Mitigating Insider Threats in Cybersecurity: A Design Thinking Approach

Emmanuel Anti[1], Rebekah Rousi [2,]

[1] *University of Vaasa, Wolffintie 34 65200, Vaasa, Finland*
[2] *University of Vaasa, Wolffintie 34 65200, Vaasa, Finland*

Abstract

Insider threats in cybersecurity (ITC) are increasing in frequency and impact, while current technical, psychological, and organizational approaches remain insufficient. These strategies often address narrow aspects, such as system vulnerabilities or individual behavior, without offering a holistic, multidisciplinary solution. This study presents DESTIC, a design thinking (DT) framework to study insider threats. Unlike existing research emphasizing only the "Empathize" phase, DESTIC engages all six DT stages: empathize, define, ideate, prototype, test, and implement to uncover root causes and develop targeted interventions. We apply organizational design workshops, a methodology that combines diverse stakeholders to co-create solutions by examining behavioral, technical, and organizational factors. This study offers a structured, human-centered approach to understanding and proactively preventing insider threats through iterative, collaborative cybersecurity innovation.

Keywords
Design thinking; insider threats; human-centered design; cybersecurity; framework

1. Introduction

Insider threats in cybersecurity are becoming more frequent and expensive, with malicious insider attacks now accounting for 7% of incidents and averaging USD 4.99 million in damages [1]. Unlike external threats, insiders are trusted personnel with legitimate access, making their actions, whether intentional or accidental, particularly harmful and harder to detect [2], [3]. From 2019 to 2024, insider attacks rose from 66% to 76%, with financial gain as the top motivation, increasing from 60% to 74% [4]. These threats can take various forms, including sabotage, data theft, unauthorized sharing, and policy violations, often remaining undetected for an average of 308 days [1].

Insider threats can lead to financial losses, legal consequences, reputational harm, and internal distrust, damaging both an organization's external standing and internal culture [5], [6], [7], [8], [9]. Despite traditional security measures like access controls, monitoring, and awareness training, insider threats persist due to organizational culture, evolving threat dynamics, and complex human motivations [10], [11]. These gaps call for more adaptive, human-focused strategies.

This study proposes applying human-centered design (HCD), specifically design thinking (DT), to insider threat mitigation. In Information Systems, systems thinking – "a system of thinking about systems" [94] – has been a popular paradigm for studying threats [12], [13], [14]. However, rather than focusing on the systems per se, DT centers on human behavior, needs, and motivations through a transdisciplinary, empathy-driven, and creative approach [15],[16],[17], that not only accounts for systems or actor networks, but also thought processes within these dynamic relations. DT offers a psychologically grounded, multidisciplinary approach to understanding the human factors that drive insider actions and to designing responses accordingly [18].

TKTP 2025: Annual Doctoral Symposium of Computer Science, 2.-3.6.2025 Helsinki, Finland

emmanuel.anti@uwasa.fi (E. Anti); rebekah.rousi@uwasa.fi (R. Rousi)
0009-0007-3802-4875 (E. Anti); 0000-0001-5771-3528 (R. Rousi)

The guiding question is: How can design thinking be applied to develop effective, proactive strategies to prevent insider threats while offering a deeper understanding of prior cases? This study explores DT's potential to map insider agents' emotional and cognitive dimensions and introduces the DESTIC framework—a human-centered model integrating psychological, social, and environmental insights to develop actionable, adaptive strategies to prevent insider threats.

2. Literature Review

Research in insider threats has spanned technological, psychological, and organizational domains, yet these threats remain a persistent concern for organizations. Despite extensive efforts by governments, academics, and research institutions, much of the existing research is anecdotal or based on limited data, resulting in fragmented mitigation strategies [11]. Tools supported by generative AI, such as personas, depend heavily on the quality of user data and research inputs [19], [20]. Consequently, insider threat mitigation remains split between purely technical approaches and broader socio-technical methods [21], [22], [23], [24].

