MIS Quarterly Executive

Volume 25 | Issue 3 Article 7

August 2026

Insights from Simulation Exercises on Strengthening Cyber Risk Governance

Sander Zeijlemaker

Jeffrey G. Proudfoot

Ranjan Pal

Michael Siegel

Follow this and additional works at: https://aisel.aisnet.org/misqe

Recommended Citation
Zeijlemaker, Sander; Proudfoot, Jeffrey G.; Pal, Ranjan; and Siegel, Michael (2026) "Insights from Simulation Exercises on Strengthening Cyber Risk Governance," *MIS Quarterly Executive*: Vol. 25: Iss. 3, Article 7.
Available at: https://aisel.aisnet.org/misqe/vol25/iss3/7

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in MIS Quarterly Executive by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

MIS Quarterly Executive

Insights from Simulation Exercises on Strengthening Cyber Risk Governance

Cyber risk is now a board-level governance challenge, as increasingly sophisticated threats undermine organizations' ability to balance resilience and business performance. Drawing on more than 1,800 simulation exercises and executive interviews, we find that decision quality declines sharply as threat complexity increases. We identify four managerial heuristics for strengthening cyber resilience: faster adaptation, iterative learning, business-wide responsibility for managing cyber risk and proactively building capabilities. These findings suggest that effective cyber risk governance depends less on technology than on maintaining decision quality under uncertainty.[1]

Sander Zeijlemaker
Massachusetts Institute of Technology (U.S.)

Jeffrey G. Proudfoot
Bentley University and Massachusetts Institute of Technology (U.S.)

Ranjan Pal
MIT Sloan School of Management (U.S.)

Michael Siegel
MIT Sloan School of Management (U.S.)

Cyber Risk Governance Faces Significant Challenges

Cyber risk has transformed from a purely technical issue into a core business and governance challenge. Though cyberattacks once affected isolated systems through simple attack vectors, organizations today face an estimated 9.3%[2] annual probability of experiencing a cyber incident, with average recovery costs of approximately $4.8 million.[3] Modern attacks have become increasingly sophisticated, leveraging tactics such as ransomware, lateral movement and privilege escalation to spread rapidly across interconnected technology environments. The emergence of adversarial artificial intelligence (AI) is expected to further accelerate this trend,[4] reducing the time required to identify and exploit vulnerabilities from hours to near machine speed.[5] Simultaneously, global cybercrime costs are projected to exceed $1 trillion per month by 2031.[6]

The implications extend far beyond technological failure. Cyber incidents can quickly escalate into enterprise-wide crises, causing operational disruptions, reputational damage,

1 Blake Ives is the senior accepting editor for this MISQE Insight.
2 *Information Risk Insights Study 2025,* Cyentia Institute, 2025, available at https://www.cyentia.com/iris2025.
3 *Cost of Data Breach Report 2025,* IBM, 2025, available at https://www.ibm.com/reports/data-breach.
4 Zeijlemaker, S., Lemiesa, Y. K., Schröer, S. L., Abhishta, A. and Siegel, M. "How Does AI Transform Cyber Risk Management?" *Systems* (13:10), October 2025, p. 835.
5 *Zero Day Clock,* Zero Day Clock (n.d.), available at https://zerodayclock.com.
6 Morgan, S. *Official 2026 Cybersecurity Market Report: Predictions and Statistics,* Cybersecurity Ventures, November 14, 2025, available at https://cybersecurityventures.com/official-2026-cybersecurity-market-report-predictions-and-statistics.

regulatory sanctions, legal liabilities and erosion of stakeholder trust. As a consequence, regulators and industry frameworks increasingly emphasize cyber resilience as a board-level accountability.[7] Cybersecurity can no longer be treated as a specialized IT responsibility; it has become a central component of enterprise risk management and organizational continuity.

This fundamentally transforms the role of executive leadership. Though cybersecurity controls are implemented at the operational level, an organization's resilience is largely determined by strategic choices regarding governance, investment priorities, risk appetite, organizational structure and culture. Boards and executives must continuously balance resilience, compliance, operational efficiency and long-term value creation amid persistent uncertainty.

Our findings suggest that the central challenge of cyber risk governance lies not only in technological vulnerabilities but also in maintaining decision quality within increasingly complex and adversarial environments. Many governance mechanisms, including annual planning cycles, static investment roadmaps, periodic audits and retrospective risk assessments, were designed for conditions where risks evolved gradually and predictably. In contrast, cyber risk is dynamic, adaptive and interconnected, continuously reshaping the relationship among risk, investment and organizational resilience. Organizations thus face a growing disconnect between traditional governance processes and the evolving realities of cyber risk.

