MIS Quarterly Executive

Volume 23 | Issue 4 Article 8

December 2024

How to Design a Better Cybersecurity Readiness Program

Kaveh Abhari

Morteza Safaei Pour

Hossein Shirazi

MIS Quarterly Executive

How to Design a Better Cybersecurity Readiness Program

Mistraining and overtraining can cause cybersecurity training programs to fail. We explore the pitfalls of four common types of cybersecurity training—compliance awareness, threat simulation, specialized instruction and incident response planning. Based on insights from large accounting firms, we identify four unintended consequences—threat anxiety, security fatigue, risk passivity and cyber hesitancy—that result in adverse individual effects and organizational impacts. We recommend that organizations design a comprehensive cybersecurity readiness program using our LEAN model, which comprises four strategies: Localize, Empower, Activate and Normalize.[1,2,3]

Kaveh Abhari
San Diego State University (U.S.)

Morteza Safaei Pour
San Diego State University (U.S.)

Hossein Shirazi
San Diego State University (U.S.)

The Challenges of Cybersecurity Readiness Programs

The ever-widening cyber threat landscape and growing frequency and cost of successful cyberattacks are compelling business leaders to make what we term "cybersecurity readiness programs" a strategic priority. These programs are supposedly comprehensive initiatives designed to fortify an organization against digital threats through education, policy enforcement and technological safeguards. They provide employees with a blend of training, rules and tools to prepare and protect organizations from the multifaceted and ever-evolving cyber threats. However, developing effective cybersecurity readiness programs is challenging, complex and highly nuanced.[4]

The belief that simply allocating resources and ensuring strategic alignment guarantees the success of these programs is misguided; such an approach often results in poor outcomes,

1 Jeffrey Proudfoot is the senior accepting editor for this article.

2 The authors extend their sincere gratitude to Jeffrey Proudfoot and the review team members for their invaluable insights and guidance throughout the review process. We also gratefully acknowledge the support of Nhat Huynh and Claire Wu, whose work on cybersecurity initiatives at San Diego State University's Digital Innovation Lab inspired us to pursue this project.

3 This research was partially funded by the U.S. National Science Foundation (NSF) under Grant No. 2219773.

4 For a study on employees' negative perceptions of cybersecurity training, see Reeves, A., Calic, D. and Delfabbro, P. H. "'Get a Red-Hot Poker and Open Up My Eyes, It's So Boring': Employee perceptions of cybersecurity training," *Computers & Security* (106), July 2021, Article 102281.

DOI: 10.17705/2msqe.00107

particularly for non-technical employees.[5] Recognizing this dilemma, digital leaders and cybersecurity practitioners frequently respond to suboptimal results by implementing intensive training regimes, along with more diverse training approaches.[6] Yet this response often exacerbates the problem.[7]

Overlooking the complexity of employee behavior leads to poorly designed programs, while ignoring the integration of training with broader readiness efforts, results in fragmented initiatives. These programs frequently overemphasize knowledge dissemination, rote compliance and short-term engagement, neglecting the importance of retention, ownership and integration into daily routines. These oversights contribute to employees being *mistrained* (i.e., incorrectly or badly trained) and *overtrained*, ultimately amplifying existing cyber vulnerabilities. Mistraining occurs when employees receive irrelevant or impractical training, while overtraining involves excessive or repetitive sessions that overwhelm employees with redundant information. Even fully funded, comprehensive programs can fall victim to these flaws.

To provide recommendations for systematically addressing these challenges, we conducted 23 interviews with employees working for the four major U.S. accounting firms (see the Appendix A for our research methodology). Based on these interviews, we first analyze the consequences of mistraining and overtraining within four common types of cybersecurity training: compliance awareness, threat simulation, specialized instruction and incident response planning. Despite their various benefits, these types of training can lead to unintended consequences, which we discuss under the headings of *threat anxiety, security fatigue, risk passivity* and *cyber hesitancy*. If left unaddressed, these adverse effects can diminish individual performance, disrupt team dynamics, erode client experiences and ultimately degrade an organization's cybersecurity culture.

To counter these effects and foster a more integrated approach, we introduce the LEAN model for designing a cybersecurity readiness program, grounded in four core strategies: *Localize, Empower, Activate* and *Normalize*. The Localize strategy emphasizes tailoring training to specific roles, contexts and workflows rather than focusing solely on individual needs and learning styles. The Empower strategy ensures that decision-making authority is appropriately delegated and fosters a sense of ownership by moving beyond rigid rules and mandates. The Activate strategy focuses on cultivating and scaling mastery through coordinated actions and collaborative learning, not just isolated simulations and boot camps. Finally, the Normalize strategy embeds cybersecurity practices within daily operations, reducing reliance on deterrence and threat arguments.

The article concludes by providing two data-driven recommendations for each of the four strategies. These recommendations will help organizations avoid common pitfalls, enhance cyber resilience and cultivate a security culture that transcends mere compliance.

How Employees Perceive Common Cybersecurity Training Methods

As cybersecurity threats become more pervasive,[8] many organizations disproportionately focus on expanding their training regimes. However, these initiatives often suffer from poor design decisions, leaving human error the predominant cause of cyber

5 For an insightful work that differentiates effective from ineffective cybersecurity training frameworks, see Chowdhury, N., Katsikas, S. K. and Gkioulos, V. "Modeling Effective Cybersecurity Training Frameworks: A Delphi Method-Based Study," *Computers & Security* (113:3), November 2021, Article 102551.

6 For a practical examination of both effective and ineffective practices for enhancing employee adherence to cybersecurity policies, see Cram, W. A., Proudfoot, J. G. and D'Arcy, J. "Maximizing Employee Compliance with Cybersecurity Policies," *MIS Quarterly Executive* (19:3), March 2020, pp. 183-198.

7 Different studies have shown the ineffectiveness of common approaches. For example, see Cram, W. A. and D'Arcy, J. "'What a Waste of Time': An Examination of Cybersecurity Legitimacy," *Information Systems Journal* (33:6), July 2023, pp. 1396-1422.

8 Predictions suggest global cyber-related damages could hit $10.5 trillion by 2025. See Morgan, S. *Cybersecurity Boardroom Report 2023*, Cybercrime Magazine Press Release, December 13, 2023, available at https://cybersecurityventures.com/cybersecurity-board-room-report-2023/. For statistics on cybercrime and the cybersecurity market, see Morgan, S. 2022 *Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics*, Cybercrime Magazine, January 19, 2022, available at: https://cybersecurityventures.com/cybersecurity-almanac-2022/.

Table 1: Common Types of Cybersecurity Training

Type of Training	Definition
Compliance Awareness	Educating employees on the legal, regulatory, procedural and policy aspects of cybersecurity to ensure adherence to essential compliance standards and best practices.
Threat Simulation	Engaging employees with realistic, hands-on exercises that mimic cyber threats such as social engineering attacks, enhancing their awareness, vigilance and response capabilities.
Specialized Instruction	Delivering targeted cybersecurity education tailored to specific roles or departments, addressing their unique risks, needs and operational protocols.
Incident Response Planning	Offering scenario-based planning through interactive workshops and security management sessions, ensuring effective crisis response and fostering organizational resilience.

breaches.[9] Though organizations do explore innovative training approaches, poor design frequently results in mistraining or overtraining with adverse effects such as security fatigue and stress[10] that ultimately undermine the very outcomes these programs aim to achieve.[11] To illustrate the problems arising from poorly designed training regimes, we first review four common types of cybersecurity training (compliance awareness, threat simulation, specialized instruction and incident response planning), summarized in Table 1, along with employee perceptions and reception of the methods used within the studied organizations.