2.1. Technical Approaches

Technical approaches focus on policies, system specifications, and controls to detect or prevent insider activity [11]. These include user activity monitoring, intrusion detection systems (IDS), and VPN analysis [25], [26]. For example, Wasko et al. [27] used reality games to simulate insider threats and observed increased deviant behavior in controlled environments. Emerging methods like deep learning enhance detection by analyzing large datasets for subtle behavioral changes [28]. However, these models face limited labeled data, difficulty detecting adaptive behavior, and distinguishing malicious from accidental threats [28], [29].

2.2. Socio-Technical Approaches

Socio-technical strategies integrate human and technical elements, combining rules, training, behavioral monitoring, and organizational culture assessment [10], [30]. Anomaly detection and machine learning help build dynamic user profiles [19]. Despite these strengths, limitations include high implementation costs, difficulty addressing individual motivations, and challenges distinguishing between different types of insider threats [10], [29]. Human-based attacks like social engineering can also bypass technological defenses, as technological solutions cannot fully address the social dimension of insider threats [31].

2.3. Social, Psychological, and Organizational Approaches

These approaches examine the social and psychological drivers of insider behavior, such as personal stress, entitlement, or workplace dissatisfaction [7], [32]. Theories such as deterrence and rational choice have been applied to understand the factors contributing to insider threats [33], [34], [35], [36], [37]. However, these methods can be resource-intensive, assume uniform employee responses, and may fail without strong managerial enforcement [37], [38]. Their subjective nature can also lead to bias or misinterpretation, and they may miss threats posed by unintentional actors or those outside typical profiles [32], [37]. These approaches offer insight into human and organizational factors but are often ineffective without technical support.

2.4. Previous research on Design Thinking in Cybersecurity

While systems thinking is well-established in cybersecurity, design thinking (DT) remains underutilized. Some researchers, however, have begun to apply DT in this space. For example,

Dorasamy et al. [39] used DT to address IoT-related cybersecurity issues among youths, generating insights, solutions, a prototype, and feedback. Snow et al. [40] applied DT and behavioral theory to identify key smart grid threats through expert workshops, drawing on Nykodym et al.'s [41] insider threat profiles and Fogg's [42] behavior model. Tseng et al. [43] developed a cybersecurity board game using DT to enhance student awareness in education. Ashenden et al. [44] used DT to design cyber deception tools, producing journey maps that visualized tactics and guided evaluation discussions.

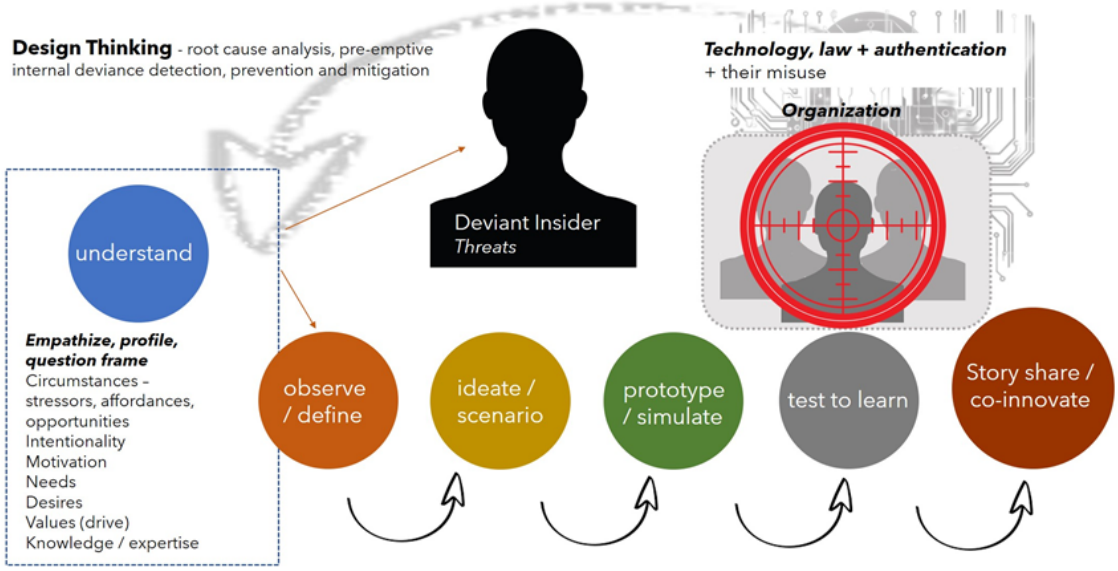

Fig. 1. Design Thinking for ITC framework – DESTIC – the framework offers an order of process from developing an intial understanding of the situation (Understand stage) to observing and defining, ideating and scenario-building, prototyping and simulating, testing and learning, then the official outward communication stage of story sharing and further co-innovation. The process can be implemented in iterative cycles, and the objective is to use each stage with its increasing fidelity as a means of generating more detailed strategic insight on what is happening and can happen, where, and how it can be addressed.