Organizations employ various methods to manage cyber risk. Tabletop exercises, in the form of simulation-based training tools,[8] allow leaders to rehearse incident responses but typically focus on decisions made after systems have already been compromised. For pre-incident cyber risk governance, organizations have traditionally relied on security assessments, benchmarking, consultant advice and post-breach investment adjustments. Though these approaches provide valuable insights, they often offer limited opportunities for leaders to evaluate how strategic cyber risk decisions perform under changing threat conditions.

Drawing on 1,800 simulation exercises involving 240 participants, as well as interviews with 12 Fortune 100 board members, we examine how organizations govern cyber risk under conditions of uncertainty. Across both datasets, failures rarely stemmed from technology alone; rather, they emerged when organizations were unable to adapt their decision-making processes to increasing complexity and uncertainty. Our contribution is not to propose a new cybersecurity framework, but to explain why organizations struggle to make effective cyber risk decisions as threat environments become increasingly complex. From these observations, we derive four managerial heuristics (i.e., rules of thumb) associated with more effective cyber risk governance: 1) continuous adaptation, 2) iterative learning, 3) business-wide responsibility, and 4) proactive capability development.

Strategic Digital Twins Provide "Flight Simulators" for Cyber Risk

Executives will never deliberately subject their organization to a test of a risky cyber strategy because the consequences of failure are simply too severe. This creates a fundamental dilemma: Leaders are expected to make high-impact cyber investment decisions without safely experiencing their long-term consequences before facing them in reality. Strategic digital twins[9] address this problem by creating a virtual replica of the executive decision environment, allowing organizations to experiment, fail, adapt and learn without jeopardizing the real enterprise. Through calibration, alignment with organizational data and back-testing against historical scenarios, these simulation games can

7 Examples of this regulatory landscape include the EU's Network and Information Security Directive (NIS2), the U.S. Securities and Exchange Commission's Cybersecurity Rules and the World Economic Forum's Cyber Risk Governance Principles.

8 For more information about cybersecurity tabletop exercises, see Crandford, J. J. "Tabletop Exercises Explained," CrowdStrike, October 24, 2024, available at https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/tabletop-exercise.

9 Zeijlemaker, S. "Strengthening Cyber Risk Management and Oversight through Digital Twin Technology and Simulation Gaming," *Security Insight*, October 21, 2024, available at https://securityinsight.nl/article-alert/strengthening-cyber-risk-management-and-oversight-through-digital-twin-technology-and-simulation-gaming.

achieve a high degree of strategic realism.[10] If the strategy fails, executives can simply restart the simulation rather than having to recover the company.

The strategic digital twin concept is based on the same principles used in flight simulators, where pilots rehearse complex emergencies in a controlled environment before encountering them in real flight. In a flight simulator, the value lies in making decisions under realistic pressure, responding to equipment failures, changing weather, incomplete information and cascading consequences without endangering passengers or aircraft. Similarly, a strategic digital twin places executives in realistic cyber crisis scenarios that move beyond abstract theory, compelling them to practice judgment, coordination, communication and prioritization as conditions evolve. By observing the outcomes of each strategic decision, leaders can build the same kind of readiness that pilots achieve through repeated simulation.

In our simulation games (for more information, see the Appendix), decision makers had to balance three competing objectives over five rounds, each representing one year of decision-making: 1) allocate limited budgets across prevention, detection, response and recovery capabilities; 2) maximize financial performance, measured by accumulated profit; and 3) maintain cyber resilience by limiting the number of compromised systems[11] (used as a proxy for risk). The simulations highlighted a core governance dilemma: Prioritizing one objective often undermines another. Decision makers must therefore find the optimal balance based on their organization's unique strategic priorities.

Though most simulation participants understood the cyber risk conceptually, many struggled to translate that understanding into resilient strategic actions under pressure. In the following section, we introduce four heuristics derived from participant performance in the simulations that help explain why organizations continue to underperform in managing cyber risk despite increasing awareness and investment.[12]

Four Managerial Heuristics Essential for Governing Cyber Risk

Our simulations and interviews identified four managerial heuristics for improving cyber risk governance: 1) adapt faster than the evolving threat landscape; 2) learn through iteration, not optimization; 3) make cyber risk management a business-wide responsibility; and 4) proactively build capabilities before you need them. These heuristics emerged from recurring patterns across simulation outcomes, participant debriefings, executive interviews and board-level discussions, and were reinforced through sensitivity analyses of alternative threat and investment scenarios. Though each heuristic addresses a different aspect of cyber resilience, together they highlight a common governance challenge: maintaining decision quality as cyber threats become increasingly complex and uncertain. The consistency of these patterns across multiple sources of evidence suggests that the insights extend beyond the simulation environment and reflect broader organizational challenges in practice.

