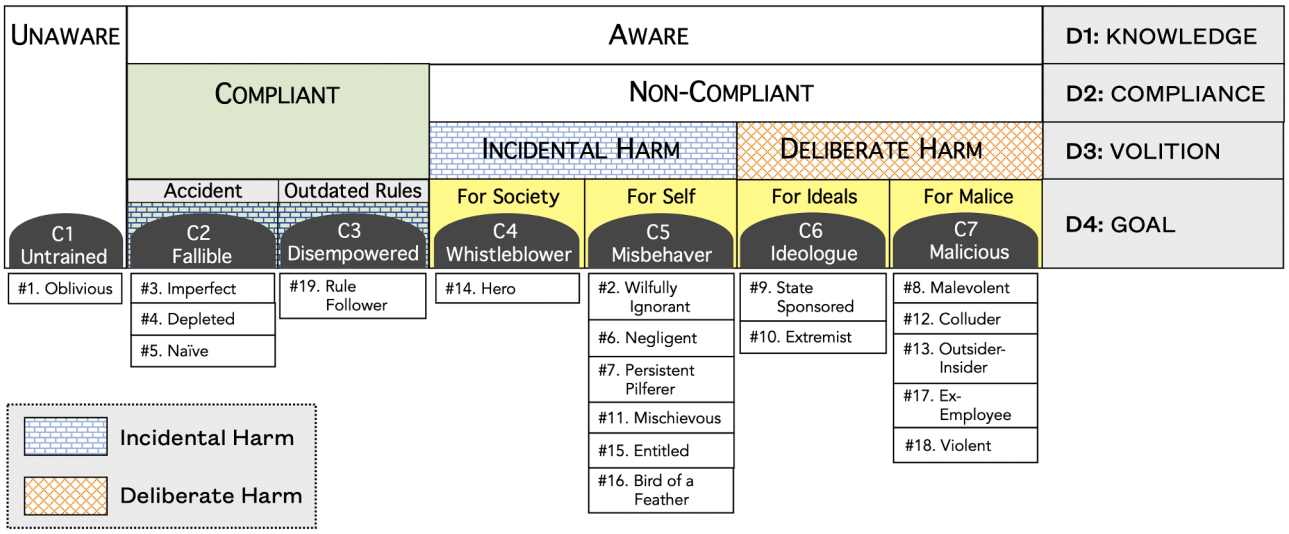


Fig. 3. Allocation of insider threat categories (Ci – Fig. 2) based on insider threat dimensions (Di – Fig. 1).

expectations [73], or perhaps because they are particularly susceptible to being deceived by cyber criminals [192,193].
(D1: Aware; D2: Compliant; D3: Incidental Harm)

Category 3 (C3). **Disempowered – rigidly follows (outdated) rules** (#19: *Rule Follower*) — insiders who are not agile in terms of being keen to resist emerging, novel threats: the new reality in the GAI era of cybersecurity.
(D1: Aware; D2: Compliant; D3: Incidental Harm)

Category 4 (C4). **Whistleblower – acts for the benefit of society** (#14: *Hero*) — seeks to benefit society because they consider the organisation to be acting unethically or unlawfully. Does not deliberately seek to harm the organisation but rather seeks to improve the way it functions.
(D1: Aware; D2: Non-Compliant; D3: Incidental Harm; D4: For Society)

Category 5 (C5). **Misbehaver – acts for own best interests** (#2: *Wilfully Ignorant*, #6: *Negligent*, #7: *Persistent Pilferer*, #11: *Mischievous*, #15: *Entitled*, #16: *Bird of a Feather*) — knows what to do, but chooses not to comply e.g., saving effort or acting on a desire for convenience [154].
(D1: Aware; D2: Non-Compliant; D3: Incidental Harm; D4: For Self)

Category 6 (C6). **Ideologue – acts for ideals** (#9: *State Sponsored*, #10: *Extremist*) — deliberately acts against the organisation, but not for personal gain. They are driven by ideologies, which means that they are happy to sacrifice themselves.
(D1: Aware; D2: Non-Compliant; D3: Deliberate Harm; D4: For Ideals)

Category 7 (C7). **Malicious – acts to hurt the organisation** (#8: *Malevolent*, #12: *Colluder*, #13: *Outsider Insider*, #17: *Ex-Employee; #18: Violent*) — deliberately seeks to harm the organisation, often, but not always, because they are disgruntled [80,121].
(D1: Aware; D2: Non-Compliant; D3: Deliberate Harm; D4: For Malice)

These categories make tailored mitigations more feasible. For example, for the untrained, mitigations involve retraining – and such training should empower rather than creating rule followers given the dynamism of the cyber crime domain. For the fallible group, mitigations should rather seek to ensure that employees are not overworked or stressed. Traditional measures for improving compliance [94] are unlikely to prevent whistleblowers from acting: they are gathering evidence to prove their case and this is a powerful incentive for non-compliance. We will return to the topic of tailored mitigations in Section 3.

Step 7 - End conditions met? We repeated Steps 4–6 until no new objects were added.

Visualising the taxonomy:
Fig. 4 offers a visualisation to inform the way interventions can be tailored based on the dimensions mentioned in Section 2.4 (Step 1). In particular, Dimension 1 can be addressed by delivering more effective training. Dimension 2 can be addressed with measures calculated to increase compliance. Dimension 3 informs mitigations: if someone is ill-intended the organisation's response is very different from when they have made a mistake and inadvertently compromised organisational assets. Human fallibility can only be ameliorated, but never prevented - these insiders need support, not sanctions. Volitional (damaging) behaviours, on the other hand, can be discouraged using a range of interventions. The fourth dimension is related to whether the person acts for self, for society (whistleblowers), or against the organisation. Addressing the malicious and ideologues requires different types of interventions, as we will discuss in the next section. Table 2 compares and contrasts our VISTA taxonomy with pre-existing taxonomies.

3. Insider threat mitigation

The National Infrastructure Advisory Council (NIAC) [4] reports that "*...preventing all insider threats is neither possible nor economically feasible...*" (p.13). Even so, there are some measures we can take to reduce the threat. The Gartner report by Heidt [139] suggests that only a minority of organisations have a formal [counter-insider] program in place. It should be mentioned that their 'insiders' align with our C5, C6 and C7 categories, not the fallible nor untrained, and they do not address whistleblowers or rule-followers.

There is a need to apply a more nuanced approach to that espoused by industry at present i.e., *train and mandate compliance, train often and remind of compliance, and train after people make mistakes* [113,197–200]. VISTA covers a far greater range of issues which lead to employees becoming insider threats. While training is essential, and encouraging compliance advisable, it can hardly address the full range of threats.

Approaches for addressing the insider threats are categorized by Alsowail and AlShehari into three classes: (1) detection approaches e.g., [201–203], (2) detection & prevention approaches e.g., [125,204,205] or (3) prevention approaches [206].

The first two involve technological measures, and many of these have been proposed. For example, technical monitoring [63,207–209], anomaly detection [2,206], tracking and controlling access paths [208, 210,211] ensuring that appropriate trust is given [212]. Technical

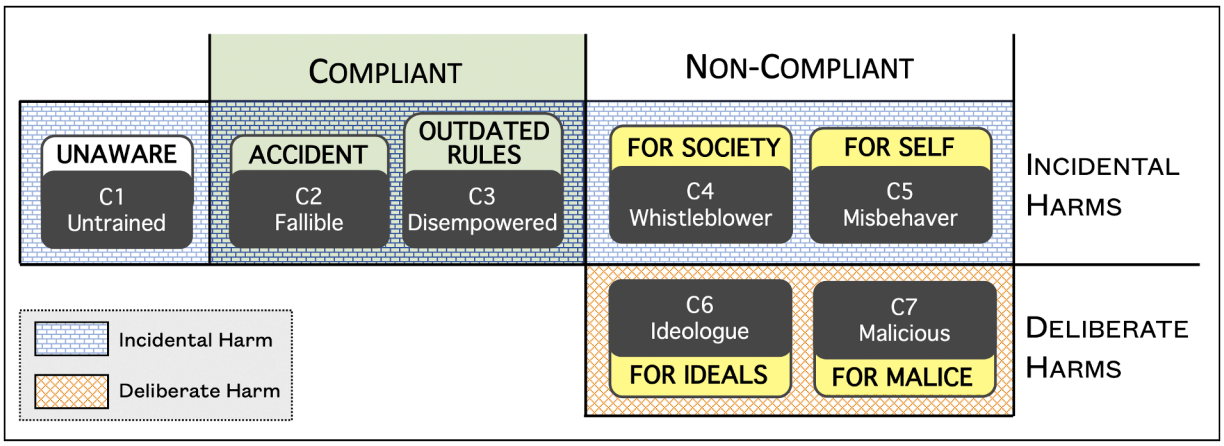


Fig. 4. VISTA (inclusiVe InSider Threat tAxonomy) visualisation (Ci refers to insider threat categories from Fig. 2).

Table 2
Circling back to compare to other insider threat taxonomies.

	C1 Untrained	C2 Fallible	C3 Disempowered	C4 Whistle blower	C5 Misbehaver	C6 Ideologue	C7 Malicious
	Oblivious	Imperfect Depleted Naïve	Rule Follower	Hero	Wilfully Ignorant Negligent Persistent Pilferer Mischievous Entitled Bird of a Feather	State Sponsored Extremist	Malevolent Colluder Outsider-Insider Ex-Employee Violent
INSA [194]	Unintentional Insider Threat				Insider Fraud	Theft of IP	Sabotage Workplace Violence
Loch et al. [79]	Accidental				Deliberate		
Willison & Warkentin [13]		Passive Non-Volitional Non-Compliance			Volitional (but not malicious) Non-Compliance		Intentional malicious computer abuse
Hashem et al. [85]		Apathetic			Apathetic		Malicious
Al-Mhiqani et al. [48]		Unintentional			Masquerader		Misfeasor
Homoliak et al. [2]	Unintentional	Benign		Whistle blower		Malicious	
Anderson [69] Salem [62]					Misfeasors Clandestine		Masqueraders Traitors Masqueraders Traitor
Cappelli [141]					Fraud	Theft of Intellectual Property	IT Sabotage
Hayden [11] Shaw & Fischer [132]	Well-intentioned			Zealot	Browser Explorers Samaritans Machiavellians Proprietors	Moles	Traitor Hackers Avengers Career thieves
SOFIT [195]	Unintentional/Accidental			Intentional/Malicious			
					Fraud	IP Theft	Workplace Violence Sabotage
Cole & Ring [25]				Self-motivated		Planted	Recruited Self-motivated
Wall [73]	Well Meaning	Socially engineered			Negligent Underminers Overambitious		
				Data Leakers			
Green [123]					Property Deviance Production Deviance		Personal Aggression
Ray [196]					Careless		Malicious Compromised

measures do have some disadvantages [103]: (1) they detect behaviours that have already occurred, (2) they often generate false positives, (3) nefarious activities may merge into the 'normal', and (4) employee privacy might easily be violated. Indeed, other authors also argue that technical measures cannot, by themselves, mitigate the insider threat [30,193,213].

In this paper, we consider the third class - also the most challenging according to Alsowail [206]. Yet, Ashford [214] argues that insider threats are indeed preventable if the right people management processes and tools are used. Hence, we focus purely on prevention of

human-based insider threat prevention strategies from the research literature to address the insider threat in each of the categories identified in Fig. 2 referred to as Ci.

We first searched the literature for insider threat mitigations and interventions and excluded technical measures. Table 3 maps interventions to different categories. Consider that training will only be effective to those who wish to be compliant (C1, C2). In the case of C3, training might actually be counter-productive if it is too rigidly rule-based. Those who are non-compliant and are *not* deliberately harming the organisation, certainly know what to do, but are choosing not to do it (C4 & C5). Those who seek to harm the organisation (C6 & C7) are probably resistant to training and policy dictates, so prevention, in these cases, is likely to rely heavily on detection, but vetting of new employees can also help to prevent nefarious insider activities in these cases. Finally, C3 is a new category, which highlights the need for more nuanced training to develop the ability to detect new and emerging exploits. We now briefly discuss each of the insider categories, and the most appropriate mitigations, in turn.

3.1. C1: untrained (D1-unaware)

People may have been poorly trained [89] or trained too long ago to remember the security measures [232]. The way training is delivered is important. Donalds et al. [92] suggest that training should be made fun and learning made as easy as possible. Boss et al. [233] found that if, during training, the principle of 'mandatoriness' is conveyed, people would be more likely to take security precautions, yet we have to bear in mind that this might convert the unaware (C1) to a rule follower (C3).

Unfortunately, some commonly used behavioural control mechanisms can actually backfire. For example, both Wall & Buche [234] and Renaud & Dupuis [235] warn against the use of fear tactics during training sessions. Moreover, Cram et al. [236] found that threats of punishment or rewards were not particularly effective.

In summary, periodic training is essential because human memory is an unreliable mechanism – leading to forgetting over time. Moreover, new threats emerge [237], so training materials must be kept up to date. As such, train people when they enter the company, and have regular refresher courses. Moreover, ensure that they develop self-efficacy and competence in the actions security requires [91,236,238,239].

