Journal of Behavioral and Applied Management
2024, Vol. 24, No. 3, 161–172
https://jbam.scholasticahq.com/

Adoption of Advanced Cybersecurity Tools by Organizations: Motivations, Barriers, and Leader Responses

Robert T. Anthony
Hult International Business School

This study explores the adoption of advanced cybersecurity tools in organizations, focusing on the motivations, barriers, and leadership responses that shape adoption decisions. As cyber threats grow in sophistication, organizations must adopt increasingly complex tools to defend against attacks. However, despite the availability of cutting-edge technologies, adoption remains inconsistent. Through semi-structured interviews with 19 executive decision-makers and cybersecurity experts from high-threat industries, the study identifies key drivers for tool adoption, including an escalating threat environment and the need to enhance defense capabilities. It also highlights significant barriers, such as challenges of technical integration, organization readiness, and vendor management. Leadership plays a pivotal role in overcoming these obstacles by aligning organizational goals, securing resources, and fostering a culture of collaboration. The findings contribute to the literature on innovation adoption and cybersecurity management, offering insights into how organizations can better integrate advanced tools to enhance their security posture.

The Internet is essential for information exchange and commercial operations, yet the rise in cybercrime poses a serious threat. Malicious network intrusions and bot-led misinformation campaigns are increasing in frequency and severity, putting critical infrastructure and entire supply chains at risk (Goel & Nussbam, 2021; Kaloudi & Li, 2020). Responsible estimates place the costs of cybercrime at roughly .8% of global GDP, translating to over $800 billion in current damages (Lewis, 2018). Growth drivers of malicious activity are numerous, multidimensional, and unlikely to abate.

There is urgent interest in the dual use of artificial intelligence ("AI") for both automating and defending against cyber-attacks (Zeadally et al. 2020). AI use has become a staple of well-funded, sophisticated, and collaborative threat actors, who have made attacks more precise, stealthy, scaled, and effective (Kaloudi & Li, 2020). AI enabled attacks are difficult to detect and combat using conventional methods (Zeadally et al. 2020). Attacks include pattern analysis to select valuable targets, use of stealth techniques to conceal infiltration, and intelligent malware to control target behavior (Kaloudi & Li, 2020). Use of generative AI by threat actors also makes attacks initiated by personalized messaging more effective (Sebastian, 2023).

At the same time, artificial intelligence drives platforms and applications for cyber defense termed "advanced tools," which automate and elevate critical security functions. Advanced tools increasingly are essential for cloud, application, and network security, wherever the scale and complexity of data outpaces the capabilities of human analysts (Kaur et al. 2023; Wiafe et al. 2020). Advanced tools perform threat intelligence, identity and access management, intrusion detection, dynamic case management, security analytics, and more (Kaur et al. 2023). According to Wiafe et al. (2020), AI driven cybersecurity applications have been generally successful, especially for intrusion detection and prevention. There still is variable adoption across organizations and business functions, and implementation failures are common (Chui & Malhotra, 2018; Rocha & Kissimoto, 2022). Even as threat actors refine their capabilities, organizations struggle to adopt comparable technologies (Zeadally et al. 2020).

This paper gives insight into organizational adoption of advanced tools for predicting, monitoring, and responding to the most sophisticated cyber intrusions. It explores motivations, challenges, and leader responses common to organizations facing the highest level of threats. The analysis connects cybersecurity innovation, the considerations of decision makers, and the organization dynamics of companies that adopt advanced cybersecurity tools.

Prior Literature

Innovation adoption has been a continuing field of inquiry for scholars since Rogers' (2003) seminal work on the diffusion of innovation. A bibliometric analysis by van Orschot et al. (2018) probes the theoretical foundations of adoption research and reviews current trends. The authors distinguish four theoretical clusters: 1) behavioral theories of the firm; 2) technology acceptance models; 3) the determinants of innovation adoption in context; 4) diffusion theory. Studies of innovation adoption in context seek to identify variation in adoption behavior based on the interplay of the characteristics of an innovation with specific adoption contexts.

The largest body of cluster three "focuses mainly on the adoption of information technology and the determinants that impede or stimulate adoption" (van Orschot et al. 2018, p. 12). The most common strategy is to analyze the effects of technological, organizational, and environmental determinants of adoption behavior, with results presumed to vary within alternative contexts (van Orschot et

Article citation: Anthony, R. T. (2024). Adoption of advanced cybersecurity tools by organizations: Motivations, barriers, and leader responses. *Journal of Behavioral and Applied Management*, *24*(3), 161-172.

al. 2018). The present study joins this tradition by addressing the determinants of advanced cybersecurity technology adoption common to the highest threat industries. It adds a focus on leadership dynamics that contribute to adoption decisions.

Digital innovation adoption is recognized as a multi-level phenomenon (Zhang et al. 2019). The adoption readiness of individuals and the effects of the innovation ecosystem have been shown to impact the timing, cost, and effectiveness of information security technologies (Emmanuel-Avina, 2017). There is broad consensus that perceived usefulness and ease of use of new technologies are powerful determinants of individual adoption (Venkatesh et al. 2003). The role of threat messaging is especially salient for adoption of information security technologies (Emmanuel-Avina, 2017). Opportunistic behavior among interdependent networks of suppliers and business partners has been identified as a central concern within innovation ecosystems (Cobben & Roijakkers, 2019). Other environmental challenges include technical uncertainty, rapid change, and talent shortages (Rocha & Kissimoto, 2022). Complex layers of regulatory burdens have been identified as a special issue for cybersecurity (Marotta & Madnick, 2020).

Organization-level adoption has been a central concern of innovation management scholars. Organizational factors driving information system adoption include technology readiness, internal expertise, organization size, top management support, and organization culture (Ali et al. 2022). Certain organization capabilities underlie these factors and are recognized as needed for adoption of complex digital innovations. Organization flexibility, capacity for learning, support for collaboration across social networks, and the presence of complementary strategies and structures have long been associated with adoption of highly integrated, experimental technologies (Khanagha et al. 2013; Rycroft & Kash, 2000; Tidd, 2001). Unfortunately, many organizations lack the required capabilities (Damanpour & Schneider, 2006).

Recent inquiry has shifted from theory to applications in specific domains (Xu et al. 2021). The cybersecurity literature is predominantly technical. Well documented challenges include the complexity of tools, system interoperability, data fitness, and the prospect of adversarial attacks on AI models (Kaloudi & Li, 2020). The rate of technical change further complicates the challenges (Kaur et al. 2023; Wiafe et al. 2020).