2.5. Design Thinking - From Forensics to Process

In cybersecurity, digital and traditional forensic methods, including psychological profiling, are widely applied [5], [6], [7]. Nevertheless, digital forensics faces challenges such as big data, tool diversity, encryption, legal complexities, and shortages of skilled professionals [48]. As socio-technical systems grow more complex, managing insider threats demands interdisciplinary expertise. No single individual can address all aspects of socio-technical deviance, underscoring the need for multi-professional collaboration. We propose DT as a structured, transdisciplinary approach to address this. Developed by John E. Arnold at Stanford to reduce bias and foster creativity across disciplines [49],[8], [9], [10], DT has evolved through contributions from Dreyfuss, Maslow, Kahn, and Guilford, emphasizing collaboration and tool-based exploration [16], [53], [54]. Grounded in empathy, it isolates creativity blocks that may serve as deviant trajectories, like stress and fear of failure, through iterative, human-focused methods [50], [55]. This study introduces DESTIC (Figure 1), an adapted six-step DT framework for insider threat mitigation in ITCs, enabling root cause analysis and proactive prevention [58].

2.5.1. Understand

To identify the "what" of insider threats, a systematic review by Anti & Vartiainen [59] identifies ten types of insider deviant behaviors, including computer abuse, fraud, IS misuse, policy violations, shadow IT, unauthorized disclosure, and access breaches. However, recognizing these behaviors is only the first step. Understanding insider threats also requires examining individual motivations and external factors such as stressors, technological affordances, and situational opportunities.

Organizations must assess human factors such as values, beliefs, expertise, and cultural health [59]. Insider risk may also arise from underutilized or disengaged employees who feel undervalued or bored, increasing the likelihood of deviant behavior [60], [61].

2.5.2. Observe/ Define

The observing and defining stage involves analyzing organizational and individual behaviors to uncover factors contributing to insider deviance. Key organizational factors include culture [11], [12], [13], formal and informal controls [65],[66],[67], fairness and justice [68],[69],[70], clear policy enforcement [68], [69], [71], and organizational citizenship [72]. From a psychological perspective, it is essential to assess stress triggers [65], [73], sense of responsibility [74], [75], boundary management [76], [77], and goal framing [78], [79]. Additionally, socio-cultural influences—such as social bonds, cultural norms, and controls [63], [68], [75]—and emotional coping behaviors [59] should be mapped to identify the root causes of deviance.

2.5.3. Ideate / Scenario

In the ideation phase, the investigator(s) – team, strategists – endeavor to list different ideas of matters that can go wrong from an internal information security perspective and map relationships between these ideas and various factors. Ideally, the team will reach a stage where they create storyboards or 'scenarios' depicting how individuals, their environments, and socio-technical conditions may lead to deviant behavior and potential risk. This process stage involves divergent creative thinking, when the team can generate as many ideas as possible that do not necessarily need to be entirely credible, possible, or feasible [14]. The main aim is to gather a spectrum of ideas from the highly likely to the highly unlikely (as yet), which can form the basis of ascertaining the current state-of-the-art in internal socio-technical deviance and may also prepare the team for future roadmapping.

2.5.4. Prototype / Simulate

The prototype or simulation stage involves simulation or enactment – i.e., testing the systems and qualified individuals (i.e., recruiting individuals with technical and cybersecurity expertise) to understand how these high-level ideas and scenarios may unfold in practice. The prototyping phase provides an actionable communication platform for testing and learning [15]. Prototyping is not simply a mode of actualizing ideas and plans in concrete form, but is an extension of cognition itself [16], [17]. We may see that through producing prototypes and simulations, practitioners can further understand the motives, materials, and possibilities of deviant insiders (i.e., via simulation-enabled shared cognition, see [18], [19]). The aim is to cause as much damage as possible in a safe and controlled way. The prototype or simulation should be developed to a standard that allows the development team and bystanders (i.e., stakeholders) to envision realistically how the behavior and its causalities can be realized in practice.

