MIS Quarterly

GUEST EDITORIAL

"COMPLEXITY IS THE WORST ENEMY OF SECURITY": STUDYING CYBERSECURITY THROUGH THE LENS OF ORGANIZATIONAL COMPLEXITY[1]

Bruce Schneier
Harvard Kennedy School, Harvard University, Cambridge, MA, U.S.A. {schneier@schneier.com}

Anthony Vance
Department of Business Information Technology, Pamplin College of Business, Virginia Tech
Blacksburg, VA, U.S.A. {anthony@vance.name}

Writing about computer systems twenty-five years ago, Schneier wrote that "the worst enemy of security is complexity" (Schneier, 1999), because complex systems are both easier to attack and harder to secure than simpler ones. In this essay, we provide an overview of Schneier's complexity principle and provide our observations of how two articles in this issue, Liang et al. (2025) and Tanriverdi et al. (2025), employed this principle in their research. We also offer our ideas for why complexity and cybersecurity are especially amenable for study in the field of information systems and where future research can go from here.

Keywords: Complexity theory, mergers and acquisitions, multihospital systems, data breaches, cybersecurity

Complexity and Cybersecurity

Complexity is inimical to security. As Schneier explained (2018, p. 197):

> *More complexity means more people involved, more parts, more interactions, more mistakes in the design and development process, more of everything where hidden insecurities can be found. Computer-security experts like to speak about the attack surface of a system: all the possible points an attacker might target and that must be secured. A complex system means a large attack surface. The defender has to secure the entire attack surface. The attacker just has to find one vulnerability—one unsecured avenue for attack—and gets to choose how and when to attack. It's simply not a fair battle.*

The underlying reasons for this are myriad (Schneier, 2000b). For example, more complex software means more lines of source code, which means more potential for software bugs.[2] Some of those bugs turn out to be vulnerabilities, and some of those vulnerabilities are exploitable.

Complexity also means more software modules, resulting in more potential interconnections and more potential for vulnerabilities. Complex systems are also more difficult to understand, analyze, and test, which also makes them harder to secure. The result of all these factors is that the software we use is filled with software vulnerabilities. These are the vulnerabilities that software vendors patch—either regularly or occasionally—when they release software updates. They are also the vulnerabilities that remain because the vendors don't have any effective mechanisms for patching the vulnerabilities that attackers discover and exploit. The U.S.

[1] This editorial is intended as a companion piece for the subsequent two papers in this issue: (1) "How Mergers and Acquisitions Increase Data Breaches: A Complexity Perspective" (Liang et al., 2025) and (2) "Taming Complexity in the Cybersecurity of Multihospital Systems: The Role of Enterprise-wide Data Analytics Platforms" (Tanriverdi et al., 2025).

[2] Many studies have tried to estimate how many bugs are in commercial software; estimates range from 1 to 25 per 1000 lines of code (McConnell, 2004). For reference, the current Linux kernel has 40 million lines of code (Palani, 2025).

Cybersecurity and Infrastructure Security Agency (CISA) has introduced projects like Secure by Design in an attempt to address this issue (CISA, 2023).

CISA's initiative demonstrates that the complexity principle is even more true today than it was in 1999. Software today is increasingly complex, due to things like the growth of the internet, mobile and cloud computing, the internet of things, and—most recently—generative AI. This does not necessarily mean that cybersecurity is worse today than it was two decades ago; there has been a steady stream of improvements in that field. But it does mean that we are in something of a Red Queen's Race: We lose ground even as we improve (Solé, 2022).

While these are all properties of software, the principle of complexity negatively impacting security is more general. It should also apply to organizations, which can be seen as complex hierarchical systems of human coordination (Simon, 1962; Anderson, 1999). This is the case because as organizations grow more complex, coordination costs within the organization increase (Zhou, 2011), identifying and requiring the accountability of responsible persons becomes more problematic (Lerner & Tetlock, 1999), understanding how different departments of the organizations interact becomes more difficult (Anderson, 1999), and tracking and maintaining organizational assets becomes more burdensome (Whyte et al., 2016). All of this complexity carries over to an organization's IT systems, making them harder to secure.