Compliance Awareness Training

Compliance awareness training, aimed at educating employees on essential legal, regulatory and policy aspects of cybersecurity, is the cornerstone of the cybersecurity readiness programs we studied. Typically mandated and delivered through virtual platforms, these programs are designed to help employees—especially new hires—grasp cybersecurity fundamentals such as confidentiality, privacy and common cyber threats. The training often consists of web-based training videos accompanied by interactive quizzes, the completion of which is necessary for progression. To reinforce awareness, some organizations also distribute internal agreements, documentation and procedural guides. Though compliance training often included formal assessments as part of regulatory requirements, employees frequently bypassed these evaluations, especially when generative AI tools enabled them to complete questions without fully engaging with the material.

Our interviews revealed widespread disinterest among participants, primarily due to poor program design. Several employees described the training as "boring yet mandatory," "easy yet long," "alarming yet irrelevant" and "tedious yet unhelpful." A few even admitted to circumventing the material to meet assessment requirements, with one participant stating, "It's very easy to get by without watching the content." Interestingly, the primary issue was not the mode of delivery but the lack of content customization for specific roles and responsibilities—a clear

9 Nearly 90% of data breach incidents are caused by employees' mistakes. Despite training, these mistakes include falling for phishing scams, misconfiguring systems and other errors. For more information, see *Psychology of Human Error Could Help Businesses Prevent Security Breaches*, CISOMAG, September 20, 2020, available https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/.

10 Security fatigue refers to exhaustion and diminished vigilance caused by constant exposure to cybersecurity threats and protocols, leading to carelessness and non-compliance. Similarly, security stress is the strain from the ongoing threat of cyber breaches and the pressure of maintaining security measures, causing anxiety and burnout. For more insights, see: 1) "When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue," *Information Systems Journal* (31:2), December 2021, pp. 521-549; and 2) and Chen, H., Liu, M. and Lyu, T. "Understanding Employees' Information Security-Related Stress and Policy Compliance Intention: The Roles of Information Security Fatigue and Psychological Capital," *Information and Computer Security* (30:5), May 2022, pp. 751-770.

11 For a comprehensive review of cybersecurity training methods and their negative outcomes, see Prümmer, J., Van Steen, T. and Van den Berg, B. "A Systematic Review of Current Cybersecurity Training Methods," *Computers & Security* (136), January 2024, Article 103585.

example of mistraining. The interviewees viewed the training as "too generic to be useful," prompting comments like, "If it's meant for everyone, it's not really for me," and questioning the time commitment for what they considered "common sense" material.

Threat Simulation Training

Training based on simulating threats was the second most widely implemented cybersecurity readiness method and offered practical, scalable training. Such training primarily simulated common phishing cyber threats by sending deceptive emails to employees to gauge their responses and test their vigilance. This approach aims at familiarizing employees with social engineering[12] tactics and reducing the likelihood of errors during actual cyber incidents. Some individuals who fail these tests receive additional training.

Our interviewees described their interactions with threat simulation as mostly positive, using terms such as "practical," "educational," "engaging," "eye-opening," "roleplaying," "integrated [with email]," "shared experience" and "game-like." However, some found it "deceptive," "punitive" and "demoralizing." Though many appreciated the realism, which heightened their caution and awareness, others found the experience stressful, particularly when failures led to reports to managers and additional training. A few also criticized the frequency of simulations, with some noting that it encouraged them to "ignore all external emails with links."

Specialized Instruction

As well as traditional training methods, we observed a rise in specialized instruction events tailored to specific roles and departmental needs, addressing unique vulnerabilities and protocols. These sessions, often conducted in person, focused on topics like incident reporting, data protection and risk assessment within the particular department's context. These events, with limited participants, combined practical exercises and group discussions to offer deeper insights into security procedures.

Participant feedback highlighted a strong desire for deeper engagement, with many calling for more "dynamic," "collaborative" and "hands-on" interactions instead of "extensive lectures." Others found the sessions "overwhelming," "confusing" or "unfocused," often because they found the sessions complex or lacked practical relevance—another example of mistraining. Only those who felt a sense of ownership and viewed the training as timely and integral to their responsibilities responded positively. Despite the emphasis on responsibility during these training sessions, some participants felt that cybersecurity was not a priority or part of their role, with one stating, "I'd rather focus on my main tasks than sit through another training session [like that]."

Incident Response Planning Training

Incident response planning sessions trained participants and equipped them with actionable crisis plans. They featured interactive case studies, scenario-based planning, and regular crisis management meetings centered on incidents like data breaches and best practices. The sessions focused on operational strategies and coordinated responses, enabling participants to identify, contain and mitigate security threats swiftly. Decision-making under pressure, role delegation and effective crisis communication were also emphasized for rapid recovery.

Employees described this training method as "strategic," "applied," "managerial" and "realistic," noting that it moved beyond "simple information sharing." They appreciated how it fostered "critical thinking," "problem-solving" and "co-planning." Many felt they gained insights into practical trade-offs and priorities beyond the scope of traditional training. While employees did not consider the training a "waste of time," they often felt overwhelmed and deeply concerned when tasked with managing cybersecurity risks, with one interviewee remarking: "It's overwhelming to balance all the risks and make the right call."

Adverse Effects of Cybersecurity Mistraining and Overtraining on Employees

We delved deeper into the interviewees' concerns about the design flaws in the four common types of cybersecurity training. Though formal complaints often centered on time

12 Social engineering involves deceiving individuals to disclose confidential information or compromise security through psychological tricks, impersonation or trust exploitation.

Table 2: Individual Adverse Effects of Cybersecurity Mistraining or Overtraining

Effect	Definition	Manifestations
Threat Anxiety	Hypervigilance and excessive caution due to fear of triggering a security breach or similar issues.	• Emotional anxiety (emotional overload): overwhelming worry about handling sensitive tasks. • Work-security balance anxiety: difficulty managing regular work and additional security tasks. • Skill-acquisition anxiety: doubts about the ability to learn and apply cybersecurity practices. • Procedural time anxiety: stress from time pressure when following security protocols.
Security Fatigue	Cognitive fatigue and diminished concentration caused by repetitive, frequent or overly complex security protocols	• Disengagement fatigue: viewing compliance initiatives as chores. • Distraction fatigue: constant interruptions from security drills and simulations. • Information fatigue: overload with technical or procedural content. • Decision fatigue: struggling with numerous procedural steps and options. • Support fatigue: difficulty in troubleshooting due to lack or complexity of support system.
Risk Passivity	Inaction or desensitization to threats, resulting in indecision, procrastination or risky decision-making.	• Behavioral inhibition: inaction due to perceived risks (decision and analysis paralysis) • Habituation: decreased responsiveness from repeated warnings (desensitization)
Cyber Hesitancy	Reluctance to engage with or try new cybersecurity practices, tools and approaches.	• Hesitancy to share: reluctance to communicate about security issues. • Hesitancy to trust: fear of revealing vulnerabilities in team settings. • Hesitancy to try: avoidance of new approaches due to fear of mistakes.

commitments, irrelevance, and "disownership,"[13] deeper and more troubling concerns emerged, demanding the attention of digital leaders. These concerns affected employees on a personal level and posed significant risks for undermining organizational effectiveness. The root causes of these concerns are mistraining and overtraining, indicating that resources were misallocated and misguided, rendering the training not only ineffective but, paradoxically, counterproductive. This misalignment led to unintended consequences, manifested as four key adverse effects at the individual level: *threat anxiety, security fatigue, risk passivity* and *cyber hesitancy* (see Table 2). We found that threat anxiety was the most prevalent adverse effect, followed by hesitancy, fatigue and passivity.

Threat Anxiety

Threat anxiety is a state of hypervigilance[14] (constant alertness) caused by information security stress. Among our interviewees, threat anxiety arose as a direct result of both mistraining and overtraining. For instance, compliance awareness and threat simulations often engendered anxiety in performing individual tasks, such as hesitation in opening emails. More advanced training, like specialized instruction and incident response planning, heightened anxiety in team settings and project management, leading to reluctance to share

13 Cybersecurity disownership signifies reluctance to acknowledge cybersecurity duties, as in the attitude "cybersecurity is not my responsibility."