2.5.5. Test to Learn

Testing comes into play with other expert and non-expert communities. Other experts can pinpoint the precision and likelihood of particular scenarios. They can also highlight unaccounted-for challenges while critiquing vulnerabilities within the present simulations. On the other hand, non-experts may highlight blind spots inherent to expertise – i.e., a fixation on specific details - while people with expertise in other fields and experiences may notice other details. The non-expert community is also valuable from an educational perspective. The learning they undergo while witnessing the unfolding of information security breaches will undoubtedly be enlightening in shaping their behavior. This learning will have additional social benefits in that insight may be shared with colleagues after the simulation experiences (i.e., social learning [20].

2.5.6. Story Share / Co-Innovate

At this stage, learning and innovation intersect. When teams and stakeholders engage in both the DT process and testing, they gain shared insight into insider threats and the environments that enable them, enabling co-innovation [17], [87]. Scenarios and mock-ups serve as reference points for focused, convergent ideation, bringing together DT findings in a meaningful way. The resulting design solution is only part of the outcome. Equally important is communicating its root causes: what problems it addresses and how. Storytelling plays a critical role in this meaning-making process, helping translate complex findings into accessible narratives for non-experts [88]. It raises awareness of how insider threats emerge and how socio-technical systems can address them, fostering broader engagement in cybersecurity practices.

For these solutions to have a lasting impact, they must support co-innovation and contribute to culture generation within organizations [89].

3. Proposed Methodology

This study will adopt a qualitative, exploratory methodology using organizational design workshops to investigate insider threats through a human-centered DT lens. Design workshops are particularly suited for socio-technical IS research and development, offering a collaborative space to engage diverse stakeholders in structured problem-solving while serving as a focus group to identify concerns, vulnerabilities, and structural challenges [90], [91]. These workshops enable the application of DT tools, such as empathy mapping, journey mapping, and root cause analysis, to surface the complex behavioral and organizational dynamics underlying insider threats.

The study will be implemented in three main phases over twelve months. After the initial planning, preparation, and recruitment phase that includes the development of the workshop materials and protocols based on the proposed framework (DESTIC) and established DT practices, piloting the design, and securing partnerships with four organizations in high-risk sectors such as finance, healthcare, or public institutions in Finland, the process will launch into the exploratory phase. A multidisciplinary group of participants of five to ten individuals (Cybersecurity experts, IT professionals, managers, HR personnel, general employees, cognitive psychologists, and behavioral experts) from the partner organizations and specialist organizations will be recruited. This multi-professional group will help generate rich, contextual insights aligning with IS research goals of theory-building, system design, and actionable socio-technical innovation [93].

The second phase is expected to take five months, during which one intensive design workshop lasting a full day will be organized for each organization. Each session will consist of iterative ideation, prototyping, feedback, and refinement sprints. Participants will engage with DT tools, such as empathy mapping, journey mapping, root cause analysis, and persona building, to explore and reframe the complex behavioral and organizational dynamics underlying insider threats. Focus groups and forensic-style inquiry sessions will further deepen understanding of behaviors, motivations, and systemic vulnerabilities. The iterative format will enable rapid testing and idea evolution within each session, creating space for participants to refine interventions in response to group feedback and emergent insights. All sessions will be documented through recordings, field notes, and workshop artifacts such as sketches, models, and system maps.

Thematic and qualitative profiling will be applied to analyze the data, a process that will take three months. Triangulation across roles, organizations, and data types will support the development of grounded theories and practical models for managing insider threats. The iterative workshop design ensures that emerging findings are collaboratively shaped and refined in real time, thereby strengthening their relevance and applicability. A socio-technical map of possible solutions that adequately address root causes and threat networks will be a key deliverable from this phase.