Although it seems logical that Schneier's complexity principle should generalize to organizations and their IT infrastructure in this way, this premise has largely gone untested. However, in this issue of *MIS Quarterly*, two articles provide convincing evidence for this effect (Liang et al., 2025; Tanriverdi et al., 2025). Both explicitly draw on Schneier's complexity principle, use complexity theory, and show through large panel datasets how organizational measures of complexity increase data breach risk. We provide our observations on both articles below.

Observations of Liang et al. (2025)

Mergers and acquisitions (M&As) are an essential strategy for firm growth; there were over 50,000 in 2024 alone (PwC 2025). At the same time, M&As can be enormously complex and difficult to successfully execute for both technical and managerial reasons (Aboagye-Darko et al., 2024). Given this complexity, security practitioners have long suspected that M&As increase vulnerability and security incidents (Goldstein et al., 2014). A notable example is the 2024 breach of Change Healthcare, which lost data for 190 million Americans and snarled insurance payments to health providers across the U.S. (Rundle, 2025). The initial point of compromise for this breach was attributed to the failure to implement multifactor authentication on a server as part of a technology upgrade process in connection with UnitedHealth Group's acquisition of Change Healthcare in 2022 (U.S. House Energy and Commerce Committee, 2024).

Tanriverdi et al. (2019) theorize that M&As increase data breach risk by increasing an organization's structural complexity, which they define as the number of new business units and the IT interlinkages among them. They found that the number of a firm's M&As in a given year significantly predicted the likelihood of a data breach the following year. However, they did not use complexity theory, nor did they operationalize complexity.

Liang et al. (2025) build on the work of Tanriverdi et al. (2019) by explicitly generalizing the complexity principle to M&As, using complexity theory. They examined an 18-year (2004-2021) panel of 5,072 public U.S. firms, comprising 61,209 firm years and 19,175 M&As. They found that the number of M&As of a firm in a year strongly predicts the number of data breaches experienced by the parent firm (or for both firms, if a merger), after considering control variables.

Both Tanriverdi et al. (2019) and Liang et al. (2025) give different explanations for the source of complexity in M&As that contributes to data breach risk. Both theorize that the M&A process requires many technical changes and, according to the nonlinearity property of complexity, even small changes can have large and unexpected consequences. Both also point to complexity that results in changes to business processes and employee roles. Ultimately, however, neither Liang et al. nor Tanriverdi et al. test these assumptions directly; rather, they use a count of the number of M&As in a given year as a proxy for the underlying complexity involved.

Liang et al. (2025) also use matching theory (Mitsuhashi & Greve, 2009) to theorize that the effect of M&As on data breaches is amplified by the organizational diversity of the merged or acquired firm. They operationalize organizational diversity by the business domain, firm size, and type of strategy that the merger represents (same or different business domain). The reasoning is that the greater the dissimilarity, the more effort will be required to integrate the organizational processes, practices, and IT systems of the two firms. They found that the greater the diversity in these dimensions, the greater the likelihood that an M&A will result in a data breach.

Liang et al.'s (2025) use of diversity to augment predictions of complexity is at once innovative and appropriate, given that diversity and complexity are understood to be closely related concepts in a wide range of fields (Page, 2011). Therefore,

their findings should be properly seen not as an extension of the complexity principle but as another example of its effects. Although Schneier and coauthors have argued for the dangers of firms operating an IT monoculture in which all systems are the same and thus can be exploited simultaneously through the same vulnerabilities (Greer et al., 2003), it is also true that some forms of diversity can also lead to risk because diverse components are harder to integrate and manage and thus also are more difficult to collectively understand and secure.

Finally, Liang et al. (2025) argue that publicity of a firm's M&A will increase the likelihood of an M&A leading to a data breach. To make this prediction, they use routine activity theory from criminology (Cohen & Felson, 1979), which explains that more visible targets face a greater risk of attack. This is not an extension of the complexity principle—at least, not directly. Yet, as Liang et al. point out, research suggests that attackers specifically target firms involved with M&As because they recognize the vulnerabilities that come from the complexities involved (Meyrick et al., 2020). Therefore, the moderating influence of publicity in this case can be seen as a secondary effect of complexity.

