Managing insider risk ‘entities’ as the route to security convergence.

Robert Kennedy

University of Portsmouth, School of Criminology and Criminal Justice, Portsmouth, United Kingdom

Abstract

The threat posed by human insiders and technological insider ‘entities’, be they intentional or unintentional, can provide substantial harm to an organization. However, the current practices to manage insider risk often work within a siloed environment without engagement with the wider security disciplines and organization. This paper provides results from an exploratory study using qualitative research in the form of semi-structured interviews with fourteen security practitioners from both the public and private sectors to ascertain the current practices to manage insider risk. The key findings show that there is a lack of organizational understanding and engagement to manage this risk, a rebrand is required to enable insider risk management to be more palatable to the wider organization, the current taxonomy is outdated due to the emergence of insider ‘entities’, and that insider risk management could provide the route to security convergence as part of a socio-technical system design. Whilst this paper focuses on practice within the United Kingdom (UK), the suggestions raised within this paper are not necessarily limited to the UK.

Keywords

Insider Risk- Insider Threat- Personnel Security- AI Risk- Security Convergence- Enterprise Security Risk Management- Sociotechnical Systems

1. Introduction

The UK National Protective Security Authority (NPSA) currently define an insider as “any person who has, or previously had, authorized access to or knowledge of the organization’s resources, including people, processes, information, technology, and facilities” [38].The risk to organizations posed by insiders can be especially perilous [63, 35] requiring organizations to assess insider threat and prioritize risk proactively as opposed to reactively [17, 53]. The management of insider risk requires a personnel security strategy to mitigate, personnel security is defined by Martin [30] as “the system of protective security measures by which an organization understands and manages insider risk” [2023, p.12]. As an exploratory study, conducted from an interpretive stance, this study aimed to understand the barriers and enablers to manage the insider risk posed to organizations, and to explore the potential contribution that security convergence could provide to enable organizations to embed effective personnel security to mitigate risk. The research method used semi-structured qualitative interviews to gain an understanding of practitioner knowledge from fourteen individuals with experience in both the public and private sectors. The remainder of this paper is organized as follows: the next section presents the background research conducted by means of a narrative literature review. Section three summarizes the research design and method. The fourth section details the key findings followed by the fifth section which provides a discussion of the findings. Finally, a conclusion summarizes this paper to end.

[1]The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS’25) September 17-18 2025, Skopje, North Macedonia.

Robert Kennedy

Robert.Kennedy1@myport.ac.uk

0009-0008-7818-9372 (R. Kennedy)

2. Background Research

A narrative literature review was undertaken which incorporated the subjects of; insider threat actors, assessing insider risk, insider 'entities', security governance, the socio-technical approach to manage insider risk, security convergence and enterprise security risk management.

2.1 Insider Threat Actors

Cyber, physical and technical security makeup three of the four main security disciplines [33] and can be used to mitigate risk by combining security risk management and security products. The management of insider risk employing the fourth discipline of personnel security is often a challenge as organizations are complex, the larger the organization the more complex it becomes [66, 53]. Insiders can potentially provide a substantial and credible threat to organizations [54, 5] with the manifestation of deviant behavior potentially capable of harming organizations in many ways [62, 21]. Insiders do not always take the form of those capable of expressing malevolent creativity with the deliberate intent to cause harm [18] as unintentional actions have also been found to be contributing factors to security incidents and events [35]. Such incidents include the unauthorized disclosure of sensitive information, the corruption of processes, the sabotage of assets, enabling third-party access into networks and buildings [60, 5] and even violent assault to include murder [51].

The harm an insider can potentially inflict on an organization often surpasses that which external threat actors are capable of. This is mainly due to insiders having legitimate and sometimes privileged access to organizational assets, an understanding of organizational vulnerabilities and the ability to bypass security controls [14, 30, 8]. Research conducted regarding security failure also supports the notion that insiders can potentially provide, either intentionally or unintentionally, a credible threat [44]. Martin [30], argues that malicious insiders, often referred to as intentional insiders, are difficult to detect, however, non-malicious insiders, often referred to as unintentional insiders also potentially provide a considerable threat to organizations. Moneva and Leukfeldt [35] support this notion and identify two types of unintentional insiders as the 'negligent' insider or the 'well-meaning' insider, with the latter believing they are acting in the best interest of the organization, usually as they have been victim to social engineering.

Renaud *et al.* [43] argue that the financial cost of an insider event can reach millions of pounds/dollars, which should provide a concern for many organizations. However, the occurrence of insider events continues to arise across many nations and organizations [30, 43]. Armstrong-Smith [5] argues that the COVID-19 pandemic, which enhanced individuals' stress and levels of despondency provided an increase to the number of insider events, including industrial espionage and the evolvement of the 'super malicious insider', which is a threat actor with enhanced technical ability and knowledge of the organizations' techniques to detect insider threat. Insider events are often enabled by the lack of an effective detection capability, a lethargic response even if detected, and a lack of consistency regarding mitigation measures [24]. Vigilance is therefore required within organizations to recognize early signs of disgruntlement to enable a swift organizational response to intervene and prevent individuals from becoming an insider [51]. Despite the risk to organizations provided by potential insiders which would benefit from a proactive risk management approach [1], Martin and Mercer [31] argue that personnel security is often based on immature custom and practice, with little basis on actual evidence. This is supported by Wood [66] who argues that the challenge of mitigating insider risk is not addressed by current security systems with Stewart and Hobbs [56] adding that existing methodology to manage insider risk is limited and lacks transparency.

2.2 Assessing Insider Risk

An organization's protective security, business continuity and resilience rely on the effective management of risk exposure [27] to meet the challenges posed by dynamic and adaptive security risks [30]. The available data regarding threat information in general often focuses on external threat actors [17] that often pose physical or cyber security risk [28], which could impact the effective risk management of insider events. Many organizations therefore focus on dangerous outsiders [61]; however, Kotb *et al.* [28] argue that insiders, be they malicious or negligent, pose a considerable risk, accounting for 79% of cyber security breaches alone. Cappelli *et al.* [14] support the notion that the threat posed by the insider is often overlooked with organizations in the main concentrating on external threats, this narrow framing potentially impedes the effective allocation of resources [41] which in turn would potentially influence an organization's risk exposure.