3.2. C2: fallible (D1-aware, D2-accidentally non-compliant, D3-incidental harm)

Humans make errors [74] and cannot be 'fixed' to prevent this. Reason explains that there are two types of human error: (1) slips, and (2) lapses. An example of the former is when someone knows exactly what to do but makes an error in carrying out the action; perhaps clicking on the wrong button by mistake. Lapses, on the other hand, often occur when someone forgets to do something. For example, someone may forget to encrypt a file, or to unplug a memory stick before leaving a computer. Every human on the planet has made a slip or experienced a lapse. Moreover, training will never prevent either of these [100]; they are due to our humanity.

Lapses are more likely to occur if people are fatigued, burnt out, upset or frequently interrupted [44,89,232,240], so managers should be trained to spot signs that people are distressed so that steps can be taken to prevent a lapse [241].

However, if someone *does* cause a cybersecurity incident due to a slip or lapse, it is crucial for them not to be victimised or shamed [218], because that might lead to their becoming a far greater threat due to a perception of being treated unfairly (e.g., C7) [242].

3.3. C3: disempowered (D1-aware, D2-compliant with outdated rules, D3-incidental harm)

This category might seem counter-intuitive. After all, the formulating, disseminating and enforcing of security policies, basically sets of rules, is at the core of cybersecurity preventative measures, and often checked by auditors. However, secure computing, like safe driving, requires agile responses that necessitate knowledge breadth, depth, and finesse [228]. Drivers must respond to driving threats by slowing down or engaging in evasive manoeuvres, regardless of legal compliance or violation. These poorly-defined ambiguous actions make for safe drivers, because they rely on the discretion of the individual. Similarly,

Table 3
Mapping interventions to insider threat categories (Ci refers to category in Fig. 4).

	Untrained	Fallible	Disempowered	Whistleblower	Misbehaver	Ideologue	Malicious
Individual employees	C1	C2	C3	C4	C5	C6	C7
Regular training [132,208,211,215,] which specifically addresses evolving threats [76].	•	•	•		•		
Just-in-time reminders [216]		•			•		
Empower employees [31,216,217]		•	•		•		
Employee support [208,209,212,218]		•			•		
Employee counselling [208,219]				•	•		•
Reduce provocations [210,211,212]				•	•		•
Policy/process	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
Screen new hires [11,220,211,221]						•	•
Design security policies holistically [222]; report response efficacy [31]; renew regularly [132,221]	•	•			•		
Remove neutralisation excuses [90,210]					•		•
Sanctions [4,31,208,210,215,219,223]					•		
Management effort	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
Educate management about insider threats [220] and show organisational commitment [31]; Educate management on employee needs [218]		•		•	•	•	•
Non-blame organisational culture [217]	•	•	•		•		
Identify employees with highest potential to cause harm [229,132]					•		
Do not have a toxic work culture [177,209]	•	•			•		•
Reduce rewards [210]					•	•	•
Social interventions [230,231]			•		•		•
Termination of employment [132,208]						•	•
Have an insider threat program [132,207]					•	•	•
Whistleblowing	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
Behave ethically [224,225]				•			
Incentivise internal whistleblowing [226]				•			
Act upon internal whistleblowing reports [227]				•			
Allow rule breaking and develop anomaly spotting [228]			•				

strict compliance with formal information security policies is sometimes insufficient - employees should be empowered to develop and apply nuanced insights as they engage in agile vigilance to identify emerging and novel threats [228]. This means that training employees to apply security knowledge appropriately is the best way to address undefined and emerging security threats [243] and empowering employees to break rules if the situation requires this and doing so serves to secure organisational information and devices. In effect, trusting employees to behave securely, and allowing them to exercise their judgement in situations where the regular rules (having lapsed due to GAI capabilities) no longer meet the needs of organisational cybersecurity.

3.4. C4: whistleblower (D1-aware, D2-deliberately non-compliant, D3-incidental harm, D4-for society)

Valentine et al. [224] argue that whistleblowing is motivated by a desire for ethical decision making to take place within organisations. If organisations do indeed want to behave ethically, they should want to be informed about areas of unethical practice within their organisations [244]. Hence, create an internal whistleblowing process to ensure the organisation is informed about areas of unethical practice within their organisations [244]. They must act on reports. Finally ensure that the whistleblower is given feedback on investigations and actions taken in response to their reports., so that an external whistleblowing event does not occur.

To this end, Chen et al. [226] suggest that internal whistleblowing ought to be incentivised so that any unethical practices can be uncovered as quickly as possible. King et al. [245] suggest that organisations ought to establish alternative reporting mechanisms to facilitate internal whistleblowing. Dungan et al. [246] find that educating employees in terms of *how* to blow the whistle makes it more likely that they will do this internally rather than externally, where it becomes a damaging insider threat incident.

3.5. C5: misbehaver (D1-aware, D2-deliberately non-compliant, D3-incidental harm, D4-for self)

This group includes a number of different kinds of insider threat (see Fig. 2). Amaro [247] argues that managers should be on the lookout for people engaging in *vices* such as gambling, which could push them towards bad behaviours such as *persistent pilfering*. He also suggests that employee training include an element of insider misbehaviour stigmatisation. It is clearly important for such training to occur regularly [216].

Hwang and Cha warn that situational stressors within an organisation can trigger destructive behaviours [127]. Sarkar et al. [94] also find that the organisation's culture has a substantial impact on policy compliance. For example, if the organisation has a culture of mistrust, employees may feel that they do not have to behave in a trustworthy way [212]. If there is a culture of counterproductive workplace behaviours or deviance, insiders might well become misbehavers [248].

Barlow et al. [90] found that informational and anti-neutralisation communication had the ability to reduce violation intentions. This is confirmed by Bauer et al. [222]. Bore [109] suggests that the principle of least privilege or principle of least authority is the best defence against this particular kind of insider. However, he also points out that overly strict controls can lead to the use of *shadow IT* [106], a form of non-malicious policy violation.

Litan [135] suggests using continuous insider screening to detect anomalous behaviours. Bore recommends that the rationale behind implemented controls be communicated to all staff members so that they understand their usage [106]. Organisations have to tread a fine line in terms of formulating policies that they expect employees to comply with. Lowry and Moody [249] find that employees will sometimes react negatively to new security controls, instead of complying with them. Jeong and Zo [250] also warn against overly hard security enhancement measures that impinge too much on employee autonomy. They explain that doing so could lead to the opposite of the intended outcome of the security measures: less security.

3.6. C6: ideologue (D1-aware, D2-deliberately non-compliant, D3-deliberate harm, D4-for ideals)

Thompson [152] says of hacktivists: "*These attackers possess varied levels of sophistication similar to those of state-sponsored and APT groups or script kiddies.*" (p. 72) and confirms that they are not motivated by financial gain, but rather their own ideologies. Hence, security awareness training and other similar measures are likely to be ineffective in mitigating this kind of insider threat. Thompson argues that when considering interventions, it makes sense to combine all kinds of ideologues. He recommends doing a rigorous risk analysis, and to enforce the NIST Cybersecurity Framework [251], using internal controls as well as using technical measures to highlight anomalies and to monitor systems to detect events as quickly as possible. BaMaung et al. [104] agree with this approach, when referring to mitigating the threat from extremists. Beena and Humayoon [153] conclude that both technical and sound security management principles can mitigate this threat type, the latter including the principle of least privilege, background checks and monitoring of user behaviours to detect signs of anomalous or malicious activities.

3.7. C7: malicious (D1-aware, D2-deliberately non-compliant, D3-deliberate harm, D4-for malice)

Cressey's fraud triangle suggests that pressure, opportunity, and rationalisation are necessary for people to commit fraud [252]. Researchers have addressed each of these in addressing the wider category of insider threats. CERT [80] explain that most malicious insiders act due to becoming disgruntled (*motivation*). This might occur due to a denied promotion or a lack of recognition [212,247]. Other employees might act maliciously because they are able to [106,109] (*opportunity*). Hence, using technical measures to control access is essential in mitigating this threat Others might have debts they are unable to pay [253] (*pressure*), which may lead to fraud. Cline [254] agrees that even though Cressey's three factors are present, the individual must also have the *capability* of intentionally committing the crime. These four factors align with Wolfe and Hermanson's [255] fraud *diamond* factors.

Weber et al. [256] argue that it is worth trying to spot the signs that someone might become an insider threat, because early interventions can prevent this. Other researchers [33,148] also contend that employees will exhibit warning signs that can be detected. This makes it possible for remediation to be attempted before the person becomes committed to carrying out actions that will harm the organisation [103]. However, Bell et al. [257] find that this is non-trivial and that there is a general reluctance amongst staff to report concerning behaviours by other staff.

4. Discussion

This paper brings together the extensive literature on insider threats, synthesising and consolidating all recommendations to provide a helpful summary for organisations to benefit from. What we are proposing is a "*tailored insider threat mitigation strategy*". To tailor insider threat mitigations, we needed first to scope the full range of insiders, which led us to derive VISTA, we developed in Section 2, visualised in Fig. 4. We then reviewed the literature on mitigations and provided a tailored set of mitigations for the different categories of insider threats in Section 3.

Our contributions to *practice* include informing managers of the types of threats and their motives, so that strategies can be tailored to thwart (in advance) or ameliorate and recover from (afterwards) the actions of insider threats. Rather than treating all anthropomorphic threats monolithically, effective measures require a nuanced understanding of the motivations and precursors of insider threat actor behaviours.

Though the outcomes of various insider-originated data breaches may be similar, companies would be advised to look 'left of bang' [13] to explore the root causes of these events to formulate managerial responses and programs to detect and prevent them. In other words, in the same way that tailored instruction is considered 'best practice' [18,258], the insider threat management field could benefit from considering the same approach.

Our contribution to *research* starts with a finer-grained framework for identifying the full range of insider threat types. Previous efforts have provided insights and informed our work, which we assert provides even greater perspective on the numerous factors and circumstances that contribute to this important omnibus research problem. To problematise the phenomena and the established research in this area, we have drilled more deeply into the opportunities to explore and understand the 'edges' and boundary conditions of theories related to each prior category of insiders to offer a deeper look at the many types of insiders. Though a broad unified theory about insiders may never be possible, our framework provides a meaningful tool for further theorising about this important nomological network.

4.1. Bringing everything together

At this point, it makes sense to return to the topics that emerged from the survey reported in Section 2.3 for elaboration (Table 1 - Numbers in this list refer to topic numbers in the table).

1 ***Limitations of current taxonomies:*** we use four different dimensions to distinguish insiders from each other, which is more fine-grained than many other taxonomies as shown in Table 2. Moreover, we include one new category of insider (C3) which reflects the new era of cyber that has been ushered in by widespread use of Generative AI [5,229].

2 ***Unintentional insider threats***: Addressed by: C1 (Untrained), C2 (Fallible) and C3 (Disempowered) categories.

3 ***Incomplete coverage of insider behaviours***: Addressed by: Categories C4 & C6 (Whistleblowers & Ideologues) address those who act from personal convictions. Category C5 (Misbehaver) includes those who act for personal convenience or effort saving. Moreover, the newly emerged C3 category has not been included by any existing taxonomies.

4 ***Need for comprehensive & adaptive approaches***: Covered by C3 (Disempowered). We include the need to ensure that training addresses evolving threat types (see Table 3) as well as acknowledging that rules might be outdated and insufficient, so that employers should be empowered to break ruled if necessary.

5 ***Insider threats from Ex-employees***: Covered by C7 (Malicious).

6 ***Insider threats due to poor security awareness and training***: Covered by C1 (Untrained).

7 ***Insiders misusing privileges and access***: Covered by C5 (Misbehaver).

8 ***Overcoming simplification & reductionism***: Our taxonomy has sought to be more inclusive and nuanced, which addresses this issue, as can be seen in Table 2. Moreover, we introduce a new kind of insider threat, Category C3 (Disempowered). Before the advent of generative AI, this was not an insider threat category, but now that hackers have these tools, the traditional rule-based approach is no longer sufficient (Fig. 5).