14 Hypervigilance is the opposite of "eustress," a positive form of stress having a beneficial effect on health, motivation, performance and emotional well-being.

information due to fears of violating policies. Overtraining further exacerbated this anxiety, resulting in fear of being penalized or publicly embarrassed for making mistakes.

We identified four forms of anxiety resulting from overtraining or mistraining. The first and most prevalent was *emotional overload*, driven by constant reminders of threats and complex protocols.[15] This led to "techno-stress," fostering self-doubt and exaggerated stress responses. One interviewee remarked: "[Training] makes me second-guess every action I take." The second form of threat anxiety is *work-security balance anxiety*, which emerges when employees struggle to manage client demands alongside cybersecurity tasks. A participant suggested that to minimize such anxiety, "managers need to prioritize client work over attending training." The third is *skill-acquisition anxiety*, which arises from doubts about effectively learning and applying cybersecurity procedures. One interviewee attributed this form of anxiety stress to his firm providing only a "broad understanding of cyber threats ... without technical depth." Finally, *procedural time anxiety* stems from the pressure of adhering to cybersecurity protocols, which often compromises deadlines during busy periods. Such anxiety could exist independently but frequently coexists with work-security balance anxiety.

Security Fatigue

Our interviewees also showed signs of security fatigue,[16] induced by cognitive overload and feeling overwhelmed. Examples included:

- Inconsistent guidance, where conflicting instructions from different training modules or managers caused confusion and uncertainty
- Excessive complexity, due to security protocols with too many intricate steps that were difficult to remember and apply correctly
- Irrelevant content, where training sessions were overly generic or insufficiently tailored to specific job roles, thus increasing cognitive strain without providing practical, applicable knowledge.

Our interviews revealed that security fatigue could manifest in five distinct forms across various training contexts and was frequently exacerbated by overtraining. First, *disengagement fatigue* emerged from basic compliance training, including refreshers, which was often perceived as unnecessary. One interviewee described these sessions as "like a chore," resulting in diminished intellectual curiosity and apathy toward training. Second, *distraction fatigue* was associated with simulation training, such as phishing emails. One employee noted that gamified phishing simulations were a "constant distraction." Third, *information fatigue* was the most severe form of security fatigue and arose from training workshops and boot camps. Two employees admitted they could retain less than half of the content from recent workshops due to the overwhelming amount of information presented in a single day. Fourth, *decision fatigue* was observed in incident response training, characterized by its numerous procedural steps, without any integration with established processes, which made decision-making arduous and mentally taxing. Finally, *support fatigue* was noted when employees had to troubleshoot and resolve cybersecurity issues independently on "self-help days." Although support and resources were available, the sheer volume of training materials necessitated extensive filtering to find relevant information, contributing to a sense of being overwhelmed.

Risk Passivity

Risk passivity is a paradoxical outcome of training where employees display excessive caution or indifference to threats. We observed that excessive caution could result in indecision, procrastination and risk-aversion on the part of employees and also desensitize them to repeated warnings and thus foster complacency and risky behavior. Risk passivity manifests in two ways: *behavioral inhibition*, where perceived risk hinders action, and *habituation*, where repeated warnings diminish responsiveness.

Behavioral inhibition (i.e., hesitation to act) is primarily triggered by overtraining. Interviewees reported increased hypervigilance in routine client interactions, causing them to double-

15 Anxiety stems from complexity in two ways: technical training content that erodes self-efficacy, and convoluted procedures that inundate employees with uncertainty.

16 Security fatigue is relatively well-researched but less accounted for in practice. For example, see Cram, W. A., Proudfoot, J. G. and D'Arcy, J. op. cit., December 2021.

check details and hesitate before engaging in common tasks like screen sharing. Though they found vigilance to be beneficial, hypervigilance often became paralyzing as employees struggled to justify any inherent risk. Similarly, advanced training, intended to strengthen decision-making skills, occasionally backfired, leading to "analysis paralysis." One interviewee noted, "I was so overwhelmed [with choices] that I couldn't make a simple decision."

Conversely, habituation resulting from overtraining, especially compliance refreshers and repeated phishing simulations, caused employees to become desensitized to security warnings, making them more likely to overlook genuine threats. One employee admitted to initially being vigilant but eventually ignoring alerts due to fatigue from "constant notifications." Another echoed this sentiment, stating, "At some point, you just start ignoring them because it's too much of a distraction."

Cyber Hesitancy

Cyber hesitancy is the reluctance to engage with or adopt new cybersecurity practices, tools and approaches. Interestingly, our interviewees attributed this to overemphasizing individual errors and insider threats rather than technology. Cyber hesitation manifested in three interconnected forms: *hesitancy to share, hesitancy to trust* and *hesitancy to try*, each exacerbating the others.

Hesitancy to share emerged when organizations were overly focused on the socio-professional impacts of individual errors. One interviewee reflecting on a recent incident, said: "People are aware, but it is not talked about." Reluctance to communicate about potential security issues stems from fears of blame and ostracism. Additionally, collaborative exercises such as "policy puzzles" or "recovery plans" often exposed individuals' weaknesses, reinforcing employees' reluctance to communicate and stifling open dialogue, thereby hampering effective threat management.

Hesitancy to trust is prevalent when mistraining accentuates the risk of insider threats. Interviewees noted a growing sense of suspicion due to a culture focused on identifying and penalizing individual errors. One employee remarked that specialized training "fostered independence and zero trust," which, while important, could hinder the necessary coordinated response to cyber threats. Another reported that the training intended to promote teamwork instead generated "mistrust" by emphasizing the "weakest link" and "internal threats," stating that "75% of data breaches involved human error."

Hesitancy to try arises from competitive elements in training programs, such as gamified simulations, which sometimes backfire. These simulations can create fears of ridicule and judgment. One interviewee noted that a colleague "joked about the people that click on the fake phishing emails." When such simulations lead to public embarrassment or penalties, employees become more concerned with safeguarding their reputations than learning from mistakes.

Organizational Impacts of Poorly Designed Cybersecurity Readiness Programs

From the interviews, we found that the organizational impacts of mistraining and overtraining were substantial. Though some impacts had been anticipated, their extensive prevalence and profound impact on the organization were surprising. As detailed in Table 3, we categorize the impacts into four key areas: *individual performance erosion, team dynamics fragmentation, client experience disruption* and *security culture stagnation*. Our interviewees highlighted that the biggest impact was on security culture, with equal impacts on individual performance and team dynamics, followed by client experience. However, these organizational impacts are not stand-alone; they are interlinked and often exacerbate one another.

Our findings indicate that even well-funded cybersecurity readiness programs can suffer from the negative organizational impacts of mistraining and overtraining, acting as a cautionary tale for others. To tackle the individual and organizational shortcomings effectively, we propose the LEAN model for designing cybersecurity readiness programs.

Table 3: Organizational Impacts of Cybersecurity Mistraining and Overtraining

Impact	Definition	Example Manifestations
Individual Performance Erosion	Decline in productivity due to cybersecurity-induced stress and avoidance behaviors.	• Avoidance: hesitation to handle sensitive tasks. • Negligence: increased mistakes due to cognitive overload. • Resistance: rejection of new digital tools or solutions.
Team Dynamics Fragmentation	Breakdown of team cohesion and responsibility due to conflicting perceptions of cybersecurity risks.	• Internal avoidance: shunning sensitive tasks. • Inter-team friction: misalignment and conflict between teams over security protocols.
Client Experience Disruption	Negative impact on client satisfaction due to security-induced delays and added complexities.	• Service disruptions: delays and withholding of services. • Service friction: conflict due to procedural and communication gaps with clients.
Security Culture Stagnation	Stagnation in developing a proactive security culture due to an overemphasis on compliance and fear of making mistakes.	• Innovation aversion: suppressed creativity and risk-taking. • Indifference: hesitation to report incidents proactively. • Individualism: decreased collective security actions.