Quantitative risk management methodology employed in the management of insurance or project risk is often also applied to manage security risk. Martin [30] however argues that security risk is significantly different from other risks as it is the combination of threat, vulnerability and impact, therefore quantitative methodology employed to manage risk in other contexts is not always effective when applied to security. Another factor that should be considered is that risk is a subjective topic and often influenced by an individual's experience along with the cultural, social and political factors that the individual has been exposed to [27]. Cappelli *et al.* [14] also provide a further dynamic that could hinder the mitigation of insider risk, as such mitigations most certainly will rely on the protection provided by potential threats i.e. organizational staff, who could be insiders themselves.

Insider risk is often complex and is present across organizational contexts, often generated by multiple factors [53]. Ideally, multiple stakeholders from each business unit should participate and contribute to the security risk assessment process by employing a systematic approach [27]. This would support the notion that protective security should be managed holistically with a converged approach which recognizes the interdependencies across the main security disciplines [30]. By incorporating wider business functions into the security risk assessment process interdependencies can be identified to support security risk management. For example, Wright and Roy [67] argue that industrial espionage cannot be dealt with by the security department alone as the threat comes from insiders, therefore an organization's Human Resource department plays a pivotal role in managing insider risk. Antonucci [4] supports this notion arguing that insider risk should be managed by an organizational 'Human Resources Security' function.

2.3 Insider 'Entities'

Wood [66] argues that the development of Artificial Intelligence (AI) and Machine Learning could support malevolent actors to enhance social engineering attack vectors and also enable the interrogation of large data sets to exfiltrate valuable data. Thite & Iyer [58] argue that generative AI-based applications provide organizations with both potential and danger. This is supported by Carpenter [15] who states that AI provides the ability to add value to organizations, however, the consequences could be catastrophic should adversaries use it to manipulate, deceive and exploit unintentional insiders. Kotb *et al.* [28] also highlights the danger posed by generative AI, which can enable adversaries to create synthetic behaviors and or profiles capable of mimicking legitimate users, which in turn makes detection considerably more difficult. Sadok *et al.* [44] argue that human imagination should be utilized to explore and consider the unintended consequences of using AI, to identify proactive and combative measures to mitigate the impact to organizations.

Martin & Mercer [31] argue that advancements in AI, to include agentic AI, provide a risk to organizations from not only human insiders, but also artificial insiders. Skorich & Manning [53] support this argument, adding that any code with decision making capability could potentially provide an insider risk. This provides a potential problem if practitioners of protective security are not considering AI, and AI experts are not considering AI as a potential 'insider entity' [31]. Renaud *et al.* [43] therefore propose that due to the insider risk posed by the advances of technologies such as AI, Machine Learning and the Internet of Things (IoT), the current taxonomy used for insider risk emanating from human sources only is outdated and requires an update to meet the demands of the present, let alone the future.

2.4 Security Governance

According to Wakefield [60], security governance involves the collaborative efforts of multiple stakeholders to enable the provision of effective protective security through organizational hierarchy and networks. Skorich and Manning [53] highlight that organizational control requires a top-down approach with legal and practical accountability for decisions made occupying the objectives of an organization's peak authorities such as the board or chief executive officers. Organizational governance therefore is the ability to have both a decision-making and a control function to enable the investment of resources to create or protect the value of the organization. The governance function should be underpinned by strong leadership which provides both oversight and executive commitment [42]. However, even when an organization has a governance structure which involves the security disciplines reporting to a Chief Security Officer (CSO), this does not necessarily enable a governance function championing risk mitigation with security convergence. Should an organization not understand the interdependencies of each business unit and their risks, organizations could potentially operate with an ineffective governance model [2], which does not necessarily provide organizations with a valid single overview of security risk [48].

Whilst the CSO is responsible for ensuring an organization's executive leadership, governance and management functions participate and contribute towards discussions involving protective security and provide instruction as to responsibilities and the discharging of actions [37], ideally this should form part of an enterprise risk management strategy [48]. Sadok *et al.* [44] argue that the development of policy and process with a top-down managerial approach without the consultation of stakeholders and integration of an organization's security functions could impede the usability of policy and processes and would therefore potentially encourage employees to find a workaround or alternatively circumvent developed security measures. Security design should therefore include the convergence of the interdependent security disciplines [30] and consider and contextualize the role of the end-user when designing security policy and procedure [44, 47] to support a personnel security strategy to mitigate insider risk in practice.

2.5 The Socio-Technical Approach to Mitigate Insider Risk

Personnel security has been criticized as many organizations tend to employ technical-centric approaches [30], with Steinmetz [55] arguing that such an approach is ineffective. Sadok *et al.* [45] suggest that organizations need to employ a socio-technical approach as technology-centered approaches alone, without consideration towards people and processes provide potentially flawed security mitigations. Sutton [57] supports this notion arguing that the monitoring of user accounts, internet access and the employment of intrusion detection software may identify some insider activity, however, it is not guaranteed to detect it all. Martin [30] argues that technical-centric mitigations can potentially be gamified, this is supported by Sutton [57] who states that an insider will likely be aware of an organization's insider detection capabilities and will adapt their behavior accordingly to mitigate the arousing of suspicion against them.

The UK National Protective Security Authority (NPSA) advocate a combined approach employing social, physical and technical mitigation methods within their Insider Risk Mitigation Framework guidance [39] in support of the 'Critical Path to Insider Risk' (CPIR) methodology. The CPIR methodology identifies factors that potentially contribute to insider risk manifestation within individuals, those factors being personal predispositions, individual stressors, concerning behaviors, a problematic response from the organization [51] and crime scripts which refer to insider attack planning [52]. It must be noted that the CPIR does not incorporate criminological theory such as routine activity theory and crime prevention through environmental design (CPTED) as advocated by Skorich and Manning [53] to support situational crime prevention measures to mitigate insider risk [35]. The CPIR also does not advocate the COM-B model widely preferred by behavioral scientists, COM-B focusses on the interaction between capability, opportunity and motivation for any behavior change intervention to be effective [64, 3]. The author of the CPIR methodology has identified limitations of the framework which includes the pathway following a criterion-based approach, it was created using a heterogeneous insider sample, and therefore only focuses on intentional insider threat actors and does not consider different types of insider events [52]. It could be argued that unintentional insider acts are more prevalent across organizations, arising from negligent or well-meaning individuals [35] who have for example, been targeted by social engineering, however, the CPIR does not encompass this, which potentially provides limitations with this approach.

