Microsoft

Skilling for Secure AI: How Frontier Firms Lead the Way

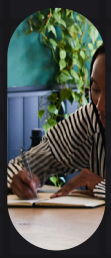


Table of contents

Access this document in additional languages. The English version of this document always has the most up-to-date information.

English | French | German | Japanese | Portuguese | Chinese | Spanish

EXECUTIVE SUMMARY

AI accelerates both innovation and threat sophistication, reshaping the way organizations create value and manage risk.

Frontier Firms—those at the leading edge of innovation, agility, and data-driven operations—are proving that AI can unlock new levels of competitive advantage. One key part of their strategy is grounding their transformation into a continuous AI and security skilling strategy that grows with both the business and the workforce.

> For Frontier Firms, skilling is not a one-time initiative but an ongoing discipline, developing both the expertise to securely implement and use AI, as well as the skills to defend against AI-powered threats.

In this environment, security skills determine whether innovation scales securely or creates new vulnerabilities.

This e-book is designed to help leaders assess their own organization's security skilling readiness in the era of AI—using Frontier Firms as the benchmark for what success looks like. Rather than prescribing a one-size-fits-all security skilling blueprint, this e-book outlines the considerations leaders should weigh as they evaluate their team's readiness. The focus is on connecting strategy to reality by understanding how security responsibilities play out differently across functions.

To bring these dynamics to life, we explore six common functions—**business leaders, line-of-business users, security teams, IT teams, developers, and data specialists**—highlighting the environments they work in, the risks they encounter, and the AI and security skills they need. While the specifics of each organization will differ, beginning with these personas can provide a starting point for evaluating knowledge gaps and shaping strategies that bring security skilling closer to the Frontier Firm model.

Does your organization have the security skills to defend against rising risks in the era of AI?

2,200

cyberattacks occur each day, equating to more than 800,000 attacks around the world every year.[1]

80%

of organizations currently have a dedicated team or plan to have to address security for GenAI.[2]

95%

of security and risk leaders agree their company needs to have security measures in place for their AI apps.[2]

$23.84T

is the forecasted global cost of cybercrime by 2027. [1]

As cyberthreats become more sophisticated, now is the time to prioritize security skills. Empower your entire organization to prepare for, respond to, and prevail against today's evolving technology landscape.

Get started today with Microsoft Learn for Organizations

[1] World Economic Forum, 2023 was a big year for cybercrime – here's how we can make our systems safer, 2024

[2] Microsoft, Accelerate AI transformation with strong security, 2025

Becoming a Frontier Firm in today's evolving security landscape demands continuous, enterprise-wide skill development

By embedding AI across processes and decisions, organizations are driving a new era of innovation while simultaneously expanding the threat landscape. In this environment, security risks must be addressed proactively, making security skills a critical determinant of whether an organization can move fast without breaking trust.

Frontier Firms are prime examples of organizations that are navigating this moment successfully. They treat AI as both a catalyst for innovation and a new vector of risk, recognizing that how it's used matters as much as where it's deployed. For example, AI tools can take on repetitive security tasks, freeing experts to focus on high-value work. But using a new tool effectively requires the right skilling to help ensure employees can maximize the benefits of AI while minimizing risk.

> With AI influencing how every team works, security is no longer confined to a single team's domain—risks can surface in tools, processes, and day-to-day choices made across the organization. Frontier Firms recognize that security is less about one team's mandate and more about a shared responsibility embedded into everyday work.

With this shared responsibility, every employee (regardless of role) must be equipped with the skills to understand, identify, and mitigate risks in the context of their daily responsibilities.

That's why generalized, once-a-year security trainings simply don't cut it in today's evolving landscape. Security skilling must be role-specific and directly tied to how people actually work. It's up to leadership to assess where the security knowledge gaps exist and to drive cross-functional collaboration between security teams and other departments. When organizations embed skilling as a cultural pillar, they unlock faster adoption of secure practices, enable secure innovation, and build long-term resilience into the fabric of their operations.

This e-book is designed help you contextualize and identify AI and security learning opportunities across your organization to better understand and respond to today's rapidly evolving climate. It begins with a look at why our current environment makes security a shared responsibility, and then explores how you can assess knowledge gaps and prioritize learning needs across different roles, all with the goal of improving security skilling.

Security is everyone's responsibility: Assessing knowledge gaps and learning needs

Frontier Firms show us that security skilling succeeds when it's role-specific and grounded in daily work. There isn't a single blueprint for security skilling since every organization will look different, but certain patterns emerge. Teams across functions need both a baseline of shared security awareness and specialized skills tied to their day-to-day responsibilities.

The following sections highlight six core functions we commonly see: Business leaders, line of business users, security teams, IT teams, developers, and data specialists.