4.2. The ideal insider

What does the "ideal insider" look like, given that we have argued that rule-following insiders can still unwittingly become insider threats? The reality is that rules very quickly become outdated and policy changes cannot hope to keep up with evolving exploits, especially in the

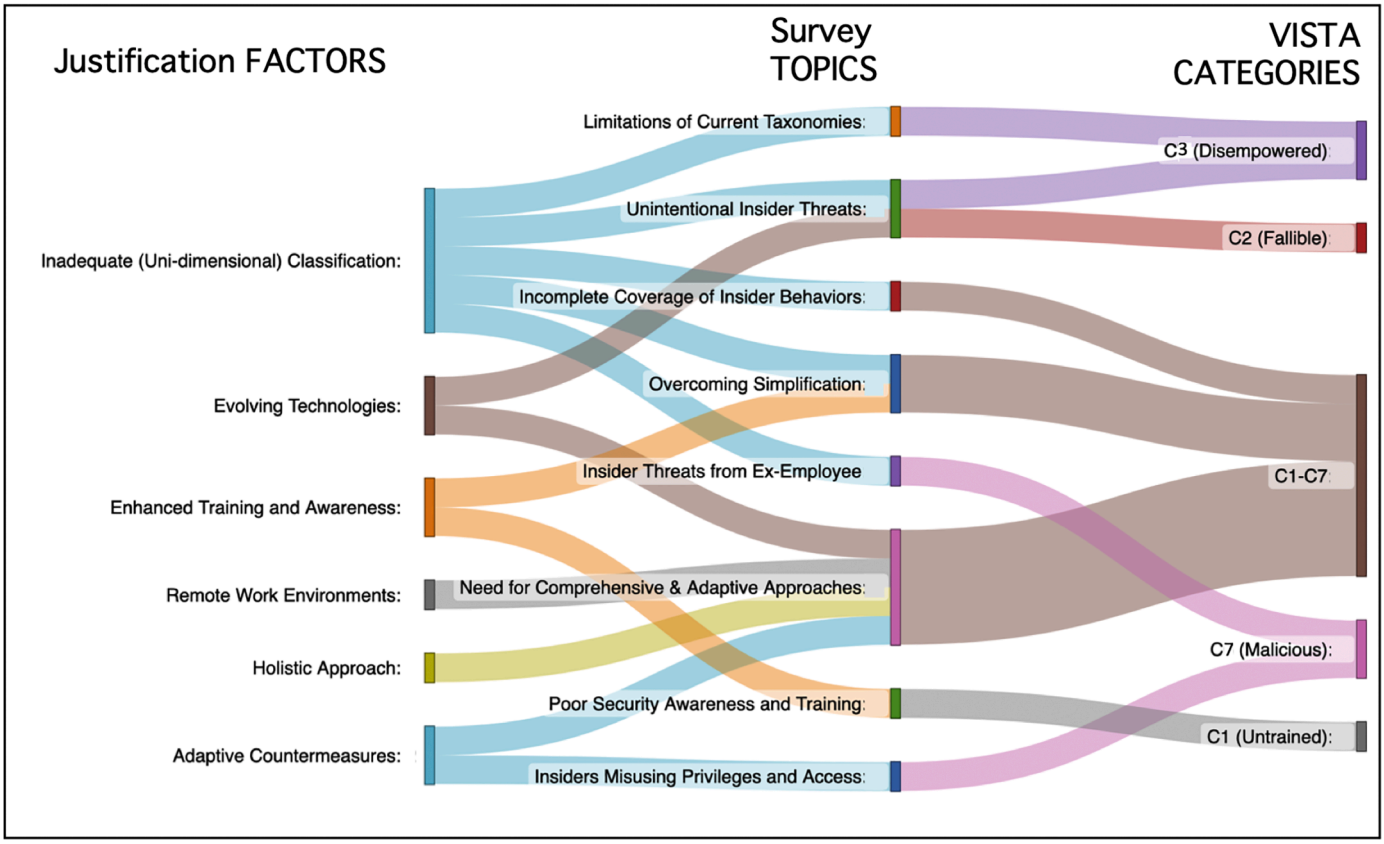


Fig. 5. Mapping initial justification factors from Section 2.3 to C-suite survey response topics (Table 1) and VISTA categories (Fig. 3).

GAI era. Cybersecurity needs to shift from constraining and controlling employees with information security policy rules [172] if we are to withstand the new kinds of exploits enabled by GAI. We should rather benefit from the proven human ability to spot anomalies. We should encourage commitment to organisational cybersecurity, instil the ability to be agile in spotting new exploits, and give insiders permission to break rules if doing so will preserve organisational cybersecurity. This, then, is the insider the new GAI era requires to preserve organisational cybersecurity. This insider is less likely to become a threat, and far more likely to be part of the solution.

5. Conclusion

Archileta says: "*Employers often have the opportunity to help move workers away from the ledge and back into the fold as productive and trusted employees*" [212] (p. 42). As such, the employer and the employee should be seen as a team, not as adversaries, in preventing insiders from becoming threats. This applies to fallible and untrained employees. Whistleblowing, too, can be averted by the organisation's practices and management being ethical and law-abiding. On the other hand, there are undeniably insiders who set out to harm the organisation, and these insiders need to be deterred and mechanisms should be implemented to prevent such activities. Table 3 proposes a number of measures that can be used to reduce each kind of insider threat.

Organisations should not rely only on awareness and training initiatives combined with punitive enforcement of compliance. While these are helpful strategies, they are not sufficient in terms of addressing the full range of insider threats. As such, we propose that insider threat mitigations be tailored: *the **most effective** mitigation for the **particular kind of insider** at the **right time**.*

CRediT authorship contribution statement

Karen Renaud: Conceptualization; Methodology; Derivation; Validation; Writing - original draft; Writing - review & editing. **Merrill Warkentin:** Conceptualization; Writing - original draft; Writing - review & editing. **Ganna Pogrebna:** Data Curation, Formal Analysis, Software, Visualization; Writing - original draft; Writing - review & editing. **Karl van der Schyff:** Writing - original draft; Writing - review & editing.

Appendix A

Table 4
Mapping interventions to insider threat dimensions (Di refers to dimension in Section 2.4) & categories (Ci refers to Insider threat categories in Fig. 2).

Knowledge (aware vs. unaware)	Compliance (compliance vs. non-compliance)	Volition (incidental vs. deliberate harm)	Goal (for self; for society; for ideals; for malice)			
D1	D2	D3	D4			
Individual employees			D1	D2	D3	D4
Regular training [132,208,211,215] which specifically addresses evolving threats [76].			•			
Just-in-time reminders [216]				•		
Empower employees [31,216,217]				•		
Employee support [208,209,212,218]				•		
Employee counselling [208,219]				•		
Reduce provocations [210,211,212]					•	
Policy/process			**D1**	**D2**	**D3**	**D4**
Screen new hires [11,211,220,221]						•
Design security policies holistically [222]; report response efficacy [31]; renew regularly [132,221]				•		
Remove neutralisation excuses [90,210]				•		
Sanctions [4,31,208,210,215,219,223]					•	•
Allow rule breaking and develop anomaly spotting [228]						•
Management effort			**D1**	**D2**	**D3**	**D4**
Educate management about insider threats [220] and show organisational commitment [31]; Educate Management on employee needs [218]				•	•	•
Non-blame organisational culture [217]				•		
Identify employees with highest potential to cause harm [132,229]					•	•
Do not have a toxic work culture [177,209]					•	•
Reduce rewards [210]					•	•
Social interventions [230,231]				•		
Termination of employment [132,208]					•	•
Have an insider threat program [132,207]					•	•
Whistleblowing			**D1**	**D2**	**D3**	**D4**
Behave ethically [224,225]					•	•
Incentivise internal whistleblowing [226]					•	•
Act upon internal whistleblowing reports [227]					•	•

Appendix B

We conducted separate LDA exercises for answers to each of the open-ended questions. Resulting analysis confirms the general topics, presented in

Section 2 of the paper. Below, we present the Python code along with the Intertopic Distance Map for each answer and top-30 most salient terms in each answer as revealed by the LDA analysis (Fig. B.1, Fig. B.2, Fig. B.3).

Python code for replication

```
import pandas as pd
import torch
from transformers import GPT2Tokenizer, GPT2Model
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.decomposition import LatentDirichletAllocation
import pyLDAvis
import pyLDAvis.sklearn
import nltk
from nltk.corpus import stopwords

# Load GPT-2 pre-trained model and tokenizer
model_name = 'gpt2'
tokenizer = GPT2Tokenizer.from_pretrained(model_name)

# Load the data from CSV file
data = pd.read_csv('data.csv') # Replace 'data.csv' with your actual file path

# Extract the text data from the CSV file
documents = data['text'].tolist()

# Define custom stop words
custom_stopwords = ['insider', 'insiders', 'taxonomies','taxonomy','ve']  # Add your custom stop words here

# Combine custom stop words with NLTK stopwords
stopwords_list = stopwords.words('english') + custom_stopwords

# Tokenize and encode the documents using GPT-2 tokenizer
encoded_inputs = []
max_length = 0
for doc in documents:
    encoded_input = tokenizer.encode(doc, truncation=True, max_length=512, return_tensors='pt')[0]
    encoded_inputs.append(encoded_input)
    max_length = max(max_length, len(encoded_input))

# Pad the sequences to the same length
padded_inputs = []
for input in encoded_inputs:
    padded_input = torch.nn.functional.pad(input, (0, max_length - input.shape[0]), value=0)
    padded_inputs.append(padded_input)

padded_inputs = torch.stack(padded_inputs)

# Extract the document embeddings from GPT-2 model
model = GPT2Model.from_pretrained(model_name)
with torch.no_grad():
    model_outputs = model(input_ids=padded_inputs)
    embeddings = model_outputs.last_hidden_state[:, 0, :].numpy()  # Use the representation of the [CLS] token

# Apply topic modeling using Latent Dirichlet Allocation (LDA)
vectorizer = CountVectorizer(max_features=1000, lowercase=True, stop_words=stopwords_list)
X = vectorizer.fit_transform(documents)
feature_names = vectorizer.get_feature_names()

# Set the number of topics for LDA
n_topics = 8

# Fit LDA model to the document-term matrix
lda_model = LatentDirichletAllocation(n_components=n_topics, random_state=42)
lda_model.fit(X)

# Visualize the LDA model
lda_vis_data = pyLDAvis.sklearn.prepare(lda_model, X, vectorizer)
pyLDAvis.display(lda_vis_data)
```

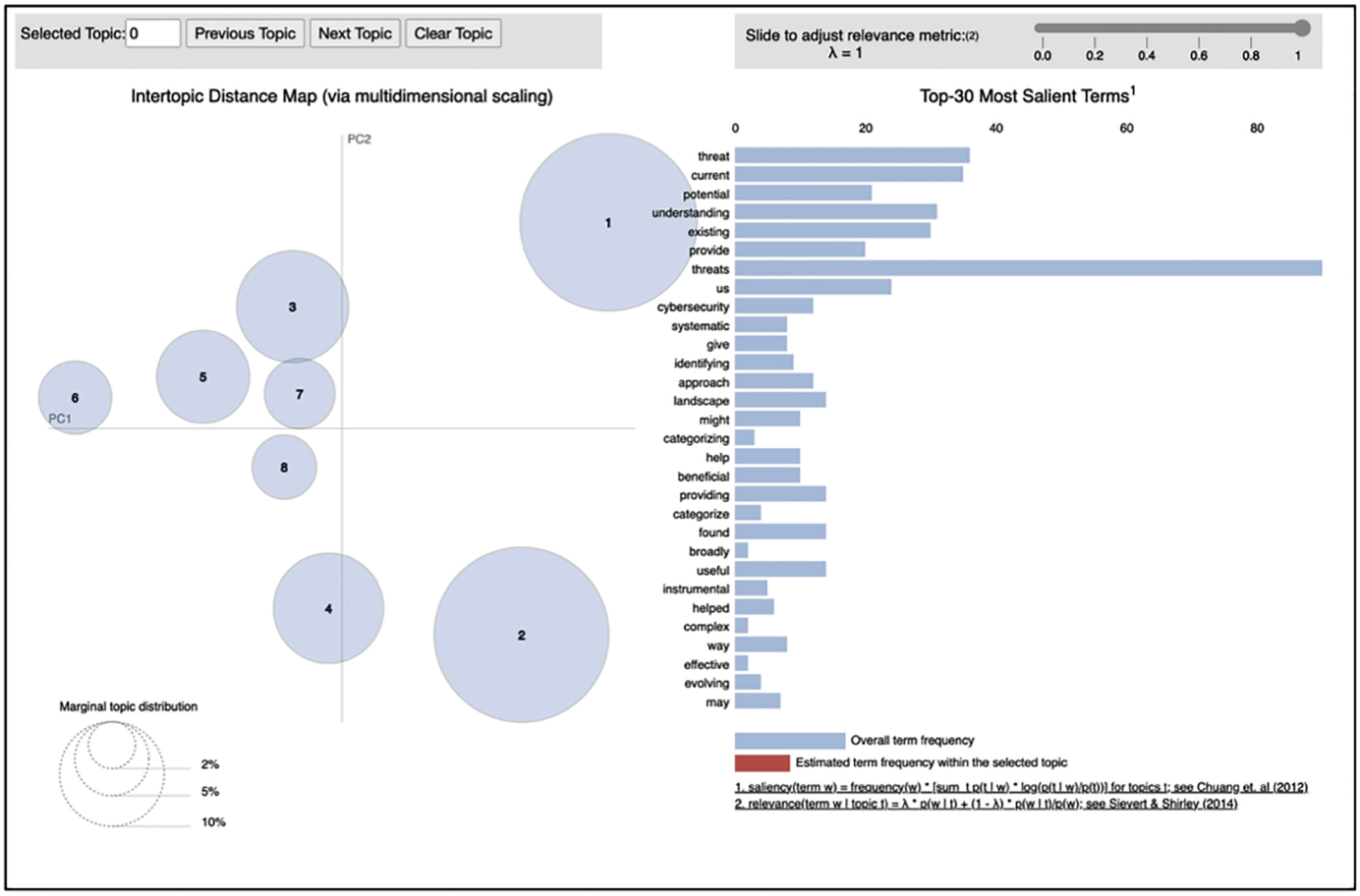


Fig. B.1. Results of the LDA allocation model for question (b).