The elements that form the CPIR methodology when applied by organizations alongside a combination of social, physical and technical security mitigations, would potentially benefit from utilizing 'Work Systems Theory' to design a socio-technical approach [45]. Fischer and Herrmann

[22] support the use of a socio-technical system as they argue that the use of technology alone does not influence or impact human behavior or social structures positively. Button [13] also supports the argument that the design of a socio-technical system is fundamental to reducing the risk of insiders which can exacerbate technical risks. This is supported by Asiri *et al.* [6] who argue that human intuition is often adept at the detection of often subtle deviations, which supports the notion that humans-in-the-loop models incorporating the use of computing algorithms that involve the final decision making undertaken by a human [58] are paramount to the mitigation of insider risk.

A socio-technical system incorporating the inclusion of human, social, organizational and technical factors [9, 19] could potentially enable a strategy that bridges the organization's protective security functions with the identification, acknowledgement and augmentation of the interdependencies across the security disciplines. This converged approach potentially being more effective to mitigate insider risk [30]. There are numerous challenges to embedding security design into an organization with the need to balance security and usability against the context of the organizational practices [44]. A democracy-driven approach encouraging employees to collaborate with the forming of security design is a fundamental value of socio-technical system design [36] and would arguably better support usability.

Effective personnel security often enables an organization to work towards being a high-trust organization nurturing a healthy culture [30]. Organizations that nurture a sense of confidence in their employees with individuals not feeling they need to be on guard or suspicious of the organization's intentions, fostering a culture where employees are confident that the management act in a responsible manner, often outperform organizations that do not encourage such a relationship [65]. There is evidence that high-performing organizations demonstrate high levels of mutual trust between employees, employers and stakeholders and in general, have less insider activity [30]. Sadok *et al.* [44] offer a possible explanation for this as they argue that engaged, motivated staff that align and believe in the organization's objectives are more likely to support the protection of organizational interests. Therefore, the benefits associated with the employment of a socio-technical system could potentially support organizations to become high-performing organizations [34], with an organization described as high-performing when it supports an organization to operate at levels of excellence above and beyond the capability of competitors [12].

2.6 Security Convergence

Developing security strategy to mitigate risk relies on an organization ensuring that it has considered the full range of security risks that it faces [59]. The step change from the third industrial revolution, also known as the digital revolution to the present fourth industrial revolution (4IR) summarized as the fusion of technology and how it interacts across the digital, physical and biological domains [49, 50] arguably changes the risk landscape for many organizations. The Internet of Things (IoT) which enables physical devices to be linked via the Internet, and is now used in smart homes, buildings and cities as societies develop and harness the benefits of 4IR, increases the attack surface available for threat actors to target [11, 60]. Therefore, a holistic approach is required to mitigate protective security risk which is often referred to as security convergence [2, 48] and usually requires a 'systems thinking' approach to be employed to best manage security risk [30]. Security convergence requires the formal collaboration and integration of an organizations pooled security resources [59] and is viewed as a contemporary subject within both academia and industry to provide a commensurate approach to security risk management [32, 10].

As societies continue the journey from 4IR towards the fifth industrial revolution (5IR), often referred to as Industry 5.0, the potential attack surface available for threat actors to exploit will increase. 5IR is summarized as the harmonious human and machine collaboration demonstrating the core values of human-centricity, sustainability and resilience [68]. One such example of the advances in technology to support 5IR include Brain-Computer Interfaces (BCI) which is currently being tested as a military tool to enable a single soldier to command a swarm of drones, as well as being used in the medical sector to provide individuals with severe communication and motor impairments with a better quality of life [26]. BCI is just one example of human-machine interaction technology, which is one of a suite of technologies identified as 5IR enabling technology along with; bio-inspired technology and smart materials, digital twins and simulation, data transmission, storage and analysis technology with the ability to handle data and system interoperability, AI to detect causality in dynamic systems which leads to actionable intelligence, and technology for energy efficiency to include renewables, storage and autonomous technology [68]. The societal and financial benefits of developing 5IR enabling technologies, often dual use in their nature, could potentially encourage threat actors to target the Intellectual Property (IP) related to such technologies to gain a strategic advantage. Blended, or converged attacks, including a combination of attacks involving technical physical and cyber vectors [20] will often use insiders to bypass existing security controls [30, 53]. This not only supports the notion that security convergence would enable organizations to meet the security challenges posed by 4IR and better prepare for the future challenges of 5IR by providing a single overview of security risk to identify appropriate mitigations.

2.7 Enterprise Security Risk Management

Schneller *et al.* [48] argue that a fully converged security function operating within a unified and interconnected model can support an integrated organizational defense system. The traditional organizational risk management approach has been to treat individual risks in isolation, assigning individuals or teams within different departments to manage this risk [2]. By recognizing security as a subdomain of the organizations overall wider risk management, an understanding of interconnectivity and dependent activities relating to risk management can be gained [27, 29]. This is supported by Aleem *et al.* [2], who argue that ignoring interdependent business risks provides both an inefficient and ineffective method to manage organizational risk. The need to adopt and adapt a strategic approach to risk management in a modern environment described as volatile, uncertain, complex and ambiguous (VUCA) has become a priority for many organizations [29]. This has been fueled by the rising numbers of diverse and interconnected organizational risks [2], which has led some risk practitioners to transition from an Enterprise Risk Management (ERM) approach, which linked organizational risk management activities, to an Enterprise Security Risk Management (ESRM) approach. Security management employing the strategic approach of ESRM aligns security risk management to an organization's mission and goals by employing globally recognized and established risk management principles [29].

