SECURANCE CONSULTING

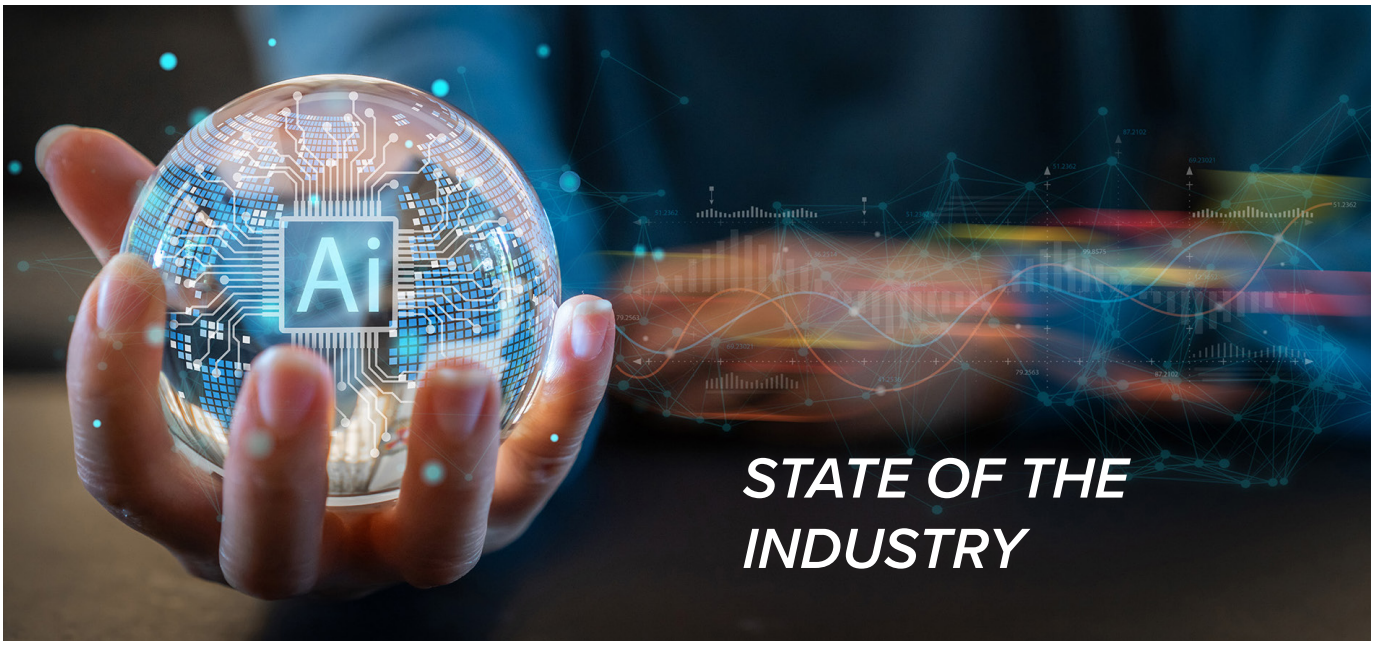
Advantage of Insight | AI

STATE OF THE INDUSTRY:

CYBERSECURITY AT THE CLOSE OF 2025

www.securanceconsulting.com

EXECUTIVE SUMMARY



The first three quarters of 2025 proved that cybersecurity has become much more than a line item in the IT budget. It is now a boardroom priority and a driver of resilience, trust, and growth. Over this past year, leaders faced an unprecedented mix of AI-powered fraud, large-scale attacks, supply chain disruptions, and mounting regulatory pressure.

Those who treated security as a strategic investment came out ahead of their competitors because their organizations more effectively restored operations and minimized the impact of attacks, preserved customer trust, and safeguarded revenue streams. Organizations that combined AI detection tools with incident response planning and playbooks cut containment times dramatically, and those that embedded cybersecurity into board-level planning gained investor confidence and stronger partner relationships.