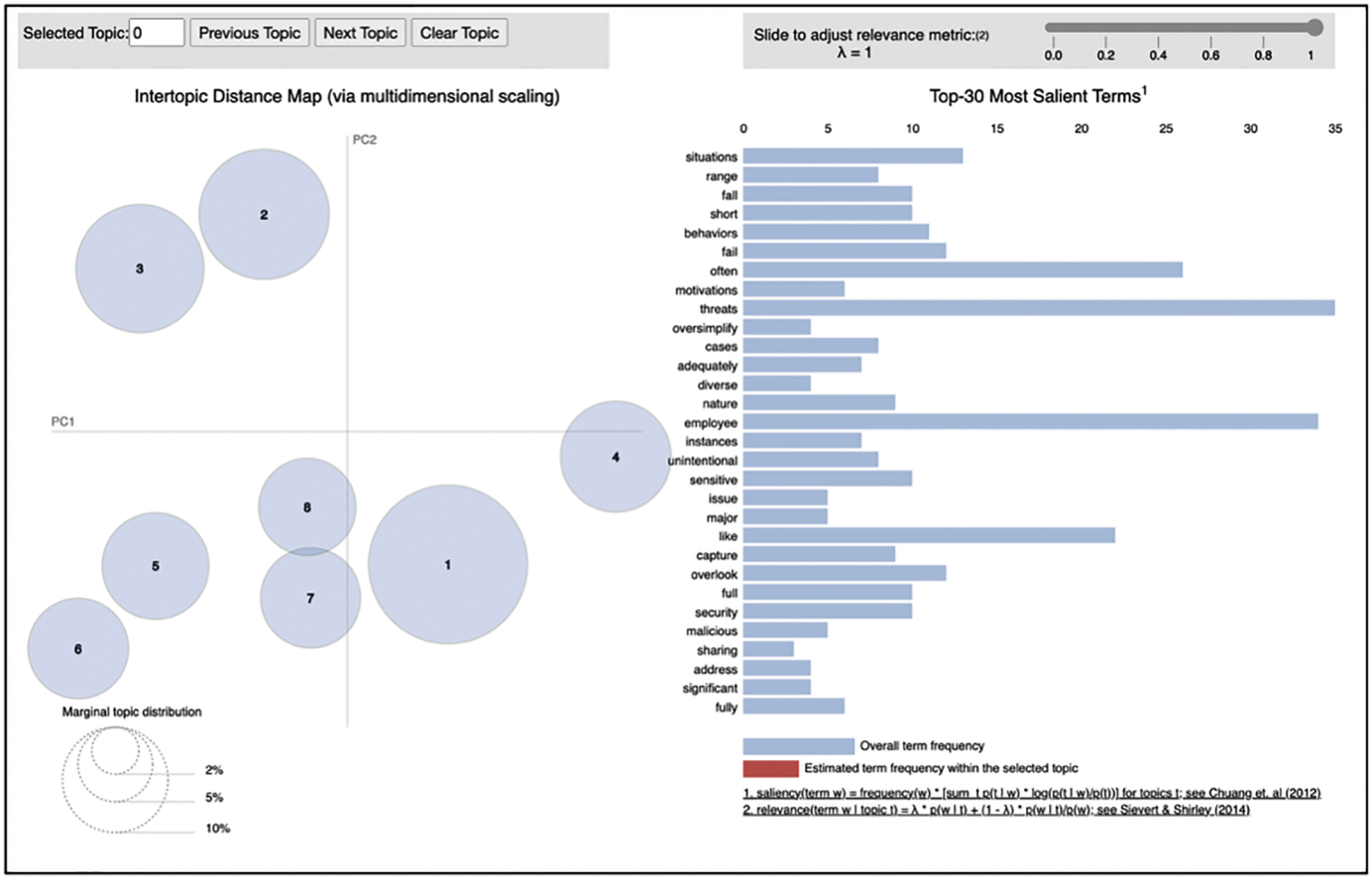


Fig. B.2. Results of the LDA allocation model for question (c).

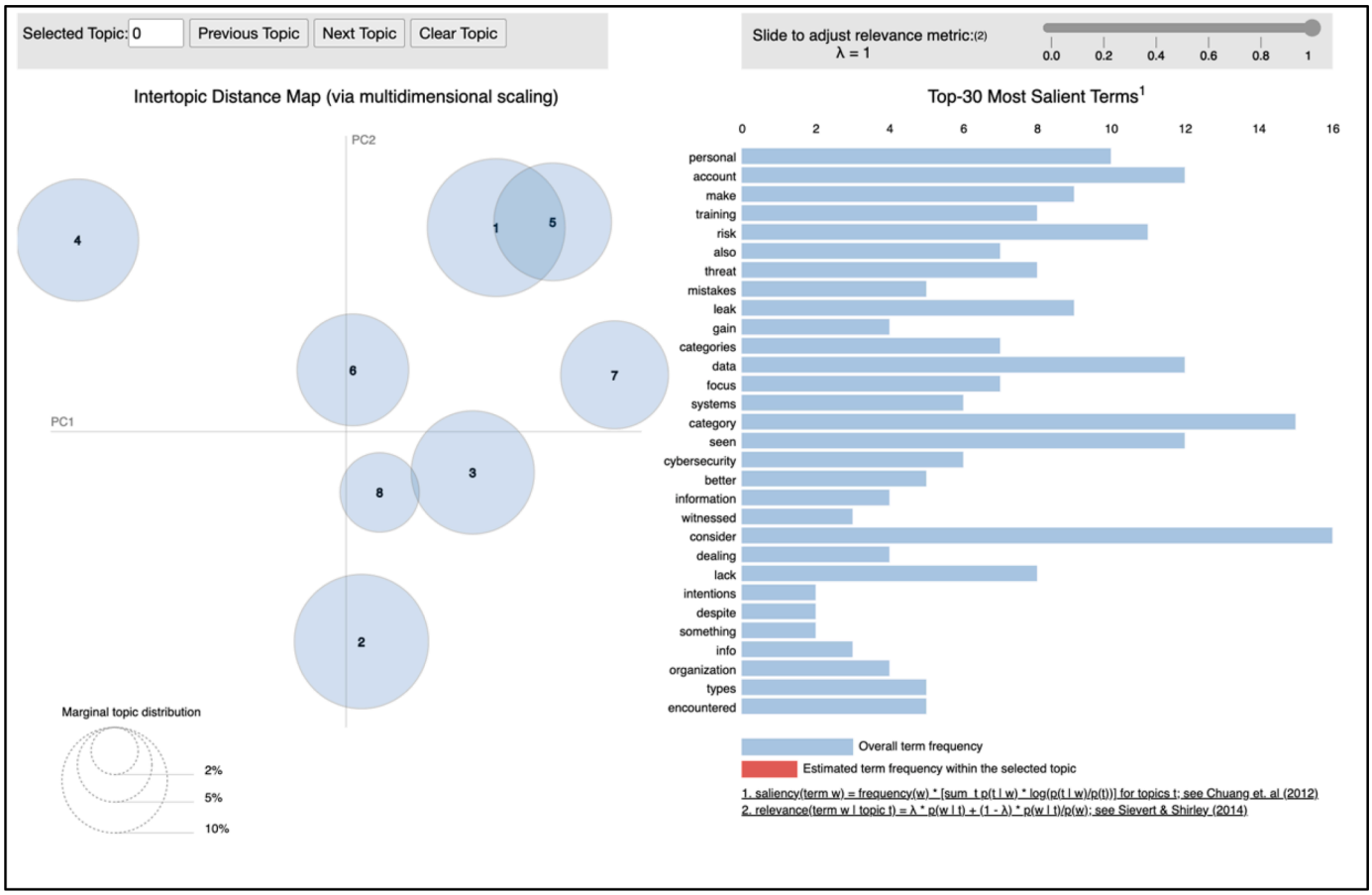


Fig. B.3. Results of the LDA allocation model for question (d).

References

[1] G. Fyffe, Addressing the insider threat, Network Security 2008 (3) (2008) 11–14, https://doi.org/10.1016/S1353-4858(08)70031-X.

[2] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, M. Ochoa, Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures, ACM Comput. Surveys (CSUR) 52 (2) (2019) 1–40, https://doi.org/10.1145/3303771.

[3] H.W. Rittel, M.M. Webber, Dilemmas in a general theory of planning, Policy Sci. 4 (2) (1973) 155–169, https://doi.org/10.1007/BF01405730.

[4] Homeland Security. A roadmap for cybersecurity research. 2009 https://www.dhs.gov/publication/cybersecurity-roadmap. Accessed 8 June 2023.

[5] Bitglass. 2020 insider threat report, 2020. https://www.forcepoint.com/resources/reports/2020-insider-threat-report? Accessed 18 March 2023.

[6] Kaspersky. Kaspersky 2022 IT security economics survey, 2022. https://calculator.kaspersky.com/report Accessed 29 April 2023.

[7] G. Finnney, Well Aware, Greenleaf, Texas, USA, 2020.

[8] A. Munshi, P. Dell, H. Armstrong, Insider threat behavior factors: a comparison of theory with reported incidents, in: 45th Hawaii International Conference on System Sciences, IEEE, 2012, pp. 2402–2411, https://doi.org/10.1109/HICSS.2012.326, pages.

[9] E.D. Shaw, The role of behavioral research and profiling in malicious cyber insider investigations, Digit. Invest. 3 (1) (2006) 20–31, https://doi.org/10.1016/j.diin.2006.01.006.

[10] M. Warkentin, R. Willison, Behavioral and policy issues in information systems security: the insider threat, Eur. J. Inform. Syst. 18 (2) (2009) 101–105, https://doi.org/10.1057/ejis.2009.12.

[11] M. Hayden. The insider threat to US government information systems. Technical report, National Security Agency/Central Security Service Fort George G Meade MD, 1999. https://apps.dtic.mil/sti/pdfs/ADA406622.pdf Accessed 28 Feb 2021.

[12] G. Mazzarolo, A.D. Jurcut, Insider threats in cyber security: The enemy within the gates, Eur. Cybersecur. J. 6 (1) (2019) 57–63, https://doi.org/10.48550/arXiv.1911.09575.

[13] R. Willison, M. Warkentin, Beyond deterrence: An expanded view of employee computer abuse, Manage. Inform. Syst. Quart. 37 (1) (2013) 1–20. https://www.jstor.org/stable/43825935.

[14] PWC. US cybercrime: rising risks, reduced readiness – KEy findings from the 2014 US State of cybercrime survey, 2014. https://www.ojp.gov/ncjrs/virtual-library/abstracts/us-cybercrimerising-risks-reduced-readiness-key-findings-2014-us Accessed 3 April 2023.

[15] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. Insider threat study: Illicit cyber activity in the banking and finance sector. Technical Report ADA441249, Carnegie-Mellon Univ Pittsburgh Software Engineering Inst, 2005. https://apps.dtic.mil/sti/citations/ADA441249.

[16] M. Rosenthal. Insider threats examples: 17 real examples of insider threats, 2021. https://www.tessian.com/blog/insider-threats-types-and-realworld-examples/Accessed 3 April 2023.

[17] C. Gopalakrishnan, Insider Data Breaches Continue to Worry IT Leaders, SC Media, 2020. https://www.scmaga-zineuk.com/insider-data-breachescontinue-worry-leaders/article/1674454. Accessed March 2020.

[18] S. Watts-Taffe, B. Laster, L. Broach, B. Marinak, C.McDonald Connor, D. Walker-Dalhouse, Differentiated instruction: Making informed teacher decisions, Reading Teacher 66 (4) (2012) 303–314, https://doi.org/10.1002/TRTR.01126.

[19] A. Harvey, A. Brand, S.T. Holgate, L.V. Kristiansen, H. Lehrach, A. Palotie, B. Prainsack, The future of technologies for personalised medicine, New Biotechnol. 29 (6) (2012) 625–633, https://doi.org/10.1016/j.nbt.2012.03.009.

[20] S. Casey. Why cybersecurity education is taking off at Heathrow Airport, 2022. https://www.kaspersky.com/blog/secure-futures-magazine/heathrow-airport-cybersecurity-education/44618/.

[21] C.W. Probst, J. Hunker, M. Bishop, D. Gollmann, Insider threats in cyber security, Springer 49 (2010), https://doi.org/10.1007/978-1-4419-7133-3.

[22] Cybersecurity & Infrastructure Security Agency. Defining insider threats, no date. https://www.cisa.gov/defining-insider-threats Accessed 18 March 2023.

[23] FBI. Yanqing Ye, 2020. https://www.fbi.gov/wanted/counterintelligence/yanqing-ye Accessed 11 April 2021.

[24] FBI. A Chinese medical researcher who was stopped with vials of medical research in his suitcase has been sent back to his country, 2021. https://www.bostonglobe.com/2021/01/17/metro/chinese-medicalresearcher-who-was-stopped-with-vials-medical-research-hissuitcase-has-been-sent-back-his-country/Accessed 11 April 2021.

[25] E. Cole, S. Ring, Insider threat: Protecting the Enterprise from sabotage, spying, and Theft, Syngress, Rockland, MA, 2005.

[26] F.L. Greitzer, D.A. Frincke, Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation, editors, in: C.W. Probst, J. Hunker, D. Gollmann, M. Bishop (Eds.), Insider Threats in Cyber Security, Springer, New York, 2010, pp. 85–113, https://doi.org/10.1007/978-1-4419-7133-3. pages.

[27] A.P. Moore, D.M. Cappelli, R.F. Trzeciak, The "big picture" of insider it sabotage across us critical infrastructures, editors, in: S.J. Stolfo, S.M. Bellovin, A. D. Keromytis, S. Hershkop, S.W. Smith (Eds.), Insider Attack and Cyber Security, Springer, 2008, pp. 17–52, https://doi.org/10.1007/978-0-38777322-33. pages.