The LEAN Model for Addressing the Effects and Impacts of Poorly Designed Cybersecurity Readiness Programs

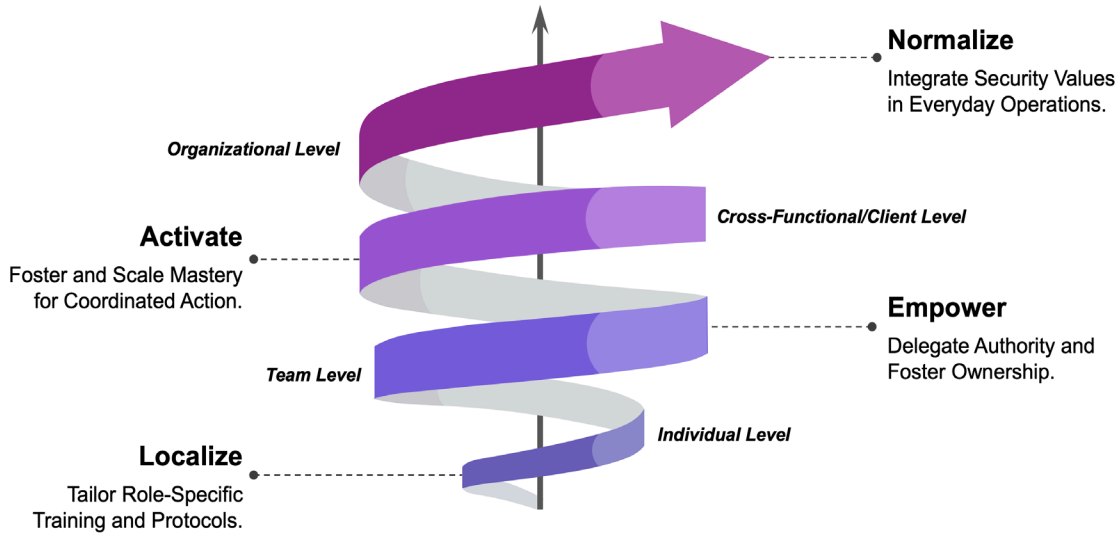
Our LEAN model comprises four core strategies: Localize, Enable, Activate and Normalize (see Figure 1 and Table 4). The goal is to design a program that streamlines cybersecurity readiness by focusing on role-specific, context-relevant local knowledge, enabling employees by giving them relevant authority and ownership, and activating coordinated action by fostering mastery and collaboration. Finally, the model normalizes (embeds) cybersecurity deeply into the organizational workflow, ensuring a culture that moves beyond mere compliance or rhetoric into genuine, proactive security engagement. Together, these strategies address the organizational impacts of cybersecurity mistraining and overtraining identified in Table 3. Initially developed as a cybersecurity benchmark for large accounting firms, the LEAN model is adaptable across similar industries, though subject to certain limitations, as discussed in Appendix B.

Each strategy builds on the preceding one: without localized training, empowerment remains unattainable; without empowered employees, the activation strategy lacks both direction and impact; and without activation, the normalization of a strong cybersecurity culture becomes elusive. These strategies, when implemented collectively, have the potential to significantly reduce both the effects on individuals and the organizational impacts of a poorly designed cybersecurity readiness program. Tailored and streamlined training will alleviate security fatigue at the individual level, while empowerment addresses cyber hesitancy by reinforcing team dynamics. Fostering and scaling mastery will mitigate risk passivity by promoting coordinated action and cross-functional collaboration. Lastly, the impact of threat anxiety can be optimized by embedding a security-first mindset and seamlessly integrating security into daily operations, thereby reinforcing a resilient organizational culture.

The Localize Strategy

The Localize strategy combats individual performance erosion. Employees are often

Figure 1: The LEAN Model for Cybersecurity Readiness Program Design



mistrained because training focuses on compliance rather than on providing practical value and employs a one-size-fits-all approach that burdens employees with irrelevant details while neglecting the unique needs of specific roles. As one employee put it, "It's hard to take [training] seriously when it feels like it's just 'cybersecurity 101' for everyone." This lack of tailored relevance leaves employees feeling overwhelmed, disengaged and uninvested. An interviewee commented: "I even put the company's training on auto-play … that's how pointless it is," and "It's just stating the obvious. I don't have the patience for this." Attempts to address these concerns with incentivized, gamified or immersive training often fail to address the core problem: the absence of role-specific context. This mistraining, typically associated with poor content design,[17] may lead to employees avoiding sensitive tasks, neglecting critical situations and rejecting digital tools, ultimately hurting performance.

The Localized strategy addresses mistraining by acknowledging that not all threats are relevant to everyone and that even when they are, employees experience them differently, with varying degrees of impact. Thus, this strategy streamlines training and protocols, optimizes content and tailors materials to the specific context of each business function, avoiding any embellishment or dramatization. The Localized strategy aligns with our interviewees' frequent requests to "make it relevant to me, and I'd actually pay more attention," "keep it real" and "[make the training] more personalized to our roles, so I could see how these security practices fit into my daily work." Instead of diversifying delivery methods or accommodating individual learning styles—neither requested by our interviewees nor proven to be consistently effective[18]—this strategy emphasizes relevance and contextualization. It aligns cybersecurity training with employees' actual work practices and excludes unnecessary technical details and generalized regulations.

17 Poor content design often results in training materials that lack specificity, relevance and actionable guidance, or that are misleading, fear-inducing or confusing. This frequently stems from an over-reliance on material developed by third-party training providers. These providers understandably prioritize creating broadly applicable content that fulfills compliance requirements and can be easily adapted for various clients, rather than tailoring it to the specific group and context of each client's organization.

18 While acknowledging the benefits of personalized learning, we caution against over-reliance on it, as it may not always be feasible or necessary. This is in line with research findings such as Kirschner, P. A. "Stop propagating the learning styles myth," *Computers & Education* (106:1), March 2017, pp. 166-171.

Table 4: Definition of the Four LEAN Model Strategies

Strategy	Aim	Definition
Localize	Improve individual security behavior	Tailor cybersecurity training to align with employees' specific roles, contexts and workflows, ensuring relevance to their daily tasks rather than focusing on generic or individual learning styles.
Empower	Improve team security dynamics	Delegate decision-making authority and foster ownership, moving beyond rules and mandates to mitigate team dysfunction and encourage responsibility at the team level.
Activate	Improve collective response to security	Foster and scale mastery through coordinated actions and collaborative learning, ensuring that security practices are seamlessly integrated into daily workflows to reduce operational disruptions and external friction.
Normalize	Improve security culture	Embed a positive security culture within daily operations, moving away from deterrence-based and fear-driven approaches to seeing security as a core organizational value.

The Localize strategy begins by establishing a clear rationale for security responsibilities and articulating the immediate benefits for individual employees. Next, it focuses on building confidence, which, from our interviews, we identified as a crucial distinguishing factor of effective training. One participant noted that fear-based narratives, when disconnected from contextually relevant risks, diminished employees' self-efficacy, leading to the avoidance of sensitive tasks due to being "anxious about security mistakes" and "constantly second-guessing." Additionally, this strategy reduces cognitive load and information fatigue by providing concise, actionable guidance that employees can directly apply, thereby minimizing errors arising from security fatigue.

Finally, by aligning training and related protocols with each department's specific technical needs, tailored to the technologies employees rely on, the Localized strategy fosters a greater willingness among them to embrace new digital tools and solutions. For example, we observed a consistent pattern of resistance to new software requests due to security fatigue driven by multi-step approval processes—often described as "unnecessary," "counterproductive" and "time-consuming"—which employees found challenging to understand and navigate.

The Empower Strategy

The Empower strategy mitigates the impact of team dynamics fragmentation. Mistraining and overtraining can foster risk passivity and cyber hesitancy in individuals by instilling a sense of powerlessness, uncertainty, mistrust and blame during cyber-related crises. These effects disrupt team dynamics in two fundamental ways: internal avoidance of responsibility due to heightened risk perceptions; and inter-team friction driven by fears of compromising security.