The lesson is clear. Adversaries industrialized their tactics, but organizations that prioritized cybersecurity kept pace by scaling their defensive strategies in response. Leaders must anchor strategies in resilience, AI oversight, board governance, and stronger third-party risk management. These approaches deliver measurable benefits such as accelerating recovery, reducing compliance costs, and ensuring that vendor weaknesses do not expose the enterprise. Organizations that embrace them will not only withstand the next wave of attacks but also capture trust, contracts, and long-term growth.

> ***Global cybercrime is expected to cost $13 trillion in 2025.[1]***

THE THREAT LANDSCAPE IN 2025

Looking back on the year, one takeaway stands out: in cybersecurity, speed and adaptability determine success. The organizations that responded quickly and adjusted their defenses in real time were able to contain damage and maintain trust. Those that moved too slowly or relied on static defenses were left exposed, and some paid the price for their complacency in financial and reputational damage.

The new reality came into sharp focus through four major shifts in the threat landscape. These included the rise of AI-powered attacks at scale; the increasing fragility of supply chains; the evolution of ransomware beyond prevention; and the reinvention of social engineering through artificial intelligence, with attackers using AI to create highly targeted, convincing deceptions that are far harder for individuals to detect.

- ## AI-Powered Attacks

  Hackers increasingly used generative AI to automate cyberattacks. Malware that rewrites itself to avoid detection, automated vulnerability scans that exploit flaws at scale, and AI-powered denial-of-service attacks can now be launched in seconds instead of days. Targeted phishing powered by AI succeeds far more often than standard phishing email campaigns. Traditional detection methods have struggled to keep up, pushing defenders to adopt AI-driven tools to match the speed and scale of these attacks.

- ## Social Engineering Reinvented by AI

  AI-engineered spear phishing fooled over half of targeted employees, more than doubling the success of traditional campaigns.[2] Even well-trained employees may struggle to detect these deceptions, as AI analyzes data to craft personalized and credible messages. Layered defenses, including measures such as multi-factor authentication, advanced email filtering, real-time threat intelligence, and rapid incident response, have proven to be the only effective tactics.

- ## Supply Chain Fragility

  Breaches impacting cloud providers and HR platforms like Workday rippled across hundreds of organizations.[3] The lesson for executives is that third-party controls are just as critical as internal ones. Boards need visibility and accountability across the vendor ecosystem. Achieving this requires a structured third-party risk management program that includes conducting due diligence before onboarding vendors, classifying suppliers by criticality, requiring evidence of compliance with external standards like SOC 2, and continuously monitoring vendor security posture through questionnaires, audits, and automated tools.

- ## Ransomware Beyond Prevention

  Ransomware groups such as Yurei have shown how attackers can steal and encrypt data simultaneously, leaving organizations with both downtime and data exposure.[4] Prevention alone is not enough, so organizations must be prepared to respond to ransomware incidents.

The Takeaway:

Adversaries are faster and smarter than ever before. Resilient organizations must adopt new strategies to keep up. That means not only matching speed with speed through AI-driven defenses but also building resilience into every organizational layer, including people, processes, and technology. The winners in 2025 treated cybersecurity as a continuous discipline rather than a checklist and built adaptability into how they operate.

In the last two years alone, the global average number of weekly attacks encountered by organizations grew by 58%.[5]

SHIFTS IN TECHNOLOGY AND STRATEGY

New threats forced organizations to rethink their security defenses. In 2025, cybersecurity continued its shift from an afterthought to a top priority, becoming more deeply embedded in strategy, operations, and governance.

- ## Zero Trust as the Minimum Standard

  Zero-trust architecture became the baseline. Regulators, insurers, and investors now expect it. For example, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) requires federal agencies to align their cybersecurity architecture and practices with its Zero Trust Maturity Model (ZTMM), while insurers increasingly tie premium rates to an organization's ability to enforce identity-based access controls.[6] Even private equity firms ask portfolio companies to demonstrate zero-trust practices before funding or acquisition. Companies that lag in implementation risk losing contracts and market credibility.

- ## Defense AI at Full Scale

  Defenders who failed to adopt AI were outpaced by attackers who did. AI is effective because it processes massive data streams in real time and can spot patterns and anomalies that humans alone are likely to miss. This advantage is most reliable when organizations pair AI tools with human oversight, ensuring that automated insights are validated, contextualized, and acted on appropriately.