Observations of Tanriverdi et al. (2025) ■

Tanriverdi et al. (2025) examine Schneier's complexity principle in the context of multihospital systems (MHSs), which are interconnected hospitals that share patient data through a shared IT system. They found that as forms of complexity related to service, health IT, and governance increase, so does the risk of the MHS suffering a data breach. They also found that MHSs' use of enterprise-wide data analytics platforms (EWDAPs)—which they define as "common, enterprise-wide data warehouse and analytics platforms for enabling patient data sharing, integration, and analyses among member hospitals" (Tanriverdi et al., 2025)—decrease the likelihood of a data breach.

Following complexity theory, Tanriverdi et al. (2025) differentiate between *complicatedness* and *complexity*. Within complicated systems, interconnections between system components are linear and well-structured. In contrast, within complex systems, interconnections can be ad hoc, nonlinear, and tightly coupled, making understanding the overall system more difficult. They further conceptualize three different sources of complexity: service complicatedness, health IT complicatedness, and governance complicatedness. *Service complicatedness* is conceptualized as the extent to which a single hospital refers patients to other members of the MHS for needed services. *Health IT complicatedness* is the number of unique IT systems that a hospital uses compared to other members of the MHS. *Governance complicatedness* is the extent to which the MHS decentralizes decisions such as medical services to member hospitals.

Additionally, Tanriverdi et al. (2025) argue that:

> *Practitioners often use "complicated" and "complex" interchangeably to refer to systems that are made up of a large number of interconnected components. According to complexity science, a large number of interconnected components are necessary but not sufficient for distinguishing whether a system is complicated or complex. The nature of interactions among the interconnected components should also be examined (Dekker et al., 2013). In a complicated system, interactions among the interconnected components are linear and well-structured. Such interaction characteristics allow for the analysis, testing, and understanding of cybersecurity risks, vulnerabilities, and controls (Dekker et al., 2013; Page, 2009). Although these activities are challenging, as explained by Schneier (1999, 2000), ultimately, they are feasible. On the other hand, in a complex system, interactions are ad hoc and nonlinear. These interaction features make it infeasible to fully analyze, test, understand, and control system-level cybersecurity behaviors and outcomes of a complex system (Cilliers, 1998; Tanriverdi & Du, 2020).*

Tanriverdi et al. (2025) are correct that complexity is not simply a function of the number of interconnected components. It's also how they are interconnected. Schneier similarly observed that insecurity comes from nonlinear, tightly coupled systems (Schneier, 2008):

> *The single biggest threat is the technology itself. Technological systems, especially newer ones, are exceedingly complex—and complexity is the worst enemy of security. This is true for a number of reasons. One is that in our rush to build new systems, we generally ignore security or only pay attention to it at the last minute. But the other is that complex systems, especially non-linear and tightly coupled systems, are naturally less secure.*[3]

However, there are additional distinctions of complexity beyond complicatedness and complexity. Researchers in the field of complexity science arrange systems in order of increasing complexity: simple, complicated, complex, and

[3] This point about nonlinearity and tight coupling was first made by Charles Perrow in his book *Normal Accidents* (1984).

chaotic[4] (Snowden & Boone, 2007). Furthermore, although it may be infeasible to fully understand complex systems as Tanriverdi et al. argue, the contributions of the field of complexity science and complex systems theory are enabling us to comprehend complex systems to an increasing degree. In fact, complexity scientists have even begun to understand chaotic systems (e.g., Skiadas & Skiadas, 2017). Regardless, as it relates to the complexity principle, all types of complexity described by complexity theory are potentially bad for security, with each level being progressively more treacherous.