Management oriented explanations are more difficult to come by. The literature remains fragmented across practitioner and academic sources, and some researchers question the reliability of grey literature due to commercial motivations (Bahrami et al. 2019; Florencio & Herley, 2013). Recent academic reviews do summarize barriers to adoption of information security technologies within organizations. These include high implementation costs, a shortage of skilled personnel, inadequate leadership support, low prioritization of initiatives, inadequate communication and training, and lack of cybersecurity awareness (Alshaikh, 2020; Soomro et al. 2020). Marotta and Madnick (2020) point to a bias towards over-emphasis on policy compliance, which can provide a false sense of security and obscure emerging threats.

Given the complex and multi-faceted nature of the challenges, leader behavior in the information security community becomes critical. In fact, leader characteristics and practices have been long identified as essential for creating conditions for innovation adoption (Crossan & Paydin, 2010; Klein & Sorra, 1996)). For example, Damanpour and Schneider (2006) emphasize the importance of strategic vision and openness to change for leaders of digital innovation. Bunjak et al. (2022) demonstrate that change oriented leadership encourages collaborative knowledge sharing and facilitates internal diffusion of complex and uncertain technologies. In addition, recent literature emphasizes the crucial importance of information technology leaders acquiring budgets, galvanizing top management support, and encouraging employees to exchange insights and troubleshoot challenges (AlSheibani et al. 2018; Bunjak et al. 2022).

An influential stream of research around communities of practice ("COPs") addresses complex innovations requiring rapid learning and knowledge exchange across a professional organization. COPs are characterized by a shared understanding of opportunities and problems ("mutual engagement"), a process by which people work together towards common goals ("joint enterprise"), and joint resources and language systems people use as they facilitate knowledge exchange and learning in the group ("shared repertoire") (Wenger et. al, 2002). Leaders create innovation communities by aligning goals within an organization, balancing support such as funding, tools and training with accountability, and bringing professionals together for knowledge exchange in a supportive social environment (Brown & Duguid, 1991; Pattison et al. 2016; Wenger et al. 2002). Disciplinary competition and bureaucracy are critical barriers that leaders must overcome (Ferlie et al. 2005; Wenger, 2002).

While factors impacting technology adoption are identified in numerous accounts, the determinants of advanced tool adoption remain under studied. Researchers call for studies that lend empirical support for AI adoption in practice and additional studies of human factors in cybersecurity (Bawack et al. 2021; Cubric, 2020; Dalal et al. 2022). Soomro et al. (2016) call for a more holistic approach integrating technical, social, and organizational considerations for cybersecurity management. Johnston (2023) notes that studies of social structures and innovation disposition for cybersecurity are "conspicuously underrepresented from the literature" (p. 127). Preis and Susskind (2022) summarize, "We examine the existing academic research and demonstrate the significant growth in cybersecurity practice that has cropped up in spite of the relative sparsity of academic work. Theory and practice need to catch up with each other" (p. 614).

Conceptual Framework

The core analytic framework for the study is the Inter-organizational Systems Model ("IOS"), which is used to guide exploration and frame data analysis (Iacovou, et al. 1995). The IOS is one of two most applied frameworks for studying innovation adoption in context and is part of "the birthplace of middle range theories of adoption" (Van Oorschot et al. 2018, p. 10). The IOS is justified for purposes of this study because AI-based cybersecurity tools are largely interorganizational systems characterized by complex layers of interorganizational relationships.

Iacovou et al. (1995) theorize three constructs determining adoption decisions. They are perceived benefits, organizational readiness, and external pressure. Van Orschot et al. (2018) note that adapting indicators from complementary theory to form a more comprehensive model is a common strategy for this genre of research. Accordingly, this study supplements the analytic categories with additional indicators. Relative technical advantage, compatibility, and complexity are drawn from Rogers' (2003) classic study of adoption behavior. Organization analysis and leader evaluation is guided by COP categories of mutual engagement, joint enterprise, and shared repertoire. Exploration of external pressures is informed by convergent assumptions of resource dependence theory and institutional theory, which emphasize the interaction of inter-connected stakeholders as organizations pursue performance and legitimacy (Oliver, 1991).

Methods

The study is problem-centered, exploratory, and inductive. Data gathering consists of semi-structured interviews with a purposeful sample of 19 executive decision makers and experts, supplemented by a review of archival materials. The number of informants and interviews is within the inter-quartile range of studies published in leading information systems journals (Marshall et al. 2013). The boundary of the study is large organizations in municipal government, professional services, information technology services, education, and financial services. These industries have had the highest incidence of cyberattacks in a recent five year period, according to Verizon (2022).

The study sample includes a highly qualified group of cybersecurity experts. At the time of the interviews each informant had substantial experience in their area of expertise, operated at senior levels of their respective organizations, and were well positioned to speak to current events in their respective fields. At the time of interviews, 10 informants had direct accountability for adopting advanced cybersecurity tools within their organizations, including six CISOs, three CIOs, and one with a dual CIO/CISO role. Together these 10 informants represent the focus industries and practice in the upper echelons of the information security field. The sample is rare, as access to an organization's risk management activities is difficult to obtain (Johnston, 2023). At the time of the interviews, nine of the informants were experts or industry participants having high level contact with issues under study. An anonymized description of informants is listed in Table 1, with the naming convention applied in the section on findings ("Px").

Interviews were conducted from October 2022 to June 2023 utilizing a core interview guide that was revised and supplemented with experience. A total of 24 interviews

