Pluralsight

Cybersecurity in the AI Age

How to Go from Skills Gaps to Cyber Resilience

Executive summary

Cyberattacks are growing in number and complexity with no signs of slowing down. According to the World Economic Forum, 72% of organizations have reported an increase in organizational cyber risks. And between AI-accelerated threats and the persistent skills shortage, it's getting harder for organizations to protect themselves.

But here's the bitter reality: No matter how strong your defenses or how detailed your policy documents, attacks happen. Ideally, you have sufficient depth of controls to eliminate the majority of attacks. But when an attack is successful, what truly matters is how you respond and recover.

In this guide, you'll learn how to close security skills gaps and improve your organization's cyber resilience to maintain business continuity and customer trust in the AI era.

If there's one thing you take away from this guide, it should be this: **You can't buy cybersecurity resilience**. It doesn't come equipped with a specific cybersecurity solution or tool. Building resilience requires a mix of technology, culture, and skills working in tandem to protect your organization and maintain operations even when (not if) incidents occur.

Table of Contents

Section 1

The evolving threat landscape: AI and post-quantum encryption change the game

The threat landscape never stands still, and AI and quantum computing are accelerating current risks and introducing new ones.

In fact, Gartner predicts that 17% of cyberattacks will employ generative AI by 2027. And 73% of organizations in the US believe "it's only a matter of time" before cybercriminals are using the power of quantum to decrypt and disrupt today's cybersecurity protocols.

> The biggest shifts ahead are AI-driven offense and defense battles, post-quantum cryptography adoption, continuous adaptive trust replacing static zero trust, unified security platforms across cloud and identity, and a stronger focus on resilience over pure prevention. It's likely these will redefine how organizations secure data, systems, and people in 2026 and beyond.
>
> **Christopher Rees**
> Pluralsight Author, Principal AI Strategist for Unisys, and Cybersecurity Expert

Here's how AI and quantum are changing the cybersecurity landscape:

Automated, personalized social engineering tactics become more prevalent

Identity abuse and social engineering remain dominant initial-access paths. Verizon's Data Breach Investigations Report found that the "human element" plays a role in a majority of breaches (e.g., via phishing, credential misuse, or user error). And in 2025, CrowdStrike reported that adversaries increasingly favor hands-on-keyboard intrusion and social engineering—particularly vishing—over commodity malware.

One example is a vishing campaign that targeted multiple Salesforce customers. Threat actors posed as IT support and persuaded employees to take actions (like approving a malicious app connection or sharing credentials) that enabled access.

The result? The attackers claim they stole nearly 1 billion customer records, though actual record counts varied by victim.

Regardless of the exact count, threat actors will use AI to conduct similar social engineering attacks with greater sophistication and frequency, including:

- Scoping targets with AI to build detailed profiles based on digital footprints like social media and online activity
- Personalizing attacks with LLMs using data about a target's family, friends, and colleagues
- Crafting convincing phishing emails and fake audio and video clips (deepfakes) to deceive their target

These tasks can be automated, raising the bar for defenders who will face daily AI-enhanced cyberattacks that are highly personalized to the intended victim.

Adaptive malware rewrites code to avoid detection or adapt to defenses

While bad actors have generally favored using AI for social engineering, they're starting to turn its power to malware, too.

Unlike traditional malware with static or unchanging code, adaptive malware uses AI to adapt in real time when attacking. This includes the ability to:

- Dynamically generate new scripts to avoid detection or adapt to security measures
- Create new attack vectors in response to a target's defenses
- Personalize attacks based on a target's unique vulnerabilities
- Hide their code from security software

Adaptive malware is still relatively new, but it's expected to grow, making it harder for defenders to detect and eradicate threats as it does. To prepare, organizations will need to move beyond traditional detection tools.

Quantum computing renders some traditional encryption algorithms ineffective

Quantum computing isn't a drop-in replacement for today's computers. However, a sufficiently large, fault-tolerant quantum computer could break widely used public-key cryptography like RSA and elliptic-curve cryptography. As a result, threat actors with access to a quantum computer could decrypt data they wouldn't be able to touch with a classic computer.

Some threat actors are already using "harvest now, decrypt later" tactics. By stealing and holding encrypted data today, they can decrypt it with future quantum capabilities.

This is especially relevant for data with long-lived confidentiality requirements. Even though 69% of senior cybersecurity managers recognize the risk quantum computing poses to legacy encryption technologies, only 5% have implemented quantum-safe encryption. It's critical to start preparing now. Early quantum capabilities will be scarce and expensive, so attackers will prioritize high-value data with long-lived confidentiality.