Another interesting finding of Tanriverdi et al. (2025) is that EWDAPs introduce a "beneficial" form of complexity that can actually reduce overall security risk to the MHS. They explain:

> *[EWDAPs] can elevate IT complexity by introducing additional technologies, interconnections, and dependencies. Counterintuitively, however, this represents a beneficial type of IT complexity that reduces cybersecurity breaches … by strengthening process controls … and reducing external cybersecurity breaches … These results provide more nuanced insights into the relationship between IT complexity and cybersecurity than are currently assumed in practice (Schneier, 2015) and academia (Liang et al., 2025).*

In other words, Tanriverdi et al. (2025) argue against the assumption that all complexity is bad for security on the basis of their finding that MHSs' use of EWDAPs reduces the risk of data breaches. However, most technological complexity is "good" in the sense that it provides useful capabilities. The late 1990s Windows NT operating system is far less complex—only 11 million lines of code—than the Windows 11 operating system of 2025 and therefore easier to understand and secure. However, no business would be willing to give up the capabilities of modern versions of Windows.

In the same way, EWDAPs provide increased structure and control in data exchanges, thus reducing data breaches. However, this finding alone does not negate the principle that complexity is the enemy of security. Indeed, in an analysis of how EWDAPs affect various control weaknesses, Tanriverdi et al. (2025) found that the use of an EWDAP reduces process control weakness, but "amplifies the technical and people control weaknesses created by health IT complicatedness" and significantly increases internal breaches. This finding illustrates that although complexity may provide expected benefits most of the time, the potential for unexpected vulnerabilities is still unavoidable.

Where Complexity Research in Cybersecurity Can Go from Here

Liang et al. (2025) and Tanriverdi et al. (2025) show the potential for complexity as a lens to understand security issues as well as demonstrate its application at the organizational level. They also make clear that more research is needed to understand how complexity in its many forms negatively impacts security.

For example, both Liang et al. (2025) and Tanriverdi et al. (2025) use large panel datasets to predict data breaches, using measures of complexity. While valuable, a consequence of this approach is a reliance on proxies of complexity measures (e.g., the number of M&As for a firm in a year or the number of medical services a hospital offers under referral), rather than observing complexity within an organization itself. We see an opportunity for future field research—both quantitative and qualitative—to improve the understanding of how technical and organizational complexity leads to cybersecurity risk. For example, it would be interesting to quantify complexity in a system. As mentioned previously, complexity typically brings benefits as well as potential risks. Future research could attempt to identify an optimum level of complexity that strikes a balance between benefits and risk.

Another opportunity for future research would be to examine how human behavior contributes to organizations' overall complexity. Human behavior is emergent and can interact with technical systems in unforeseen ways. For example, individuals' use of shadow IT, workarounds, and other misuse of systems can add complexity to IT environments and, through the property of nonlinearity, may result in outsized consequences for cybersecurity.

At the organizational level, organizational complexity involves an organization's structure, management bureaucracy, and relationships with individual and institutional stakeholders. Third-party vendors can also increase organizational complexity by increasing the number of contractual relationships and requiring the integration of vendors' people, practices, and software—which may be poorly understood—with those of the organization. The tracking of hardware and software assets in an organization can be surprisingly complex, as management must coordinate across organizational departments, divisions, and international offices to ensure that assets are secured and kept up to date.

[4] We generally try to rely on systems one level down to control systems of that level. That is, we try to implement complicated systems to control complex systems, and complex systems to control chaotic systems. This has obvious problems.

Theoretically, although complexity theory has been used to study cybersecurity in other fields (e.g., Becote & Rimal, 2023; Brantly, 2019) and various problems in IS (e.g., Merali, 2006; Vessey & Ward, 2013; Park & Mithas, 2020), little IS research has examined security through the lens of complexity. Given the strong implications outlined in this article of complexity affecting security, there is a need to develop IS theories of cybersecurity and complexity that integrate the human, technology, and organizational domains.

These research directions correspond well to the definition of information systems as being "at the confluence of people, organizations, and technology" (Hevner et al., 2004, p. 77). It may be argued that this definition is inherently about the complexity involved in the interaction of these three components. Therefore, information systems, as a field, is uniquely suited to understand complexity in all of its manifestations as well as its implications for cybersecurity.