- ## Cloud-Native Security

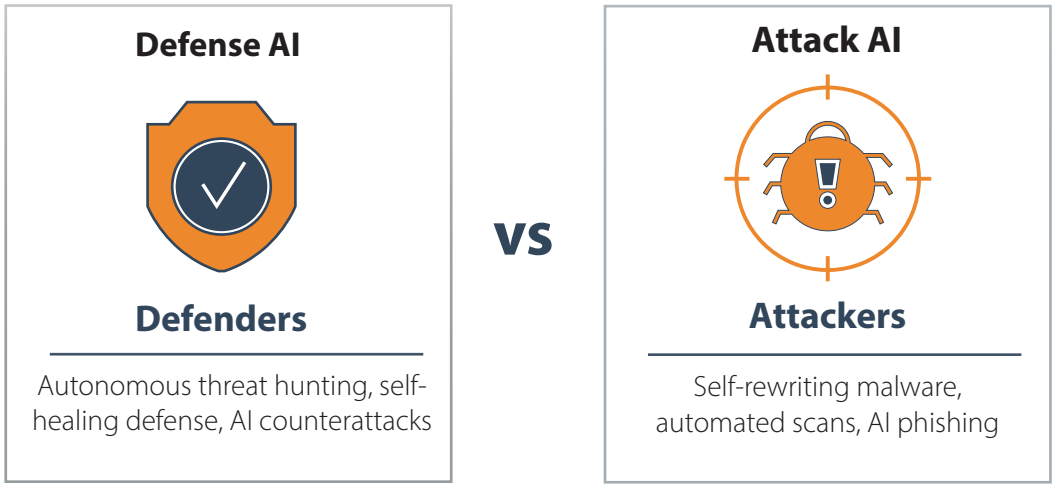
  Businesses moved away from bolt-on solutions. Instead, they built protections directly into workloads and applications, recognizing that cloud-native security is the most efficient way to scale. Embedding security into the architecture ensures consistent protection across dynamic environments and prevents the gaps that attackers can exploit in hybrid and multi-cloud settings.

- ## Cybersecurity in the Boardroom

  Security shifted from a back-office concern to a board-level priority on par with financial performance. Instead of being treated as a technical issue, it became a standing item in executive discussions. New and advanced threats have blurred the line between cyber risk and business risk, making board oversight essential. At this level, decisions about investment, risk tolerance, and reputation directly shape how resilient an organization can be.

The Takeaway:

Cybersecurity can no longer be reactive. It must be embedded in governance and strategy. Executives who treat it as purely an IT function will fall behind. The organizations that succeed will be those that integrate security into decision-making at every level, from the boardroom to daily operations, and view it as a driver of resilience, trust, and long-term business value.



REGULATORY COMPLIANCE

To meet evolving regulatory expectations, organizations can no longer treat compliance as an annual paperwork exercise. They must demonstrate continuous improvement in their security postures by providing evidence of ongoing monitoring, measurable risk reduction, and disciplined remediation efforts.

This often includes maintaining current risk registers, tracking vulnerability and incident response metrics, mapping progress against frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) or the ZTTM, and validating controls through regular assessments. Regulators and industry bodies also expect board-level oversight, documented decisions, and clear linkage between cybersecurity investments and business resilience.

- ## U.S. Federal Pressure

  For defense contracts, the governing requirement is the Cybersecurity Maturity Model Certification (CMMC). CMMC is based on NIST Special Publication (SP) 800-171 standards and requires both prime contractors and subcontractors to safeguard Controlled Unclassified Information (CUI) through defined security controls.[7] While some contractors can complete self-attestations, others must undergo rigorous third-party assessments to verify compliance. Unmet requirements must be recorded in a Plan of Action and Milestones (POA&M) and resolved within a defined time period.