Table 1

Anonymized Description of Interviewees

(P1)	Chief Information Security Officer – Division of Large, Global Financial Services Firm
(P2)	Chief Information Security Officer – Large, Global Information Services Company
(P3)	Chief Information Security Officer – Large, Global Professional Services Firm
(P4)	Chief Information Security Officer – Major Metropolitan Area
(P5)	Chief Information Security Officer – Major Metropolitan Area
(P6)	Chief Information Security Officer – Major Metropolitan Area
(P7)	Chief Information Officer – Large, Global Professional Services Firm
(P8)	Chief Information Officer – Multi-campus, Global University
(P9)	Chief Information Officer – Division of Large, Global Professional Services Firm
(P10)	Chief Information Officer and Chief Information Security Officer – Medium Sized Technology Services Firm
(P11)	Vice President of Business Development – Cybersecurity Managed Services Provider
(P12)	Director of Operations Technology – Large, Global University
(P13)	Director of Compliance – Large, Global Technology Services Company
(P14)	Senior Cybersecurity Litigator and Forensics Expert – Large, Global Law Firm
(P15)	Regional Vice President for Threat Analysis – Major Cybersecurity Vendor
(P16)	Vice President of Security Software Development – Large, Global Systems Supplier
(P17)	Professor of Law – Expert in Governmental, Inter-Agency Decision Making
(P18)	Professor of Computer Science ("Top 3" University for Engineering) and Chief Executive Officer – Machine Learning Startup
(P19)	Venture Capitalist – Financial Technology

were conducted over 22 1/2 hours, 14 of which included CIOs and CISOs. Interviews proceeded to a point of saturation, whereby analysis of transcripts indicated redundant information and no new emerging codes. Interviews were conducted in person, on Zoom, or by phone. Respondents were sent an informed consent form and general background of the study prior to the interview. Each interview began with agreement to the informed consent and a request for recording. If consent was given, then a recording was made with an L87 Digital Voice Recorder, uploaded for transcription (Otter.ai), downloaded and stored on a password protected laptop, and uploaded to coding software for analysis (Quirkos). In many cases the transcripts contained repeated words (e.g., "the the") and punctuation errors, which were cleaned during analysis. If consent to record was not given, then contemporaneous notes of the interview were made. Follow-up interviews were conducted with 5 of the informants. Follow up questions were given to informants prior to interviews. Study findings were reviewed and verified by two of the CISOs who participated.

Data is analyzed using content analysis and thematic analysis. Interview data is coded based on the theoretical framework, and themes are generated inductively within codes where observations of individual informants agree with the reports of other informants (Ayre & McCaffery, 2022; Braun & Clarke, 2014; Yin, 2003). Findings are reported via a conceptualized narrative that illustrates the theoretical significance of findings while at the same time letting the data speak (Berends & Deken, 2019). Together the analysis sheds light on likely advanced tool adoption experiences of organizations in high threat industries.

Findings

Findings represent a cross-case synthesis of emerging themes in the research data, organized based on the theoretical framework. Detailed support for the themes is offered via direct quotes generally representative of multiple views in the sample. Themes are summarized in tables. Table 2 indicates the percentage of quotes coded by IOS category. Tables 3, 4, and 5 summarize themes by analytic code. Table 6 summarizes executive-level motivations for adopting advanced tools. Table 7 summarizes barriers perceived by informants. Table 8 summarizes leader responses to the barriers. Table 9 summarizes potential industry and organization contingencies.

Findings for Perceived Benefits

Perceived benefits relate to the functionality and fitness of advanced tools. Specific codes within the category include relative advantage, complexity, and compatibility. Together these themes point to motivations for adopting advanced tools and powerful technical barriers, both familiar and emerging. Advanced tools were viewed as non-discretionary by the research sample given the threat landscape. At the same time, newly developed security systems were subject to complicated technical issues, made even more challenging by digital transformation and transitions to the cloud.

Table 2

Percentage of Quotes Analyzed by IOS Category

IOS Category	% of Quotes Coded
Perceived Benefits	29.5%
Organization Readiness	49.8%
External Pressure	20.7%

Perceptions of Relative Advantage

Relative advantage consists of the perceived balance of advantages and disadvantages versus available alternatives. These themes describe executive motivations for adopting advanced tools. Two themes frame perceptions of advantage: theme 1) an intensifying threat environment motivates advanced tool adoption; theme 2) advanced tools enhance defense capabilities.

Theme one is "an intensifying threat environment motivates advanced tool adoption." Informants reported that increased volume, speed, and sophistication of attacks translated into an avalanche of troublesome alerts and incidents in their operations. Some also expressed a belief that attackers generally have superior resources and capabilities versus defenders. For example, P15 noted that attackers utilize "advanced techniques" and "are capable of acquiring or developing the most powerful technology," while most defenders have limited maturity and resources. Observing that often "the advantage lies with the attacker," P18 speculated that threats will only grow in the future because "we're potentially entering a phase where you don't have to be very talented to do malware." P15 declared, "To be honest with you… it's not a fair fight." P5 put the matter succinctly, "The bad guys and gals are constantly innovating. We have to keep up."

Theme two is "advanced tools enhance defense capabilities" by effortlessly processing large amounts of data and detecting anomalies that might go unnoticed by humans. When tools leverage human resources, they believe, then their companies can implement a layered defense strategy. For example, P5 identified that automated tools allow him to widely scale a small, centralized team and be effective in a large, diverse organization, concluding, "Automation is the only ticket to remain vigilant, and, you know, maintain our edge and fight the good fight. We have to have tools. The right tools are what allows our people to do the tasks that are better suited to people."

Informants noted several challenges when discussing the relative advantage of advanced tools versus other security tactics. Two themes stood out across the sample: theme 3) total cost of ownership is a barrier; theme 4) advanced tools are risky to deploy. The challenges tempered assessments of overall benefits of advanced tools.

Theme three is "total cost of ownership is a barrier." Informants all cited the high cost of tools and sometimes hidden total costs of ownership. The cost of tools themselves produced what P11 described as "sticker shock." From there they offered examples of additional costs,

Table 3

Overview of Perceived Benefits Themes

Code	Theme
Relative Advantage	Theme 1: An intensifying threat environment motivates advanced tool adoption
	Theme 2: Advanced tools enhance defense capabilities
	Theme 3: Total cost of ownership is a barrier
	Theme 4: Advanced tools are risky to deploy
Complexity	Theme 5: Problems adapting tools to legacy software
	Theme 6: Complications of cloud security
Compatibility	Theme 7: Tool adoption drives difficult integration challenges

Table 4

Overview of Organization Readiness Themes

Code	Theme
Mutual Engagement	Theme 8: CISOs and CIOs have highly compatible goals and constructive relationships
	Theme 9: Friction between security goals and ease of doing business
	Theme 10: Threat messaging and goal alignment are essential for tool adoption
	Theme 11: Budgets for tool acquisition are available for well demonstrated needs
Joint Enterprise	Theme 12: Structural impediments to collaboration
	Theme 13: Human resource shortages
Shared Repertoire	Theme 14: Creative approaches to routine knowledge exchange
	Theme 15: Special forums for knowledge exchange

Table 5

Overview of External Pressures Themes

Theme 16: External pressures motivate adoption of advanced tools
Theme 17: Tool vendor product claims can be misleading

Table 6

Summary of Executive Motivations for Adoption of Advanced Tools

Response to an intensifying threat environment
Enhanced defense capabilities
Leverage scarce human resources
Customer and insurance audits
Potential for reputational harm
Potential for lawsuits
Availability of educational programs and certifications

including excessive workload potential of a natural language processing tool and behind the scenes dedicated engineering support for new tools. P5 explained, "I operate in an environment with 50 agencies, right? I can't just go and buy a tool.… It's a whole program, right? The tool by itself is meaningless without all the support."