[28] M. Maasberg, J. Warren, N.L. Beebe, The dark side of the insider: detecting the insider threat through examination of dark triad personality traits, in: 48th Hawaii International Conference on System Sciences, IEEE, 2015, pp. 3518–3526, https://doi.org/10.1109/HICSS.2015.423, pages.

[29] S.R. Band, D.M. Cappelli, L.F. Fischer, A.P. Moore, E.D. Shaw, and R.F. Trzeciak. Comparing insider IT sabotage and espionage: A model-based analysis. Technical Report ADA459911, Carnegie-Mellon Univ Pittsburgh Software Engineering Inst, 2006. https://apps.dtic.mil/sti/citations/ADA459911.

[30] E.E. Schultz, A framework for understanding and predicting insider attacks, Comput. Secur. 21 (6) (2002) 526–531, https://doi.org/10.1016/S0167-4048(02)01009-X.

[31] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, Eur. J. Inform. Syst. 18 (2) (2009) 106–125, https://doi.org/10.1057/ejis.2009.6.

[32] BBC. Brighton hospital fined record £325,000 over data theft., 2012. https://www.bbc.com/news/uk-england-sussex-18293565 Accessed 17 March 2023.

[33] T. Miller. 5 things security executives need to know about insider threat, 2019.https://www.helpnetsecurity.com/2019/10/14/insider-threatessentials/Accessed 11 April 2021.

[34] E. Boehm, For Airline Employees, TSA Insider Threat Program Is Little More Than Random Molestation: How the TSA Turned a long-time, Trusted Employee Into an "insider threat" For No Clear Reason, WashingtonReason Foundation Copyright Reason Foundation, 2017. Aug 11,, https://reason.com/2017/08/11/for-airline-employee-targeted-by-random/.

[35] E. Snowden, Here's How We Take Back the Internet, TED Talks, 2014. http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript. Accessed 22 March 2023.

[36] P.D. Thacker, Covid-19: researcher blows the whistle on data integrity issues in Pfizer's vaccine trial, Br. Medical J. 375 (2021), https://doi.org/10.1136/bmj.n2635. Paper n2635.

[37] C. Burgess. Army contractor convicted of cyber-sabotage highlights the reality of insider threats, 2018. https://news.clearancejobs.com/2018/09/18/armycontractor-convicted-of-cyber-sabotage-highlights-the-reality-ofinsider-threats/ Accessed 11 April 2021.

[38] B. Mann. The biggest leaks revealed by Edward Snowden, 2020. https://blokt.com/guides/edward-snowden-leaks Accessed 11 April 2021.

[39] A. Marcon, Master's thesis, Sociology, Carleton University, 2015.

[40] E. Stevens. Chelsea manning: hero or traitor? It's complicated, 2019. https://www.thegryphon.co.uk/2019/03/23/chelsea-manning-heroor-traitor-its-complicated/Accessed 11 April 2021.

[41] K. Klarenberg. Whistleblower exposes multiple issues with Pfizer's Covid-19 vaccine trial, 2021. https://www.rt.com/usa/539247-whistleblower-issuespfizer-trial/Accessed 22 March 2023.

[42] R. Mac. Who is Frances Haugen, the Facebook whistle-blower? 2015. https://www.nytimes.com/2021/10/05/technology/who-is-franceshaugen.html Accessed 16 Dec 2021.

[43] P. Rost, The whistleblower: Confessions of a Healthcare Hitman, Soft Skull Press, Brooklyn, New York, 2006.

[44] CERT Insider Threat Team. Unintentional insider threats: a foundational study. Technical Report CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2013.

[45] S. Furnell, Enemies within: the problem of insider attacks, Comput. Fraud Secur. 2004 (7) (2004) 6–11, https://doi.org/10.1016/S1361-3723(04)00087-9.

[46] A.P. Moore, W. Novak, M. Collins, R. Trzeciak, and M. Theis. Effective insider threat programs: understanding and avoiding potential pitfalls. Technical report, Software Engineering Institute White Paper, Pittsburgh, 2015. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367 Accessed 3 April 2023.

[47] E. Smith. 5 things security executives need to know about insider threat, 2019. https://www.observeit.com/press/survey-reveals-organizationsseek-to-increase-trust-in-their-workforce-around-cybersecurityto-build-competitive-advantage/Accessed 11 April 2021.

[48] M.N. Al-Mhiqani, R. Ahmad, Z.Z. Abidin, W.M. Yassin, A. Hassan, A. N. Mohammad, N.L. Clarke, A new taxonomy of insider threats: an initial step in understanding authorised attack, Int. J. Inform. Syst. Manage. 1 (4) (2018) 343–359, https://doi.org/10.1504/IJISAM.2018.0947771504/IJISAM.2018.094777.

[49] BBC. Morrisons employee Andrew Skelton jailed over data leak, 2015. https://www.bbc.co.uk/news/uk-england-leeds-33566633 Accessed 11 April 2021.

[50] W.R. Claycomb, C.L. Huth, L. Flynn, D.M. McIntire, T.B. Lewellen, Chronological examination of insider threat sabotage: Preliminary observations, J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 3 (4) (2012) 4–20, https://doi.org/10.22667/JOWUA.2012.12.31.004. CERT Insider Threat Center.

[51] K.L. Herbig and M.F. Wiskoff. Espionage against the United States by American citizens 1947-2001. Technical Report ADA411004, Defense Personnel Security Research Centre Monterey CA, 2002. https://apps.dtic.mil/sti/citations/ADA411004.

[52] D. McKay. The disgruntled employee and the damage they can do, Cloud Savvy IT. 2020. https://www.cloudsavvyit.com/7285/the-disgruntledemployee-and-the-damage-they-can-do/Accessed 16 April 2021.

[53] A. Moneva, & R. Leukfeldt, Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures, J. Criminol. (2022), https://doi.org/10.1177/263380762311618.

[54] E.D. Shaw, K.G. Ruby, J.M. Post, The insider threat to information systems. The psychology of the dangerous insider, Secur. Awareness Bull. 2 (98) (1998) 1–10.

[55] Department of Justice. Former network engineer pleads guilty to crashing employer's computer system, 2014. https://www.justice.gov/usaosdwv/pr/former-network-engineer-pleads-guilty-crashing-employerscomputer-system Accessed 17 March 2023.

[56] D.H. Doty, W.H. Glick, Typologies as a unique form of theory building: toward improved understanding and modeling, Acad. Manage. Rev. 19 (2) (1994) 230–251.

[57] R.L. Glass, I. Vessey, Contemporary application-domain taxonomies, IEEE Softw. 12 (4) (1995) 63–76, https://doi.org/10.1109/52.391837.

[58] F. De Waal, F.B. Waal, H.C. Lodge, The Bonobo and the Atheist: In search of Humanism Among the Primates, WW Norton & Company, New York, 2013.

[59] O. Okonya, B. Siddiqui, D. George, C. Fugate, M. Hartwell, M. Vassar, Use of behavioural change taxonomies in systematic reviews and meta-analyses regarding obesity management, Clin. Obes. 13 (1) (2023) e12574, https://doi.org/10.1111/cob.12574.

[60] S. Michie, S. Ashford, F.F. Sniehotta, S.U. Dombrowski, A. Bishop, D.P. French, A refined taxonomy of behaviour change techniques to help people change their physical activity and healthy eating behaviours: the CALO-RE taxonomy, Psychol. Health 26 (11) (2011) 1479–1498, https://doi.org/10.1080/08870446.2010.540664.

[61] C. Abraham, S. Michie, A taxonomy of behavior change techniques used in interventions, Health Psychol. 27 (3) (2008) 379–387, https://doi.org/10.1037/0278-6133.27.3.379.

[62] M.B. Salem, S. Hershkop, S.J. Stolfo, A survey of insider attack detection research, in: Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith, Sara Sinclair (Eds.), Insider Attack and Cyber Security, 2008, pp. 69–90, pages.

[63] J. Hunker, C.W. Probst, Insiders and insider threats-an overview of definitions and mitigation techniques, J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. 2 (1) (2011) 4–27, https://doi.org/10.22667/JOWUA.2011.03.31.004.

[64] A. Azaria, A. Richardson, S. Kraus, V.S. Subrahmanian, Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data, IEEE Trans. Comput. Soc. Syst. 1 (2) (2014) 135–155, https://doi.org/10.1109/TCSS.2014.2377811.

[65] A. Abdallah, M.A. Maarof, A. Zainal, Fraud detection system: a survey, J. Netw. Comput. Appl. 68 (2016) 90–113, https://doi.org/10.1016/j.jnca.2016.04.007.

[66] A. Sanzgiri, D. Dasgupta, Classification of insider threat detection techniques, in: Proceedings of the 11th Annual Cyber and Information Security Research Conference, 2016, pp. 1–4, https://doi.org/10.1145/2897795.2897799, pages.

[67] J. Ophoff, A. Jensen, J. Sanderson-Smith, M. Porter, K. Johnston, A descriptive literature review and classification of insider threat research, in: Proceedings of Informing Science & IT Education Conference (InSITE), 2014.

[68] CERT Insider Threat Centre. A multi-dimensional approach to insider threat. 2013. https://insights.sei.cmu.edu/blog/a-multi-dimensional-approach-to-insider-threat/Accessed 18 July 2023.

[69] J.P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, 1980.

[70] S.M. Bellovin. The insider attack problem nature and scope. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, and S. Sinclair, editors, Insider Attack and Cyber Security: Beyond the Hacker, volume 39, pages 1–4. Springer, 2008. https://doi.org/10.1007/978-0-387-77322-3_1.

[71] J. Myers, M.R. Grimaila, R.F. Mills, Towards insider threat detection using web server logs, in: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009, pp. 1–4, https://doi.org/10.1145/1558607.1558670, pages.

[72] F.L. Greitzer, J.R. Strozer, S. Cohen, A.P. Moore, D. Mundie, J. Cowley, Analysis of unintentional insider threats deriving from social engineering exploits. IEEE Security and Privacy Workshops, IEEE, 2014, pp. 236–250, https://doi.org/10.1109/SPW.2014.39, pages.

[73] D.S. Wall, Enemies within: Redefining the insider threat in organizational security policy, Secur. J. 26 (2) (2013) 107–124, https://doi.org/10.1057/sj.2012.1.

[74] J. Reason, Human Error, Cambridge University Press, Cambridge, UK, 1990.

[75] Q. Shi, B. Dong, T. He, Z. Sun, J. Zhu, Z. Zhang, C. Lee, Progress in wearable electronics/photonics—moving toward the era of artificial intelligence and internet of things, InfoMat 2 (6) (2020) 1131–1162, https://doi.org/10.1002/inf2.12122.

[76] K.V. Renaud, M. Warkentin, G Westerman, From ChatGPT to HackGPT: meeting the cybersecurity threat of generative AI, MIT Sloan Manage. Rev. (2023) 64428.

[77] N.N. Hartmann, B. Lussier, Managing the sales force through the unexpected exogenous covid-19 crisis, Ind. Market. Manage. 88 (2020) 101–111, https://doi.org/10.1016/j.indmarman.2020.05.005.

[78] V Masterson. Fewer women CEOs have been appointed since the start of the COVID-19 crisis - here's why. 2020. https://www.weforum.org/agenda/2020/12/fewer-women-ceos-covid-gender-gap/Accessed 18 July 2023.

[79] K.D. Loch, H.H. Carr, M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, Manage. Inform. Syst. Quart. 16 (2) (1992) 173–186, https://doi.org/10.2307/249574.

[80] CERT Insider Threat Center. Handling threats from disgruntled employees, 2015. https://insights.sei.cmu.edu/blog/handling-threats-fromdisgruntled-employees/ Accessed 17 March 2023.

[81] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, Eur. J. Inform. Syst. 22 (3) (2013) 336–359, https://doi.org/10.1057/ejis.2012.26.

[82] C. Alberts and A. Dorofee. OCTAVESM Threat Profiles. Technical report, Pittsburgh, Software Engineering Institute, 2001.

[83] M.J. Alhanahnah, A. Jhumka, S. Alouneh, A multidimension taxonomy of insider threats in cloud computing, Comput. J. 59 (11) (2016) 1612–1622, https://doi.org/10.1093/comjnl/bxw020.

[84] S. Chaipa, E.K. Ngassam, S. Singh, Towards a new taxonomy of insider threats, in: 2022 IST-Africa Conference (IST-Africa), IEEE, 2022, pp. 1–10.

[85] Y. Hashem, H. Takabi, M. GhasemiGol, R. Dantu, Towards insider threat detection using psychophysiological signals, in: Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats, 2015, pp. 71–74, https://doi.org/10.1145/2808783.2808792, pages.

[86] N.A.N. Mohammad, W.M. Yassin, R. Ahmad, A. Hassan, M.N.A. Al Mhiqani, An insider threat categorization framework for automated manufacturing execution system, Int.J. Innov. Enterprise Syst. 3 (02) (2019) 31–41, https://doi.org/10.25124/ijies.v3i02.38.

[87] D.A. Mundie, S.J. Perl, C.L. Huth, Insider threat defined: Discovering the prototypical case, J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. 5 (2) (2014) 7–23, https://doi.org/10.22667/JOWUA.2014.06.31.007.

[88] M. Sas, M. Reveraert, W. Hardyns, G. Reniers, T. Sauer, Towards a typology of insider threats in higher education, in: Workshop Insider Threat Awareness & Mitigation, Online, 2020.