  At the same time, frameworks like the NIST CSF and NIST AI Risk Management Framework (AI RMF) continue to guide broader governance. NIST CSF standards help organizations identify, protect against, detect, respond to, and recover from cyber threats, while the AI RMF provides structure for safe and trustworthy use of artificial intelligence. Across all federal expectations, one theme is clear: compliance is no longer achieved through one-time audits. Organizations must demonstrate continuous improvement and maturity over time.

Healthcare Enforcement

In 2025, healthcare compliance and cybersecurity grew more closely linked. The Yale New Haven Health System (YNHHS) breach exposed names, Social Security numbers, and medical record numbers of 5.5 million patients, though financial data and electronic medical record systems were not impacted. The fallout included class-action lawsuits and an $18 million settlement, underscoring that breaches carry legal, financial, and reputational risks in addition to regulatory fines.[8]

Originally designed to improve insurance portability and combat fraud, the scope of the Health Insurance Portability and Accountability Act (HIPAA) has expanded dramatically since the Privacy and Security Rules were introduced in the early 2000s. Today, regulators and courts judge organizations on their ability to prevent and contain intrusions across interconnected systems, not just maintain documentation.

Coinciding with the YNHHS breach, the Department of Health and Human Services proposed sweeping Security Rule updates mandating encryption, multi-factor authentication, asset inventories, risk analyses, technical testing, and contingency planning, while eliminating "addressable" flexibility.[9] The changes are expected to take effect in 2026 and will be the first major updates to the Security Rule in over a decade. The Privacy rule received its last update in 2024, with changes that aim to accelerate patient access and enable secure application integration. These developments signal a fundamental shift — compliance is no longer a paperwork exercise but an enterprise-wide security imperative tied directly to patient safety and continuity of care.

Energy and Utility Standards

The energy sector must also adhere to industry-specific regulatory requirements. Electric utilities that own or operate assets within the bulk electric system are required to comply with the North American Electric Reliability Corporation Critical Infrastructure Protection standards, known as NERC CIP. These are mandatory standards, not voluntary best practices, and violations can result in significant financial penalties and increased regulatory scrutiny.

Many utilities also align with International Society of Automation (ISA) and International Electrotechnical Commission (IEC) standards, such as ISA | IEC 62443, which provide internationally recognized guidance for securing industrial control systems and operational technology (OT). This includes OT environments, which are the hardware and software that monitor, control, and automate physical processes such as power generation, transmission, and distribution, helping utilities strengthen cybersecurity across both generation and transmission assets.

Utilities voluntarily adopt these frameworks because they recognize that cybersecurity in critical infrastructure is tied directly to public trust, reliable service, physical safety, and the broader stability of the power grid. As cyber threats increasingly target OT networks, supply chain dependencies, and interdependencies between IT and grid operations, alignment with these standards is becoming a strategic priority rather than a purely technical choice.

The Takeaway:

Compliance is no longer a matter of passing periodic audits but requires proving maturity over time. In 2025, compliance shifted from a checkbox exercise to a test of resilience. Regulators, insurers, and investors now expect organizations to demonstrate continuous improvements in their cybersecurity maturity, tying security performance directly to trust, safety, and long-term business viability.

TALENT, SERVICE, AND WORKFORCE DYNAMICS

Even the strongest strategies and compliance frameworks depend on people. Throughout 2025, the persistent talent gap reshaped how organizations staffed and supported their security programs.

Rather than treating cybersecurity as a hiring problem, more organizations began treating it as a capability problem. The question changed from “Who can we hire?” to “How can we access the expertise we need when we need it?” As a result, several models gained traction:

- ## Virtual CISO (vCISO) Services as a Force Multiplier

  Most mid-sized companies and public agencies lack executive-level security leadership. Rather than delaying strategy development, many turned to vCISO services. Demand is rising across the industry; according to the 2025 State of the vCISO Report by Cynomi, the share of MSPs and MSSPs offering vCISO services increased from 21 percent in 2024 to 67 percent in 2025, with 79 percent reporting high demand from small and mid-sized clients.[10]

  These services provide access to an experienced security leader who can build policies, guide compliance efforts, present to the board, and align cybersecurity with business priorities without the cost of a full-time executive.