First, when training inflates risk perception, team members may avoid managing sensitive tasks, fearing the consequences of potential mistakes. One interviewee commented on her team dynamics: "New tools or ideas are immediately dismissed due to potential security risks." Such reluctance also leads to fragmented and counterproductive security measures, impeding collaboration and creating bottlenecks in workflow. Second, overemphasizing security concerns can cause teams to become overly cautious, prioritizing risk avoidance at the expense of operational efficiency. Exaggerating risks may foster a culture of evading responsibility and assigning blame rather than encouraging cross-functional collaboration. For instance, one interviewee observed: "There are three separate teams: IT, cybersecurity

and compliance. Sometimes they pass things [approval requests] between each other, and in the end, you don't know if it's okay or not."[19]

The Empower strategy addresses team dynamics fragmentation by mitigating both intra- and inter-team frictions and instilling a sense of responsibility and agency among employees, transforming them into active participants in security efforts. Empowerment involves more than merely being involved in training; it grants a select group of employees the authority and identity to take proactive steps in cybersecurity. Given that about a third of our interviewees voiced dissatisfaction with the lack of empowerment, the Empowerment strategy addresses a significant concern. In the words of three of the interviewees: 1) "We're always being told what to do when it comes to security, but we're never part of the conversation"; 2) "I think if we got a say in how things are done—like maybe being part of discussions about what protocols make sense for us"; and 3) "I want to be part of the solution, not just a passive follower."

Employees can be empowered at different levels, with varied scopes of responsibility depending on their skillset and level of interest. At the team level, empowering individuals enables organizations to establish team-specific norms that encourage individual responsibility, supported by designated security liaisons within the team. These individuals act as go-to resources, helping to embed security practices into daily routines and workflows. They can also enhance team cohesion during disagreements or periods of confusion. Furthermore, they act as intermediaries, representing their teams in cross-functional interactions, engaging in productive dialogue, providing feedback and helping establish security protocols that balance efficiency with security needs. This in-team support enables a team to make more confident decisions without fear of criticism or blame from colleagues or other departments. Empowerment also fosters a proactive approach to security, where issues are tackled head-on with minimal need for unnecessary external approvals or unproductive interventions from other departments.

The Activate Strategy

The Activate strategy minimizes service and client experience disruption. Mistraining often results in inaction or fragmented knowledge that fails to integrate with broader workflows and practices, particularly when employees engage with external clients. A secure organization, however, requires critical thinkers who understand the interconnections of security practices and can apply their knowledge with awareness of its broader impact. Without this integrated approach, the repercussions extend beyond isolated silos, leading to significant operational and client-facing failures. Any misalignment can have considerable consequences, because individuals may act correctly within their limited scope while missing the larger picture. These issues often manifest as service disruptions and friction, particularly in business contexts where collaboration is paramount.

An exaggerated sense of risk can lead employees to delay or withhold essential services out of fear of security breaches. For example, our interviewees mentioned consequences such as "all they do is create massive bottlenecks" and "they delay services because they're paralyzed by the fear." This lack of coordination between internal and external security protocols often results in unmet collaboration expectations. Additionally, poorly designed cybersecurity readiness programs can impose cumbersome security procedures on external parties, including clients. One interviewee put it succinctly: "They might make us feel safer internally, [but] they're creating barriers to effective business." Another mentioned that his team struggled to provide client information on time due to "endless authorizations, verifications, and paperwork." These additional layers of friction not only inconvenience clients but also hinder employees' ability to address client-triggered security concerns effectively. This can lead to halted

19 These issues are exemplified by the following two case snippets. First, within an accounting firm, a divide emerged over client data security. One group, influenced by recent breaches, insisted on strict encryption for all records. Another group, prioritizing client convenience and efficiency, viewed these measures as cumbersome. This impasse led to resentment: the security-focused team disengaged to avoid blame. In contrast, the efficiency-focused team neglected minor security lapses to meet deadlines, resulting in an avoidable data breach. Second, a project team in a financial services firm, influenced by cybersecurity training, avoided handling sensitive customer data transfers and passed the responsibility to the IT team. Feeling overwhelmed, the IT team involved the compliance department to sidestep responsibility, leading to delays and incomplete data transfers.

services or shifting security responsibilities to clients, ultimately undermining their confidence in the firm's efficiency and security.[20]

The Activate strategy prevents service disruptions and friction by transforming cybersecurity knowledge into coordinated actions that employees can confidently execute. This strategy fosters mastery in coordinated action by integrated learning efforts and collaboration. First, the strategy emphasizes practical training that simulates the organization's cybersecurity ecosystem in an integrated manner rather than using isolated and fragmented training approaches. Many interviewees expressed interest in this type of training; as one put it: "It would help to have more of those group exercises where we can discuss what to do in real situations." Mastery, however, demands training on more than common threats and should incorporate high-impact localized scenarios that align seamlessly with broader organizational workflows—especially when dealing with external stakeholders.

Second, the Activate strategy focuses on scaling mastery by fostering collaborative learning. Recognizing that not every employee can fully experience the breadth of security incidents or understand processes across all departments or client interactions, this collaborative approach facilitates the exchange of insights and lessons learned through formal and informal communication channels. For example, an interviewee shared how she learned from a colleague's experience during an incident response planning session: "In those few minutes, I learned more security practices than I had in hours of formal training." Collaborative learning empowers employees to apply their cybersecurity knowledge with greater confidence and enhance their ability to coordinate effectively with colleagues. This unified approach helps employees navigate the interconnectivity of security protocols without compromising service quality or trust, fostering secure yet seamless interactions with clients and other internal and external stakeholders.

The Normalize Strategy

The Normalize strategy prevents security culture stagnation. A persistent challenge resulting from mistraining is a poor security culture, driven by the perception of security as an isolated compliance task rather than a core organizational value. Many participants viewed cybersecurity readiness programs as disconnected from their daily work and overly individualistic. One shared: "It feels like security is something we only think about when we're forced to do the training, and then it's out of sight, out of mind." When cybersecurity readiness programs are seen as forced training aimed solely at compliance, security measures are perceived as burdensome or designed with a specific audience in mind. This perception fosters a stagnant culture focused on minimal compliance rather than proactive engagement. Threat-driven security messaging further reinforces this culture, normalizing fear, stifling creativity, contributing to cyber hesitancy and ultimately compromising organizational resilience. One interviewee reflected that his company's security protocols were "a list of dos and don'ts, with more don'ts," leading employees to avoid anything with security implications, even if it meant missing opportunities for beneficial collaboration or innovation.

The Normalize strategy addresses these cultural challenges by embedding security values and practices seamlessly into daily operations and organizational norms. This integration goes beyond arbitrary mentions of security values or generic reminders of shared responsibility. Instead, it involves embedding security into daily workflows, decision-making processes, performance evaluations and the broader operational framework of the organization. The strategy therefore allows employees to perceive security as a fundamental operational value rather than an externally imposed burden. As one interviewee suggested, "If it was presented as something that supports our work and makes what we do better, rather than just avoiding disasters, I think people would care more."

The Normalize strategy operates at two complementary levels: the operational level and

20 Imagine a financial advisory firm implementing a new multi-factor authentication (MFA) system. One team encounters major service issues because employees hesitate to handle client onboarding. This creates tension, prompting some advisors to deactivate the MFA, thus jeopardizing client data security. As a result, the client ends its association with the firm, expressing a loss of trust in its security protocols.

the mindset level. At the operational level, the strategy seeks to cultivate a security-first culture by embedding security logic directly into work practices, moving away from excessive directives, frequent refreshers or forced compliance. The Normalize strategy achieves this by embedding security protocols into existing processes and automating security routines. A simple example frequently praised by the interviewees was a phishing reporting tool integrated directly into email clients, allowing employees to treat it as part of their regular workflow. In other words, security should not be treated as stand-alone "security checkpoints" or secondary protocols for established workflows. One interviewee reflected on such integration: "I think it's smart and innovative because it integrates security into our daily workflow, not just during training sessions." The strategy thus ensures that security becomes an inherent aspect of all core activities, making secure practices a natural part of operations rather than an added burden.