Adapt Faster Than the Evolving Threat Environment

Many organizations still approach cybersecurity as a long-term optimization problem: defining a strategy, investing in controls and periodically updating the roadmap. Our findings, however, suggest that this approach is fundamentally flawed. Static cyber strategies fail against adaptive threats. Cyber threats evolve faster than traditional planning cycles, rendering even well-designed security approaches obsolete within short periods. Cyber resilience therefore depends less on having a "good strategy" and more on maintaining the ability to continuously adapt under pressure.

10 Zeijlemaker, S. and Siegel, M. "Capturing the Dynamic Nature of Cyber Risk: Evidence from an Explorative Case Study," *Proceedings of Hawaii International Conference on System Sciences,* January 2023.

11 These foundational cybersecurity principles are inspired by the capabilities featured in prominent cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) cybersecurity framework, Centre for Internet Security Control (CIS) and International Organization for Standardization (ISO) 2700X series.

12 90% of participants reported the simulations to be very relevant to their day-to-day cyber risk management activities.

A board member of a finance and insurance company summarized this reality bluntly: "Cybercrime is very successful. It's really just about putting out the fires. We have no idea who these arsonists are or how to stop them."

The ransomware crisis at The Clorox Company in 2024 illustrates this challenge.[13] Despite substantial cybersecurity investments and industry recognition, the company still suffered severe operational disruption following the attack. The lesson is sobering: past cybersecurity successes may create a false sense of resilience.

Our simulation results reinforce this concern. In 75% of the simulations, cybersecurity approaches that were effective against routine threats failed against sophisticated attacks such as ransomware, privilege escalation and lateral movement. Organizations relying primarily on reactive responses, including ransom payments, consistently underperformed. In contrast, those investing in anomaly detection, network segmentation and rapid recovery mechanisms achieved stronger financial outcomes and lower systemic risk.

Another important insight was that even effective cybersecurity approaches deteriorate rapidly when investment timing or resource allocation deviates from evolving threat conditions. Small delays or underinvestment often resulted in disproportionate increases in organizational exposure. This helps explain why many organizations appear secure until the moment they suddenly are not.

Cyber resilience should not be treated as a stable end-state achieved through periodic investments or static long-term plans. The critical question is no longer whether organizations have a cybersecurity strategy, but whether they can adapt faster than the adversaries targeting them.

Boards and executives should strengthen managerial foresight by regularly challenging whether current cybersecurity strategies would remain effective under alternative future threat scenarios. Tools such as Monte Carlo analyses, strategic digital twins and simulated attacker-defender exercises[14] allow leaders to explore uncertainties, test strategic assumptions and evaluate the potential consequences of decisions before they occur. Rather than relying solely on periodic reviews or historical performance, organizations should use these approaches to identify conditions under which existing strategies may fail, assess resilience amid changing threat environments and adjust strategic priorities proactively to prevent vulnerabilities from escalating into crises.

Learn Through Iteration, Not Optimization

Organizations often assume that stronger cybersecurity outcomes depend primarily on better planning rather than on adaptive organizational resilience.[15] However, our findings suggest the opposite: Under conditions of uncertainty, cyber resilience emerges through iterative learning rather than static optimization. The challenge is that executives rarely have the opportunity to safely learn from failure before facing real-world consequences. A board member of an education business succinctly summarized this tension: "We have spent disproportionate economic and personnel effort in the last five years trying to address all the penetration opportunities and capabilities."

Faced with evolving threats, organizations frequently oscillate between overinvesting in cybersecurity controls and underinvesting, leaving themselves dangerously exposed. In our simulation games, increasing threat complexity sharply reduced the number of participants achieving strong risk-performance outcomes, dropping from 42% to 16% (see Figure 1). Participants increasingly drifted toward two extremes: excessive investment accompanied by declining business performance, or insufficient investment combined with high cyber exposure.

The most important finding was not merely that participants improved with repetition but that repeated experimentation improved

13 Coleman, J. "Clorox CEO Describes Comeback Process After Massive Cyberattack," *CNBC*, October 31, 2024, available at https://www.cnbc.com/2024/10/31/clorox-ceo-describes-comeback-process-after-massive-cyberattack.html.

14 Siegel, M. *Three Key Ways to Make Supply Chains More Resilient to Cyber Risks,* World Economic Forum, April 23, 2025, available at https://www.weforum.org/stories/2025/04/three-key-directions-for-the-cyber-resiliency-crisis-in-global-supply-chains.

15 Tsen, E., Ko, R. K. L. and Slapničar, S. "The Effect of Organizational Cyber Resilience on Cyber Incident Outcomes," *Journal of Cybersecurity* (11:1), December 2025, pp. 1-15.

