An exploration into organizational practice to address insider risk: A socio-technical perspective

Robert Kennedy

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

Abstract

Insiders can inadvertently or purposefully pose serious threats to organizations by facilitating access to or misuse of proprietary sensitive data. However, technological-centric security solutions have rather limited scope to tackle this problem, with a holistic approach to security potentially providing a better means to address the challenge of preventing and responding to insider threats. In this paper, we explore organizational practices when it comes to security convergence to prevent and address insider risk. The empirical inquiry will involve 12-16 security professionals using semi-structured interviews and conducted from an interpretive stance.

Keywords

Insider threat, socio-technical, converged security, work practice, security professionals

1. Introduction

The harm that the insider threat can potentially provide to organizations is widely recognized [27], however, insider risk is often managed with a technological-centric approach [19]. The current approach to insider risk mitigation would arguably benefit from a socio-technical approach supporting security convergence [29]. Research into insider risk management suggests that in general, organizational approaches lack maturity, often operate within a silo and fail to utilize interdependent business functions efficiently [19].

This short paper aims to present early ideas and receive feedback on research-in-progress designed to emphasize the importance of a better understanding of how security governance and risk management can potentially be enhanced by utilizing a socio-technical system. This will inform practice to enable a converged security approach with the interdependent disciplines of protective security and wider business functions.

The remainder of this paper is organized as follows: the next section presents the background research. Section three summarizes the research method and design and provides details about data collection process and data analysis method. As this is research in progress, key findings, discussion and conclusion are not yet available, however, potential implications in practice have been reviewed.

2. Background

Organizations cannot attain a reasonable level of assurance against security risk unless it considers all of its security risk when developing security strategy and risk mitigation [36]. This holistic approach to protective security is known as security convergence [1, 31] and requires organizations to employ a 'systems thinking' approach to manage security [19]. Security

STPIS'24: The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) August 16-17 2024 Jönköping, Sweden.

Robert Kennedy
Robert.kennedy1@myport.ac.uk (R. Kennedy).
0009-0008-7818-9372 (R. Kennedy)

CEUR Workshop Proceedings (CEUR-WS.org)

convergence is therefore the formal, collaborative and strategic integration of the combined organizational security resources to deliver organizational wide benefits through effective risk mitigation, enhanced operational effectiveness, increased efficiency and financial savings [36]. The converged approach to protective security is viewed by many to provide organizations with a better security risk management approach to enable senior risk owners to make informed decisions whilst also streamlining security teams to enable organizational efficiency [20]. Security convergence is perceived as a contemporary subject amongst both academia and those working within the protective security sector. The risk posed by human activity can be especially dangerous to organizations [39] with insider threat and risk requiring organizations to undertake assessments, risk prioritization and action as opposed to reaction [8]. Insider risk mitigation requires personnel security to mitigate, personnel security being defined by Martin [19] as "the system of protective security measures by which an organization understands and manages insider risk" (2023, p. 12).

2.1 Insider Threat Actors

Whilst three of the four security disciplines; cyber, physical and technical security [19] can be employed by an organization with a combination of security risk management and commercially available products, the same cannot be said for personnel security. Insiders have the potential to inflict harm with a variety of methods [19] and can potentially provide a substantial threat as they possess the knowledge of an organizations vulnerabilities and have the ability to bypass security mitigations due to their legitimate access to organizational assets [6]. Insiders can provide a major threat to organizations [34] with deviant behavior capable of harming an organization via several pathways [38, 11]. A host of factors including malevolent creativity; the deliberate intent to cause harm [9] and unintentional actions have contributed to enabling unauthorized disclosure of sensitive information, process corruption, physical or IT sabotage, the facilitation of third-party access [37] and violent assault [32] including murder. An insider intent on causing harm to an organization can potentially be far more effective than an external threat actor due to insiders having legitimate, sometimes even privileged access to organizational facilities and information, combined with the knowledge they possess regarding organizational vulnerabilities and assets [8]. This is supported by research conducted on security failure identifying that insiders can provide a credible threat to organizations, either intentionally or unintentionally, by enabling third party access or the misuse of sensitive data [28]. As the average cost of an insider event has been estimated to be $11.45 million [27], this should be a concern to organizations. However, examples of insider events continue to surface across the globe and include; the former head of the Swiss bank Raiffeisen profiting from illicit deals, a former Chinese based employee of a Dutch semiconductor manufacturer stealing confidential information regarding chip-making machinery, an Arctic University of Norway researcher arrested for being a Russian spy [19], and a disgruntled EnerVest employee sabotaging infrastructure [27]. Such breaches amplify the risk to organizations due to the lack of, or even absence of detection, a slow response to insider activity if detected, and inconsistent remediation measures [14]. Early detection requires vigilance by organizations to identify when signs of potential disgruntlement arise within individuals to act early and prevent the said individual from progressing down a critical pathway to become an insider [32].