Theme four is "advanced tools are risky to deploy." Informants acknowledged that introducing any new technology into an already complicated infrastructure has risks, and they were especially concerned about the unpredictability of AI in the environment. For example, P6 identified an "inherent risk if we're allowing AI machine learning take action on things like, say, locking down a system, resetting someone's password, or what have you." P7 echoed the concern that "if AI is doing too much of it, that it can create a false positive and shut down access and start to shut down, you know, the ability of people to work."

Perceptions of Complexity and Compatibility

Interviews probed system complexity and system compatibility. With respect to complexity, two problems consistently surfaced: theme 5) problems adapting tools to legacy software; theme 6) complications of cloud security. Consistent themes emerged with respect to compatibility: theme 7) tool adoption drives costly and complex integration challenges.

Theme five is "problems adapting tools to legacy software" in complicated and outdated IT environments. Informants stated, "The biggest risk or the base threat is around just legacy technology that we're required to continue to support in some cases, because there is no other technology" (P6); "we have some technical debt… and lots of legacy systems" (P4); "we work with a ton of

Table 7

Summary of Barriers to Advanced Tool Adoption

Total cost of advanced tool ownership
Perceived risks of adoption
The presence of legacy systems
Complexities of cloud usage
Incompatible vendor product suites
Difficulties integrating multiple tools
Friction between security goals and ease of doing business
Absence of CISO leadership priming activities
Structural impediments to decision making
Human resource shortages
Distrust of vendors

Table 8

Summary of Leader Responses to the Barriers

Mutual goals and constructive relationships among CISOs and CIOs
Awareness building among line executives and the organization at large
Clearly demonstrated needs to secure budgets
Creative approaches to staffing and training
Routine knowledge exchange processes to facilitate tool adoption
Special forums for knowledge exchange to facilitate tool adoption
Partnerships with fewer, select vendors
Rigorous risk assessment preceding investigation of specific tools

Table 9

Summary of Industry and Organization Contingencies

Organization size
Organization structure (degree of centralization)
Process maturity
The extent of legacy systems
The degree of cloud-based digitalization
The degree of regulation and compliance orientation
Industry threat patterns
The experience of firms being the target of attack
For profit versus mission driven
Quality of leadership support

healthcare companies, and health care companies routinely have had legacy old technology that's hard to update, and so they're easy to be hit" (P14); "one of the biggest concerns is legacy software that is very important to the business not going through this process of making sure it was secure and cloud ready and (so)… being highly vulnerable, but the business not wanting to give it up…. It's very difficult to ensure that the sins of the past don't go out to the cloud, essentially" (P1).

Theme six is "complications of cloud security." Most organizations maintained what was described as a "cloud first" strategy for tools. While P10 stated that cloud vendors have made great strides around security, others were not as sure. P3 stated, "Just conceptually thinking about if everything is in one place, you got to think it's a big target pool." P1 discussed the speed of the transition to the cloud and expressed discomfort controlling the migration of data from a security standpoint. P3 summarized, "You don't own it, you can't control it, you can't always see it, everyone can access it, there are frequent changes to it, and there is a shared responsibility for protecting it. This equals a security professional's worst nightmare." Specific worries include multi-cloud digitalization strategies, the interoperability of cloud security technologies across competing vendors, data visibility and control, and bottom-line ownership of security. P8 emphasized the limits of vendor responsibility, concluding, "When that comes to a, you know, an instance of threats, often contractually, they're not actually obliged to do much. So, you know, we have a set of tools, and we have some awareness, but equally, it's not our system. Right?"

Theme seven is "tool adoption drives difficult integration challenges." A baseline concern was technical integration. As illustrated by P14, "CrowdStrike has the Falcon tool, and Mandiant has the Advantage tool... And, yeah, I mean, it's, it's clunky. They always think that it's going to be easy… but there's always (problems)." Informants also emphasized usability issues where analysts were forced to rely on independent systems for a comprehensive view of alerts and events.

Informants reported an underlying integration issue, which is that tools in vendor product suites are often incompatible. Integration issues were exacerbated when departments operating in silos independently purchase tools from competing vendors, as was reported by P5. P3 summarized, "Some of these tools play nicely together with each other and some of them really don't. And so, where we've had to introduce new tools… the interoperability and compatibility with other tools is a key component." P2 stated, "The answer on PowerPoint is that the tools are always compatible with each other, but, in practice, real life experience differs with PowerPoint."

Findings for Organization Readiness

Organization dynamics of adoption were probed. Shared goals ("mutual engagement") and knowledge exchange ("shared repertoire") were identified as both critical and common. Coordinated decision making ("joint enterprise") was reported as more problematic. Together, these themes highlight complex social factors frustrating advanced tool adoption as well as the importance of leadership in the adoption process. Challenges revolved around goal alignment and inter-departmental decision making in the context of competing interests. Leadership emerged as the decisive factor for overcoming the barriers and enabling the adoption of advanced tools. Through

strategic vision, resource mobilization, and effective communication, leaders were able to navigate the complexities of tool adoption, align organizational goals, and secure the necessary resources.

Perceptions of Mutual Engagement (Shared Goals)

Informants discussed shared information security goals from several vantage points. Four themes are elaborated below: theme 8) CISOs and CIOs have highly compatible goals and constructive relationships; theme 9) friction between security goals and ease of doing business is a barrier; theme 10) threat messaging and goal alignment are essential for tool adoption; theme 11) budgets are readily available for well demonstrated needs.

Theme eight is "CISOs and CIOs have highly compatible goals and constructive relationships." Constructive partnerships were reported by P2, P4, P5, P6, P8, P9, P10, and P12. As stated by P2, "The IT function gets it. It's in their face all the time." P6 summarized, "Our CIO… has historically had the support of the security program and support in our team's recommendations."