3.1. Feasibility

The study is designed to be practical and feasible, and to directly contribute to scientific advancement and to applicable socio-technical solutions (key technologies, guidelines, protocols, etc.). It requires the modest resources of a facilitation team (two to three members), basic materials (sticky notes, markers, whiteboards, or large flip charts), and reasonable logistical support from partner organizations. This support includes providing a physical or virtual space for the workshop, allocating employee time to participate (one full day), and granting access to relevant contextual information, such as organizational policies, workflows, or anonymized incident data, to inform the design work. The most challenging component could be allocating employee time. Nevertheless, several solutions may be found to aid this challenge, such as utilizing the process for *professional development* and even team-building. Most pertinent is calculating the return on investment for potential savings of internal deviance incidents versus the costs of engaging several staff members in intensive research and development. This is essential for meaningful participation and scientifically and professionally grounded results.

4. Expected Contributions and Conclusions

This paper deliberates how Design Thinking (DT) can be applied in cybersecurity to proactively design, mitigate, and prevent insider threats. By leveraging DT's human-centered, multidisciplinary structure, we propose a framework (DESTIC) to address insider socio-technical deviance through convergent and divergent creativity, including the underexplored domain of deviant creativity. Our adapted "understand" phase synthesizes behavioral and motivational theories to uncover the conditions that enable insider threats, building on prior DT applications in cybersecurity [39], [43], [44]. We argue that DT's iterative, transdisciplinary collaborative process is uniquely positioned to anticipate future insider threats and co-create preventive solutions with diverse stakeholders. Additionally, we highlight the crucial interplay of technology, law, and authentication, particularly as emerging technologies outpace legal frameworks. DT can assist not only in identifying vulnerabilities but also in shaping adaptive legal and regulatory responses. Ultimately, we position DT as a diagnostic and generative tool for advancing anti-threat innovation in cybersecurity.

Declaration on Generative AI

The author(s) used Grammarly for grammar and spelling checks, followed by manual review and editing. They take full responsibility for the final content.

References

[1] IBM and Ponemon Institute, "Cost of a Data Breach Report 2024," 2024. Accessed: Sep. 17, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[2] M. Bishop and C. Gates, "Defining the insider threat," in Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, 2008, pp. 1–3.

[3] C. Colwill, "Human factors in information security: The insider threat–Who can you trust these days?," Information security technical report, vol. 14, no. 4, pp. 186–196, 2009.

[4] Cybersecurity Insiders, "Insider Threat Report Trends, Challenges, and Solution," 2024. Accessed: Feb. 23, 2024. [Online]. Available: www.securonix.com

[5] J. R. Nurse et al., "Understanding insider threat: A framework for characterising attacks," in 2014 IEEE security and privacy workshops, IEEE, 2014, pp. 214–228.

[6] S. Duggineni, "Impact of controls on data integrity and information systems," Science and Technology, vol. 13, no. 2, pp. 29–35, 2023.

[7] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data breach management: An integrated risk model," Information & Management, vol. 58, no. 1, p. 103392, 2021.

[8] J. D'Arcy, I. Adjerid, C. M. Angst, and A. Glavas, "Too good to be true: Firm social performance and the risk of data breach," Information Systems Research, vol. 31, no. 4, pp. 1200–1223, 2020.