3. Research design and method

This study involved qualitative research in the form of semi-structured interviews. Participants in this empirical study were identified by the use of a snowball sampling technique. A total of 14 participants contributed to this study with the participants demonstrating considerable experience of personnel security ranging from 5 to 45 years. The participants came from varied backgrounds, having worked within a combination of both the public and private sectors. The research assumption is that the participants would possess the knowledge to support this qualitative research. The requirement for participant sampling and selection included that participants shall work in personnel security and their role should involve managing insider risk. Participants would be excluded should they not work within personnel security or interdependent business functions.

The research was an exploratory study, conducted from an interpretive stance which aimed to shed light on experienced practices within the sample. A qualitative approach was taken to mitigate the challenges identified by Noaks & Wincup [40] who argue that quantitative methods of criminological enquiry are rarely effective with regards to insider activity. To achieve the concept of 'Verstehen' this research employed the ontological approach of constructionism along with an epistemological interpretive stance [16, 7]. The main purpose of this study is to employ semi-structured interviews to discover through interactions, discussion and dialogue the tacit knowledge possessed by security practitioners to influence the production of new Mode 2 knowledge [25, 46, 23]. A thematic analysis was conducted using the NVivo software package which enabled the coding and analysis of the data.

The study aims to research the following questions:

RQ1- To explore to what extent organizations are aware of insider threat.

RQ2- To explore organizations' practices when it comes to assessing and addressing insider risk.

RQ3- To explore the potential contribution of security convergence to prevent and address insider risk.

The semi-structured interview themes to ascertain; how well organizations manage insider risk, the barriers to managing insider risk, and the contribution that governance and leadership contribute to personnel security. The interviews also aimed to explore the relationship that non-security functions of an organization can provide to manage insider risk, the future challenges organizations will face from emerging technology, and how security convergence can support the mitigation of insider risk.

4. Key findings

This study provided a wealth of data which was thematically analyzed, however, for the purpose of this paper the key findings will focus on the following five themes:

(i) the lack of insider risk management conducted by organizations.
(ii) the role that non-security functions of an organization should contribute to managing insider risk.
(iii) the potential opportunity security convergence would provide to organizations to support insider risk mitigation.
(iv) the challenges and benefits of emerging technology to manage insider risk.
(v) the limitations of a technical centric approach to mitigate insider risk.

4.1 Insider Risk Management

All the participants in this research stated that insider risk management in general is not undertaken effectively by organizations. One participant stated that "*organizations haven't actually assessed their risk to be able to manage it*" with another adding *"I think organizations think it's covered by pre-employment screening"*. The lack of risk assessment was a theme that all participants stated was a problem with one adding that *"they're not proactively managing it because they haven't done the threat assessment, they haven't done the risk assessment, they've just gone we need some level of assurance that the people that we're employing into this organization aren't a terrorist or aren't working for the Chinese or Russians"*. The participants all stated that there was a lack of understanding regarding insider risk with one commenting that *"they have a narrow perception about what an insider is, I think for most organizations the insider threat is about fraud and circles around that, and not about stealing intellectual property or certainly not espionage or state sponsored espionage"* with another participant adding *"most organizations have some insider risk programs in place, but they might call it fraud, they might call it anti-corruption, they might call it standards, might just be HR practices, but it's never coordinated and it's never linked with security and it's very rarely linked with external threat actors"*. This supports the literature review which identified that insider risk is not, in general, effectively managed by organizations due to the lack of understanding of the problem and poor risk management practices which do not reflect that security risk is the product of threat, vulnerability and impact.

The majority of participants (nine) highlighted a gap in education relating to managing the insider risk. One participant stated, *"I don't think there is professionalism in personnel security, there aren't really courses and training out there"* which was supported by another participant who stated that personnel security *"needs to be properly taught and people need to be trained appropriately"*. Furthermore, the current immaturity of personnel security was identified during the interviews with one participant commenting that *"there needs to be standards and competency frameworks"*, with another adding that *“there’s nothing out there which helps people broaden their horizons and think about how to mitigate these risks or approach these problems in new ways”*. This was further supported by another participant who stressed the need for underpinning knowledge from the social sciences commenting that *“there needs to be expertise, and consideration for personnel security from the psychological and behavioral sciences”*. This supports the literature review which identified that current methodology to manage insider risk is immature, is not evidence based and lacks transparency.

All of the participants were of the opinion that engagement with the wider organization to land the correct messaging around insider risk was a challenge. One participant stated, *“I think a lot of organizations are risk averse to the perception that their staff might pose a risk”* with another adding that *“one of the biggest barriers is that people do not engage because they think it’s somebody trying to get at them or the other members of the workforce”*. This was supported further with another participant communicating that *“there’s a fear that if you bear down on insider risk through personnel security, that somehow you’re creating this kind of, you know, ‘Stasi culture’ in your organization, you’re spying on your staff or you’re signaling to them that you don’t trust them and that in itself can be harmful”*. The literature review details the importance of trust within an organization; however, this suggests that a lack of engagement and understanding from the wider organization could be because they do not trust the personnel security mitigations organizations attempt to employ.

As the semi-structured interviews progressed a theme arose regarding the language used by security practitioners with participants (five) voicing concerns such as *“security uses language that is understood by security, it makes no attempt to think about its language in a way that is palatable to HR or other parts of the organization. It’s a secret language. It’s a dark art which is ‘need to know’, when it comes to insider risk, it’s not ‘need to know’ because people need to do the right things”*. A further participant stated that *“there seems to be an issue where senior leadership don’t like the term insider risk or insider threat”*. Participants suggested that a change of terminology may be required with one adding *“I think rather than calling it insider risk, it should be about employee vulnerability and how to mitigate that because that then brings onboard everybody because this isn’t a case you’re trying to catch them out, you’re trying to help them”*. This was further supported by other participants with one stating that *“if you talk about insider threat to staff, it’s a really hostile term, that’s why HR don’t like it either and that’s why I’ve gone down the route that it should be seen more as about welfare”* with another adding *“I think the insider threat pitch is growing, I also think obviously it can mitigate loads of other threats as well if done right, mental health for instance, if you show you’re a caring organization, it can help mitigate the insider threat”*. This was not previously identified within the literature review and suggests that common terms and phrases used by security practitioners are potentially impeding effective personnel security. The notion that the communications should be tweaked to focus on staff welfare or well-being was also not identified within the literature review.