Contrasting this was theme nine, "friction between security goals and ease of doing business is a barrier." Line managers commonly resisted new tools, according to informants, even when the IT community was aligned in their own commitment. In fact, P18 conjectured that "pressure from the business" for friction-free work processes is the main impediment to advanced tool adoption. P7 cited excessive alerts and false positives from advanced tools as a source of resistance. P16, a security engineer, noted intense customer impatience with security related protocols, even in the face of known threats and incidents. P8 reported that awareness training sparked negativity among line managers when they learned automated tools might necessitate process change.

Theme ten is "threat messaging and goal alignment are essential for tool adoption." P3, P4, P10, and P11 voiced a preference for collaborative "new school" leadership approaches versus "old school" policy compliance postures to prime resource acquisition and line manager acceptance. They observed that the former justifies new investments while the latter generates resistance. P1 supported the theme, "Working on rapport is the key to success. You can't just be a gate at the end of the process."

P10 provided context by stressing the difficulty of aligning the executive team around risk assessments. Security leaders prioritized related activity. For example, P2 emphasized, "I find my role is often education… A lot of what I think I should be doing and have been doing is educating (senior executives, the Board, the Audit Committee, and the risk management team) on the risk… If you think back a couple of years, it wasn't on anyone's agenda." Security leaders found creative ways to strike the right tone. P2 noted that it doesn't work to "scare people into it," but that relating real statistics and stories of incidents and from the company's experience was helpful.

Informants clarified that resource acquisition was a critical task for leaders. Theme eleven is "budgets for tool acquisition are available for well demonstrated needs." Discussions of the costs of tools naturally turned to a discussion of budgets, and informants agreed that requests for expensive advanced tools are scrutinized. Acquiring resources was seen to take effort and perseverance. For example, P1 offered, "It's important to have the debates in the budget process. Sometimes you win and sometimes you lose. Mostly you win because you have to win."

At the same time, informants expressed that adoption is most often funded if the investments are meticulously justified. The budget process was viewed both formally and opportunistically. P3, P4, and P6 all reviewed careful strategies to quantify risks in business terms, frame options, gain broad support, and navigate lengthy budget processes. Informants also echoed that external events such as a breach in the industry or an unwelcome lawsuit could be capitalized upon to justify funding.

Perceptions of Joint Enterprise (Common Processes)

Achieving common processes was described as essential but problematic. Two themes stood out: theme 12) structural impediments to collaboration; and theme 13) human resource shortages.

Theme twelve is "structural impediments to collaboration." P9 explained a common context, "It's a much wider conversation in our organization (because) you want scale. The bigger the solution, the more scale you want. So, I (need) to talk to my fellow CIOs… to drive the unit cost down." P8 elaborated on the challenge, "Getting everybody on the same page when you have different priorities is really very difficult."

Behavioral dynamics across divisional/agency or departmental boundaries were commonly referenced. P17 discussed differences in "coordinating authority" among public sector CISOs, a point that was supported by a review of archival materials. Other informants reported frustration due to the decentralized nature of corporate decision making for advanced tool adoption. P1 discussed the challenge of navigating a sometimes-opaque interdivisional structure where divisions had different priorities and timelines. P8 observed that other divisions in the company were "a little bit more unwieldy, just due to size" and were slower to adopt new technologies. Similarly, P3 referred to the challenges of a "very political" multi -divisional, global footprint, stating that consensus could be hard to achieve across a broad scope of operations, concluding, "Everybody's got lots of different opinions, meaning that often we don't reach consensus." P5 and P6 offered examples where decentralized decision-making frustrated tool adoption, noting inefficiencies, redundancies, and compatibility problems. P5 summarized, "That is my biggest challenge is this idea of optimization, where each agency is optimizing for themselves." P6 concluded of federated decision making, "I think it's all around control. It's the perception of control. They feel like they're going to lose control over their endpoints or their environment if we all agree on a tool and work off the same platform."

Theme thirteen is "human resource shortages." Inform-

ants voiced frustration with the overall availability of cybersecurity professionals, the cost of acquiring needed skills, and difficulties obtaining specialized skill sets. P1 summarized the frustration, "There are simply not the skills and skilled up people around the world to be able to support (robust cyber defenses). And most organizations have got a shortfall of cybersecurity and a big variation of percentages of what they need." He concluded, "If you don't have all the people that can run these things that you don't want to be having that many of them." P6 agreed by stating, "We've historically been a well-funded security program. I think our biggest challenges are around staffing and our ability… to actually grow the team."

P3, P4, and P6 attributed the problem to salaries needed to attract skilled talent. P1, P7, P18, and P19 stated the problem differently, pointing to the prestige of top technology companies. P1 succinctly stated, "Everybody wants to work for Google." P18 and P19 described intense labor market competition from technology startups, with P19 noting "a flood" of venture capital going into the space that diverts talent to startups. P6 noted an acute deficit of emerging, in-demand skill sets, such as cloud security.

Perceptions of Shared Repertoire (Knowledge Exchange and Learning)

Shared repertoire refers to community resources for interactive communication, learning, and knowledge exchange. Informants considered shared repertoires as an enabling factor for to adoption and an essential role for leadership. Emerging themes centered on mechanisms for developing shared repertoires: theme 14) creative approaches to routine knowledge exchange; theme 15) special forums for knowledge exchange.

Theme fourteen is "creative approaches to routine knowledge exchange" to support ongoing operations. For example, P3 described the importance of unusually interactive risk assessments at customer sites, concluding, "Capturing the risk at (an early) stage means that it's understood by everybody, all the way up to the top of the organization." P4 facilitates regular communication by informally "deputizing" liaisons with the security team, offering, "That's a badge of honor for some folks. So, I have several people like that now." P4 also uses a specialized mailbox for communication of security related developments and concerns, stating, "Instead of us receiving 20 - 25 emails a day, we may receive 200 to 300 a day now, because it's taken off across the city." P5 prioritizes communication providing "political cover" for his team to compensate for matrix reporting relationships.

Theme fifteen is "special forums for knowledge exchange." P7 discussed the importance of, and support for, industry interactions as a way for his security team to stay current, stating, "The community is so vibrant… that they're finding out about what other people are doing and what's useful, and they're constantly evaluating." P5 voiced agreement, "We have continuous learning… where my team goes to conferences," and, "we hold a bimonthly forum where we meet six to seven times a year. We bring them all together, usually virtually, and we talk to them about what the office of security is involved in, but oftentimes I invite some folks from the industry (to give talks)." P6 described similar initiatives, including "quarterly roundtables" wherein security officers from independent departments convened occasionally to share challenges and best practices. One goal of all these approaches was described as priming uniform adoption of the most relevant and effective advanced tools. Beyond situational awareness, P3, P4, P5, and P6 discussed the importance of active training initiatives to build needed competence for adoption, giving several examples of programs and techniques.