For each role, we describe the environment they operate in, the security skills needed, and takeaways you can act on. Together, these perspectives provide a starting point for identifying knowledge gaps and building the skills across your organization to operate like a Frontier Firm.

SECURITY IS EVERYONE'S RESPONSIBILITY

Business leaders

Business leaders play a defining role in shaping how their organizations evolve into Frontier Firms. Their role extends beyond setting strategy, by establishing the culture, priorities, and investment choices that determine how AI and security skilling are integrated. In this era of AI, leadership decisions can carry greater weight and require a clear understanding of security implications. It's in the hands of executives to champion a culture of continuous learning—where developing new AI and security skills is encouraged, supported, and trusted across every team.

Skills needed

When leaders align skilling initiatives to broader business goals and make them visible in their own work, they create the cultural foundation that allows their workforce to adapt securely as technology and threats evolve. Leaders should be equipped for risk-aware decision-making, practicing secure collaboration in their own work, and cultivating enough AI literacy to fully understand the opportunities and risks their teams encounter. For example, when approving the adoption of a new AI-driven customer platform, leaders need the skills to evaluate how data sharing is managed and whether security practices align with business priorities. Similarly, when entering a strategic partnership, leaders must apply secure collaboration skills to ensure agreements are structured with trust in mind.

Key takeaways

- Recognize that culture starts with leadership by modeling continuous AI and security learning, and make it visible.
- Incorporate security and AI literacy into leadership development programs.
- Champion security skilling as a core business priority, and lead by example with your own skilling journey.
- Align AI and security skilling investments with strategic outcomes, such as resilience, innovation, and trust.

SECURITY IS EVERYONE'S RESPONSIBILITY

Line-of-business users

Line-of-business users now play a critical role in shaping their organization's security posture. Their interactions with data, platforms, and AI tools may seem routine, but each decision has the potential to introduce risk. A marketing manager using generative AI to draft campaign content needs to understand how to handle customer data appropriately, while an operations analyst leveraging AI for reporting needs the skills to validate results and ensure accuracy. These day-to-day choices highlight why continuous role-specific skilling is essential.

Skills needed

To operate securely, line-of-business users need the ability to recognize when tools introduce risk, apply secure practices to protect sensitive information, and act quickly when something feels off. For instance, a sales associate using an AI assistant to prepare client proposals should be well-versed to apply guardrails to keep proprietary data protected. Equally important is knowing how and when to collaborate with security teams, so concerns are surfaced and addressed before they escalate. With the right skills, line-of-business users help strengthen organizational security rather than inadvertently creating vulnerabilities.

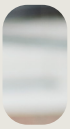
Key takeaways

- Pair AI tool rollouts with contextual, role-specific security training.
- Encourage regular collaboration between business units and security teams to address risks early.
- Foster an environment where employees feel safe escalating concerns to security teams.
- Provide practical, scenario-based skilling that mirrors actual workflows and security threats.

SECURITY IS EVERYONE'S RESPONSIBILITY

Security teams

Security teams have always been the frontline defenders of organizational security, but their responsibilities have evolved. Threat actors are now using AI to scale attacks, automate reconnaissance, and exploit vulnerabilities at unprecedented speed. At the same time, security teams are being asked to enable secure AI adoption inside the business—reviewing vendor solutions, advising on internal AI projects, and shaping governance policies. Their work no longer stops at detection and response; it now includes acting as a cross-functional educator, guiding colleagues across IT, data, and development teams to innovate securely.



Skills needed

To keep pace, security teams must build skills in collaboration and enablement, ensuring they can work effectively with IT, developers, and data specialists on shared challenges. They also need the ability to stay ahead of AI-driven threats, such as adversarial model manipulation or automated phishing, which requires continual learning and threat intelligence adaptation. Just as important is the ability to proactively assess internal risks, including shadow AI use by employees or poorly configured AI integrations.

Key takeaways

- **Equip security teams with the time and resources to act as cross-functional partners.**
- **Support continuous learning focused on AI-specific threats and emerging attack techniques.**
- **Measure security team success by their enablement impact across departments, not just by incident metrics.**
- **Encourage security teams to take ownership of security education, shaping tailored programs that empower other functions.**

SECURITY IS EVERYONE'S RESPONSIBILITY

IT teams

IT teams manage the backbone of digital infrastructure, which now includes a growing ecosystem of AI-powered tools and platforms. Their role has become more central than ever: the way they configure, integrate, and maintain systems directly shapes the organization's overall security posture. As AI adoption scales, IT's responsibility extends beyond uptime and efficiency to ensure the technologies empowering productivity are also reinforcing secure practices. In Frontier Firms, IT is viewed as a strategic partner in secure transformation by helping the organization innovate with confidence—keeping systems strong, stable, and aligned to evolving security expectations.