4.2 The Contribution Required from Non-Security Functions of an Organization

A common theme that surfaced was that security departments alone cannot manage insider risk, with one participant stating that *“non-security functions are massively key to managing insider risk on a day-to-day basis”*, however, numerous participants (eleven) stated that in general, other non-security functions do not collaborate well to support personnel security with one participant stating that *“non-security functions at times work against rather than work with security”*. The role which HR plays was criticized as one participant contributed that *“functions such as HR can impact it negatively because it doesn’t work with it, it tends to work against it, even though ultimately they’re both after the same goal”*. Participants widely agreed that HR was key as one participant stated *“insider risks quite often first appear in an HR context”* with another adding that *“HR don’t see themselves as having a role with personnel security, whereas their role is absolutely critical”* which was supported by another participant who added, *“there’s often individuals that will be subject to some kind of formal disciplinary or investigation from an HR perspective that doesn’t crossover into security”*. This supports the findings within the literature review with Wright and Roy [67] arguing that HR plays a crucial role in insider risk management.

Participants stated that access to the Big Data held by organizations was key to managing insider risk with one participant stating that *“getting security to talk to HR, IT and legal, compliance and audit* *and all the other functions, there's often barriers to sharing information, you know security think that everything they do is terribly secret and confidential, HR won't talk about it because it's, you know, HR confidential, likewise legal departments and so on".* Another participant supported this notion adding that organizations need to *"look at the data you've already got, which you may have collected for all sorts of different purposes"* with a further participant adding that *"HR has loads of information, audit have loads of information about the bits that are broken, but they don't think of it in terms of insider risk".* Access to big data was not identified within the literature review and will therefore be discussed within the next section.

Furthermore, participants all stated that insider risk would most likely not be detected by security teams in the first instance with one participant stating, *"the people who are best placed to detect the early signs of insider risk are other people, so colleagues, managers and so on".* The participants all stated the importance of the crucial role line managers play in managing insider risk with one adding that *"the role of the line manager is absolutely vital, and they do have a security function".* However, the lack of training and awareness that line managers are provided with regarding personnel security was criticized as one participant added that *"line managers need to be trained, and there needs to be guidance and support centrally".* This supports the gaps identified within the literature review regarding the lack of criminological theory used within the CPIR methodology and would suggest that there is a place for security and crime science to support personnel security.

4.3 Security Convergence

All of the participants stated that a socio-technical system provided the best strategy to mitigate insider risk, however, two participants had reservations regarding the implementation of security convergence with one stating *that "if I'm honest, I don't see security convergence being of any use to effectively manage personnel security and insider risk because it's an organizational problem, it requires HR operations, all of the business functions to be able to deliver an effective end to end organizational wide insider risk mitigation program"* with another adding *"you are simply going to have physical, personnel, technical and cyber teams, all in their own swim lanes, all with their own ideas about what security looks like and what they can do to think about it, just a bigger silo".* The challenges of governance and risk management arose during the interviews with one participant stating, *"I think there needs to be a grown-up conversation about enterprise risk"* with another adding that *"I would like to see an individual within an organization charged with all of the elements of protecting an organization from harm".*

The majority of participants (twelve) supported the concept of security convergence to enhance personnel security with one participant stating that *"if you're bringing the consideration of personnel security to the table as an equal alongside physical, cyber and technical security, and considering it holistically and in the round then it can support personnel security"* with another adding that *"the thread that links cyber or IT security and physical security is the people, it's the cement in the middle".* The notion of a single overview of security risk was deemed crucial by all the participants with one stating *"you need a shared understanding of what risk you're actually talking about"* with another participant adding that *"you've got to have convergence because the risks effectively are already converged".* Security convergence was further supported by a participant who stated *"let's operate as our adversaries do, and as an adversary we say, what is the route to this information? What is the route to this target? And they don't care about what vector is used to do that".* The need for a security strategy to be part of the wider ESRM strategy was identified within the literature review along with the importance of an appropriate governance model, however, the notion that security convergence will simply provide a bigger silo is concerning and will be considered further within the discussion section.

4.4 AI and Insider Risk

The participants expressed mixed feelings regarding the use of AI to mitigate insider risk. One participant stated that AI can *"generate a great picture of the threat landscape and threat modelling, but it will still require human analysis"* with another adding that *"it could be a huge tool in our locker, and I think if we use it wisely, it could help us".* The ability for AI to interrogate Big Data and identify patterns and trends was seen as a positive by all participants with one commenting that *"the self-learning systems, if they see something they could become a whistleblower, which is not a bad thing*", this was supported with another participant adding *"it brings us closer to this kind of Holy Grail of continuous evaluation".* However, every participant highlighted the notion that AI also provides a challenge for security practitioners, with one adding that *"I'm convinced that AI will increasingly be part of the problem as well as part of the solution"* and another stating that *"AI would be a good way of detecting indicators that require a human being to pay attention to them, on the flip side, like literally any technology apart from nuclear weapons, they're all dual use, AI is no exception".* All of the participants acknowledged that AI provides a potential protective security risk as threat actors could harness AI as an attack vector. One participant stated that *"AI might increase the volume of social engineering attacks",* with another adding *"hostile cyber actors can do better at more scale to trick people*". The threat from social engineering was further supported by participants with one commenting that *"you can collect far more data and you can make patterns with it and use it offensively in terms of what is effectively spear phishing at a sort of spam level"* this was supported by another participant who suggested *"you could have thousands of AI bots slowly socially engineering information out of people".*

Furthermore, participants (eleven) voiced their concerns regarding AI being used to subvert information with one commenting that *"you could find that potentially hostile state actors could be feeding information into an AI system, in for example a threat assessment, you could find that the information isn't correct and it's been skewed".* All participants were in agreement that AI has the potential to become an insider itself, with one participant suggesting *"AI has the potential to become an insider itself, so as AI increasingly take on functions that hitherto have been done by human beings, you know, they can go wrong and cause harm or they can be subverted by external threat actors"* which was supported by another participant who poses the question *"how do we weed out bias in AI?".* This supports the findings of the literature review which identified that AI could potentially be used as a powerful tool to employ social engineering as an attack vector. The literature review also identified that AI could provide organizations with risk as a potential 'insider entity'.