[89] F.L. Greitzer, J. Purl, Y.M. Leong, D.S. Becker, SOFIT: Sociotechnical and organizational factors for insider threat. Security and Privacy Workshops (SPW), IEEE, 2018, pp. 197–206, https://doi.org/10.1109/SPW.2018.00035, pages.

[90] J.B. Barlow, M. Warkentin, D. Ormond, A. Dennis, Don't even think about it! The effects of anti neutralization, informational, and normative communication on information security compliance, J. Assoc. Inform. Syst. 19 (8) (2018). Paper 3, https://aisel.aisnet.org/jais/vol19/iss8/3.

[91] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, Manage. Inform. Syst. Quart. 34 (3) (2010) 523–548, https://doi.org/10.2307/25750690.

[92] C. Donalds, C. Barclay, Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance, Eur. J. Inform. Syst. 31 (1) (2022) 58–73, https://doi.org/10.1080/0960085X.2021.1978344.

[93] A. Onumo, I. Ullah-Awan, A. Cullen, Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures, ACM Trans. Manage. Inform. Syst. (TMIS) 12 (2) (2021) 1–29, https://doi.org/10.1145/3424282.

[94] S. Sarkar, A. Vance, B. Ramesh, M. Demestihas, D.T. Wu, The influence of professional subculture on information security policy violations: A field study in a healthcare context, Inf. Syst. Res. 31 (4) (2020) 1240–1259, https://doi.org/10.1287/isre.2020.0941.

[95] L.-W. Wong, V.-H. Lee, G.W.-H. Tan, K.-B. Ooi, A. Sohal, The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities, Int. J. Inf. Manage. 66 (2022), https://doi.org/10.1016/j.ijinfomgt.2022.102520. Paper 102520.

[96] S. Yusif, A. Hafeez-Baig, Cybersecurity policy compliance in higher education: a theoretical framework, J. Appl. Secur. Res. 18 (2) (2021) 267–288, https://doi.org/10.1080/19361610.2021.1989271.

[97] A. Al-Harrasi, A.K. Shaikh, A. Al-Badi, Towards protecting organisations' data by preventing data theft by malicious insiders, Int. J. Organ. Anal. 31 (3) (2021) 875–888, https://doi.org/10.1108/IJOA-01-2021-2598.

[98] H.R. Brafford, PhD thesis, Business Administration, Northcentral University, 2021.

[99] T.E. Carroll, F.L. Greitzer, A.D. Roberts, Security informatics research challenges for mitigating cyber friendly fire, Secur. Inform. 3 (1) (2014) 1–14, https://doi.org/10.1186/s13388-014-0013-5.

[100] M. Canham, C. Posey, P.S. Bockelman, Confronting information security's elephant, the unintentional insider threat, in: International Conference on Human-Computer Interaction, Springer, 2020, pp. 316–334, https://doi.org/10.1007/978-3-030-50439-7_22, pages.

[101] J.R. Schoenherr, R. Thomson, Insider threat detection: a solution in search of a problem, in: International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2020, pp. 1–7, https://doi.org/10.1109/CyberSecurity49315.2020.9138862.

[102] D. Porter, Insider fraud: spotting the wolf in sheep's clothing, Comput. Fraud Secur. 2003 (4) (2003) 12–15, https://doi.org/10.1016/S1361-3723(03)04011-9.

[103] T. Bailey, B. Kolo, K. Rajagopalan, D. Ware, Insider threat: The human Element of Cyberrisk, McKinsey & Co, 2018. September 2018, https://www.mckinsey.com/business-functions/risk/ourinsights/insider-threat-the-human-element-of-cyberrisk. Accessed 22 March 2023.

[104] D. BaMaung, D. McIlhatton, M. MacDonald, R. Beattie, The enemy within? The connection between insider threat and terrorism, Stud. Conflict Terror. 41 (2) (2018) 133–150, https://doi.org/10.1080/1057610X.2016.1249776.

[105] P. Balozian, D. Leidner, Review of IS security policy compliance: Toward the building blocks of an IS security theory, ACM SIGMIS Database: DATABASE Adv. Inform. Syst. 48 (3) (2017) 11–43, https://doi.org/10.1145/3130515.3130518.

[106] M. Silic, D. Kolak, M. Leontic, Emerging from the shadows: survey evidence of shadow IT use from blissfully ignorant employees, Glob. J. Bus. Integral Secur. 1 (1) (2021) 32–44. https://www.gbis.ch/index.php/gbis/article/view/4.

[107] N. Thompson, A unified classification model of insider threats to information security, in: 31st Australasian Conference on Information Systems, Dec 1-4, 2020, Wellington, New Zealand, 2020. https://aisel.aisnet.org/acis2020/40.

[108] S. Fadilpăsíc. Lack of cybersecurity training is leaving businesses at risk, 2023. https://www.techradar.com/news/lack-of-cybersecuritytraining-is-leaving-businesses-at-risk Accessed 29 April 2023.

[109] J. Bore, Insider threat, editors, in: H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, J. Ibarra (Eds.), Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Springer, 2020, pp. 431–450, https://doi.org/10.1007/978-3-030-35746-7_19. pages.

[110] K. Gülen. The elephant in the room: Employees ignore cybersecurity training sessions, 2022. https://dataconomy.com/2022/07/employees-ignorecybersecurity-training/Accessed 29 April 2023.

[111] A.T. Tunggal. What is an insider threat? Definition, examples, and mitigations, 2022. https://www.upguard.com/blog/insider-threat Accessed 3 April 2023.

[112] M. Reveraert, T. Sauer, Redefining insider threats: a distinction between insider hazards and insider threats, Secur. J. 34 (4) (2021) 755–775, https://doi.org/10.1057/s41284-020-00259-x.

[113] K. Amorosa, K., & B. Yankson. Human error-a critical contributing factor to the rise in data breaches: a case study of higher education. HOLISTICA–J. Bus. Public Administration, 14(1): 110–132. S. Anania. Is a cybersecurity incident cause for a disciplinary? People Management https://www.peoplemanagement.co.uk/article/1803078/cybersecurity-incident-cause-disciplinary 2022.

[114] L. Hadlington, The "Human Factor" in cybersecurity: exploring the accidental insider. Research Anthology on Artificial Intelligence Applications in Security, IGI Global, 2021, pp. 1960–1977, https://doi.org/10.4018/978-1-7998-7705-9.ch087, pages.

[115] J.M. Stanton, K.R. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviors, Comput. Secur. 24 (2) (2005) 124–133, https://doi.org/10.1016/j.cose.2004.07.001.

[116] E.S. Mbewe, J. Chavula, Security mental models and personal security practices of internet users in Africa, editors, in: Y.H. Sheikh, I.A. Rai, A.D. Bakar (Eds.), International Conference on e-Infrastructure and e-Services for Developing Countries, Springer, 2022, pp. 47–68, https://doi.org/10.1007/978-3-031-06374-9_4. pages.

[117] B. Debusmann Jr, Millions of military emails have accidentally been directed to Mali exposing highly sensitive information because of a 'typo' despite repeated warnings for the last decade, BBC (2023). https://www.bbc.com/news/world-us-canada-66226873. Accessed 18 July.

[118] S. Prabhu, N. Thompson, A primer on insider threats in cybersecurity, Inform. Secur. J. Glob. Perspect. (2021) 1–10, https://doi.org/10.1080/19393555.2021.1971802, pages.

[119] M. Ahmed, L. Sharif, M. Kabir, M. Al-Maimani, Human errors in information security, Int. J. Adv. Trends Comput. Sci. Eng. 1 (3) (2012) 82–87.

[120] S. Eftimie, C. Răcuciu, R. Moinescu, D. Glăvan, Insider threats and thermal stress in the working environment, Scient. Bull. " Mircea cel Batran" Naval Academy, 23 (1) (2020) 271A–2276, https://doi.org/10.21279/1454-864X-20I1-038.

[121] D. Sandler. 3 most dangerous insider threats and how to deal with them, 2019. https://www.niceguysonbusiness.com/blog/3-most-dangerousinsider-threats-and-how-to-deal-with-them/Accessed 25 March 2023.

[122] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K.R. Choo, P. Burnap, Impact and key challenges of insider threats on organizations and critical businesses, Electronics, 9 (9) (2020), https://doi.org/10.3390/electronics9091460. Paper 1460.

[123] D. Green, Insider threats and employee deviance: developing an updated typology of deviant workplace behaviors, Issues Inform. Syst. 15 (II) (2014) 185–189, https://doi.org/10.48009/2_iis_2014_185-189.

[124] F.L. Greitzer, Insider threats: It's the human, stupid!, in: Proceedings of the Northwest Cybersecurity Symposium, New York, NY; United States, 2019, pp. 1–8, https://doi.org/10.1145/3332448.3332458, pages.

[125] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, Y. Xiang, Detecting and preventing cyber insider threats: a survey, IEEE Commun. Surveys Tutor. 20 (2) (2018) 1397–1417, https://doi.org/10.1109/COMST.2018.2800740.

[126] M. Aldridge. How overwork and stress can undermine even the most robust cybersecurity posture, 2019. https://www.itproportal.com/news/how-overwork-and-stress-can-undermine-even-the-most-robustcybersecurity-posture/ Accessed 17 March 2023.

[127] I. Hwang, O. Cha, Examining technostress creators and role stress as potential threats to employees' information security compliance, Comput. Hum. Behav. 81 (2018) 282–293, https://doi.org/10.1016/j.chb.2017.12.022.

[128] J. D'Arcy, T. Herath, M.K. Shoss, Understanding employee responses to stressful information security requirements: A coping perspective, J. Manage. Inform. Syst. 31 (2) (2014) 285–318, https://doi.org/10.2753/MIS0742-1222310210.

[129] J. Predd, S.L. Pfleeger, J. Hunker, C. Bulford, Insiders behaving badly, IEEE Secur. Privacy 6 (4) (2008) 66–70, https://doi.org/10.1109/MSP.2008.87.

[130] R. Alavi, S. Islam, H. Mouratidis, S. Lee, Managing social engineering attacks-considering human factors and security investment, in: Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA), Mytilene, Greece, 2015, pp. 161–171, pages.

[131] L. Xiangyu, L. Qiuyang, S. Chandel, Social engineering and insider threats, in: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2017, pp. 25–34, https://doi.org/10.1109/CyberC.2017.91, pages.