Skills needed

To meet these challenges, IT teams must strengthen skills in secure cloud configuration and identity governance, ensuring that systems are designed with the principles of least privilege and evolving access needs in mind. They also need capabilities in AI-aware monitoring, so they can recognize new usage patterns, anomalies, and risks introduced by AI workloads. As organizations automate more processes with AI, IT teams must build skills in secure automation deployment—rolling out new tools without creating exploitable gaps. Finally, IT must enhance cross-team coordination skills by working closely with security teams to align configurations, share intelligence, and anticipate potential risks before they escalate. With the right skilling, IT teams become more than operators of infrastructure by actively partnering in building organizational resilience.

Key takeaways

- **Position IT as a strategic partner in secure AI adoption and the integration of new systems.**
- **Invest in continuous training for IT teams on cloud, identity, and AI-aware monitoring.**
- **Encourage joint training and planning between IT and security teams to close knowledge gaps.**
- **Reward secure deployment outcomes alongside efficiency and uptime metrics.**

SECURITY IS EVERYONE'S RESPONSIBILITY

Developers

Developers are the center of how organizations innovate. The systems, applications, and tools they build become core to business operations—when security is embedded from the start, these solutions drive both innovation and resilience. Today's development cycles are accelerating with the help of AI-powered assistance, giving teams new ways to build faster and experiment more. But speed also places greater importance on secure practices. In this environment, developers are not just builders of products, but key contributors for secure innovation across the enterprise, becoming early collaborators with security teams, so potential issues are surfaced and resolved before code moves into production.

Skills needed

Developers need to strengthen secure coding practices to make security an integral part of the software development lifecycle. They also need the ability to perform threat modeling, thinking ahead about how attackers might exploit design choices before a single line of code is written. As AI coding assistants become more common, developers must build skills in prompt engineering hygiene, understanding how the prompts they use can inadvertently introduce security flaws or intellectual property exposure.

Key takeaways

- Make secure coding and threat modeling core parts of developer onboarding and ongoing training.
- Provide secure-by-default tools and guardrails for AI-assisted coding.
- Incorporate early collaboration between development and security teams as a core part of the developer's skilling strategy.
- Provide guidance on how to integrate security metrics into engineering performance goals to reinforce accountability.

SECURITY IS EVERYONE'S RESPONSIBILITY

Data specialists

Data specialists shape how information is collected, stored, and used—making their work central to both AI innovation and organizational security. The datasets they build and manage power AI models, analytics, and decision-making, which means their contributions directly influence the quality and impact of business outcomes. With AI advancing rapidly, the opportunity for data specialists is immense: they can fuel more accurate insights, enable new capabilities, and create systems that drive competitive advantage. But to maximize this potential, data specialists must apply strong security and governance practices that ensure the data is protected, responsibly managed, and used in ways that maintain trust.

Skills needed

To succeed in their role, data specialists must be able to keep sensitive information secure while ensuring that AI systems remain reliable and ethical. That means knowing how to train models without exposing confidential data, setting clear guardrails for data governance and access, and addressing risks like bias or drift that can compromise both performance and trust. Beyond understanding technical safeguards, such as encryption, they also need the ability to work closely with security teams to help prevent isolated data issues from becoming enterprise-wide problems.

Key takeaways

- Elevate data specialists as key stakeholders in skilling strategies for both AI and security governance.
- Provide specialized training in AI-specific data risks, including bias and drift mitigation.
- Educate data specialists on how to align data governance practices closely with security policies and compliance requirements.
- Help ensure data teams are integrated into incident response planning and drills by providing training on how their roles impact the process and why their contribution matters.

Leading with skilling in today's security landscape

Securing the organization in the age of AI is not only about the tools you deploy but also about the culture you build. Frontier Firms treat AI and security skilling as a core commitment that helps fuel their transformation and agility. They model continuous learning at the top, set expectations across teams, and invest in training that equips people with the skills to make secure choices in their daily work.

Security resilience can grow when leaders allocate resources for ongoing, cross-functional learning and create accountability structures that ensure progress continues over time. By embedding skilling into daily operations and decision-making, organizations turn security from a compliance exercise into a competitive advantage—one that enables innovation to scale securely.

The path to becoming a Frontier Firm looks different in every enterprise, but the starting point is clear: treat security skilling as a foundational pillar.