2.2 Security Risk Exposure

The importance of managing risk exposure is critical to enabling organizational security, business continuity and resilience [16] with security risk being both dynamic and adaptive [19]. The disparity between the volume of threat information regarding external actors, currently outweighs the available data regarding insider events [8], which could conceivably hinder commensurate security risk management. Many organizations focus on external threats and overlook the threat posed by the insider [6] which could potentially impact their exposure to risk. The use of quantitative risk methodology developed and used for managing project or insurance risks is often misapplied to manage security risk. Security risks differ significantly from other risks, as security risk is a combination of threat, vulnerability and impact, quantitative tools used to manage risk in other contexts may not always work for security [19]. Risk is also often perceived subjectively and shaped by the individual's experience and political, social, and cultural factors [16] with insider risk mitigation, often relying on protection provided by potential threats, the insiders themselves [6]. Ideally, the risk assessment process should be undertaken with a systematical approach involving multiple stakeholders from each business unit within an organization [16]. This is supported by the doctrine that protective security should be managed holistically as opposed to individually, with a converged approach recognizing the interdependencies within the security disciplines [19] of cyber, personnel, physical and technical security. Such interdependencies would also include wider business functions, for example Human Resources (HR). Wright and Roy [41] argue that with regards to industrial espionage, the key to the problem is people, i.e. insiders, and therefore the HR manager has a significant role to play with regards to insider risk management and should ideally understand the security requirements of the organization to enable appropriate security messaging etc.

2.3 Security Governance

Security governance is the combined efforts of multiple stakeholders to ensure the delivery of effective security through organizational hierarchies and networks [37]. Leadership is required to provide executive commitment and oversight [23] to support and underpin the governance process. However, a governance structure that has each security discipline reporting to a Chief Security Officer (CSO) would not necessarily provide a converged security governance function. Without an understanding of the interdependence of different business risks, an organization is conceivably operating an inefficient governance model [1] which may not provide an accurate single overview of risk [31]. Whilst the CSO should ensure that executive leadership, governance groups and senior management contribute towards protective security discussion and define responsibilities to discharge actions [23], this should ideally be part of a wider enterprise risk management approach [31]. Sadok et al [28] argue that a top-down approach to managerial instruction, and the development of policy and process without the integration of all security functions and active engagement with stakeholders, may encourage employees to work around security compliance and potentially circumvent security measures altogether. The design of security should therefore not only consider the integration of the interdependent security functions [19], but also consider the context of the work role from each employee and stakeholder when designing security [28], which would include policy and process to mitigate the insider risk in practice.

2.4 The socio-technical approach to mitigate insider risk.

Criticism of insider risk mitigation methods has included that this tends to be technological-centric [19], with Steinmetz [35] arguing that a technological approach alone is not effective. Sadok et al. [29] argue that a socio-technical approach is required as technology-centered solutions, without the inclusion of people and processes, induces flaws within potential security solutions. The United Kingdom National Protective Security Authority (NPSA) encourage the combination of social, physical and technical mitigations within their Insider Risk Mitigation Framework [24], with NPSA advocating the use of 'the critical path' approach. The critical-path approach identifies four factors that contribute to insider risk, those being personal predispositions, stressors, concerning behaviors and problematic organizational response [32]. The critical-path elements have been applied by NPSA to the case study involving David Smith, who was imprisoned for spying on behalf of a hostile state [25]. The four elements of the critical-path approach employing a combination of social, physical and technical security measures would potentially benefit from employing 'Work Systems Theory' to develop a system employing a socio-technical approach [29] The development and use of a socio-technical system is supported by Fischer and Herrmann [12] who argue that technology alone does not impact social structures or human behavior positively. As a socio-technical system would enable a security design incorporating human, social, organizational and technical factors [3, 10] this could potentially bridge the security disciplines by identifying, acknowledging and capitalizing on the interdependencies between each security function, it could conceivably be argued that a converged security approach would better support the management of insider risk [19]. Of course, any security design is challenging to embed within an organization as the balance between security and usability needs to be contextualized to the organization's everyday practices [28]. This would require democracy, which is a fundamental socio-technical value, with employees encouraged to collaborate in security design [22] to better support usability.