Findings for External Pressures

Perceived external pressures were probed. These discussions expanded upon executive level commitment to advanced tools by detailing institutional factors encouraging their adoption. Informants also provided insight into a unique set of challenges for cybersecurity technologies, as they consistently voiced deep skepticism over the readiness of the products available in the market for tools.

Theme sixteen is "external pressures motivate adoption of advanced tools." Motivating pressures include: an awareness of threats (all); a common assumption that using monitoring tools is a standard practice (P1, P2, P3, P5, P6, P7 P8, P10, P11, P14); the broad availability of conferences and educational programs (P5, P6, P7); certifications (P2, P7, P14); customer and insurance audits (P2, P3, P7, P11); potential for customer impact, reputational harm, and lawsuits (P1, P3, P4, P5, P9, P10, P14); and contracts with vendors (P1, P2, P7).

On the other hand, external pressure from tool vendors stood out as a barrier to advanced tool adoption. Theme seventeen is "tool vendor product claims can be misleading." Informants questioned the authenticity and fitness of artificial intelligence in some advanced tools. P3 stated that artificial intelligence and machine learning are not synonymous, and that machine learning was a better underlying technology for cybersecurity. P10 bluntly stated, "It's not a helpful term. We make vendors drop a quarter in the jar every time they use the words 'artificial intelligence.' You have to go in deep and figure out what these things really do." P1 concurred, "The effectiveness of a lot of these tools is unsubstantiated…, and that's been the case for such a long time." P8 similarly expressed, "When you get down to the nitty gritty (they aren't ready)…. So, product quality, you're worried about product quality." He noted that he has seen peer companies get "burned" by adopting immature solutions.

Informants were skeptical over the perception that vendors over-sell tools. P3's view is representative, "Working with the security tooling industry… I'm somewhat cautious because cybersecurity companies and vendors that develop technology, in my experience, have a justified bad reputation in promising the world." P8 was more blunt, "There is a lot of noise in this area. There are a lot of platforms, there's a lot of change, and there's a lot of snake oil in the industry." P2 expressed a similar senti-

ment in a more measured way, stating, “The vendor community would love me to think that if I buy more tools, I will have less risk. And I don't find that to be true.” P18 offered a vendor perspective, “Everyone wants to sprinkle the magic AI pixie dust on whatever it is they're selling. You can pretend it's AI and sell it for more.” P1 summarized, “You start thinking, well, maybe all of this is just kind of overhyped and, you know, no good.”

Informants speculated on the drivers of inconsistent product quality. P1 blamed the ready availability of venture capital to fund unproven technologies and the proliferation of multi-vendor software marketplaces to find a market for them. P19 agreed, stating that capital markets value the perception of robust cyber defense but are not able to assess effectiveness. P2 and P15 identified merger activity as a driver of distrust. P15 stated that pressure on vendors to be early to market with integrated solutions encouraged acquisitions without sufficient integration. P2 noted, “It's not like it (is described) in the QA. It's not baked into the same console. The patches don't come out at the same time… Like there's nothing the same other than the splash screen that has the same vendor's name on it.” P3 offered that when customers don’t “kick the tires,” then they contribute to a climate of loose product claims. P18 confirmed the role of customers, stating, “I’ve spent a lot of time explaining our AI products. The buyers don't really understand it.”

CISOs in the sample responded through vendor consolidation and rigorous risk assessment. The statement of P3 was representative, “It's a very busy place with lots of different tools out there. When I'm looking at purchasing it all, before I even go to market… I'm very well informed of exactly what I need and exactly what I don't need.”

Discussion

The study explores motivations for adoption of advanced cybersecurity tools, organization level barriers, and leader responses to the barriers. It addresses the need for empirical validation of AI adoption in practice, analysis of human factors in cybersecurity, and a holistic approach to managing information security. Findings contribute to research on the determinants of innovation adoption in technology contexts, confirming the relevance of existing theories while introducing new considerations specific to cybersecurity. The analysis also highlights how leaders navigate the complexities of advanced tool adoption despite significant barriers unique to the domain.

Determinants of Advanced Tool Adoption in Context

Iacovou et al. (1995) suggest that adoption of interorganizational systems such as advanced tools is a function of perceived benefits of a technology, organization readiness, and external pressures to adopt. Against this background, researchers such as Kaloudi and Li (2020) and Kaur et al. (2023) predict artificial intelligence will figure prominently in cyber-attacks and cyber defense in the future. Findings reveal informants take the conclusions of the literature for granted. Motivations for adopting advanced tools are relatively straightforward and uniform. High stakes and elevated stakeholder expectations coupled with an acute threat environment strongly encourage organizations in high-threat industries to adopt advanced tools. The relative advantage of these tools for enhancing capabilities and leveraging human resources is decisive.

Existing literature also suggests technical characteristics of an innovation could temper the perception of benefits and will influence adoption behavior (van Orschot et al., 2018). Reviews by Ali et al. (2022) and Cubric et al. (2020) demonstrate that factors such as cost, infrastructure complexity, system integration, and system interoperability will be barriers to adoption of complex digital innovations. First person accounts of security leaders support these conclusions for the domain of cybersecurity and add granularity to the concerns. They emphasize that advanced tools often are internally incompatible and have been implemented as a patchwork over time, with elevated needs for costly technical support. In addition, rapid digitalization and a "cloud-first" strategy add complexities unique to advanced tools, especially in hybrid cloud environments. Decision makers are faced with relying on incompatible systems from competing vendors, partially visible data, and unclear accountability for mission critical operating functions.

Organization readiness to adopt is the second analytic category developed by Iacovou et al. (1995). Organization design factors have long been associated with innovation management in general and the adoption of complex digital innovation in particular (Crossan & Apaydin, 2010; Ali et. al., 2022). Within the domain of cybersecurity, factors such as strategic alignment, organization structure, organization culture, and compliance orientation have been seen to influence adoption behavior (Alshaikh, 2020; Marotta & Madnick (2020); Soomro et al. 2020). Once again, the present study confirms the influence of these factors and add insight into their dynamic impact on advanced tool adoption.