Figure 1: Complexity Hampers Cyber Risk Management Investment Optimization

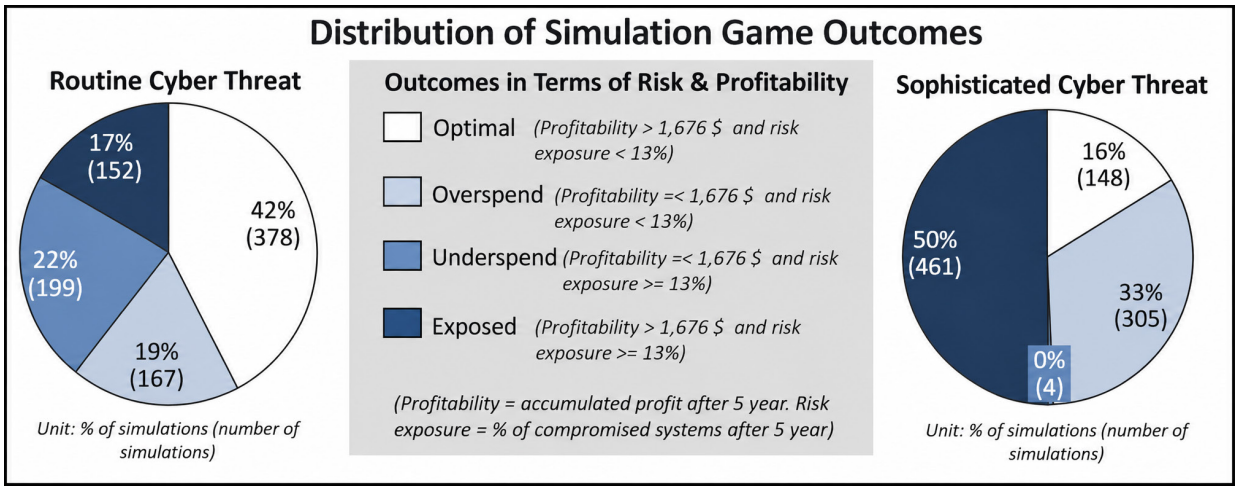
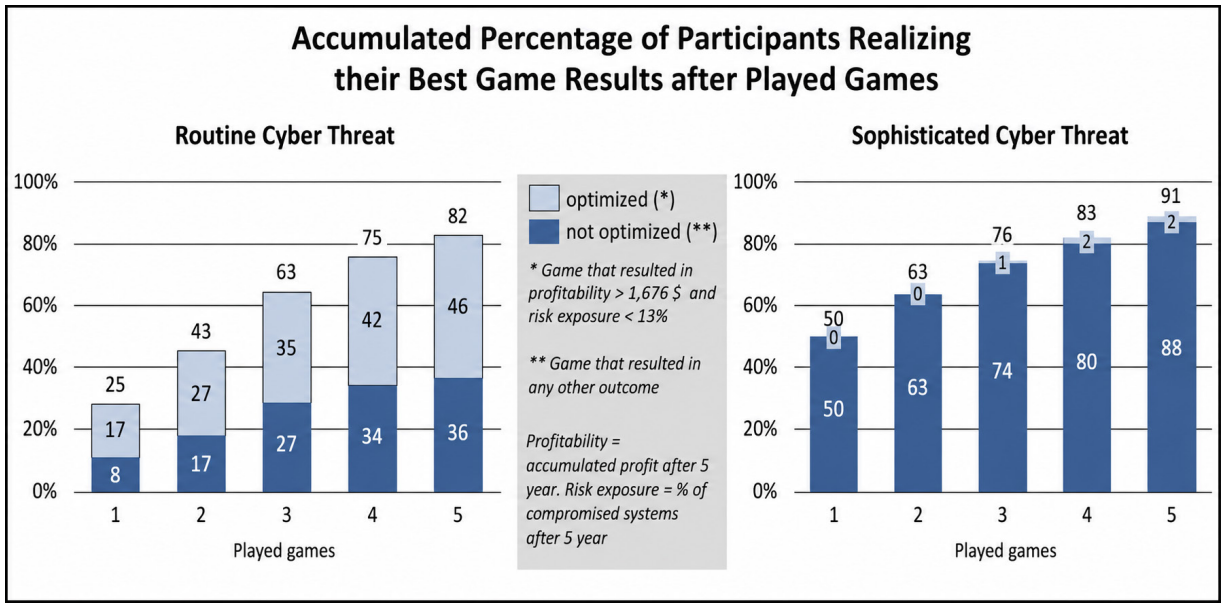