At the mindset level, the Normalize strategy redefines cybersecurity as an intrinsic part of every employee's talent, role and contribution, akin to core competencies such as time management, innovativeness and effective communication. Cybersecurity readiness programs can support this shift by moving from fear-inducing and anxiety-provoking messaging to value-centered communication. Interviewees highlighted the impact of positive messaging with sentiments such as "protecting what we've built," "focused on what we can achieve rather than lose," "supporting our work and making what we do better" and "[It] felt like we were working towards something good."

To demonstrate the advantages of perceiving cybersecurity as a core competency, organizations can quantify tangible benefits—such as financial savings, increased profits, enhanced client trust and improved reputation—that result from following specific security protocols. Doing this will encourage employees to consider the cybersecurity readiness program as "just a natural thing we do" rather than "just a formality to avoid lawsuits."

Recommendations for Using the LEAN Model to Design Cybersecurity Readiness Programs

The LEAN model provides a high-level framework, but actionable steps are essential for the practical implementation of each of the four strategies. Table 5 summarizes the goal of each strategy and our two recommendations for implementing it. Together, the eight recommendations (two for each strategy) will enable digital leaders to design cybersecurity readiness programs within existing constraints and operational realities. By adopting these recommendations, organizations will strengthen their cybersecurity without excessive investment in untested methods or reliance on external training partners. The recommendations also align with the current benchmarks and emerging cybersecurity training technologies we studied. Though they are derived from the data acquired from our interviews with representatives of major U.S. accounting firms, the recommendations can be adapted for broader contexts, allowing for necessary adjustments during implementation and taking account of contextual relevance (see Appendix B).

Recommendations for Implementing the Localize Strategy

Aligning cybersecurity training with employees' specific roles, contexts and workflows ensures its relevance and practicality. By tailoring the content, employees can connect more meaningfully with the material, making it more actionable and applicable to their daily responsibilities. As one interviewee stated, "I think the cybersecurity training would hit home a lot more if it was connected to what I actually do day-to-day. Right now, it's just too broad. ... Make it relevant to me, and I'd actually pay more attention."

There was also consensus among the interviewees that foundational cybersecurity knowledge should be established during the onboarding or hiring process, with a focus on role-specific training thereafter. With this tailored approach, employees are less likely to perceive training as "pointless," a "waste of time"

Table 5: Recommendations for Implementing the Four LEAN Model Strategies

Strategy	Goal	Recommendations
Localize	Tailor cybersecurity training to align with employees' specific roles and responsibilities, ensuring relevance and improving engagement.	1. Adopt a role-based adaptive learning regime. 2. Use targeted simulations for situational preparedness.
Empower	Foster a culture of ownership where employees are empowered to make informed security decisions, driving more proactive cybersecurity practices.	3. Cultivate and elevate internal cybersecurity champions. 4. Drive ownership through collaborative development of policies and protocols.
Activate	Promote coordinated security actions through collaborative, real-world simulations that reflect the key decisions employees may face in their workflows.	5. Integrate scenario-based exercises to foster mastery. 6. Establish transparent and semi-structured communication channels to scale mastery.
Normalize	Embed security seamlessly into everyday operations, shifting the focus from compliance to cultivating a proactive, security-first organizational culture.	7. Reframe security as a value-driven enabler of success, not a threat-centric obligation. 8. Nurture middle managers as catalysts for security culture transformation.

or "nonsensical," or describe it as "irrelevant," "common sense" or "redundant." In contrast to the negative sentiment expressed toward generic compliance-awareness training, participants had a more positive outlook on specialized instruction and generally appreciated targeted simulations that were integrative but not distracting. To systematically build on these two observations, we provide two recommendations: 1) adopt an adaptive learning regime and 2) use targeted simulations. Together, these two recommendations will move the focus from generic training to relevant and role-specific training.

Recommendation 1: Adopt a Role-Based Adaptive Learning Regime. We recommend that organizations streamline the training regime to avoid generic awareness education, over-explanation or patronizing content.[21] Instead, they should focus on delivering targeted knowledge and skills tailored to employees' specific roles and contextual requirements. They should leverage technology to personalize the learning experience, using an adaptive learning platform that offers role-based mini-modules. These modules, coupled with micro-credentials, can serve as authoritative markers of learning and qualifiers for assuming more responsibilities, rather than the organization providing superficial incentives just to encourage participation in the learning.

Carefully select the content of each module based on the diverse contextual demands of cybersecurity—such as jurisdiction requirements and organizational functions. Though a centralized team can recommend modules for different employee groups, local security teams, in collaboration with managers familiar with daily workflows, should refine the list of modules and define learning priorities to suit the team's operational realities. Allow employees to bypass modules if they complete related assessments successfully, acknowledging their preexisting knowledge and competencies.[22] This approach aligns well with participants' expectations for improved training because it meets their expectations by respecting individual roles and expertise, focusing on what directly applies

21 For example, imagine the frustration of certified public accountants enduring basic cybersecurity training when they are already familiar with all the concepts as part of their certification. Though legal and compliance requirements may necessitate some awareness training, this could be assessed during the hiring process. New hires only receive such training if they fail the initial tests.

22 Leveraging generative AI offers a cost-efficient way to produce content tailored for specific contexts. Though generic generative AI solutions are anticipated to lead the corporate training sector soon, organizations must still engage in content curation to maintain relevance.

to their daily work and recognizing existing knowledge.

Recommendation 2: Use Targeted Simulations for Situational Preparedness. Organizations should avoid generic simulations and standard gamification techniques. Though these techniques may engage employees, they often lack the practical relevance necessary for genuine preparedness.[23] Engaging training methods do not guarantee meaningful learning and knowledge retention. Instead, prioritize targeted simulations that closely reflect real-world threats employees are likely to face in their specific work environments. These simulations make cybersecurity training more applicable and relatable, fostering proactive learning and heightened situational preparedness. For instance, one interviewee remarked: "A phishing simulation in email is a good example. It feels less like training and more like a real situation. … We take it seriously because there are real consequences for falling into its trap."

The benefit of these simulations lies in their seamless integration with regular workflows and their demand for real-time decision-making, where incorrect actions result in tangible consequences (e.g., temporary account lockout).[24] In contrast, isolated gamified simulations aimed solely at raising awareness often fail to provide immediate benefits, leading to diminished engagement and weaker knowledge retention. Moreover, the absence of immediate feedback for incorrect decisions can further undermine effectiveness, reducing the overall impact of the training.

Recommendations for Implementing the Empower Strategy

Effective cybersecurity readiness programs extend beyond basic education; they also include means for empowering employees to engage in proactive measures. A significant approach to empowerment is to cultivate a sense of ownership and agency among employees, thereby enabling them to make informed decisions during critical moments. For instance, in the words of one of our interviewees, "If we could get involved in shaping some of the policies or even give feedback that's actually listened to, I think I'd be more invested in keeping things secure." However, our findings indicate that not all employees are willing or able to assume greater security responsibilities, and their areas of interest in contributing are limited. To address these realities, we provide two recommendations that respect common preferences and strike a balance between encouraging participation and acknowledging operational limitations. Following, these recommendations will ensure that the cybersecurity readiness program shifts from directive instructions to empowered ownership.

Recommendation 3: Cultivate and Elevate Internal Cybersecurity Champions. Organizations should recognize that some employees are genuinely interested in becoming more involved in cybersecurity. As two of our interviewees pointed out: 1) "I'd like to feel more involved in the cybersecurity decisions we make here" and 2) "Get me more involved during designing the procedure." Employees with this mindset can be empowered to become cybersecurity liaisons or advocates (i.e., champions). Rather than striving to actively involve everyone, focus on identifying and empowering these employees.