Good personnel security requires organizations to move forwards towards being a high trust organization with a healthy security culture [19]. Organizations that can create a sense of confidence within their workforce, rather than individuals being on-guard and suspecting potential mistreatment, with employees confident that the management and organization are honorable, often perform better that those that do not [40]. High levels of mutual trust within organizations and their stakeholders are generally successful organizations in many ways and they also tend to demonstrate less insider risk [19]. This is possibly because engaged and motivated staff that demonstrate ownership of their organization's objectives are also more likely to support the protection of organizational interests through commensurate security measures [28]. The benefits of a socio-technical systems design can support organizations to become highperforming [21], with a high performing work system defined as an organization operating at levels of excellence far beyond other comparable organizations [5].

3. Research design

The study undertaken is an exploratory study, conducted from an interpretive stance. This means that it aims to shed light on actual, experienced practices within a sample of public and private sector organizations. This study will therefore not uncover any statistically significant, or indeed generalizable conclusions.

The purpose of this qualitative study is to understand the barriers and enablers to embed personnel security to manage the insider risk within organizations. Using semi-structured interviews involving security professionals to gather qualitative data, this study will explore the challenges organizations face to embed effective personnel security and explore the potential contribution that converged security could provide to mitigate risk.

Noaks & Wincup [26] argue that some aspects of criminological enquiry are challenging to investigate using quantitative methods citing insider activity in the form of 'white-collar' crime as one such relevant example. To enable the concept of Max Weber's 'Verstehen', the ontological approach of constructionism and the epistemological interpretivist stance will be used to gain such understanding [7, 2]. Qualitative research is therefore appropriate and is underpinned by philosophy to inform the research questions, research objectives and hypothesis developed. This will be conducted using semi-structured interviewing to collect data. The interviews will be scheduled at convenience, last no longer than one hour and be conducted online with the aim to encourage spontaneous interactions between the interviewer and participants [17]. This study therefore aims to use semi-structured interviews to discover through dialogue, discussion and interactions the tacit knowledge that security professionals possess to support the production of Mode 2 knowledge [15, 30, 13].

The study aims to research the below 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.

This study also aims to explore the below hypotheses:
H1- Insider risk is not well-considered or widely integrated into security risk management.
H2- Security convergence can support the prevention of insider activity.
H3- A disjoint between policy, process and usability hinders effective security mitigations. H4- Current insider activity detection is reactive not pro-active.
H5- Technological-centric solutions to manage insider risk are limited.
H6- Effective leadership and governance are necessary to mitigate insider risk.
H7- Organizational culture has a direct impact on personnel security.

The semi-structured interview themes detailed below will be used during the interviews:

1) In your experience how well do organizations in general manage the risk posed by insiders?
2) What do you think the barriers are to embedding effective personnel security into organizations?
3) How does leadership and governance contribute to effective personnel security?
4) How can other non-security functions of a business impact personnel security?
5) How effective are technological-centric only risk mitigations?
6) What do you believe is required for organizations to become a high-trust organization? 7) What blocks organizations from becoming a high-trust organization?
8) What do you envisage to be the future challenges organizations will face regarding personnel security?
9) How will emerging technology such as artificial intelligence impact personnel security?
10) How would you envisage security convergence supporting personnel security?

A snowball sampling technique will be used to recruit interview participants. Initial recruitment will involve contacting individuals within the researcher's professional network; however, this will not include individuals from the researcher's own organization. Participants from government agencies that require organizational permissions, e.g. law enforcement, will not be approached. Individuals from both public and private organizations will be invited to participate in this study. This qualitative research study will require interaction with individuals as it is the perspective of the participant regarding the topic of research that the researcher will endeavor to research [4]. Participants will be included in the research should they work within the security sector to include those within interdependent business functions regarding the management of insider risk, such as Human Resources. Participants will be excluded if they do not work within the security sector or within an interdependent business function. The researcher's ability to be flexible with the sample size may be appropriate should; the semistructured interviews identify new factors which are deemed to require further data collection, the researcher initially focuses on a small sample then use the wider sample to test emerging generalizations, or alternatively, unexpected generalizations identified during the data analysis phase leads the researcher to seek out new participants [33].