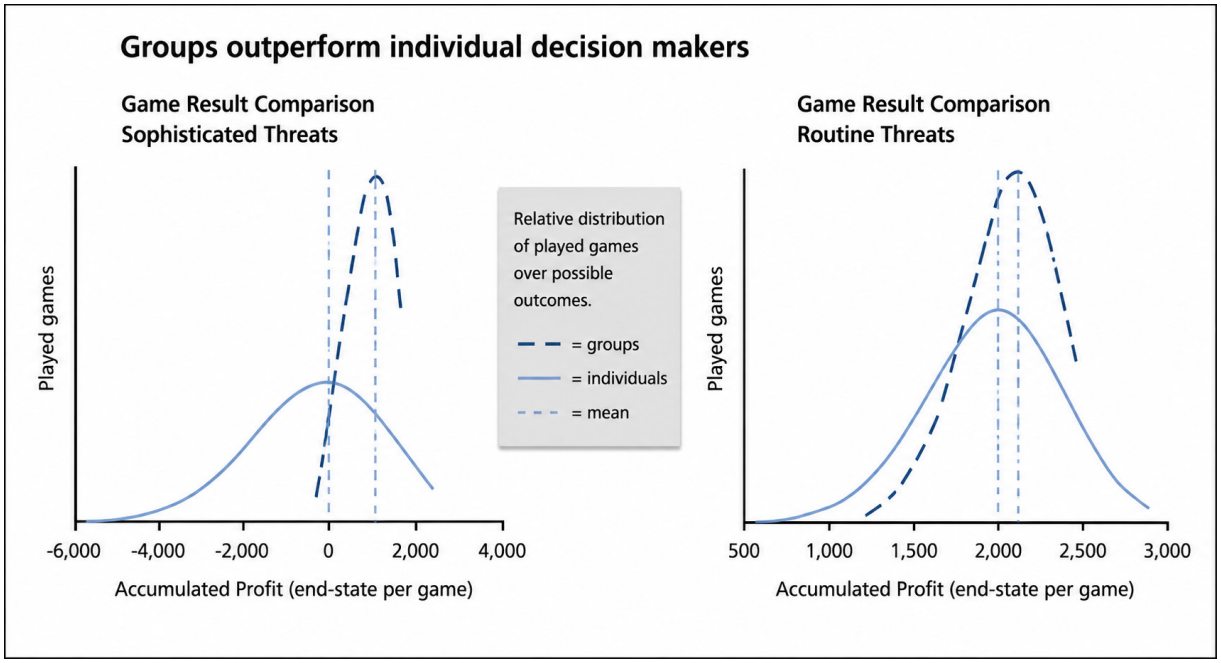
Figure 2: Learning Effects Under Uncertainty



decision quality in complex situations. Figure 2 shows that participants became more adept at balancing cyber resilience and business performance as they gained experience navigating uncertain and evolving threat environments. However, even after multiple simulation rounds, only a limited number of participants achieved optimized outcomes under sophisticated threats. This implies that learning does not eliminate the challenge but helps organizations adapt to it. The implication is that cyber resilience depends less on identifying a perfect strategy and more on developing organizational learning capabilities that enable better decision-making as conditions evolve.

This finding carries important implications for the executive governance of cyber risks. Annual reviews and static cyber roadmaps are ill-suited to counter adversaries who continuously evolve their tactics and accelerate attack speeds. Organizations should approach cyber resilience as a continuous learning capability rather

Figure 3: Groups Outperform Individuals when Combating Cyber Threats



than a one-off or periodic compliance exercise. Simulations and crisis exercises[16] are valuable not because they yield perfect strategies but because they expose leaders to the consequences of strategic failure before such failures occur in reality. Organizations that regularly challenge assumptions, evaluate trade-offs and learn from simulated failures are better positioned to adapt as threat conditions evolve.

Make Cyber Risk Management a Business-Wide Responsibility

Many organizations still view cybersecurity as a specialized technical function managed primarily by IT and security experts.[17] Our findings suggest that this approach has become increasingly perilous. Cyber risks rarely originate from technology alone; they arise from the interplay between technology, operations, supply chains, customer ecosystems, regulations and financial trade-offs. Organizations that continue to manage cyber risks through isolated technical silos may inadvertently amplify systemic exposure rather than mitigate it.

The CEO of a logistics and industrial organization explained that cyber risk management needs to evolve beyond relying solely on technical metrics: "We had to quantify each risk. We had to categorize it, we had to tie it to business outcomes—the dollar impact, profitability and customer service implications." Another executive, the chief quality manager of a healthcare business, emphasized that organizational exposure increasingly extends beyond direct technological control: "When a customer uses an app alongside a medical device, even if it's not our app, we bear responsibility for its interaction with our product."