4.5 Technical Centric Approach to Manage Insider Risk

All of the participants stated that technical only approaches to mitigate insider risk were limited. One participant stated *"fundamentally, I'm very much of the view that, like all interesting and important things in life, insider risk is a systems problem. It's something that is a characteristic of a complex adaptive system, which is what happens when you put people together, and a systems problem needs system solutions"* with another participant commenting that *"not everything is monitored, it doesn't account for things like workplace violence".* Another participant commented that *"humans are central to everything, so you have to understand that humans can also work around the technology"* which supports the findings within the literature review that technical mitigations can potentially be gamified by insiders. Furthermore, one participant added that they are *"useful as an indicator of stuff, but you can't do it all just by technological mitigations",* this was supported by another participant who commented that *"they're effective at telling you when the problems already gone wrong, they are too far up the curve of someone being on a critical pathway and doing an insider act, so they'll tell you when people have sent data, well that's great, could you not have told me before?".*

Further limitations were identified as one participant commented that *"if you're relying on your technology systems to mitigate against stuff, you still then need to have that approach to understand what it actually means, and put it into context",* with another adding that *"I think technological risk mitigations are good to an extent, they're good at identifying if somebody's online behavior is abhorrent, but they're only good up to a point because insider risk is so complex".* However, participants did display empathy towards organizations employing technical centric only mitigations as one commented *"I think over reliance on technology gives organizations that kind of false confidence that they're managing it better than they perhaps are, but it's an easy way to feel you're managing it, if you just buy lots of kit",* this was supported by another participant who added *"I think there's an understandable desire in organizations to find, you know, silver bullets, and preferably technological silver bullets, because wouldn't it be great if instead of having to worry about all this messy human stuff to do with people's relationships and attitudes and behaviors and oh, it's all very sensitive and difficult when people get upset* *and you know, launch grievances, you can save all of that by buying a blinky box that could do the job for you".*

All the participants advocated a socio-technical approach to mitigate insider risk with one stating *"it's black and white, technological centric mitigations are black and white, its yes or no, and the whole thing about personnel security and insider risk, it's firmly in that grey space"*, this was supported by another commenting *"I think technology has a role, but has to be integrated with a holistic set of measures"*. This was supported by another participant who stated that *"if someone is exhibiting disgruntlement or disaffection or if they're under stress, that won't show up in a technical measure, and that's when people provide the soft detection"* with another participant commenting that *"technology is part of the solution without a shadow of a doubt, and it can give you insights and it can collect data and it can make patterns out of things that humans won't see, but on its own, it's not, it's not an effective mitigation"*. This supports the need for insider risk to be managed with a socio-technical approach as identified within the literature review.

5. Discussion

Both the literature review and research conducted identified that organizations in general do not manage the risk posed by insiders with an effective personnel security strategy. The need to professionalize and mature the management of insider risk was also identified within the literature review and research, with training qualifications, competency frameworks and standards underpinned by key theory from not only crime and security science, but also from other social sciences such as psychology and behavioral science required to support this. The effective management of a problem in the first instance relies on an organization's understanding of the problem. At present insider risk is not understood, meaning any current mitigations in place are likely not effective. This would hinder the organizations' ability to mitigate not only intentional insider activity, but also unintentional insider events due to a lack of training or security measures not considering the usability of end users during design, forcing end users to circumvent controls to simply do their job.

The research also highlighted that non-security elements of an organization have a crucial role in mitigating insider risk; however, this is informal and is not being capitalized upon as personnel security is often left to the security department alone. The research identified a distrust towards the terms 'insider risk' and 'insider threat' and highlighted that this not only creates suspicion within employees, it also often creates a barrier and blocker to organizational-wide engagement. This distrust likely impedes the organizational understanding of what insider risk is, as the research evidenced that most organizations have a narrow focus regarding insider risk and associate it with fraud alone, disregarding unauthorized access to sensitive information, process corruption, sabotage, enabling third-party access to buildings or networks, and workplace violence. Furthermore, as emerging technologies such as agentic AI become more widely used within organizations, this provides the potential that insider risk can now not only arise from humans, but also from technological 'entities'. This new form of insider risk was identified within both the literature review and research, which suggested that the current taxonomy used in personnel security and insider risk is now outdated as it only focusses on human insiders.

The distrust evidenced towards insider risk mitigation strategy would likely prevent an organization from becoming a high-performing business as trust, as identified within this paper, is considered a vital component of high-performing organizations. However, in its current form, any strategy to mitigate insider risk will struggle to gain the trust of the organization. As such, access to the Big Data that participants stated as paramount to support insider risk mitigations will likely continue to be denied. This will not only hinder the organization from becoming a high performer but also continue to expose the business to insider risk and the inevitable cost of dealing with both intentional and unintentional insider threat actors/entities. This arguably positions insider risk as not only a security risk, but also as a business risk, with the potential to expose the organization to risk, and potentially impact business continuity.

This paper therefore suggests that a rebrand is required to soften the terminology used with regards to insider risk and insider threat to make it more palatable to the wider organization with a new taxonomy required to replace the outdated personnel security taxonomy. The research identified that approaching insider risk from an employee vulnerability and welfare perspective would prove beneficial, focusing on the wellbeing of those with access to organizational assets. This approach could potentially break down the barriers and blockers within organizations and enable personnel security teams to not only educate the organization on the risk posed by insiders but also to open the channels for wider organizational engagement. It is therefore recommended that further research is conducted to devise a new taxonomy to replace the one currently used in personnel security, to replace key terms such as insider risk and insider threat with terminology adopting an employee well-being theme. This would arguably contribute to the organization's better understanding of the risk posed by the insider and facilitate a strategy to mitigate involving the interdependent functions of an organization using the data each function possesses to identify potential risk.