Conduct a cryptography inventory and assess where your organization uses cryptography, what algorithms and keys are used, and what your data retention needs look like. Then plan migration to post-quantum cryptography (PQC) as standards and products mature, prioritizing data with high risk and a long lifetime.

Data being encrypted today could be harvested and broken in the future. Adopting quantum-safe standards early protects sensitive information with long-term value (e.g., intellectual property, finance, healthcare, government).

Christopher Rees
Pluralsight Author, Principal AI Strategist for Unisys, and Cybersecurity Expert

Key takeaways

Between AI-driven threats and quantum computing, the gap between attacker speed and defender capability is widening.

The National Institute of Standards and Technology's (NIST) preliminary Cyber AI Profile draft organizes guidance for managing AI-related cybersecurity risk into three focus areas:

- **Secure:** Focus on managing cybersecurity challenges when integrating AI into organizational ecosystems and infrastructure.
- **Defend:** Identify opportunities to use AI to enhance cybersecurity processes and activities, while understanding challenges when leveraging AI to support defensive operations.
- **Thwart:** Build resilience to protect against new AI-enabled threat vectors and cyberattacks.

Remember: While bad actors may use AI and quantum computing to power their attacks, these technologies can also be a boon for defenders, allowing them to identify vulnerabilities and analyze data faster.

But they come with their own challenges, like governance and overreliance. Most importantly, both technologies require people with the skills to use them appropriately.

Section 2

The overlooked vulnerability: Cybersecurity skills gaps

For years, organizations have kicked cybersecurity cans down the road, either unable or unwilling to deal with the human aspect of cybersecurity: lack of skilled staff, burnout, and mental health.

But as AI, quantum, and supply chain risks become more urgent, organizations will no longer be able to postpone or ignore these threats.

Cybersecurity is already the largest, and one of the most damaging, skills gaps. In 2025, this gap actually increased by 8% according to the World Economic Forum, with only 14% of organizations confident they have the people and skills they need today.

Tech practitioners also ranked cybersecurity as the most important skill for them to learn in 2026, while executives ranked it as the second-most important growth area for their business, according to the Pluralsight Tech Skills Report.

Why does this gap exist in the first place?

Lack of security talent

For one thing, there simply aren't enough cybersecurity professionals. In fact, 4.8 million cybersecurity roles remain unfilled, representing a 19% year-over-year increase.

But not all roles are needed equally. In many cases, AI and automation have replaced the need for entry-level roles. Instead, many organizations are looking for professionals who are mid-level and above or have a specialized skill set their business needs. And those folks are a lot harder to find in market.

Tightening budgets and other economic factors

36% of organizations have experienced cybersecurity budget cuts in the past 12 months, and nearly a quarter have undergone layoffs. Add in hiring freezes and the rising cost of cybercrime (the global average cost of a data breach is $4.4 million), and it's not surprising that organizations still have critical security skills gaps: They don't have the funds or resources to fill them—especially if they only want to hire externally.

Occupational burnout and stress

Constantly battling threats and anxiously anticipating the next cyberattack takes a toll on mental health. One-third (32%) of cybersecurity professionals are kept awake at night by job stress, and at least two-thirds (65%) have considered leaving their job

because of stress.

In some cases, they follow through: Among organizations that reported difficulty retaining qualified security professionals, nearly half (46%) said high work stress levels contribute to attrition.

When organizations fail to retain their security talent, their skills gaps get even bigger. If those roles sit open for an extended period of time, the gap will only widen further.

Rapid pace of tech change

Even if your organization is lucky enough to have a solid team of security professionals, a reasonable budget, and a healthy work culture, tech is changing faster than organizations are training.

Most of them are already investing in skill development. In 2025, tech professionals dramatically increased their consumption of cybersecurity-related topics such as security management (164%), cloud security (93%), and secure coding (102%).
But it's not happening fast enough—or at sufficient scale.

Like other departments, learning and development is struggling to keep pace with the latest AI vulnerabilities, quantum risks, and other threats. Annual security training and lengthy video courses are no longer enough for nontechnical professionals, much less security pros. Organizations need to level up their learning and development strategy if they want to make meaningful progress in filling the skills gap.

Key takeaways

When you consider all of these factors, it's clear that hiring isn't a sustainable long-term solution to the security skills gap. It's not going to solve the talent shortage, decreased budgets, burnout, or the fast pace of tech change. In some cases, it can even exacerbate these issues.