Cyber resilience increasingly depends on managing risks across interconnected business ecosystems rather than solely within organizational boundaries. Though this principle is widely acknowledged, its implementation often remains fragmented, with cybersecurity decisions insufficiently integrated into operational, financial, customer and supply chain decision-making.[18]

Our simulation results reinforce this concern. As shown in Figure 3, multidisciplinary

16 Pearlson, K., Thorson, B., Madnick, S. and Coden, M. "Cyberattacks Are Inevitable. Is Your Company Prepared?" *Harvard Business Review*, March 9, 2021, available at https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared.

17 *What Is Cybersecurity?* Gartner, May 20, 2026, available at https://www.gartner.com/en/topics/cybersecurity.

18 Jazairy, A., Brho, M., Manuj, I. and Goldsby, T. J. "Cyber Risk Management Strategies and Integration: Toward Supply Chain Cyber Resilience and Robustness," *International Journal of Physical Distribution & Logistics Management* (54:11), December 2024, pp. 1-29.

groups consistently outperformed individual technology-focused participants when managing routine cyber threats. Groups that combined business, operational, financial and technological perspectives achieved over 20% higher cumulative profits after five simulation rounds while maintaining comparable levels of risk exposure.

In our simulations, groups consistently achieved higher average outcomes and lower variability across all threat levels. Compared to individual participants, they were better able to balance cyber resilience with business performance, producing more stable and predictable results under conditions of uncertainty. Diverse perspectives improved participants' ability to recognize trade-offs between resilience, operations and financial performance that are often overlooked. This suggests that effective cyber risk governance benefits from integrating business, operational, financial and technical perspectives.

For executives, the challenge is not the availability of cybersecurity expertise but whether cyber risk is embedded in business decision-making. Practical approaches include multidisciplinary governance forums, cybersecurity reviews of major programs and investments, controls aligned with operational processes and human behavior and an end-to-end service perspective that strengthens resilience across business processes, technologies, suppliers and customers.

Proactively Build Capabilities Before You Need Them

Many executives still treat cybersecurity investments as flexible expenditures that can be postponed until growth objectives are secured. Our findings suggest that this logic is fundamentally flawed. In cybersecurity, delayed investment does not merely postpone protection; it compounds organizational exposure over time.[19]

A board member of a government and finance institution explicitly described the governance challenge: "If we are introducing a new type of product or going into a new business line, then what are some new risks that we are introducing to the company and how are we going to manage it? That part is still kind of fuzzy."

This ambiguity is critical because cybersecurity capabilities cannot be built instantly. Effective resilience depends on the long-term accumulation of capabilities: hiring skilled personnel, implementing controls, maturing detection processes and embedding security into operations. Organizations that defer investment often assume they can compensate later through accelerated spending once threats materialize.[20] Our simulation results strongly contradict this assumption.

In our simulations, reactive investment strategies consistently produced higher compromise rates, lower profits and greater recovery costs than sustained investment approaches (see Figure 4). Early underinvestment created vulnerabilities that could not be fully offset through later spending because cybersecurity capabilities require time to develop and mature before their benefits materialize. Understanding these time-delay effects emerged as a critical learning outcome, helping participants move beyond reactive optimization toward more adaptive and effective cyber risk investment decisions.

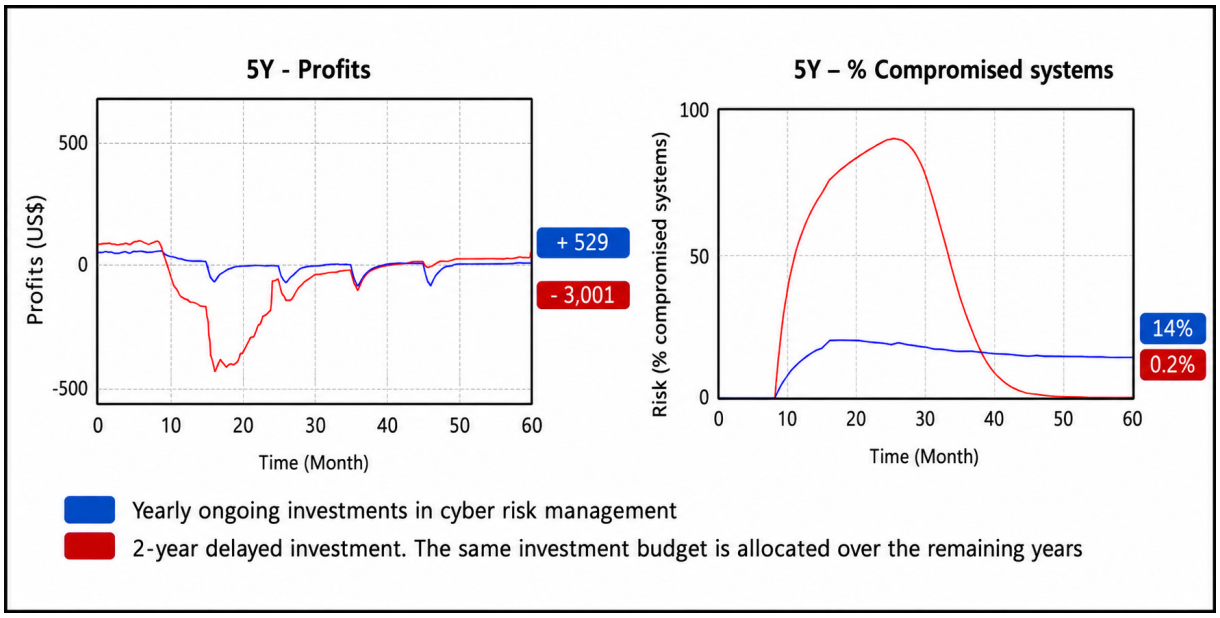
Importantly, our findings do not imply that increased cybersecurity spending is always beneficial. Excessive investment can erode business performance, while delayed investment increases exposure to risks. The critical insight is not to spend more, but to build cyber capabilities early enough for them to mature before threats emerge. Cyber resilience depends less on spending levels and more on the timing and consistency of capability development.