This research suggests that the mitigation of insider risk requires the convergence of an organization's pooled security resources and the involvement of the interdependent business functions of an organization. The collaboration of cyber security monitoring with physical security designed to mitigate surreptitious activity, supported by technical security providing an all-around defensive monitoring system, alongside insider risk mitigations would provide a socio-technical system which has been identified within this research as crucial to managing insider risk. This paper therefore suggests that security convergence is paramount alongside a governance model that supports enterprise security risk management for organizations to effectively manage the insider risk. As this research identified, a robust defense requires security teams to work as their adversaries do, and their adversaries do not work in departmental silos. Therefore, a single overview of security risk is vital to mitigate the current threats of the fourth industrial revolution and enable organizations to horizon scan with a converged security approach to mitigate potential threats posed by the fifth industrial revolution.

Conclusion and further research

This study explored the current organizational practices to mitigate insider risk from a practitioner perspective. It endeavored to ascertain if organizations had effective mitigations in place and if security convergence could support organizations to better manage insider risk. The main findings show that insider risk is not in general managed effectively by organizations, that there is a lack of organizational-wide understanding and limited engagement with strategy to mitigate insider risk. There is also a distrust and suspicion around the current taxonomy used in personnel security, which has also been identified as outdated due to the emergence of insider 'entities' such as AI, Machine Learning and any code with decision making capability. This study also identified that security convergence could support the management of the insider risk as part of a socio-technical system. This paper suggests a rebrand to soften the terminology currently used, such as finding alternatives to the terms 'insider risk' and 'insider threat' to make insider risk management more palatable to the wider organization and remove suspicion by focusing on employee vulnerability, welfare and wellbeing as a theme. Security convergence, and an appropriate governance model to support is also suggested within this paper with a focus on the wider organization playing its part to mitigate insider risk as part of an ESRM approach. Further research will be required to explore the suggestions and influence organizations to adopt and embed effective insider risk management and support the drive towards security convergence. Future research within this field should consider; the lack of a joined-up approach and the organizational responsibility to manage insider risk, the hostility and suspicion to the vocabulary currently used, and follow up research to investigate if any solutions have been attempted along with their levels of success.

Declaration on Generative AI

The author(s) have not employed any generative AI tools.

References

[1] Aldulaimi, S. H., Abdeldayem, M., Abu-AlSondos, I. A., Almazaydeh, L., Alnajjar, I. A., & Mushtaha, A. S. (2024). Robust information security for strengthening HR in organizations. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-5). 10.1109/ICCR61006.2024.10533019

[2] Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal*, *26*, 236-248. https://doi.org/10.1057/sj.2013.14

[3] Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019. https://aisel.aisnet.org/ecis2019_rp/100

[4] Antonucci, D. (2017). Human Resources Security. In D. Antonucci, The Cyber Risk Handbook: Creating and Measuring Effective Cyber Security Capabilities, 369-374, Wiley.

[5] Armstrong-Smith, S. (2024). *Understand the Cyber Attacker Mindset*, Kogan Page.

[6] Asiri, M., Arunasalam, A., Saxena, N., & Celik, Z. B. (2025). Frontline responders: Rethinking indicators of compromise for industrial control system security. *Computers & Security*, *154*, 104421. https://doi.org/10.1016/j.cose.2025.104421

[7] Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative sociology*, *42*, 139-160.

[8] BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The enemy within? The connection between insider threat and terrorism. *Studies in Conflict & Terrorism*, *41*(2), 133-150. https://doi.org/10.1080/1057610X.2016.1249776

[9] Baxter, G. & Sommerville, I. (2011), Socio-technical systems: From design methods to systems engineering. *Interacting with computers,* 23(1), 4-17 https://doi.org/10.1016/j.intcom.2010.07.003

[10] Boakes, E. (2023). *Security convergence: building an evidence-based roadmap* (Doctoral dissertation, University of Portsmouth).

[11] Bryan, E. & Larsen, A. (2017). 'Cybersecurity Policies and Procedures'. In D. Antonucci, *The Cyber Risk Handbook: Creating and Measuring Effective Cyber Security Capabilities*, 35-65, Wiley.

[12] Buchanan, D. A., & Huczynski, A. (2019). *Organizational Behaviour*. Pearson UK

[13] Button, M. (2020). Economic and industrial espionage. *Security Journal*, *33*, 1-5. https://doi.org/10.1057/s41284-019-00195-5

[14] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

[15] Carpenter, P. (2024). Faik: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-generated Deceptions. John Wiley & Sons.

[16] Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods.* Oxford University Press.

[17] Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report*, *14*(4), 186-196. https://doi.org/10.1016/j.istr.2010.04.004

[18] Cropley, D.H., & Cropley, A.J. (2019). Creativity and malevolence: past, present, and future. *The Cambridge Handbook of Creativity,* 677-690.

[19] Dalpiaz, F., Paja, E., & Giorgini, P. (2016). Security requirements engineering: designing secure socio-technical systems. MIT Press.

[20] Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429-450 https://doi.org/10.1080/23738871.2021.2000628

[21] Di Stefano, G., Scrima, F., & Parry, E. (2019). The effect of organizational culture on deviant behaviors in the workplace. *The International Journal of Human Resource Management*, 30(17), 2482-2503. https://doi.org/10.1080/09585192.2017.1326393

[22] Fischer, G., & Herrmann, T. (2011). Socio-technical systems: a meta-design perspective. *International Journal of Sociotechnology and Knowledge Development (IJSKD),* 3(1), 1-33. DOI:10.4018/jskd.2011010101

[23] Fulton, J., Kuit, J., Sanders, G., & Smith, P. (2012). The role of the professional doctorate in developing professional practice. *Journal of nursing management*, *20*(1), 130-139. https://doi.org/10.1111/j.1365-2834.2011.01345.x

[24] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. Journal of Computer Information Systems, 62(4), 706-717. https://doi.org/10.1080/08874417.2021.1903367

[25] Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P. & Trow, M. (1994). *The New Production of Knowledge*, SAGE publications.

[26] Gielas, A. M. (2025). Soldier Enhancement through Brain–Computer Interfaces: The Risks of Changing the Human Condition. *The RUSI Journal*, *170*(1), 32-47. https://doi.org/10.1080/03071847.2025.2449894

[27] Harris, W., & Sadok, M. (2023). How do professionals assess security risks in practice? An exploratory study. Security Journal, 1-15. https://doi.org/10.1057/s41284-023-00389-y

[28] Kotb, H. M., Gaber, T., AlJanah, S., Zawbaa, H. M., & Alkhathami, M. (2025). A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats. *Scientific Reports*, *15*(1), 207.