Conclusion

Schneier (2000a, p. 354) wrote: "Complexity is the worst enemy of security. This has been true since the beginning of computers, and is likely to be true for the foreseeable future. And as cyberspace continues to get more complex, it will continue to get less secure." We similarly expect that as organizations and their use of IT continue to become more complex, their inherent cybersecurity risk will also increase. In this essay, we explain why this is the case for information systems broadly, considering people, IT systems, and organizations together. The next two articles in this issue—Liang et al. (2025) and Tanriverdi et al. (2025)—illustrate the value of using complexity as a lens to better understand cybersecurity problems. We call on scholars to continue to use and test this approach on a range of cybersecurity issues.

References

Aboagye-Darko, D., Attuquayefio, S. N. B., Ankomah, N., Okronipa, A. Q., & Nyame, J. Y. (2024). Information systems research on mergers and acquisitions: a systematic literature review. *Kybernetes, 53*(12), 5560-5581. https://doi.org/10.1108/K-05-2023-0763

Anderson, P. (1999). Perspective: Complexity theory and organization science. *Organization Science, 10*(3), 216-232. https://doi.org/10.1287/orsc.10.3.216

Becote, B., & Rimal, B. P. (2023). Complexity science and cyber operations: A literature survey. *Complex System Modeling and Simulation, 3*(4), 327-342. https://doi.org/10.23919/CSMS.2023.0018

Brantly, A. F. (2019). Conceptualizing cyber policy through complexity theory. *Journal of Cyber Policy, 4*(2), 275-289. https://doi.org/10.1080/23738871.2019.1583763

CISA. (2023). Secure-by-design. https://www.cisa.gov/resources-tools/resources/secure-by-design

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Goldstein, M., Perlroth, N., & Corkery, M. (2014). Neglected server provided entry for JPMorgan hackers. *The New York Times*. https://archive.nytimes.com/dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/

Greer, D., Pfleeger, C., Schneier, B., Quarterman, J., Metzger, P., Bace, R., & Gutmann, P. (2003). *CyberInsecurity: The cost of monopoly* Computer & Communications Industry Association. https://ccianet.org/wp-content/uploads/2003/09/cyberinsecurity%20the%20cost%20of%20monopoly.pdf

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Liang, H., Srinivas, S., & Xue, Y. (2025). How mergers and acquisitions increase data breaches: A complexity perspective. *MIS Quarterly*. Advance online publication. https://doi.org/10.25300/MISQ/2023/17703

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. *Psychological Bulletin, 125*(2), 255-275. https://doi.org/10.1037/0033-2909.125.2.255

Merali, Y. (2006). Complexity and information systems: The emergent domain. *Journal of Information Technology, 21*(4), Article 2. https://doi.org/10.1057/palgrave.jit.2000081

McConnell, S. (2004). *Code complete*. Pearson Education.

Meyrick, J., Gomes, J., Coleman, N., & Getty, S. (2020). *Assessing cyber risk in M&A.* IBM. https://www.ibm.com/downloads/cas/RJX5MXJD

Mitsuhashi, H., & Greve, H. R. (2009). A matching theory of alliance formation and organizational success: Complementarity and compatibility. *Academy of Management Journal, 52*(5), 975-995. https://doi.org/10.5465/amj.2009.44634482

Page, S. (2011). *Diversity and Complexity*. Princeton University Press. https://doi.org/10.1515/9781400835140

Palani, S. (2025). *Linux kernel source code surpasses 40 million lines*. OSTechNix. https://ostechnix.com/linux-kernel-source-code-surpasses-40-million-lines/

Park, Y., & Mithas, S. (2020). Organized complexity of digital business strategy: A configurational perspective. *MIS Quarterly, 44*(1), 85-127. https://doi.org/10.25300/MISQ/2020/14477

Perrow, C. (1984). *Normal accidents: Living with high risk technologies*. Princeton University Press.