As cybersecurity champions, they can liaise between the cybersecurity team and their colleagues, establishing common ground and voicing broader cybersecurity concerns. Empower them to act as role models and mentors with the agency to influence team-level actions. Their responsibilities may span from selecting training and communicating policies to participating in security audits and reporting. Also, recognize and acknowledge their roles openly. By showcasing their real-world contributions, organizations can demonstrate the tangible impact these individuals have in safeguarding the enterprise. This approach cultivates a sense of collective responsibility at the team level, with champions as intermediaries, facilitating open communication and collective actions.

23 Our study findings were consistent with previous research, which revealed that while gamification is effective for raising cybersecurity awareness, it falls short in contributing to the development of operational skills. For example, see Yamin, M. M., Katt, B. and Nowostawski, M. "Serious Games as a Tool to Model Attack and Defense Scenarios for Cyber-Security Exercises," *Computers & Security* (110), November 2021, Article 102450.

24 Emerging AI tools can emulate threats in employees' workflows to test their real-time responses and reporting, offering a more integrated solution than current training using isolated attack simulators.

Recommendation 4: Drive Ownership through Collaborative Development of Policies and Protocols. Organizations should not expect employees to follow policies they had no role in shaping. Instead, they should involve employees directly in developing, reviewing and critiquing cybersecurity protocols, policies and procedures. This approach will create true ownership, strengthen employees' identity with the security framework and drive responsibility for its success. As one interviewee put it: "I think if we got to collaborate more—maybe have some say in the protocols we use—it would make it feel like it's something we're building together rather than just more instructions from above. It would definitely make me take ownership of the security practices more seriously." A collaborative approach ensures protocols are practical, relevant and reflect the unique challenges employees face. It also helps security teams uncover blind spots and address them proactively. Organizations that engaged employees in incident response planning reported higher confidence and better conformance with policies—not because of the plan itself, but because of the identity, ownership and preparedness instilled in the workforce.

Recommendations for Implementing the Activate Strategy

Cybersecurity is inherently interconnected; as such, cybersecurity knowledge must be applied in a coordinated and collaborative manner to achieve meaningful impact. The Activate strategy emphasizes the need to extend cybersecurity readiness beyond individual learning to collective readiness, ensuring that teams have the opportunity to practice what they have learned. One interviewee remarked: "I feel like the training we get is just too individual. I'm sitting alone, watching videos, and doing quizzes, but then, [when] I'm done, it's over. It would be way better if we could do some team exercises where we all practice together. You know, make it feel like we're working through real problems as a group. I think I'd remember a lot more that way."

More specifically, our interviewees expressed enthusiasm for applying their knowledge in two coordinated ways. First, they responded positively to scenario-planning exercises that allowed them to collaborate on tasks like developing incident responses or recovery plans. Second, they valued knowledge sharing on less common threats, appreciating the authenticity and relevance of such discussions. Both approaches foster coordinated action and build confidence, ensuring that cybersecurity readiness is not an isolated task but a shared, team-driven effort. Accordingly, we provide two recommendations: one focusing on fostering mastery through collaborative exercises, and the other on scaling this mastery for coordinated action in times of crisis. Together, these two recommendations will shift the focus of the cybersecurity readiness program from isolated learning to coordinated actions.

Recommendation 5: Integrate Scenario-Based Exercises to Foster Mastery. Organizations should prioritize the cultivation of conditional knowledge—the "why" and "when" behind cybersecurity actions—over simply imparting the "what" and "how." True security relies on critical thinkers who do not just follow rigid protocols. As one interviewee noted: "I need to see why it matters to the work I do. Otherwise, it's just another set of instructions I have to follow." In times of crisis, having a select group of employees with deep expertise who can mentor and guide their peers is far more valuable than relying on a larger group with only surface-level knowledge. To foster this level of expertise, organizations must move beyond superficial, organization-wide campaigns and compliance-driven awareness programs. Instead, they should implement scenario-based learning for key employees across different departments.

We recommend that organizations leverage emerging technology and integrate security exercises for all employees into automated support systems[25] that intermittently challenge employees to collaboratively analyze trade-offs, assess vulnerabilities, reflect on risks and make informed decisions. This approach resonates with a remark from an interviewee: "I think it'd be more effective if we did scenario-based exercises as a team. I learn better when I'm

25 Leading AI self-service chatbot solutions are now integrating cybersecurity support features to provide real-time assistance at a low cost. This integration allows employees to receive immediate help with security-related issues, such as data encryption, thereby enhancing overall cybersecurity awareness and responsiveness within the organization. The next generation of these chatbots will offer personalized and context-aware support, making cybersecurity guidance more accessible and effective for all employees.

working through a situation with others rather than just clicking through a quiz on my own." By focusing on real-world scenarios, this approach enables employees to deepen their mastery of cybersecurity actions.

Recommendation 6: Establish Transparent and Semi-Structured Communication Channels to Scale Mastery. We recommend that organizations create transparent communication channels that scale mastery and foster trust—both essential for coordinated cybersecurity actions. Start by having leadership openly discuss cybersecurity challenges and realities, setting a clear tone of transparency for the entire organization.[26] As noted by some interviewees, top management transparency "set an example," "[made cybersecurity] a priority" and "showed us that security is everyone's job." Next, establish or enhance communication pathways that encourage peer-driven learning through semi-structured[27] knowledge-sharing practices. Recognize and motivate employees to share their expertise on specific key topics[28] that require coordinated action, thereby sparking critical thinking among peers. One interviewee stated that "when insights are presented as internal stories and first-hand accounts, they resonate more deeply than top-down directives."

Such knowledge sharing builds trust in the openness and practicality of cybersecurity readiness efforts. In turn, collaboration naturally emerges from collective reflection on past actions and future opportunities, facilitating unified action when crises arise. This approach ultimately strengthens collective preparedness, but one interviewee acknowledged that there will be trade-offs, stating, "Sometimes sharing information about security issues made people nervous. But in my book, that's way better than keeping everyone in the dark and hoping for the best."

26 Historically, organizations that are not open about security challenges faced higher long-term costs than those embracing transparency. For example, openness about breaches has proven more effective in managing reputational damage and regulatory repercussions.

27 Semi-structured learning and knowledge-sharing environments foster adaptability in dynamic situations, balance individual autonomy with collective goals and promote emergent innovation through a blend of structured guidance and unstructured exploration.

28 Examples include incident response procedures, data handling best practices, access control policies and third-party risk management.

Recommendations for Implementing the Normalize Strategy

Security must be woven into the fabric of organizational culture, going beyond mere declarations or policy adherence. True culture is revealed in how employees instinctively act and interact when not under supervision. The Normalize strategy cultivates this natural behavior by seamlessly embedding security practices and values into daily operations and decision-making processes. As one interviewee remarked: "I wish they could make it part of the everyday workflow—like just a natural thing we do. Maybe if they framed it less like a chore and more like, 'Hey, this is actually a good opportunity for us to protect what we're working on,' it'd be easier to care about it."

The research participants generally expressed a negative attitude toward the compliance-centered and anxiety-inducing culture often present in cybersecurity readiness programs, where employees are constantly reminded of threats and the idea that "security feels like this big, scary thing that's going to go wrong if we don't follow the rules exactly." In contrast, they responded positively to the constructive microcultures fostered by their managers, where security was framed as a positive responsibility rather than a punitive measure. One emphasized: "But if the people we look up to at work are also talking about it and making it a priority, it's going to feel more important to all of us." Embedding security practices as a natural part of every employee's role therefore requires positive framing at the operational level and within individual mindsets. Integrating security in this manner promotes vigilance and collective responsibility, especially when cultivated as a team microculture, thereby reducing the need for constant oversight. Accordingly, we provide two recommendations, which together will ensure the focus of the cybersecurity readiness program moves from compliance-driven obligations to an embedded security culture.