[29] Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. (2021). Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management. *Security Journal*, *35*(2), 600. https://doi.org/10.1057/s41284-021-00292-4

[30] Martin, P. (2023). Insider risk and personnel security: An introduction. Routledge.

[31] Martin, P., & Mercer, S. (2025). *We Need to Talk About the Insider Risk from AI.* We Need to Talk About the Insider Risk from AI | Royal United Services Institute

[32] Mattord, H., Kotwica, K., Whitman, M., & Battaglia, E. (2023). Organizational perspectives on converged security operations. *Information & Computer Security, 2023.* Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-03-2023-0029

[33] McCallum, K. (2025). *Launch of Level 4 Protective Security Qualification* [Video]. You Tube. Launch of Level 4 Protective Security Qualification - YouTube

[34] Mohr, B. J. (2016). Creating High-Performing Organizations: The North American Open Socio-technical Systems Design Approach. In B. Mohr & P. V. Amelsvoort, *Co-Creating Humane and Innovative Organizations*, 16-33, Global STS-D Network Press.

[35] Moneva, A., & Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, *56*(4), 416-440. https://doi.org/10.1177/26338076231161842

[36] Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, 16(4), 317-342. https://doi.org/10.1111/j.1365-2575.2006.00221.x

[37] New Zealand Government (2022). *Capability Maturity Model for Protective Security.* Capability Maturity Model 2022 (protectivesecurity.govt.nz)

[38] National Protective Security Authority (2024). *Changes to Insider Risk Definitions,* NPSA Changes to Insider Risk Definitions | Blog | NPSA

[39] National Protective Security Authority (2023). *Insider Risk Mitigation Framework.* Insider Risk Mitigation Framework | NPSA

[40] Noaks, L., & Wincup, E. (2004). Criminological research: Understanding qualitative methods. Sage.

[41] Phillips, P. J., & Pohl, G. (2025). Industrial espionage: window of opportunity. *Information Security Journal: A Global Perspective*, *34*(2), 143-155.

[42] Pickett, K. S., & Pickett, J. M. (2005). Auditing for Managers. *The Ultimate Risk Management, London.*

[43] Renaud, K., Warkentin, M., Pogrebna, G., & van der Schyff, K. (2024). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. *Information & Management*, *61*(1), 103877 https://doi.org/10.1016/j.im.2023.103877

[44] Sadok, M., Welch, C., & Bednar, P. (2019). A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, *33*, 27-42 https://doi.org/10.1057/s41284-018-00198-2

[45] Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, *28*(3), 467-483. https://doi.org/10.1108/ICS-01-2019-0010

[46] San Miguel, C., & Nelson, C. D. (2007). Key writing challenges of practice-based doctorates. *Journal of English for Academic Purposes*, *6*(1), 71-86. https://doi.org/10.1016/j.jeap.2006.11.007

[47] Sasse, A., & Flechais, I. (2005). 'Usable Security'. In L.F. Cranor and S. Garfinkel, *Security and Usability,* 13-30, O'Reilly.

[48] Schneller, L., Porter, C. N., & Wakefield, A. (2023). Implementing converged security risk management: Drivers, barriers, and facilitators. *Security Journal*, *36*(2), 333-349. https://doi.org/10.1057/s41284-022-00341-6

[49] Schwab, K. (2016). The Fourth Industrial Revolution, Penguin.

[50] Schwab, K. (2018). Shaping the Future of the Fourth Industrial Revolution, Penguin.

[51] Shaw, E., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. *Studies in Intelligence*, *59*(2), 1-8.

[52] Shaw, E. (2023). *The Psychology of Insider Risk*, CRC Press.

[53] Skorich, P., & Manning, M. (2025). *Insider Threat: A Systematic Approach,* Routledge.

[54] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management,* 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[55] Steinmetz, M. (2021). The 'Insider Threat' and the 'Insider Advocate'. In P. Cornish, *The Oxford Handbook of Cyber Security*, 348-357, Oxford University Press.

[56] Stewart, A., & Hobbs, C. (2025). Systematic analysis of security advice on the topic of insider threats. *Computers & Security*, *154*. https://doi.org/10.1016/j.cose.2025.104411

[57] Sutton, D. (2022). *Cyber Security: The complete guide to cyber threats and protection* (2nd ed.), BCS, The Chartered Institute for IT.

[58] Thite, M., & Iyer, R. (2025). Addressing the gap in information security: an HR-centric and AI-driven framework for mitigating insider threats. *Personnel Review*, *54*(3), 935-951. https://doi.org/10.1108/PR-04-2023-0358

[59] Tyson, D. (2007). Security convergence: Managing enterprise security risk. Elsevier.

[60] Wakefield, A. (2021). Security and crime: converging perspectives on a complex world. Sage.

[61] Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, *26*, 107-124.

[62] Walsh, G. (2014). Extra-and intra-organizational drivers of workplace deviance. *The Service Industries Journal*, 34(14), 1134-1153. https://doi.org/10.1080/02642069.2014.939645

[63] Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105. https://doi.org/10.1057/ejis.2009.12

[64] West, R., & Michie, S. (2020). A brief introduction to the COM-B Model of behaviour and the PRIME Theory of motivation [v1]. https://doi.org/10.32388/WW04E6

[65] Whetten, D., Cameron, K., & Woods, M. (2000). *Developing Management Skills for Europe.* Prentice Hall.

[66] Wood, P. (2021). Socio-technical Security: User Behaviour, Profiling and Modelling and Privacy by Design. *Challenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics and Criminal Threats*, 75-91. https://doi.org/10.1007/978-3-030-87166-6_4

[67] Wright, P.C., & Roy, G. (1999). Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, 11(2), 53-59. https://doi.org/10.1108/13665629910260743

[68] Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. *Journal of manufacturing systems*, *61*, 530-535. https://doi.org/10.1016/j.jmsy.2021.10.006