[9] A. H. Juma'h and Y. Alnsour, "The effect of data breaches on company performance," International Journal of Accounting & Information Management, vol. 28, no. 2, pp. 275–301, 2020.
[10] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," Electronics, vol. 9, no. 9, p. 1460, 2020.
[11] J. Hunker and C. W. Probst, "Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, vol. 2, no. 1, pp. 4–27, 2011.
[12] H. M. Salim, "Cyber safety: A systems thinking and systems theory approach to managing cyber security risks," PhD Thesis, Massachusetts Institute of Technology, 2014.
[13] E. Zoto, M. Kianpour, S. J. Kowalski, and E. A. Lopez-Rojas, "A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education," Complex Systems Informatics and Modeling Quarterly, no. 18, pp. 65–75, 2019.
[14] W. Young and N. Leveson, "Systems thinking for safety and security," in Proceedings of the 29th annual computer security applications conference, 2013, pp. 1–8.
[15] D. Norman, The design of everyday things: Revised and expanded edition. Basic books, 2013.
[16] T. Brown, "Change by design: How design thinking creates new alternatives for business and society," Collins Business, 2009.
[17] J. Liedtka, "Why design thinking works," Harvard Business Review, vol. 96, no. 5, pp. 72–79, 2018.
[18] N. Liang, D. P. Biros, and A. Luse, "An empirical validation of malicious insider characteristics," Journal of Management Information Systems, vol. 33, no. 2, pp. 361–392, 2016.
[19] E. Kim, J. Yoon, J. Kwon, T. Liaw, and A. M. Agogino, "From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity," in Proceedings of the Design Society: International Conference on Engineering Design, Cambridge University Press, 2019, pp. 1773–1782.
[20] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," Computers & security, vol. 70, pp. 663–674, 2017.
[21] R. A. Alsowail and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," Electronics, vol. 10, no. 9, p. 1005, 2021.
[22] R. A. Alsowail and T. Al-Shehari, "Empirical detection techniques of insider threat incidents," IEEE Access, vol. 8, pp. 78385–78402, 2020.
[23] D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, 2012.
[24] M. Jeong and H. Zo, "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques," Telematics and Informatics, vol. 63, p. 101670, 2021.
[25] M. Mohammadi et al., "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," Journal of Network and Computer Applications, vol. 178, p. 102983, 2021.
[26] N. Elmrabit, S.-H. Yang, and L. Yang, "Insider threats in information security categories and approaches," in 2015 21st International Conference on Automation and Computing (ICAC), IEEE, 2015, pp. 1–6.
[27] S. Wasko et al., "Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods," Computers & Security, vol. 107, p. 102314, 2021.
[28] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, vol. 104, p. 102221, 2021.
[29] A. Akhunzada et al., "Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions," Journal of Network and Computer Applications, vol. 48, pp. 44–57, 2015.
[30] E. Mumford, "A socio-technical approach to systems design," Requirements engineering, vol. 5, pp. 125–133, 2000.
[31] N. Elmrabit, "A multiple-perspective approach for insider-threat risk prediction in cyber-security.," PhD Thesis, Loughborough University, 2018.
[32] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," ACM Computing Surveys (CSUR), vol. 52, no. 2, pp. 1–40, 2019.
[33] J. P. Gibbs, "Crime, punishment, and deterrence," The Southwestern Social Science Quarterly, pp. 515–530, 1968.
[34] J. J. van Dijk, "Understanding crime rates: On the interactions between the rational choices of victims and offenders," The British Journal of Criminology, vol. 34, no. 2, pp. 105–121, 1994.
[35] R. M. Hogarth and M. W. Reder, Rational choice: The contrast between economics and psychology. University of Chicago Press, 1987.