For executives, resilience cannot be purchased on demand. Delayed investments create capability gaps that often become apparent only after adversaries exploit them, at which point recovery becomes far more costly and difficult. Cybersecurity investments should therefore be evaluated not only based on current risk reduction but also on the time required for capabilities to mature and deliver

19 Gillam, B. "Is Proactive Cybersecurity Worth the Cost for Small and Midsized Businesses?" *Today's General Counsel*, August 30, 2023, available at https://todaysgeneralcounsel.com/is-proactive-cybersecurity-worth-the-cost-for-small-and-midsized-businesses.

20 Gordon, L. A., Loeb, M. P. and Lucyshyn, W. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal* (19:23), 2003, pp. 1-7.

Figure 4: Comparing Cyber Risk Strategies—Ongoing vs. Delayed Investment



value. Organizations are competing against both attackers and time.

Concluding Comments

Taken together, the four heuristics presented in this MISQE Insight highlight a fundamental cyber risk governance challenge: maintaining decision quality as threats become increasingly sophisticated. Across 1,800 simulation exercises, the proportion of participants able to identify effective cyber risk strategies declined from 45% under routine threats to 15% under sophisticated threats. Figure 5 illustrates this trend. As organizations faced more simulated complex threat environments, they increasingly struggled to balance cyber resilience with business performance. Meanwhile, cybercrime costs continue to rise globally, increasing the financial consequences of ineffective cyber risk decisions. Collectively, these trends suggest that many organizations may find it difficult to adapt governance and investment decisions at the pace required by an evolving cyber threat landscape.

Appendix: Strategic Digital Twins and Supporting Analyses

Strategic digital twins can be applied in many ways for cyber risk governance, including strategy assessments, reporting[21] and strengthening decision-making[22] across different industries. This MISQE Insight aims to raise awareness by employing a simplified version of such technology. Our scientifically[23] grounded[24] and thoroughly tested simulation game was implemented as part of an executive training program on cyber risk governance involving 240 (supervisory) board members, executives, business leaders, strategists and policy officers who participated in over 1,800