Instead, organizations will need to make a more fundamental shift at the culture layer. Tackling the cybersecurity skills gap by investing in their current people will set resilient organizations apart from the rest.

Section 3

The new cybersecurity skills stack

When we talk about the cybersecurity skills gap, we're really talking about the skills organizations currently lack—but need—to build cyber resilience. In the age of AI and quantum computing, these are the cybersecurity skills your people need to protect your organization.

1. Cloud and infrastructure security

As organizations continue to operate in multicloud and hybrid environments, misconfigurations—not zero-day exploits—remain the leading cause of breaches.

Cloud security is no longer a specialist function. Every security professional must understand how modern infrastructure is built, deployed, and exposed.

Core capabilities

- Cloud platforms (AWS, Azure, GCP) and shared responsibility models
- Identity and access management (IAM)
- Network segmentation and monitoring
- Infrastructure-as-code (IaC) security

Recommended Pluralsight learning paths

- Cloud Security
- AWS Cloud Security
- AZ-500 Microsoft Azure Security Technologies
- Google Cloud Professional Security Engineer

2. Zero trust and identity-first security

Perimeter security models with firewalls and intrusion detection aren't enough to mitigate threats. Identity is now the primary control plane.

Organizations need perimeterless security, or zero trust, following the principle of least privilege, enabling multi-factor authentication (MFA), and conducting continuous monitoring and validation.

Core capabilities

- Zero trust architecture and principles
- Identity governance and privileged access management
- Continuous authentication and authorization
- Device access control and authorization

Recommended Pluralsight learning paths

- Zero Trust Security (ZTS)
- Identity and Access Management (IAM) Tools and Techniques

> Traditional network security has been a catastrophic failure at protecting digital resources for decades. A correctly implemented and maintained zero-trust architecture treats all access as a breach and assumes all environments are hostile. Each day an organization delays maturing in its zero-trust journey is a day when the risk of exploitation grows exponentially.
>
> **Dr. Lyron Andrews**
>
> Pluralsight Author Fellow

3. Secure software development and DevSecOps

If security is bolted on after code ships, your security team will be overwhelmed trying to fix a range of costly vulnerabilities.

Secure coding and DevSecOps best practices need to be integrated into the software development lifecycle from the very beginning to reduce risk and improve efficiency.

Core capabilities

- Secure coding principles
- OWASP top 10 vulnerabilities
- CI/CD pipeline security
- Threat modeling and code scanning

Recommended Pluralsight learning paths

- The OWASP Top 10
- Secure Coding Using OWASP Top 10
- Fundamentals of DevSecOps
- Secure Coding

4. AI and data security fundamentals

From phishing attacks and AI hallucinations to data poisoning, prompt injection, and supply chain risks, AI has led to a host of new threats and vulnerabilities. AI has also

transformed security itself, requiring organizations to defend against AI-augmented attackers, use AI for better defense, and protect and secure their own AI and agentic systems.

Awareness of AI and data security is now critical for every security professional to assess risk to their organization's own use of AI, to identify areas where they can use AI to outpace attackers, and to maintain situational awareness of how attackers use AI.

Core capabilities

- AI architecture and the AI attack surface
- Threat intelligence
- AI risk and governance
- Threat detection and modeling
- Incident response automation
- Log analysis

Recommended Pluralsight learning paths

- Generative AI for Security Professionals
- AI-based Threat Detection
- Breaking News: CVEs and Hot Takes

> Security teams need to understand how to protect the AI systems deployed in their own organizations. There's lots to build on existing knowledge, but securing AI also requires a paradigm shift. We've spent years keeping data and code separate. By their very nature, prompts are data and code intertwined. Prompt injection will make SQLi and XSS look like child's play, especially when agents chain prompts from one system to another. Security professionals need to understand the new AI attack surface, which means learning AI architecture and then how to apply their existing skills to the new paradigm.
>
> **John Elliott**
>
> Pluralsight Author Fellow and Security Specialist

5. Soft skills

While AI can be a powerful way to automate things like threat detection and incident response, a human still needs to be in the loop. Soft skills are just as critical as hard technical skills to properly assess risk, relate security to business goals, and train people outside the security organization.

Core capabilities

- Critical thinking
- Cross-functional communication
- Translating risk to business leaders
- Adaptability and decision-making under pressure

Recommended Pluralsight courses

- Critical Thinking and Problem Solving
- Communication Skills for Technologists

Key takeaways

Tech has evolved, and the skills your people need to detect, respond to, and recover from threats have changed, too.