Findings reinforce the importance of strategic alignment for adoption and suggest that decentralized decision making is a critical barrier. With respect to alignment, resource needs for advanced tools are substantial, and it is evident that adoption decisions bring inter-departmental goal conflicts forward. This is because tools are seen to threaten managerial autonomy, require process changes, increase workloads, and trigger disruptive false alarms. Resulting conflicts create political tensions and organizational resistance to adopting new tools. Enterprise-wide decision making also is difficult where consensus to adopt is required. Problems include logistical hurdles and competition for resources amidst challenging matrix reporting relationships.

Iacovou et al.’s (1995) final category determining adoption of interorganizational systems is external pressure. External pressure was understood as either competitive pressure or imposition by trading partners in the original formulation (Iacovou et al., 1995). There is evidence for

both in this study's findings. Informants fear the financial impact of ransomware, and customer audits stemming from the threat of supply chain attacks motivate adoption of advanced tools. Pressure to conform to institutional environments is even stronger (Oliver, 1991). Informants note that information security is heavily regulated, and capital markets increasingly monitor cyber defense.

Powerful barriers to adoption also exist in transaction dynamics for advanced tools. Cobben and Roijakkers (2019) have identified opportunistic behavior among partners as a special problem for complex innovations. An original finding of this study is broad and deep vendor distrust in the cybersecurity technology ecosystem. Ambiguity over how the tools work and perceived risks of unintended consequences is a threshold concern. Beyond that, perceptions of "snake oil" in the industry, customers getting "burned" by products that are not ready, products that don't perform as promised, and reference to "magic AI pixie dust" indicate the breadth and depth of the issue. This distrust leads to long adoption cycles and, potentially, incentives for vendors to develop inferior tools.

In final analysis, the central barrier of tool adoption lies in the interaction of complex technical, social, and environmental factors. Adoption decisions draw on a broad group of stakeholders in industry and organization silos, with varying degrees of technical expertise and competing interests. Highly motivated threat actors with unified goals and collaborative business models face fewer hurdles, which contributes to their perceived advantage. High-level leadership skills are needed to successfully navigate this difficult terrain.

The Role of Information Security Leadership

The study shines a light on leader responses to difficult adoption barriers, especially through understanding the work of CISOs in the research sample. The responsibility of leaders for creating a climate for innovation is long established (Klein & Sorra, 1996). Influential work by Damanpour and Schneider (2006) and more recent studies by Bunjak et al. (2022) suggest that strategic, collaborative, and change oriented leadership create such a climate for adoption of complex digital systems. It further has been argued that leaders foster organizational capabilities for innovation adoption through goal alignment, resource mobilization, and bringing together communities of practice for knowledge sharing and professional growth (Brown & Duguid, 1991; Pattison et al. 2016; Wenger et al. 2002). Still, the role of leadership has not been evaluated empirically in the domain of cybersecurity technology adoption.

This study highlights the effectiveness of context-sensitive, relational, and change-oriented leadership in driving innovation and overcoming barriers, supporting existing theory. Leaders in the study exhibited skill in navigating hierarchies and organizational boundaries, solving problems, and bridging diverse interests. They adeptly combined formal management tools with adaptive social system strategies.

To address technical barriers, leaders relied on formal tools, including evidence-based advocacy to communicate threats and educate business leaders, risk assessments to justify investments, and determined resource acquisition strategies to secure funding for complex tools. Workforce challenges were mitigated through creative strategies to grow and deploy talent, countering skill gaps.

In addressing structural barriers, leaders used informal mechanisms inspired by COP literature, promoting learning, innovation, and trust. They hosted forums for collaboration, identified shared needs, cultivated partnerships with opinion leaders, and shielded teams from conflicting demands. By leveraging these practices, leaders transcended formal authority and broke down silos, facilitating collective action and enabling the adoption of advanced tools. In sum, findings demonstrate that progressive leadership effectively blended formal authority with relational influence.

Trends are in place to see continuing growth in the number, power, and sophistication of cyber-attacks. The adoption of advanced tools indicates the maturity and strategic integration of cybersecurity within an organization. It is the work of leadership to elevate the capabilities of diverse communities to meet these challenges.

Limitations and Future Research

The study has limitations. Technologies and practices may evolve rapidly, and the focus on "how" and "why" questions may limit generalizability. The statistical significance of conclusions is not claimed. In keeping with the goals of the study, several broad topics are illuminated that are worthy of a more granular investigation. These include best practices for resource acquisition, coordination, and threat messaging, and the role of trust in the innovation ecosystem for cybersecurity tools.

References

Ali, O., Murray, P. A., Muhammed, S., Dwivedi, Y. K., & Rashiti, S. (2022). Evaluating organizational level IT innovation adoption factors among global firms. *Journal of Innovation & Knowledge, 7*(3). https://doi.org/10.1016/j.jik.2022.100213

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alsheibani, S., Cheung, Y., & Messom, C. (2018). Artificial intelligence adoption: AI-readiness at firm-level. *PACIS 2018 Proceedings, 37*. https://aisel.aisnet.org/pacis2018/37

Ayre, J., & McCaffery, J. (2022). Research note: Thematic analysis in qualitative research. *Journal of Physiotherapy, 68*, 76–79. https://doi.org/10.1016/j.jphys.2021.11.010

Basheer, R., & Alkhabatib, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. Journal *of Computer Networks and Communications*, 2021. https://doi.org/10.1155/2021/1302999

Bawack, R. E., Fosso, W., Carillo, S., & André, K. D. (2021). A framework for understanding artificial intelligence research:

Insights from practice. *Journal of Enterprise Information Management, 34*(2), 645–678. https://doi.org/10.1108/JEIM-07-2020-0284

Berends, H., & Deken, F. (2019). Composing qualitative process research. *Strategic Organization, 19*(1), 134–146. https://doi.org/10.1177/1476127018824838

Braun, V., & Clarke, V. (2014). What can thematic analysis offer health and wellbeing researchers? *International Journal of Qualitative Studies on Health and Well-Being, 9*, 26152. https://doi.org/10.3402/qhw.v9.26152

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities of practice: Toward a unified view of working, learning, and innovation. *Organization Science, 2*(1), 40–57. https://doi.org/10.1287/orsc.2.1.40

Bunjak, A., Bruch, H., & Černe, M. (2022). Context is key: The joint roles of transformational and shared leadership and management innovation in predicting employee IT innovation adoption. *International Journal of Information Management, 66*, 102516. https://doi.org/10.1016/j.ijinfomgt.2022.102516

Chui, M., & Malhotra, S. (2018). *Notes from the AI frontier: AI adoption advances, but foundational barriers remain*. McKinsey Analytics.