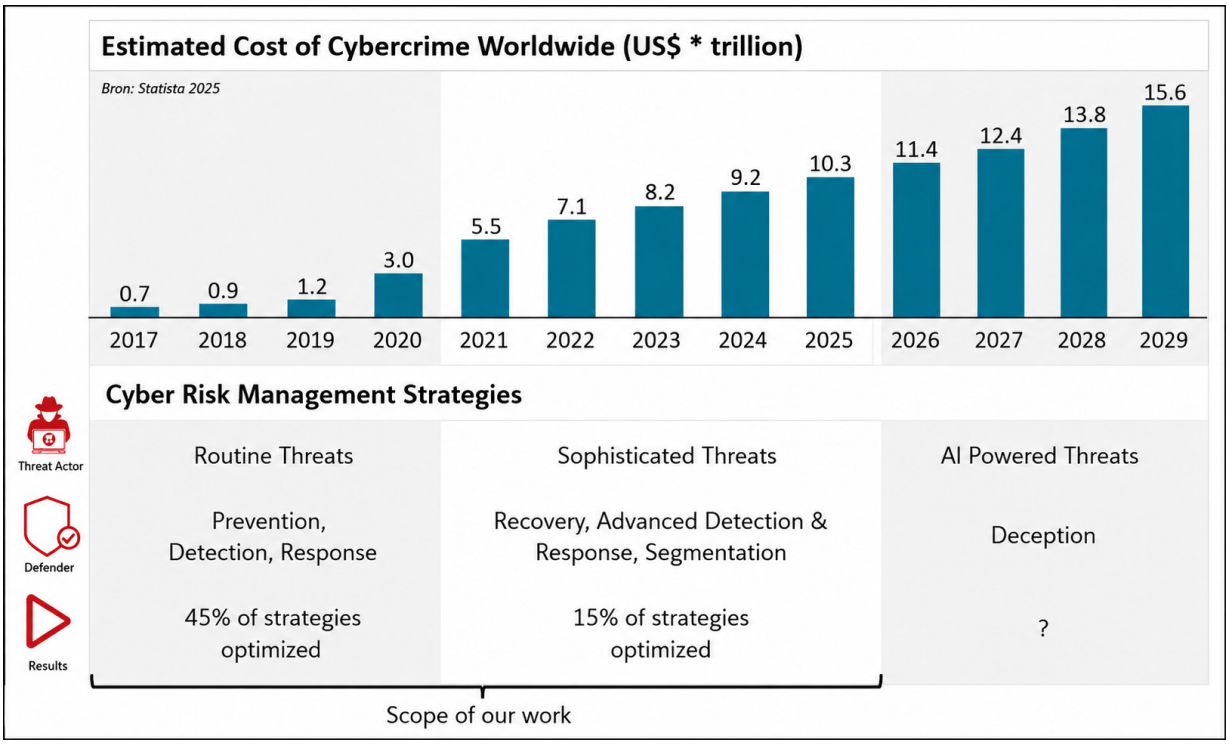
21 Zeijlemaker, S., Pal, R. and Siegel, M. "Strengthening Managerial Foresight to Defeat Cyber Threats," *Proceedings of the Americas Conference on Information Systems,* August 2024.

22 Zeijlemaker, S. and Siegel, M. *How to Prioritize Cyber Resilience in the Healthcare Sector,* World Economic Forum, February 4, 2026, available at https://www.weforum.org/stories/2026/02/how-to-prioritize-cyber-resilience-in-the-healthcare-sector.

23 Jalali, M. S., Siegel, M. and Madnick, S. "Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment," *The Journal of Strategic Information Systems* (28:1), March 2019, pp. 66-82.

24 Segar, P., Zeijlemaker, S. and Siegel, M. "Decision-Making in Ransomware Capability Development: Persona-Driven Simulation," *Proceedings of the International System Dynamics Conference,* August, 2024.

Figure 5: Evolution of Threats, Cybercrime Costs, Defenses, and Decision-Making



Source: Statista graph of estimated cost of cybercrime worldwide from 2017 to 2029 (https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide/).

simulation exercises. A total of 68 participants (a 28% response rate) completed an independent evaluation, with approximately 90% rating the training, including the simulations, as highly relevant to their day-to-day practice.

About the Authors

Sander Zeijlemaker

Dr. Sander Zeijlemaker (szeijl@mit.edu) is a CAMS research affiliate at the Massachusetts Institute of Technology (MIT), an agenda contributor to the World Economic Forum, principal research director at Z-CERT and owner of Disem Institute. His work focuses on cybersecurity, cyber resilience and digital risk management, bridging academic research with practical applications for healthcare, critical infrastructure and public-private collaboration. He regularly contributes to international initiatives that strengthen organizational and societal cyber resilience.

Jeffrey G. Proudfoot

Dr. Jeffrey Proudfoot (jproudfoot@bentley.edu) is a professor in the Computer Information Systems Department at Bentley University and a CAMS research affiliate at the Massachusetts Institute of Technology (MIT). His research focuses on a variety of information topics, including security policies and compliance, cybersecurity regulations and board-level cyber governance. His work has been published in several premier outlets, including *The Wall Street Journal, MIS Quarterly*, *MIS Quarterly Executive*, *Journal of Management Information Systems*, and *Journal of the Association for Information Systems.*

Ranjan Pal

Dr. Ranjan Pal (ranjanp@mit.edu) is a research scientist at MIT Sloan School of Management and a cybersecurity expert with Cybersecurity at MIT Sloan (CAMS). His research focuses on enterprise and supply chain cyber risk, resilience and cyber insurance,

integrating computer science, decision science and operations research. A member of the World Economic Forum's Cyber Resilience Working Group, he has published over 100 articles, advised governments and industry, spoken at more than 50 international venues, and serves as an associate editor for *ACM Transactions on Management Information Systems.*

Michael Siegel

Dr. Michael Siegel (msiegel@mit.edu) is a principal research scientist at MIT Sloan School of Management. His research focuses on management, strategy, technology and organizational issues related to cybersecurity, with specific interest in vulnerability markets, cyber risk management, dark web business models, IoT endpoint security, vulnerability management, cybersecurity workforce development and educating management in cybersecurity. With over 37 years at MIT, he has published extensively on cybersecurity, AI, and information systems strategy.