[132] E.D. Shaw and L.F. Fischer. Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations. Technical Report ADA441293, Defense Personnel Security Research Center. Monterey, CA, 2005. https://apps.dtic.mil/sti/citations/ADA441293.
[133] R. Grimmick. What is an insider threat? definition and examples, 2022. https://www.varonis.com/blog/insider-threats Accessed 18 March 2023.
[134] IBM. What are insider threats? 2020. https://www.ibm.com/topics/insider-threats Accessed 25 March 2023.
[135] A. Litan. Emerging Insider Threat Detection Solutions, 2018. Gartner https://blogs.gartner.com/avivah-litan/2018/04/05/insider-threatdetection-replaces-dying-dlp/.
[136] L.H. Yeo, J. Banfield, Human factors in electronic health records cybersecurity breach: an exploratory analysis, Perspect. Health Inform. Manage. 19 (Spring) (2022). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/.
[137] P. Ifinedo, B.A. Akinnuwesi, Employees' non-malicious, counterproductive computer security behaviors (CCSB) in Nigeria and Canada: an empirical and comparative analysis, in: IEEE 6th International Conference on Adaptive Science & Technology (ICAST), IEEE, 2014, pp. 1–7, https://doi.org/10.1109/ICASTECH.2014.7068109, pages.
[138] M.T. Whitty, Developing a conceptual model for insider threat, J. Managem. Organ. 27 (5) (2021) 911–929, https://doi.org/10.1017/jmo.2018.57.
[139] E. Heidt and A. Chuvakin. Understanding insider threats, 2016. Gartner https://www.gartner.com/en/documents/3303117.
[140] A. Chuvakin. Our "understanding insider threats" paper publishes, 2016. https://blogs.gartner.com/anton-chuvakin/2016/05/09/ourunderstanding-insider-threats-paper-publishes/.
[141] D. Cappelli, A. Moore, R. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), 2 edition, Addison-Wesley, Boston, USA, 2012.
[142] L. Coles-Kemp, M. Theoharidou, Insider threat and information security management, editors, in: C.W. Probst, J. Hunker, D. Gollmann, M. Bishop (Eds.), Insider Threats in Cyber Security, Springer, 2010, pp. 45–71, https://doi.org/10.1007/978-1-4419-7133-3_3. pages.
[143] I. Gaidarski and Z. Minchev. Insider threats to IT security of critical infrastructures. In T. Tagarev, K. T. Atanassov, V. Kharchenko, and J. Kacprzyk, editors, Digital Transformation, Cyber Security and Resilience of Modern Societies, 84: 381–394. Springer, Switzerland, 2021. https://doi.org/10.1007/978-3-030-65722-2.
[144] E.L. Lang, Seven (Science-Based) commandments for understanding and countering insider threats, Counter-Insider Threat Res. Pract. 1 (1) (2022). https://citrap.scholasticahq.com/article/37321.
[145] D. Charney, True psychology of the insider spy, Intelligencer J. US Intell. Stud. 18 (2010) 47–54.
[146] BBC. Company sues worker who fell for email scam, 2019. https://www.bbc.com/news/uk-scotland-glasgow-west-47135686 Accessed 2 January 2021.
[147] D. Cappelli, A. Moore, R. Trzeciak, T.J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd edition, Software Engineering Institute, Carnegie Mellon University, 2009. –version 3.1Published by CERT, http://www.cert.org.
[148] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers. Insider threat study: computer system sabotage in critical infrastructure sectors. Technical report, National Threat Assessment Ctr Washington DC, 2005.
[149] T. Smith. Hacker jailed for revenge sewage attacks, 2001. The Register. https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/Accessed 16 April 2021.
[150] F.L. Greitzer, M. Imran, J. Purl, E.T. Axelrad, Y.M. Leong, D. Becker, K.B. Laskey, P.J. Sticha, Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk, in: Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS), Washington DC, USA, 2016, pp. 19–27, pages.
[151] M. Maasberg, C. Van Slyke, S. Ellis, N. Beebe, The dark triad and insider threats in cyber security, Commun. ACM 63 (12) (2020) 64–80, https://doi.org/10.1145/3408864.
[152] E.C. Thompson, Building a HIPAA-Compliant Cybersecurity Program, Springer, 2017, https://doi.org/10.1007/978-1-4842-3060-2.
[153] A. Beena, K.S. Humayoon, Information security insider threats in organizations and mitigation techniques, in: International Conference on Recent Advances in Energy-efficient Computing and Communication, 2019, pp. 1–4, https://doi.org/10.1109/ICRAECC43874.2019.8995088, pages.
[154] J. Ansbach, B. Sharton, Preventing insider threats to cybersecurity, Risk Manage. 67 (8) (2020) 12–13. https://www.rmmagazine.com/articles/article/2020/09/01/-Preventing-Insider-Threats-to-Cybersecurity. Accessed 29 April 2023.
[155] W. Li, K.W.S. Choi, S.Y. Ho, Understanding the whistle-blowing intention to report breach of confidentiality, Commun. Assoc. Inform. Syst. 47 (1) (2020) 72–94, https://doi.org/10.17705/1CAIS.04704.
[156] T.A. Robayo, PhD thesis, Criminal Justice, Saint Leo University, 2022.
[157] S. Sharma, M. Warkentin, Do I really belong? Impact of employment status on information security policy compliance, Compute. Secur. 87 (2019), 101397, https://doi.org/10.1016/j.cose.2018.09.005. Paper.
[158] P. Beaumont. US intelligence leak: what do we know about 'top secret' documents? 2023. https://www.theguardian.com/world/2023/apr/11/usintelligence-leak-what-do-we-know-about-top-secret-documents Accessed 29 April 2023.
[159] D.V. Gioe, J.M. Hatfield, A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective, Cambridge Rev. Int. Affairs 34 (5) (2021) 704–738, https://doi.org/10.1080/09557571. 2020.1853053.
[160] R.M. Bowen, A.C. Call, S. Rajgopal, Whistle-blowing: Target firm characteristics and economic consequences, Account. Rev. 85 (4) (2010) 1239–1271, https://doi.org/10.2308/accr.2010.85.4.1239.
[161] E. Damiani, C. Ardagna, F. Zavatarelli, E. Rekleitis, and L. Marinos. Big data threat landscape and good practice guide. European Union Agency For Network and Information Security, 2016. https://www.academia.edu/22838790/Big_Data_Threat_Landscape_and_Good_Practice_Guide.
[162] L.C. Amo, E. Grijalva, T. Herath, G.J. Lemoine, Rao, H. Raghav, Technological Entitlement: It's My Technology and I'll (Ab)Use It How I Want To, Manage. Inform. Syst. Quart. 46 (3) (2022) 1395–1420, https://doi.org/10.25300/MISQ/2022/15499.
[163] informIT. The CERT guide to insider threats: insider theft of intellectual property, 2012. https://www.informit.com/articles/article.aspx?p=1830484&seqNum=3.
[164] D. Raywood. Top ten cases of insider threat, 2023. https://www.infosecurity-magazine.com/magazine-features/top-ten-insiderthreat/Accessed 18 March 2023.
[165] T. Cassidy. Technical Detection of Intended Violence: Workplace Violence as an Insider Threat. https://insights.sei.cmu.edu/blog/technical-detection-of-intended-violence-workplace-violence-as-an-insider-threat/2017.
[166] A.S. Cetinkaya, R. Muhammad, N. Sobia. Workplace violence: a theoretical review. In Cihan Cobanoglu, Muhittin Cavusoglu, Abdulkadir Corbaci, (Eds.) Advances In Global Business And Economics, Volume 2. 2021.
[167] A. Hale, D. Borys, Working to rule or working safely? Part 2: The management of safety rules and procedures, Saf. Sci. 55 (2013) 222–231, https://doi.org/10.1016/j.ssci.2012.05.013.
[168] A. Blake. Crimeware tool WormGPT: AI for BEC attacks. https://www.scmagazine.com/news/threat-intelligence/crimeware-tool-wormgpt-ai-bec. Accessed 14 July, 2023.
[169] E. Ajao, ChatGPT could boost phishing scams, TechTarget. (2023). https://www.techtarget.com/searchenterpriseai/news/252529600/ChatGPT-could-boost-phishing-scams. Accessed 14 July 2023.
[170] S. McDermott. The AI cyber threat to your business. 2023. https://www.irishnews.com/business/businessnews/2023/07/11/news/the_ai_cyber_threat_to_your_busines-3422969/Accessed 15 July 2023.
[171] A.F. Al-Qahtani, S. Cresci, The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19, IET Inf. Secur. 16 (5) (2022) 324–345, https://doi.org/10.1049/ise2.12073.
[172] V. Zimmermann, K.V. Renaud, Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset, Int. J. Hum. Comput. Stud. 131 (2019) 169–187, https://doi.org/10.1016/j.ijhcs.2019.05.005.
[173] TecSec. Ex-employee of Peebles Media fined after falling for an email scam, 2019. https://www.tecsec.co.uk/2019/11/ex-employeeof-peebles-media-fined-after-falling-for-an-email-scam/Accessed 22 March 2023.
[174] SecureWorld News Team. 'Reckless?' City bans leader from email after he refuses security awareness training, 2019. https://www.secureworld.io/industry-news/reckless-city-bans-leader-from-email-after-herefuses-security-awareness-training.
[175] PrivSec Report. NHS data breach exposes 24 staff data in Scotland, 2019. https://www.grcworldforums.com/privacy-and-technology/nhsdata-breach-exposes-24-staff-data-in-scotland/396.article Accessed 18 March 2023.
[176] K. Poulsen. Exclusive: CIA 'Leaker' Josh Schulte posted agency code online—And CIA never noticed, 2018. https://www.thedailybeast.com/exclusive-cia-leaker-josh-schulte-posted-agency-code-onlineandcia-never-noticed Accessed 18 March 2023.
[177] G.E. Creech, Real" insider threat: toxic workplace behavior in the intelligence community, Int. J. Intell. Counter Intell. 33 (4) (2020) 682–708, https://doi.org/10.1080/08850607.2020.1789934.
[178] N. Statt. Twitter reveals that its own employee tools contributed to unprecedented hack, 2020. https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee-tools Accessed 22 March 2023.
[179] D. Winder. Microsoft security shocker as 250 million customer records exposed online, 2020. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-recordsexposed-online/?sh=554925af4d1b Accessed 3 April 2023.
[180] WMBF News Staff. Hartsville Taco Bell worker accused of credit card, identity fraud, 2022. https://www.wmbfnews.com/2022/06/22/hartsville-tacobell-worker-accused-credit-card-identity-fraud/Accessed 3 April 2023.
[181] L. Kolodny. Elon Musk emails employees about 'extensive and damaging sabotage' by employee, 2018. https://www.cnbc.com/2018/06/18/elon-muskemail-employee-conducted-extensive-and-damaging-sabotage.html Accessed 18 March 2023.
[182] Y. Bhattacharjee. A new kind of spy, 2014. https://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy Accessed 18 March 2023.
[183] P. Carlson. Spy in the henhouse, 1998. https://www.washingtonpost.com/archive/lifestyle/1998/01/03/spy-in-the-henhouse/c683edcf-720c4c8b-a9f1-25ebcc8d5b58/ Accessed 17 March 2023.
[184] A. McIntosh. Boeing discloses 36,000-employee data breach after email to spouse for help, 2017. https://www.bizjournals.com/seattle/news/2017/02/28/boeing-discloses-36-000-employee-data-breach.html Accessed 22 March 2023.
[185] Department of Justice. Russian national indicted for conspiracy to introduce malware into a computer network, 2020. https://www.justice.gov/opa/pr/russian-national-indicted-conspiracy-introduce-malware-computernetwork Accessed 17 March 2023.