[36] E. D. Shaw, "The role of behavioral research and profiling in malicious cyber insider investigations," Digital investigation, vol. 3, no. 1, pp. 20–31, 2006.
[37] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," Journal of information security and applications, vol. 40, pp. 247–257, 2018.
[38] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?," Journal of Management Information Systems, vol. 29, no. 3, pp. 157–188, 2012.
[39] M. Dorasamy, G. C. Joanis, L. W. Jiun, M. Jambulingam, R. Samsudin, and N. J. Cheng, "Cybersecurity issues among working youths in an IOT environment: A design thinking process for solution," in 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, 2019, pp. 1–6.
[40] S. Snow, J. Happa, N. Horrocks, and M. Glencross, "Using design thinking to understand cyber-attack surfaces of future smart grids," Frontiers in Energy Research, vol. 8, p. 591999, 2020.
[41] N. Nykodym, R. Taylor, and J. Vilela, "Criminal profiling and insider cyber-crime," Computer Law & Security Review, vol. 21, no. 5, pp. 408–414, 2005.
[42] B. J. Fogg, "A behavior model for persuasive design," in Proceedings of the 4th international Conference on Persuasive Technology, 2009, pp. 1–7.
[43] S.-S. Tseng, T.-Y. Yang, Y.-J. Wang, and A.-C. Lu, "Designing a cybersecurity board game based on Design Thinking Approach," in Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 12th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2018), Springer, 2019, pp. 642–650.
[44] D. Ashenden, R. Black, I. Reid, and S. Henderson, "Design thinking for cyber deception," Proceedings of the 54th Hawaii International Conference on System Sciences | 2021., 2021, [Online]. Available: http://hdl.handle.net/10125/70853
[45] E. Casey, Handbook of digital forensics and investigation. Academic Press, 2009.
[46] M. Pollitt, "A history of digital forensics," in Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers 6, Springer, 2010, pp. 3–15.
[47] A. Årnes, Digital forensics. John Wiley & Sons, 2017.
[48] N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics," Journal of forensic sciences, vol. 60, no. 4, pp. 885–893, 2015.
[49] V. P. Seidel and S. K. Fixson, "Adopting design thinking in novice multidisciplinary teams: The application and limits of design methods and reflexive practices," Journal of Product Innovation Management, vol. 30, pp. 19–33, 2013.
[50] J. Auernhammer and B. Roth, "The origin and evolution of Stanford University's design thinking: From product design to design thinking in innovation management," Journal of Product innovation management, vol. 38, no. 6, pp. 623–644, 2021.
[51] R. F. Dam, "The 5 Stages in the Design Thinking Process |." 2024. Accessed: Jan. 01, 2024. [Online]. Available: https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process?srsltid=AfmBOopucCptPkYIIiO9iIrS_8eBUdDXuhDPdopXA24dZL1b4rOpAeLL
[52] U. Johansson-Sköldberg, J. Woodilla, and M. Çetinkaya, "Design thinking: Past, present and possible futures," Creativity and innovation management, vol. 22, no. 2, pp. 121–146, 2013.
[53] K. Dorst, "The core of 'design thinking'and its application," Design studies, vol. 32, no. 6, pp. 521–532, 2011.
[54] T. Kelley, The art of innovation: Lessons in creativity from IDEO, America's leading design firm, vol. 10. Currency, 2001.
[55] A. Dix, "What are Creative Blocks? Interaction Design Foundation." 2016. Accessed: Sep. 23, 2024. [Online]. Available: https://www.interaction-design.org/literature/topics/creative-block
[56] IDEO, "The Design Thinking Process (6 Helpful Steps) –." Accessed: Oct. 01, 2024. [Online]. Available: https://www.ideou.com/blogs/inspiration/design-thinking-process
[57] S. Gibbons, "Design Thinking 101." 2016. Accessed: Sep. 26, 2024. [Online]. Available: https://www.nngroup.com/articles/design-thinking/
[58] N. Hellesen, H. Torres, and G. Wangen, "Empirical case studies of the root-cause analysis method in information security," International Journal on Advances in Security, vol. 11, 2018.
[59] E. Anti and T. Vartiainen, "Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review," Association for Information Systems, 2024.