Discover how Microsoft Learn for Organizations can help accelerate your AI and security skill-building journey.

learn.microsoft.com/training/organizations

READINESS GUIDE

Security skilling for AI

Use this tool to help you assess how prepared your organization is for security skilling in the era of AI. This guide suggests discussion points to leverage with executive peers and functional leaders. These conversations can help surface skilling gaps, spark cross-functional collaboration, and identify priority areas for skilling investments. This guide is not a one-time checklist—it's a starting point for an ongoing conversation. Return to it regularly as your AI and security strategy evolves. By revisiting this assessment, you can help your organization move closer to the resilience and agility that define Frontier Firms.

Organizational foundations

Establish whether the organization treats security skilling as a compliance necessity, an operational requirement, or a strategic driver of resilience and trust. This step sets the tone for how prepared the organization is to evolve. Capture both points of alignment and disagreement among leaders. The aim is to reveal whether there's a shared understanding of security's role and if the conditions for continuous skilling are in place.

Discussion points

- How is security currently positioned in the organization—primarily as compliance, risk mitigation, or as a driver of innovation and trust?
- In what ways are leaders actively modeling continuous learning around AI and security? Where are there strong examples, and what areas need to be improved?
- What dedicated structures—budget, time, incentives—exist to support ongoing skilling? Where are the gaps that hold the organization back?

Shared responsibility

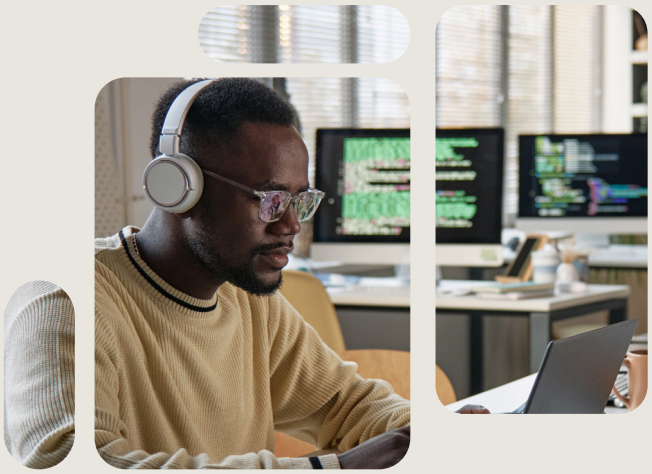
Explore how well the organization's culture reinforces that security skilling is everyone's responsibility, not just the domain of the security team. Go beyond generic annual compliance training to focus on behaviors. Identify whether employees across functions truly feel accountable for secure practices, and whether leadership is reinforcing that mindset while supporting learning opportunities.

Discussion points

- How consistently is security framed as a shared responsibility across teams? What channels, forums, or other communication touchpoints can be leveraged for new AI and security skilling initiatives?
- How well do our role-based training paths reflect day-to-day work? Where do employees feel training misses the mark?

Role-specific assessment

Surface the unique skilling needs of different functions. This is where leadership can identify the specific gaps that prevent teams from innovating securely. Work through each persona group as a team. Identify where the biggest risks come from under-skilled roles and where better collaboration could strengthen security outcomes.



Discussion points by persona

Business leaders

- At a strategic level, does the organization have the fluency to evaluate the opportunities and risks of adopting new AI tools?
- How is the organization signaling—through actions, not just words—that security skilling is a leadership priority?

Line-of-business users

- What skills do employees need to confidently and securely use AI tools in their daily work, and where are the most noticeable gaps today?
- When employees encounter suspicious activity, what skills and processes should guide them in knowing how and when to escalate the issue to security teams?

Security teams

- Do security professionals have access to the latest knowledge and skills to anticipate and counter AI-driven threats?
- How effectively are security professionals enabling other teams to innovate securely?

IT teams

- How well are IT teams trained to monitor AI systems, manage identity governance, and securely deploy automation at scale?
- In what ways are IT and security collaborating, and where do silos still exist?

Developers

- What skills do developers need to consistently apply secure coding practices and threat modeling throughout the development lifecycle, and where do gaps exist today?
- What skilling would help developers engage security teams earlier in the process—before deployment—so potential issues are addressed proactively rather than reactively?

Data specialists

- Do the data teams have the skills to securely train AI models, manage governance, and mitigate risks like bias and drift?
- How effective are data specialists at integrating security planning and incident response into their workflows?

Feedback and accountability

Ensure that security skilling doesn't stop with training—it must be measured, evolved, and reinforced over time. Close the loop by defining accountability. Agree on who owns measurement, how results are shared, and how leaders will adjust strategies as the security and AI landscape evolves.

Discussion points

- How does the organization currently track progress in security skilling across teams, and what metrics (beyond completion rates) give real insight?
- How does the organization help ensure skilling efforts evolve alongside new technologies, AI capabilities, and emerging threats?
- What gaps feel most urgent to address in the next 6–12 months, and what are the risks of delaying?

Microsoft