Recommendation 7: Reframe Security as a Value-Driven Enabler of Success, not a Threat-Centric Obligation. Organizations should shift the focus of the cybersecurity readiness program from fear to value. Rather than emphasizing threats and negative outcomes—which can breed security anxiety and fatigue—highlight

the positive impact of cybersecurity on the organization's success. For example, illustrate how robust security practices enable innovation and drive profit by safeguarding intellectual property and ensuring the confidentiality of sensitive data. Underscore how strong security measures protect customer trust, a vital component in preserving brand reputation and loyalty. Showcase how resilient security minimizes downtime and disruptions, thereby enhancing operational efficiency and overall productivity. For example, one interviewee argued: "Fear only gets you so far … it'd be way more motivating if they framed it as something positive—like, protecting what we've built, keeping our projects safe, and being proud of that."

Shifting the narrative from fear and compliance to opportunities and shared success empowers employees. To reinforce this positive mindset, celebrate security achievements and acknowledge the contributions of employees who actively adopt a strong security posture. By recognizing and honoring these accomplishments, digital leaders can create a positive feedback loop reinforcing a proactive security culture.

Recommendation 8: Nurture Middle Managers as Catalysts for Security Culture Transformation. Organizations should empower middle managers to cultivate and enhance employees' security mindset. They should provide them with specialized cybersecurity support and resources, transforming them into pivotal catalysts for security awareness and proactive behavior within their teams. Also, recognize the time and effort they invest in sustaining these efforts. Unlike top executives, middle managers possess the unique ability to influence employee mindsets and reshape operational norms at the grassroots level, making this decentralized approach more effective across the organization. As one interviewee pointed out: "You know what would make a difference? If my manager talked about security in our team meetings or set an example."

With their deep understanding of team workflows and challenges, middle managers are well-positioned to tailor security messages and expectations in ways that resonate more effectively with their employees. Organizations should therefore encourage them to lead by example, facilitate open discussions and integrate security into everyday conversations. Doing this will foster a security mindset integrated into daily work, rather than security being seen as an isolated or abstract obligation.

At the operational level, middle managers should be empowered to translate security policies and practices into team-specific contexts, making security more relatable and applicable to employees' daily tasks. For instance, middle managers can embed security practices into existing processes, job descriptions and performance evaluations. This approach instills a sense of responsibility and underscores the value of security as an integral, indispensable part of employees' roles, ensuring lasting cultural change.

Concluding Comments

Conventional cybersecurity readiness programs often fail to reach their objectives because mistraining and overtraining can lead to unintended consequences at both the individual and organizational levels. To address these failures, we propose a streamlined yet integrated approach to program design that transcends the traditional narrow focus on training methods, instead promoting human-centric strategies that empower employees, cultivate mastery and normalize a security culture for maximum impact. By adopting the LEAN model described in this article and our data-driven recommendations, digital leaders can transform their cybersecurity readiness programs from potential liabilities into strategic assets. Though the LEAN model may not turn every "weakest link" into the strongest, it crafts a chain where each link, unique in strength, contributes to a resilient network.

Appendix A: Research Methodology

Study Focus: Our study focused on large accounting firms such as Deloitte, Ernst & Young, KPMG and PwC because of their industry leadership and significant investment in cybersecurity programs. As benchmarks for best practices, these firms offer valuable insights into modern cybersecurity readiness, especially given their extensive resources, established protocols and regulatory compliance obligations.

Study Sample: The study sample was drawn from U.S.-based employees with one to three years of experience at their firm who had recently completed multiple cybersecurity training sessions. We focused on non-technical employees who frequently handle sensitive data and interact with external clients, making them particularly susceptible to cybersecurity threats. Participants were recruited through an independent LinkedIn panel to ensure a range of perspectives while upholding confidentiality and minimizing bias.

Data Collection and Analysis: We conducted 23 online interviews using open-ended questions to explore participants' experiences with cybersecurity awareness and training programs, focusing on specific practices, personal experiences and their impacts. Data analysis was conducted concurrently with the interviews to reach theoretical "saturation"—the point at which no new insights emerged. A rigorous coding process was employed to identify key insights, categorize strategies and extract major themes and patterns. Existing literature and follow-up interviews complemented this iterative analysis.

Appendix B: Limitations of the LEAN Model

Though our findings are grounded in the context of large accounting firms, they may also be applicable in other industries with similar sizes and characteristics, such as highly regulated or knowledge-intensive organizations. However, several limitations affect the broader applicability of our LEAN model.

- **Case Selection:** Our focus on large accounting firms means that many of the examples and the evidence are most relevant to service-industry and business-to-business (B2B) environments. In these contexts, employees are typically highly educated professionals with access to extensive cybersecurity resources. As such, they may be less susceptible to certain training-related issues we identified, such as risk passivity, compared to less specialized or less experienced employees in other industries. Thus, the potential negative impacts of cybersecurity training might be more severe in organizations with fewer resources or a workforce that lacks the same level of expertise.
- **Participant Recruitment:** We used a non-random, voluntary sample, which could have biased the findings by reflecting the perspectives of those more inclined to engage in cybersecurity discussions. Though ensuring confidentiality, this approach potentially excluded insights into specific organizational climates. Additionally, the sample represents a specific group in terms of experience and exposure to training, limiting the generalization of individual impacts to other employees—for example, those who do not directly work with external clients or handle sensitive data. Moreover, participants' subjective reflections on training sessions and their outcomes could not be objectively verified.
- **Temporal Factors:** The study focused on short-term outcomes and newer employees who underwent the same training programs. This temporal limitation constrains our understanding of the long-term impacts of cybersecurity readiness and its effect on seasoned professionals. Though our findings provide a valuable snapshot for guiding decision-making in similar contexts, they may not fully capture the evolving nature of cybersecurity threats or long-term training outcomes.

Given these limitations, though our LEAN model offers practical guidance, its transferability is tempered by factors such as case selection, participant recruitment and focus on short-term impacts. Thus, our findings should be regarded as heuristics rather than definitive principles—serving as a flexible framework that informs strategic decision-making rather than as absolute solutions.

About the Authors

Kaveh Abhari

Dr. Kaveh Abhari (kabhari@sdsu.edu) is a professor of management information systems at San Diego State University (SDSU) and the faculty director of SDSU's Digital Innovation Lab (DiLab). With over two decades of expertise in consulting,

teaching, and research, he is a leading advocate for humane digital transformation. His work centers on accessible digital entrepreneurship and equitable innovation, using technology as a force for societal impact. At DiLab, Dr. Abhari leads interdisciplinary teams developing intelligent digital ecosystems that enhance employee experience, promote continuous development and support adaptable, inclusive workplaces for the future of work.

Morteza Safaei Pour

Dr. Morteza Safaei Pour (msafaeipour@sdsu.edu), assistant professor of management information systems at San Diego State University, leads impactful research on data-driven approaches in cybersecurity, generative AI, and business technology ecosystems. His focus includes the Internet of Things (IoT), blockchain and machine learning applications to enhance organizational resilience and digital innovation. Supported by NSF and Microsoft grants, his work integrates AI-driven cybersecurity, advanced training techniques and decision support systems to address pressing technological and business challenges. Dr. Safaei Pour's recent studies provide actionable insights into securing digital landscapes and fostering strategic technology adoption in modern business.

Hossein Shirazi

Dr. Hosein Shirazi (hshirazi@sdsu.edu) is an assistant professor of management information systems at the Fowler College of Business, San Diego State University. His research centers on trustworthy AI, focusing on efficient, secure and fair AI applications across cybersecurity, distributed intelligence and healthcare. Dr. Shirazi's work on model compression and federated learning enables collaborative intelligence with data privacy, addressing challenges in phishing detection, the Internet of Things (IoT) and industrial security, and anomaly detection in complex networks. His natural language processing-driven research addresses misinformation detection on social media, particularly in public health contexts.