[60] D. Livingstone, "Skill underutilization," in The Oxford handbook of skills and training, Oxford University Press Oxford, 2017, pp. 281–300.
[61] T. A. Sullivan, Marginal workers, marginal jobs: underutilization in the United States labor force. The University of Chicago, 1975.
[62] D. Box and D. Pottas, "A model for information security compliant behaviour in the healthcare context," Procedia Technology, vol. 16, pp. 1462–1470, 2014.
[63] L. Y. Connolly, M. Lang, J. Gathegi, and D. J. Tygar, "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study," Information & Computer Security, vol. 25, no. 2, pp. 118–136, 2017.
[64] S. Hina, D. D. D. P. Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," Computers & Security, vol. 87, p. 101594, 2019.
[65] J. D'Arcy and P.-L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," Information & Management, vol. 56, no. 7, p. 103151, 2019.
[66] P. Ifinedo and E. C. Idemudia, "Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions," 2017.
[67] X. R. Luo, H. Li, Q. Hu, and H. Xu, "Why individual employees commit malicious computer abuse: A routine activity theory perspective," Journal of the Association for Information Systems, vol. 21, no. 6, p. 5, 2020.
[68] P. B. Lowry, C. Posey, R. (Becky) J. Bennett, and T. L. Roberts, "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust," Information Systems Journal, vol. 25, no. 3, pp. 193–273, 2015.
[69] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives," Information Systems Journal, vol. 28, no. 2, pp. 266–293, 2018.
[70] A. Nehme and J. George, "Taking it out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse," 2020.
[71] S. Farshadkhah, C. Van Slyke, and B. Fuller, "Onlooker effect and affective responses in information security violation mitigation," Computers & Security, vol. 100, p. 102082, 2021.
[72] P. Ifinedo, "Effects of organizational citizenship behavior and social cognitive factors on employees' non-malicious counterproductive computer security behaviors: an empirical analysis," 2015.
[73] A. Yazdanmehr, Y. Li, and J. Wang, "Employee responses to information security related stress: Coping and violation intention," Information Systems Journal, 2023.
[74] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," Information & Computer Security, vol. 26, no. 1, pp. 91–108, 2018.
[75] A. Yazdanmehr and J. Wang, "Can peers help reduce violations of information security policies? The role of peer monitoring," European Journal of Information Systems, vol. 32, no. 3, pp. 508–528, 2023.
[76] R. Willison and J. Backhouse, "Opportunities for computer crime: considering systems risk from a criminological perspective," European Journal of Information Systems, vol. 15, no. 4, pp. 403–414, 2006.
[77] V.-H. Trieu, V. Cooper, and D. Pallegedara, "Employee's Unauthorized Disclosure of Organizational Information on Social Media: The Role of Emotions and Boundary Permeability," in Proceedings of the 42nd International Conference on Information Systems (ICIS 2021), Association of Information Systems, 2021, pp. 1–9.
[78] P. Ifinedo, "Exploring Personal and Environmental Factors that Can Reduce Nonmalicious Information Security Violations," Information Systems Management, pp. 1–21, 2022.
[79] J. J. Kim, E. H. E. Park, and R. L. Baskerville, "A model of emotion and computer abuse," Information & Management, vol. 53, no. 1, pp. 91–108, 2016.
[80] M. A. Runco and others, "Divergent thinking, creativity, and ideation," The Cambridge handbook of creativity, vol. 413, p. 446, 2010.
[81] P. Newman, M. A. Ferrario, W. Simm, S. Forshaw, A. Friday, and J. Whittle, "The Role of Design Thinking and Physical Prototyping in Social Software Engineering".
[82] J. M. Carroll, "Scenario-based design," in Handbook of human-computer interaction, Elsevier, 1997, pp. 383–406.
[83] C. A. Lauff, D. Kotys-Schwartz, and M. E. Rentschler, "What is a Prototype? What are the Roles of Prototypes in Companies?," Journal of Mechanical Design, vol. 140, no. 6, p. 061102, 2018.

[84] J. J. Zigmont, L. J. Kappus, and S. N. Sudikoff, “Theoretical foundations of learning through simulation,” in Seminars in perinatology, Elsevier, 2011, pp. 47–51.
[85] C. S. Witt, “Instructional* simulations and the concepts of shared cognition,” [Doctoral Dissertation]University of Nevada, Las Vegas, 2008, [Online]. Available: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3859&context=rtds
[86] A. Bandura, “Social learning theory.,” Englewood Cliffs, NJ: Prentice Hall, 1977.
[87] A. Cropley, “In praise of convergent thinking,” Creativity research journal, vol. 18, no. 3, pp. 391–404, 2006.
[88] K. Stapleton and J. Wilson, “Telling the story: Meaning making in a community narrative,” Journal of Pragmatics, vol. 108, pp. 60–80, 2017.
[89] J. Leikas, Life-based design: a holistic approach to designing human-technology interaction. VTT Technical Research Centre of Finland, 2009.
[90] K. Bødker, F. Kensing, and J. Simonsen, “Participatory design in information systems development,” Reframing humans in information systems development, pp. 115–134, 2011.
[91] P. Dalsgaard and K. Halskov, “Innovation in participatory design,” in Proceedings of the 11th Biennial Participatory Design Conference, 2010, pp. 281–282.
[92] J. Simonsen and T. Robertson, Routledge international handbook of participatory design, vol. 711. Routledge New York, 2013.
[93] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, “Action design research,” MIS quarterly, pp. 37–56, 2011.
[94] R. D. Arnold and J. P. Wade, “A definition of systems thinking: A systems approach,” Procedia computer science, vol. 44, pp. 669–678, 2015.