Cobben, D., & Roijakkers, N. (2019). Dynamics of trust and control in innovation ecosystems. *Technological Forecasting and Social Change, 143*, 181–194. https://doi.org/10.1016/j.techfore.2019.03.013

Crossan, M. M., & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of Management Studies, 47*(6), 1154-1191. https://doi.org/10.1111/j.1467-6486.2009.00880.

Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. *Technology in Society, 62*. https://doi.org/10.1016/j.techsoc.2020.101257

Dalal Reeshad, S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology, 37*(1), 1–29. https://doi.org/10.1007/s10869-021-09723-4

Damanpour, F., & Schneider, M. (2006). Phases of the adoption of innovation in organizations: Effects of environment, organization, and top managers. *British Journal of Management, 17*(3), 215-236. https://doi.org/10.1111/j.1467-8551.2006.00498.x

Emmanuel-Avina, G., Gordon, S. P., Kittinger, R. B., Lakkaraju, K., & McCann, I. K. (2017). *Tailoring of cyber security technology adoption practices for operational adoption in complex organizations*. National Nuclear Security Administration. https://www.osti.gov/biblio/1596209

Ferlie, E., Fitzgerald, L., Wood, M., & Hawkins, C. (2005). The nonspread of innovations: The mediating role of professionals. *Academy of Management Journal, 48*(1), 117–134. https://doi.org/10.5465/amj.2005.15993150

Goel, S., & Nussbaum, B. (2021). Attribution across cyber attack types: Network intrusions and information operations. *IEEE Open Journal of the Communications Society, 2*, 1082. https://doi.org/10.1109/OJCOMS.2021.3085259

Harry, C., & Gallagher, N. (2018). Classifying cyber events: A proposed taxonomy. *Journal of Information Warfare, 17*(3), 17–31.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quarterly, 19*(4), 465–485. https://doi.org/10.2307/249630

Johnston, A. C. (2023). A closer look at organizational cybersecurity research: Trending topics and limitations. *Organizational Cybersecurity Journal: Practice, Process and People, 2*(2). https://doi.org/10.1108/OCJ-2023-0022

Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys, 53*(1), 1–34. https://doi.org/10.1145/3372823

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.05.003

Klein, K. J., & Sorra, J. S. (1996). The challenge of innovation implementation. *Academy of Management Review, 21*(4), 1055–1080. https://doi.org/10.5465/amr.1996.9704071863

Lewis, J. (2018). *Economic impact of cybercrime—No slowing down*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Li, L. C., Grimshaw, J. M., Nielsen, C., Judd, M., Coyte, P. C., & Graham, I. D. (2009). Evolution of Wenger's concept of community of practice. *Implementation Science, 4*(1), 11. https://doi.org/10.1186/1748-5908-4-11

Marotta, V., & Madnick, S. E. (2020). *Analyzing the interplay between regulatory compliance and cybersecurity*. In Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS-53).

Marshall, B., Poddar, A., Fontenot, R., & Cardon, P. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems, 54*(1), 11–22. https://doi.org/10.1080/08874417.2013.11645603

Oliver, C. (1991). Strategic responses to institutional processes. *The Academy of Management Review, 16*(1), 145–179. https://doi.org/10.5465/amr.1991.4279002

Pattison, S., Preece, D., & Dawson, P. (2016). In search of innovative capabilities of communities of practice: A systematic review and typology for future research. *Management Learning, 47*(5), 506–524. https://doi.org/10.1177/1350507616646698

Preis, B., & Susskind, L. (2022). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review, 58*(2), 614–629. https://doi.org/10.1177/1078087420973760

Rocha, I. F., & Kissimoto, K. O. (2022). Artificial intelligence and internet of things adoption in operations management: Barriers and benefits. *Revista De Administração Mackenzie, 23*(4), 1–30. https://doi.org/10.1590/1678-6971/eRAMR220119.en

Rogers, E. M. (2003). *Diffusion of innovations*. Free Press.

Rycroft, R. W., & Kash, D. E. (2000). Steering complex innovation. *Research-Technology Management, 43*(3), 18-23. https://doi.org/10.1080/08956308.2000.11671437

Sebastian, G. (2023). Do ChatGPT and other AI chatbots pose a cybersecurity risk? An exploratory study. International Journal of Security and *Privacy in Pervasive Computing (IJSPPC), 15*(1), 1–11. https://doi.org/10.4018/IJSPPC.320225

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2020). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 50*, 69-78. https://doi.org/10.1016/j.ijinfomgt.2019.05.002

Tidd, J. (2001). Innovation management in context: Environment, organization and performance. *International Journal of Management Reviews, 3*(3), 169–183. https://doi.org/10.1111/1468-2370.00062

van Oorschot, J. A. W. H., Hofman, E., & Halman, J. I. M. (2018). A bibliometric review of the innovation adoption literature. *Technological Forecasting and Social Change, 134*, 1–21. https://doi.org/10.1016/j.techfore.2018.04.032

Wenger, E. (1998). *Communities of practice: Learning as a social system. Systems Thinker*, 1–10. https://thesystemsthinker.com/communities-of-practice-learning-as-a-social-system

Wenger, E., McDermott, R., & Snyder, W. M. (2002). *Cultivating communities of practice: A guide to managing knowledge*. Harvard Business School.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access, 8*, 146598. https://doi.org/10.1109/ACCESS.2020.3012404

Xu, Z., Ge, Z., Wang, X., & Skare, M. (2021). Bibliometric analysis of technology adoption literature published from 1997 to 2020. *Technological Forecasting and Social Change, 170*, 120896. https://doi.org/10.1016/j.techfore.2021.120896

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Verizon. (2022). 2022 *Data breach investigations report. Verizon*. https://www.verizon.com/business/resources/reports/dbir/

Yin, R. K. (2003). *Case study research: Design and methods*. Sage.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access, 8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhang, M., Gable, G., & Tate, M. (2019). Overview of the multilevel research perspective: Implications for theory building and empirical research. *Communications of the Association for Information Systems, 45*(1), 1- 19. https://doi.org/10.17705/1CAIS.04501

Robert T. Anthony (rob.anthony@faculty.hult.edu)