[186] R. Brandom. Reality Winner accepts guilty plea for 63 months in prison on espionage charge, 2018. https://www.theverge.com/2018/6/26/17503656/reality-winner-guilty-plea-agreement-prison-time Accessed 17 March 2023.
[187] R. McMillan. Network admin Terry Childs gets 4-year sentence, 2010. https://www.computerworld.com/article/2754370/network-adminterry-childs-gets-4-year-sentence.html Accessed 22 March 2023.
[188] C. Brook. Suit claims attorneys stole, destroyed data before joining rival firm, 2021. https://digitalguardian.com/blog/suit-claims-attorneysstole-destroyed-data-joining-rival-firm Accessed 17 March 2023.
[189] L. O'Donnell. Ex-Cisco employee pleads guilty to deleting 16K Webex Teams Accounts, 2020. https://threatpost.com/ex-cisco-employee-pleadsguilty-to-deleting-16k-webex-teams-accounts/158748/Accessed 22 March 2023.
[190] S. Gatkan. Fired NY credit union employee nukes 21GB of data in revenge https://www.bleepingcomputer.com/news/security/fired-ny-credit-union-employee-nukes-21gb-of-data-in-revenge 2021.
[191] Avast Security News Team. Voice fraud scams company out of $243,000. https://blog.avast.com/deepfake-voice-fraud-causes-243k-scam. Accessed 15 July 2023.
[192] F.L. Greitzer, W. Li, K.B. Laskey, J. Lee, J. Purl, Experimental investigation of technical and human factors related to phishing susceptibility, ACM Trans. Soc. Comput. 4 (2) (2021) 1–48, https://doi.org/10.1145/3461672.
[193] W. Li, J. Lee, J. Purl, F. Greitzer, B. Yousefi, K. Laskey, Experimental investigation of demographic factors related to phishing susceptibility, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, 2020, pp. 2240–2249, pages, http://hdl.handle.net/10125/64015.
[194] Intelligence and National Security Alliance. Categories of insider threats. https://www.insaonline.org/.../insa-wp-categories-of-insider-threats-1.pdf No date.
[195] T Roberts. An insider threat framework– the SOFIT ontology. PentestPartners. https://www.pentestpartners.com/content/uploads/2021/08/An-Insider-Threat-Framework-The-SOFIT-Ontology.pdf. 2021.
[196] T. Ray. Motive doesn't matter: the three types of insider threats. 2019. https://betanews.com/2019/10/21/3-types-of-insider-threats/Accessed 22 July 2023.
[197] H. Aldawood, G. Skinner, Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues, Fut. Internet 11 (3) (2019) 73. Mar 18.
[198] R. Amin, I. Birdsey, and C. Holme. Cybercrime – are your employees a threat to operational security? https://www.clydeco.com/en/insights/2021/08/cybercrime-are-your-employees-a-threat-to-operatio 2021.
[199] F. Muhly, J. Jordan, R.B. Cialdini, Your employees are your best defense against cyberattacks, Harv. Bus. Rev. (2021). https://hbr.org/2021/08/your-employees-are-your-best-defense-against-cyberattacks.
[200] J. Speed. How to manage employees who cause cybersecurity issues. https://heliocentrix.co.uk/how-to-manage-employees-who-cause-cybersecurity-issues/2021.
[201] R.A. Alsowail, T. Al-Shehari, Empirical detection techniques of insider threat incidents, IEEE Access 8 (2020) 78385–78402, https://doi.org/10.1109/ACCESS.2020.2989739.
[202] Y. Chen, S. Nyemba, B. Malin, Detecting anomalous insiders in collaborative information systems, IEEE Trans. Dependable Secure Comput. 9 (3) (2012) 332–344, https://doi.org/10.1109/TDSC.2012.11.
[203] W. Park, Y. You, K. Lee, Detecting potential insider threat: analyzing insiders' sentiment exposed in social media, Secur. Commun. Netw. (2018), 7243296, https://doi.org/10.1155/2018/7243296.
[204] R.A. Alsowail, T. Al-Shehari, A multi-tiered framework for insider threat prevention, Electronics, 10 (9) (2021), https://doi.org/10.3390/electronics10091005. Paper 1005.
[205] M. Liu, M. Li, D. Sun, Z. Shi, B. Lv, P. Liu, Terminator: a data-level hybrid framework for intellectual property theft detection and prevention, in: Proceedings of the 17th ACM International Conference on Computing Frontiers, 2020, pp. 142–149, https://doi.org/10.1145/3387902.3392329, pages.
[206] R.A. Alsowail, T. Al-Shehari, Techniques and countermeasures for preventing insider threats, PeerJ Comput. Sci. 8 (2022) e938, https://doi.org/10.7717/peerj-cs.938.
[207] K. Boakye-Gyan, PhD thesis, Cybersecurity, Capitol Technology University, 2021.
[208] D.M. Cappelli, A.G. Desai, A.P. Moore, T.J. Shimeall, E.A. Weaver, and B.J. Willke. Management and education of the risk of insider threat (MERIT): mitigating the risk of sabotage to employers' information, systems, or networks. Technical Note CMU/SEI-2006-TN-041 CERT Program.
[209] A. Jones, C. Colwill, Dealing with the malicious insider, in: 6th Australian Information Security Management Conference, Security Research Centre, School of Computer and Security Science, Edith Cowan University, 2008, https://doi.org/10.4225/75/57b562dab876e.
[210] K. Padayachee, An assessment of opportunity-reducing techniques in information security: an insider threat perspective, Decis. Support Syst. 92 (2016) 47–56, https://doi.org/10.1016/j.dss.2016.09.012.
[211] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T.J. Shimeall, and L. Flynn. Common sense guide to mitigating insider threats. Technical Report AD1044922, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2012.
[212] E.G. Archuleta, J. Moyer, Guarding against the insider threat, J. Am. Water Works Assn. 101 (5) (2009) 38–44, https://doi.org/10.1002/j.1551-8833.2009.tb09891.x.
[213] A. Mahfuth, Human factor as insider threat in organizations, Int. J. Comput. Sci. Inform. Security (IJCSIS) 17 (12) (2019) 42–47.
[214] W. Ashford, Insider Threat Poses Major IT Risk Concern, Computer Weekly, 2016, 5 September.
[215] M. Dennehy, PhD thesis, Information Technology, Capella University, 2021.
[216] J.L. Jenkins, PhD thesis, Department of Management, The University of Arizona, 2013.
[217] N. Khan, R.J Houghton, S. Sharples, Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks, Cogn. Technol. Work 24 (3) (2022) 393–421, https://doi.org/10.1007/s10111-021-00690-z.
[218] R. Searle, K.V. Renaud, Trust and vulnerability in the cybersecurity context, in: Hawaii International Conference on System Sciences (HICSS), 2023. https://hdl.handle.net/10125/103273.
[219] A. Burns, T.L. Roberts, C. Posey, P.B. Lowry, B. Fuller, Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse, Inf. Syst. Res. 34 (1) (2022) 342–362, https://doi.org/10.1287/isre.
[220] T. Noonan and E. Archuleta. The national infrastructure advisory council's final report and recommendations on the insider threat to critical infrastructures, 2008. https://nsarchive.gwu.edu/sites/default/files/documents/3346585/Document-03-National-Infrastructure-Advisory.pdf Accessed 26 March 2023.
[221] J.L. Wunderlich, Master's thesis, Computer & Information Science, Regis University, 2011.
[222] S. Bauer, E.W. Bernroider, K. Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks, Comput. Secur. 68 (2017) 145–159, https://doi.org/10.1016/j.cose.2017.04.009.
[223] M.J. Alotaibi, S. Furnell, N. Clarke, A framework for reporting and dealing with end-user security policy compliance, Inform. Comput. Secur. 27 (1) (2019) 2–25, https://doi.org/10.1108/ICS-12-2017-0097.
[224] S. Valentine, L. Godkin, Moral intensity, ethical decision making, and whistleblowing intention, J. Bus. Res. 98 (2019) 277–288, https://doi.org/10.1016/j.jbusres.2019.01.009.
[225] W. Wong, H. Tan, K. Tan, M.-L. Tseng, Human factors in information leakage: mitigation strategies for information sharing integrity, Ind. Manage. Data Syst. 119 (6) (2019) 1242–1267, https://doi.org/10.1108/IMDS-12-2018-0546.
[226] C.X. Chen, J.E. Nichol, F.H. Zhou, The effect of incentive framing and descriptive norms on internal whistleblowing, Contemp. Account. Res. 34 (4) (2017) 1757–1778, https://doi.org/10.1111/1911-3846.12325.
[227] J.P. Near, M.P. Miceli, Effective-whistle blowing, Acad. Manage. Rev. 20 (3) (1995) 679–708, https://doi.org/10.5465/amr.1995.9508080334.
[228] A. Mady, S. Gupta, M. Warkentin, The effects of knowledge mechanisms on employees' information security threat construal, Inform. Syst. J. 33 (2023) 790–841, https://doi.org/10.1111/isj.12424.
[229] A.J. Puleo, PhD thesis, Department of Electrical and Computer Engineering Graduate School of Engineering and Management, 2006.
[230] C. Faklaris, PhD thesis, Computer Science, Carnegie Mellon University, 2022, https://doi.org/10.13140/RG.2.2.22010.77764.
[231] L.J. Osterritter, K.M. Carley, Modeling interventions for insider threat, in: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, Springer, 2020, pp. 55–64, https://doi.org/10.1007/978-3-030-61255-9_6, pages.
[232] J.L. Jenkins, B.B. Anderson, A. Vance, C.B. Kirwan, D. Eargle, More harm than good? How messages that interrupt can make us vulnerable, Inf. Syst. Res. 27 (4) (2016) 880–896, https://doi.org/10.1287/isre.2016.0644.
[233] S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss, If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, Eur. J. Inform. Syst. 18 (2) (2009) 151–164, https://doi.org/10.1057/ejis.2009.8.
[234] J.D. Wall, M.W. Buche, To fear or not to fear? A critical review and analysis of fear appeals in the information security context, Commun. Assoc. Inform. Syst. 41 (1) (2017) 277–300, https://doi.org/10.17705/1CAIS.04113.
[235] K.V. Renaud, M. Dupuis, Cyber security fear appeals: unexpectedly complicated, in: Proceedings of the New Security Paradigms Workshop, 2019, pp. 42–56, https://doi.org/10.1145/3368860.3368864, pages.
[236] W.A. Cram, J. D'Arcy, J.G. Proudfoot, Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance, Manage. Inform. Syst. Quart. 43 (2) (2019) 525–554, https://doi.org/10.25300/MISQ/2019/15117.
[237] J. Abulencia, Insider attacks: human-factors attacks and mitigation, Comput. Fraud Secur. 2021 (5) (2021) 14–17, https://doi.org/10.1016/S13613723(21)00054-3.
[238] G. Dhillon, Y.Y. Abdul Talib, W.N. Picoto, The mediating role of psychological empowerment in information security compliance intentions, J. Assoc. Inform. Syst. 21 (1) (2020), https://doi.org/10.17705/1jais.00595. Paper 5.
[239] M. Warkentin, A.C. Johnston, J. Shropshire, The influence of the informal social learning environment on information privacy policy compliance efficacy and intention, Eur. J. Inform. Syst. 20 (3) (2011) 267–284, https://doi.org/10.1057/ejis.2010.72.
[240] A. Vance, D. Eargle, D. Eggett, D.W. Straub, K. Ouimet, Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength, Manage. Inform. Syst. Quart. 46 (3) (2022) 1721–1737, https://doi.org/10.25300/MISQ/2022/15511.
[241] D.H. Andrews, J. Freeman, T.S. Andre, J. Feeney, A. Carlin, C.M. Fidopiastis, P. Fitzgerald, Training organizational supervisors to detect and prevent cyber insider threats: two approaches, EAI Endorsed Trans. Secur. Safety 1 (2) (2013) e4, https://doi.org/10.4108/trans.sesa.01-06. . 2013.e4.
[242] A. McCue. 'Disgruntled employee' hacks own company's computer system, 2003. https://www.zdnet.com/home-and-office/networking/disgruntledemployee-hacks-own-companys-computer-system/Accessed 22 March 2023.
[243] N.F. MacEwan, Doctoral Thesis, University of Southampton, 2017.

[244] S. Farooqi, G. Abid, A. Ahmed, How bad it is to be good: Impact of organizational ethical culture on whistleblowing (the ethical partners), Arab Econ. Bus. J. 12 (2) (2017) 69–80, https://doi.org/10.1016/j.aebj. 2017.06.001.
[245] G. King III, A. Hermodson, Peer reporting of coworker wrongdoing: A qualitative analysis of observer attitudes in the decision to report versus not report unethical behavior, J. Appl. Commun. Res. 28 (4) (2000) 309–329, https://doi.org/10.1080/00909880009365579.
[246] J.A. Dungan, L. Young, A. Waytz, The power of moral concerns in predicting whistleblowing decisions, J. Exp. Soc. Psychol. 85 (2019), 103848, https://doi.org/10.1016/j.jesp.2019.103848.
[247] F. Amaro, PhD thesis, Information Technology, Capella University, 2020.
[248] J. Bedford, L.V.D. Laan, Organizational vulnerability to insider threat. What do australian experts say?, editor in: C. Stephanidis (Ed.), International Conference on Human-Computer Interaction Springer, Toronto, Canada, 2016, pp. 465–470, https://doi.org/10.1007/978-3-319-40548-3_77. pages.
[249] P.B. Lowry, G.D. Moody, Explaining opposing compliance motivations towards organizational information security policies, in: 46th Hawaii International Conference on System Sciences, IEEE, 2013, pp. 2998–3007, https://doi.org/10.1109/HICSS.2013.5, pages.
[250] M. Jeong, H. Zo, Preventing insider threats to enhance organizational security: the role of opportunity-reducing techniques, Telem. Inform. 63 (2021), 101670, https://doi.org/10.1016/j.tele.2021.101670. Paper.
[251] NIST. NIST cybersecurity framework, 2023. https://www.nist.gov/cyberframework Accessed 30 March 2023.
[252] D. Cressey, Other People's Money: A Study in the Social Psychology of Embezzlement, The Free Press, Glencoe, 1953.
[253] J.R. Nurse, O. Buckley, P.A. Legg, M. Goldsmith, S. Creese, G.R. Wright, M. Whitty, Understanding insider threat: a framework for characterising attacks. IEEE Security and Privacy Workshops, IEEE, 2014, pp. 214–228, https://doi.org/10.1109/SPW.2014.38, pages.
[254] H. Cline, PhD thesis, Cybersecurity, Utica College, 2016.
[255] D. Wolfe, D.R. Hermanson, The fraud diamond: Considering four elements of fraud, CPA J. 72 (12) (2004) 38–42.
[256] K. Weber, A.E. Schütz, T. Fertig, Insider threats–der feind in den eigenen reihen, HMD Praxis der Wirtschaftsinformatik 57 (3) (2020) 613–627, https://doi.org/10.1007/978-3-658-34524-2_17.
[257] A.J. Bell, M.B. Rogers, J.M. Pearce, The insider threat: Behavioral indicators and factors influencing likelihood of intervention, Int. J. Crit. Infrastruct. Prot. 24 (2019) 166–176, https://doi.org/10.1016/j.ijcip.2018.12.001.
[258] L. Akers, P. Del Grosso, E.K. Snell, S. Atkins-Burnett, B. Wasik, J. Carta, K. Boller, S. Monahan, Tailored teaching: emerging themes from the literature on teachers use of ongoing child assessment to individualize instruction, HS Dialog Res. Pract. J. Early Childhood Field 19 (2) (2016) 133–150.

Further reading

[1] K.D. Bailey. Typologies and taxonomies: An introduction to Classification Techniques 102, Sage, 1994.
[2] A.P. Moore, D.M. Cappelli, T.C. Caron, E. Shaw, D. Spooner, and R.F. Trzeciak. A preliminary model of insider theft of intellectual property. Technical Report ADA589594, Carnegie-Mellon Univ Pittsburgh Software Engineering Inst, 2011. https://apps.dtic.mil/sti/citations/ADA589594.

Karen Renaud Karen Renaud is a Scottish computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. She collaborates with academics in 5 continents and incorporates findings and techniques from multiple disciplines in her research.

Merrill Warkentin Merrill is a William L. Giles Distinguished Professor at Mississippi State University, where he serves as the James J. Rouse Endowed Professor of Information Systems in the College of Business. His primary research focus is in behavioural IS security and privacy issues, and has appeared in MIS Quarterly, Journal of MIS, Journal of the AIS, European Journal on Information Systems, Information Systems Journal, Decision Sciences, and other leading journals. He has chaired international conferences and holds or has held editorial positions at MIS Quarterly, Information Systems Research, Journal of the AIS, European Journal of IS, Decision Sciences, and other top journals. His research has been supported by NSA, IBM, NATO, UN, and others.

Ganna Pogrebna Ganna is the Executive Director of the Artificial Intelligence and Cyber Futures Institute at Charles Sturt University (Australia), she also holds a research professorship position in behavioural Business Analytics and Data Science at the University of Sydney Business School. Additionally, Ganna serves as a Lead of behavioural Data Science strand at the Alan Turing Institute – the national centre of excellence for AI and Data Science in London (UK), where Ganna is a fellow working on hybrid modelling approaches between behavioural science and data science (e.g., anthropomorphic learning). Ganna published many articles in high-quality peer-refereed journals. She also currently serves as a methods editor at the Leadership Quarterly and an associate editor of Judgement and Decision Making journal. Ganna studied Economics at the University of Missouri Kansas City (US) and the University of Innsbruck (Austria). She holds a Ph.D. in Economics and Social Sciences. Before coming to Australia, Ganna worked at Columbia University in New York (USA), the University of Bonn (Germany), Humboldt-Universität zu Berlin (Germany), the University of Innsbruck (Austria), the University of Warwick (UK), and the University of Birmingham (UK).

Karl van der Schyff Karl (Ph.D. Rhodes University) is a Lecturer at Abertay University. His research interests include behavioural information security, information privacy, quantitative methods and cyberpsychology.