The initial identification of research participants includes a number of UK security professionals that span both the public and private sectors. This includes security leaders and consultants specializing in personnel security that support multiple clients, along with a personnel security leader working in the private sector managing insider risk within a critical infrastructure sector. The participants are relevant to this research as they have a vast amount of experience regarding the mitigation of insider risk across the national security arena and both the public and private sectors. The combined tacit knowledge and experience from the participants is expected to provide high-value qualitative data to inform this study.

4. Potential Implications in Practice

The researcher's motivation for undertaking a Professional Doctorate has been borne out of frustration with the current culture of addressing protective security with a siloed approach. This siloed approach enables threat actors to exploit the vulnerabilities provided within the gaps that exist between cyber, personnel, physical and technical security and also fails to provide a single overview of security risk to enable organizational senior risk owners to effectively manage risk. Without a converged approach to protective security organizations cannot expect to effectively mitigate converged threat vectors. Personnel security is arguably the most difficult of the protective security disciplines to embed within organizations, and therefore provides the biggest challenge for organizations to adopt a converged approach. At a time when contributing factors within society have provided a perfect storm for insider events, with some high-profile cases reported within the UK media, and potentially many more that go undetected, organizations need to consider the risk posed by insiders as part of any security strategy.

This study aims to raise awareness and understanding of this problem with a view to identifying a potential strategy to enable organizations to work towards a converged security approach incorporating the four disciplines of protective security within an interdependent model. The participants within this study will provide a wealth of data gained from their combined knowledge amassed throughout their careers working within the protective security sector. The findings from this study will hopefully contribute to the creation of new knowledge to drive change to encourage organizations to review their current security strategy and consider moving from a siloed approach to a converged approach. This study will also support the researcher's ambition to contribute to the body of knowledge to support and shape the future of protective security strategies.

The researcher is currently developing a 'Protective Security Adviser' qualification [18] with UK stakeholders that includes academia, public and private sector organizations. This training qualification aims to; educate delegates to the benefits of security convergence, provide delegates with a base level of competence across the four disciplines of security, provide a pathway for delegates to progress onto academic qualifications, and standardize the approach to protective security within the UK. This qualification also aims to boost social mobility, and as such, provide a positive impact to equality, diversity and inclusion to enable organizations to recruit and retain a workforce providing diversity of thought to enhance organizational capability to mitigate risk. The qualification is very much a 'ground-up' approach to influence the sector and provide future leaders within the security sector that are equipped with the appropriate knowledge, skills and behaviors to support a converged approach to protective security. The identified 'ground-up' approach will be supported by this academic study and the future research conducted as part of the researchers Professional Doctorate to enable a 'top-down' approach to drive change moving forwards towards security convergence underpinned by academic evidence.

References

[1] 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

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

[3] 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

[4] Bazeley, P. (2013). Qualitative Data Analysis: Practical Strategies, Sage.

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

[6] 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.

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

[8] 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

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

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

[11] 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

[12] 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

[13] 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

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

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

[16] 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 [17] James, N., & Busher, H. (2016). Online Interviewing. In D. Silverman (Ed). *Qualitative Research (4th ed., pp-245-260).* Sage.

[18] Kennedy, R. (2023, September 28). *Level 4 protective security apprenticeship brings a converged approach.* City Security Magazine. Level 4 protective security apprenticeship brings a converged approach - City Security Magazine

[19] Martin, P. (2023). Insider risk and personnel security: An introduction. Taylor & Francis. [20] 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

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

[22] 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

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

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

[25] National Protective Security Authority (2023). *If you have people, you have an Insider Risk: A David Smith case study.* If you have people, you have an Insider Risk: A David Smith case study | NPSA

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

[27] 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

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

[29] 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

[30] 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

[31] 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

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

[33] Silverman, D. (2011). *Interpreting Qualitative Data* (4th ed.), Sage.

[34] 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

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

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

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

[38] 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

[39] 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.

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

[41] 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.