The new cybersecurity skills stack consists of cloud security, zero trust, DevSecOps, AI and data fundamentals, and soft skills like communication and adaptability.

Identifying your organization's gaps is the starting point for building skills and, ultimately, cyber resilience.

Section 4

How to develop a security culture of readiness and resilience

At its core, resilience isn't about stopping cyberattacks. It's about maintaining critical business continuity throughout the attack.

Beyond cybersecurity tools and solutions, **resilience calls for a mindset shift that encompasses your people, culture, and approach to skill development.**

Here's how to build a security culture that fosters readiness and resilience.

> Cyber resilience is your organization's ability to continue operating when things go wrong. It's not just about bouncing back either. It's about absorbing the hit in the first place, adapting to new realities, and staying in motion without losing the trust of your customers, partners, or people.
>
> And that means resilience isn't just a function of how good our technical controls are. It's a function of leadership clarity, culture, investment choices, and decision-making under pressure. It's a whole system capability, not a side program.
>
> **Matt Lloyd Davies**
> Pluralsight Cybersecurity Author and Researcher

Identify current security skills gaps

If you're like many organizations, you've had to abandon projects because you didn't have the right tech skills. Are there any patterns in those projects? Are the same skills always missing? If the answer is yes, you've found a skills gap to target with upskilling.

If you don't see any noticeable patterns (and even if you do), ask employees to take skill assessments. This will give you an idea of their current skill levels and gaps so you can design upskilling initiatives to address them.

And don't forget: Your technologists are one of your best sources of insight. **38% say their leaders are not aware of the IT skills gap.** As the ones responsible for executing your key initiatives, they've felt the impact of skills gaps the most and can identify the most critical security needs.

Understand the difference between security and compliance

Treat compliance as a starting point, not a destination. Resilient organizations:

- Embed cybersecurity in decision-making across the entire organization, not just tech teams
- Develop products with resiliency in mind
- Prioritize investments and vet suppliers based on cybersecurity principles
- Provide cybersecurity awareness training
- See security as a critical part of business continuity planning

> Compliance doesn't equal readiness. I see plans that say failover to another region, but no one has ever tested DNS replication, IAM, or service endpoints. You only know you're resilient if you've tested.
>
> **Chris Jackson**
> Pluralsight Senior Cloud Security Author

Invest in hands-on learning and practice

A real security incident is messy. It's chaotic. And no matter how well-documented your

recovery plans are, a checklist doesn't cut it in the middle of a breach.

Luckily, practice builds preparation. Conduct real-world tabletop exercises and practice your recovery plans. This gives you the chance to see where your documentation fails and how your people respond to stress.

The key factor is how closely your test environment resembles production so you can create a true and effective drill while using observed Tactics, Techniques, and Procedures (TTPs) found in the MITRE ATT&CK framework.

As your security professionals go through these exercises, they'll eventually develop muscle memory, making them better equipped to respond to real threat scenarios.

Outside of these practice sessions, invest in continuous hands-on learning for your team to gain more experience with the latest threats and security techniques. Role-based learning paths are one way to do that. They provide tailored, hands-on labs with real-world scenarios for incident response, GRC, threat intelligence, and other roles.

> As AI and automation streamline many development tasks, entry-level roles are disappearing, creating a widening gap between education and employability. Without hands-on pathways, we risk losing an entire generation of emerging talent—and with it, the diversity and creativity that drive innovation.
>
> **James Willett**
> Pluralsight Author and AI/Cloud Architecture/Software Engineering Expert

Provide time to learn

Less than half (46%) of organizations provide time to learn on the job. The same number enables managers to give their team time to learn.

Dedicated learning time is critical, and it involves more than a calendar block or a vague directive to “Go learn.” Cybersecurity professionals don’t have spare time to pick up new skills. They need it built into their work schedules.

At first, it may feel like you’re falling behind on day-to-day work. But over time, continuous learning has real benefits, like faster incident response, higher retention, and better security posture.

To get started:

- **Protect learning time:** Set or allocate dedicated time to upskill and incorporate learning into the flow of work.
- **Enable managers:** Make sure they understand upskilling is a priority and that timelines will need to shift for learning.
- **Tie learning to KPIs:** Build performance metrics around learning for team members, managers, and top-level leadership.