PwC. (2025). *Global M&A industry trends.* https://www.pwc.com/gx/en/services/deals/trends.html

Rundle, J. (2025). UnitedHealth estimates change healthcare hack impacted about 190 million people. *The Wall Street Journal* https://www.wsj.com/articles/unitedhealth-estimates-change-healthcare-hack-impacted-about-190-million-people-9564533c

Simon, H. A. (1977). The organization of complex systems. In H. A. Simon (Ed.), *Models of discovery* (pp. 245-261). Springer https://doi.org/10.1007/978-94-010-9521-1_14

Schneier, B. (1999). A plea for simplicity. Schneier on Security. https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

Schneier, B. (2000a). *Secrets and lies: Digital security in a networked world.* Wiley. https://doi.org/10.1002/9781119183631

Schneier, B. (2000b). *Software complexity and security*. Schneier on Security. https://www.schneier.com/crypto-gram/archives/2000/0315.html#8

Schneier, B. (2008). *Bruce Schneier: Securing Your PC and Your Privacy.* Datamation. https://www.datamation.com/security/bruce-schneier-securing-your-pc-and-your-privacy/

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W.W. Norton & Company.

Simon, H. A. (1962). The architecture of complexity. *Proceedings of the American Philosophical Society, 106*(6), 467-482. https://www.jstor.org/stable/985254

Skiadas, C. H., & Skiadas, C. (Eds.). (2017). *Handbook of applications of chaos theory*. CRC Press. https://doi.org/10.1201/b20232

Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. *Harvard Business Review*. https://hbr.org/2007/11/a-leaders-framework-for-decision-making

Solé, R. (2022). Revisiting Leigh Van Valen's "A New Evolutionary Law" (1973). Biological Theory, *17*, 120-125. https://doi.org/10.1007/s13752-021-00391-w

Tanriverdi, H., Roumani, Y., and Nwankpa, J. (2019). Structural Complexity and Data Breach Risk. International Conference on Information Systems (ICIS) Proceedings. 36.

Tanriverdi, H., Kwon, J., & Im, G. (2025). Taming complexity in the cybersecurity of multihospital systems: The role of enterprise-wide data analytics platforms. *MIS Quarterly*. Advance online publication. https://doi.org/10.25300/MISQ/2024/17752

U.S. House Energy and Commerce Committee. (2024). *What we learned: Change healthcare cyber attack.* https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack

Vessey, I., & Ward, K. (2013). The dynamics of sustainable IS alignment: The case for IS adaptivity. *Journal of the Association for Information Systems, 14*(6), 283-311. https://doi.org/10.17705/1jais.00336

Whyte, J., Stasis, A., & Lindkvist, C. (2016). Managing change in the delivery of complex projects: Configuration management, asset information and "big data." *International Journal of Project Management, 34*(2), 339-351. https://doi.org/10.1016/j.ijproman.2015.02.006

Zhou, Y. M. (2011), Synergy, coordination costs, and diversification choices. *Strategic Management Journal, 32*, 624-639. https://doi.org/10.1002/smj.889

About the Authors

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by *The Economist*. He is the author of over one dozen books—including his latest, *A Hacker's Mind*—as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and his blog "Schneier on Security" are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University, a Lecturer in Public Policy at the Harvard Kennedy School, a board member of the Electronic Frontier Foundation and AccessNow, and an Advisory Board Member of the Electronic Privacy Information Center and VerifiedVoting.org. He is the chief of security architecture at Inrupt, Inc.

Anthony Vance is the Lenz Professor and Commonwealth Cyber Initiative Fellow in Business Information Technology at the Pamplin College of Business at Virginia Tech. He has earned Ph.D. degrees in information systems from Georgia State University, the University of Paris-Dauphine, France, and the University of Oulu, Finland. His work has been published in outlets such as *Information Systems Research*, *Journal of the Association for Information Systems*, *Journal of Management Information Systems*, *Management Science*, and *MIS Quarterly*, as well as in the proceedings of conferences such as the ACM Conference on Human Factors in Computing Systems (CHI) and the USENIX Symposium on Usable Privacy and Security (SOUPS). His research focuses on behavioral, neuroscience, and organizational approaches to cybersecurity. He is currently a senior editor at *MIS Quarterly*.