Learn how to enable managers and roll out effective upskilling campaigns with the Tech Upskilling Playbook.

Build cybersecurity fluency across teams

Cybersecurity professionals aren’t the only ones who need to understand the latest threats and the role they play in keeping their organization safe. Building fluency across the whole organization has two core benefits: First, it strengthens your entire security posture. When everyone feels a sense of responsibility and understands how to spot things like phishing attacks, you build more resilient teams and decrease risk.

Second, it helps you identify and develop people from other teams who might be a good fit for a cybersecurity role. As the number of entry-level roles shrink, internal mobility and upskilling nontechnical professionals can help you fill critical skills gaps.

> Tech leaders should look within: Identify colleagues who have tenacity and drive, who have an interest in technology, and invest in them. Train them, and give them time within work to train.
>
> **Mike McQuillan**
> Pluralsight Author, Head of IT at Halls, and Data and Software Development Specialist

Measure skill progression and create leadership accountability

The end goal of upskilling isn't to learn new skills and knowledge. It's for employees to be able to use new skills or knowledge to build better products, hit mission-critical objectives, or improve customer experiences.

When measuring upskilling success, look beyond engagement metrics like course completion or number of certifications earned. While these are still important, they don't tell the full story of upskilling's impact.

Instead, focus on outcomes like:

- Have employees' skills improved?
- How have technologists applied their new skills or knowledge on the job?
- How has upskilling increased technologists' confidence?
- How has upskilling improved work or efficiency, shortened project timelines, reduced error rates, or increased revenue?

If you really want to prioritize cybersecurity resilience, make it a board-level KPI.

Leaders should discuss resilience and recovery readiness metrics alongside other performance measures.

Key takeaways

Culture can sometimes feel like an afterthought when you're dealing with the latest vulnerabilities or a new AI threat. Don't let it be.

A security culture is what allows cyber resilience to take root. When you give your people time to learn, practice incident response, and measure skill acquisition, you make security an integral part of everyday operations. Over time, secure best practices become indistinguishable from business best practices.

As you build or strengthen your organization's security culture, move beyond policies. Leadership actions and building security into everyday operations are what really move the needle.

Conclusion

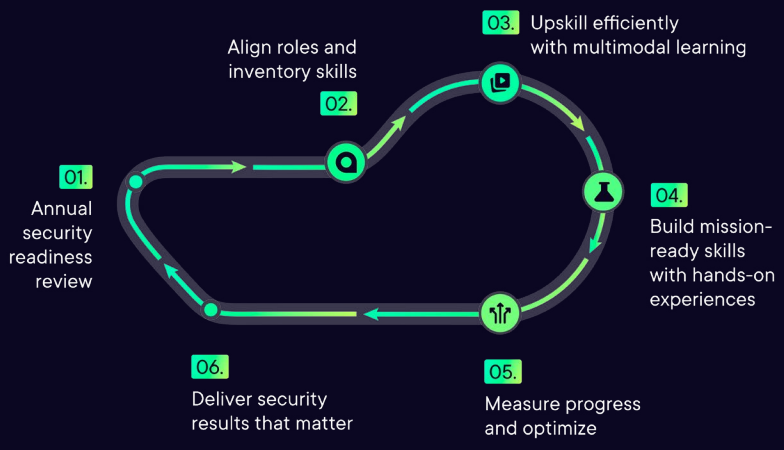
As threats evolve, cyber resilience—and your people—are your best defense

You can't completely eliminate security risks. You *can* control how you respond to them, though.

Cyber resilience empowers your organization to adapt to change and resolve incidents without significantly impacting customer trust or business continuity.

But you can't do it alone.

When more than half of cybersecurity incidents still involve a human element, your people are your best defense. As threats evolve and new risks emerge, filling skills gaps through upskilling and building a culture of readiness is the only way to truly prepare your organization for the threats of today and tomorrow.



Build your organization's security skills and readiness with a unified and affordable skill development platform. Pluralsight SecureReady combines hands-on labs, live workshops, assessments, and program management to help teams detect, respond, and defend in real-world scenarios.

Learn more about Pluralsight SecureReady →

About Pluralsight

Pluralsight is *the* learning partner for today's technology teams and professionals. With our hands-on skills platform built by vetted tech innovators and practitioners, we ensure organizations and individuals develop their tech skills, build job-ready confidence, and accelerate business outcomes. Equip yourself or your teams with the skills needed to independently adopt new technologies, execute strategic initiatives, and deliver improved outcomes.

Learn more →