- ## Staff Augmentation for Skill Gaps

  One of 2025’s most important lessons was that governance models, AI-driven tools, and regulatory frameworks cannot succeed without skilled professionals to interpret, apply, and improve them. The organizations that adapted most effectively were not those with the largest budgets, but those that invested in hybrid teams, external partnerships, and continuous skill development to close capability gaps rather than delaying strategic initiatives.

  This shift is reflected in broader labor-market trends. A 2025 analysis of IT staff augmentation trends reported that the global staff-augmentation market was valued at approximately $299.3 billion in 2023 and is projected to grow to $857.2 billion by 2031, a compound annual growth rate of roughly 13.2 percent.[11] Growth at this scale indicates that organizations are increasingly using staff augmentation to address persistent skill shortages, accelerate priority programs, and access specialized expertise that is scarce or costly to hire internally.

- ## Cybersecurity as a Service (CSaaS)

  Instead of outsourcing security entirely, many organizations adopted CSaaS models that act as extensions of their existing teams. These services provide continuous monitoring, vulnerability management, policy development, or assessments while allowing internal staff to retain ownership of strategy and decision-making. CSaaS is designed not to replace in-house teams but to strengthen them and reduce burnout.

> ### *The Takeaway:*
>
> ***Organizations that adapt with fractional leadership, service-driven security models, and flexible staffing will thrive. Those relying solely on traditional hiring will remain vulnerable to talent shortages and skill gaps.***

TRENDS TO WATCH IN 2026

As organizations close immediate gaps in staffing and services, broader shifts are already shaping the cybersecurity landscape of 2026. These trends will redefine how leaders approach security in the coming year.

1. AI Governance Moves to the Board

Poorly managed AI can reinforce bias, mishandle sensitive data, or make decisions no one can explain, leading to disruption and loss of trust. That is why AI is now a governance issue, not just a technical one.

2. Resilience Overtakes Prevention

Prevention is no longer enough. The defining metric for 2026 will be recovery speed, making incident response planning a top priority.

3. Insurance Anchored to Resilience

Carriers will expect proof of continuous monitoring, patching, and tested incident response plans. Organizations with immature security programs will see higher premiums.

4. IT and OT Convergence

The convergence of IT and OT systems introduces new risks, as AI can create vulnerabilities in both digital systems and the physical infrastructure they operate. Strong oversight is essential.

The Takeaway:

Effective cybersecurity strategies go beyond traditional defenses and require resilience, governance, and operational alignment. In 2026, success will depend on maturity across all three areas. Organizations that can demonstrate resilience through tested recovery plans and show strong governance by embedding security and AI oversight at the board level will be better positioned to withstand attacks and maintain trust with regulators, insurers, and customers.

If 2025 has proven anything, it is that cybersecurity now moves faster than business cycles. Organizations focused on passing audits rather than improving overall security outcomes were left exposed, while those that treated cybersecurity as a strategic function improved resilience and readiness.

As 2026 begins, executives must act decisively to:

- Put response capabilities on par with prevention through recovery planning and proactive threat hunting.
- Position cybersecurity as a board-level responsibility to strengthen governance and the overall risk posture.
- Demonstrate continuous improvement by showing that cybersecurity is actively managed every day. That includes addressing vulnerabilities, improving response times, learning from incidents, and keeping leadership informed.

Cybersecurity can no longer be treated as just another cost of doing business. It is now a core requirement for growth, innovation, compliance, and customer trust. Organizations that view security and resilience as strategic advantages will be better positioned to withstand future threats and earn public confidence.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://sqmagazine.co.uk/cybersecurity-statistics/
2. https://arxiv.org/abs/2412.00586
3. https://techcrunch.com/2025/08/18/hr-giant-workday-says-hackers-stole-personal-data-in-recent-breach/
4. https://research.checkpoint.com/2025/yurei-the-ghost-of-open-source-ransomware/
5. https://www.weforum.org/stories/2025/09/cybersecurity-awareness-month-cybercrime-ai-threats-2025/
6. https://www.securitymagazine.com/articles/102007-cyber-insurance-comes-of-age-from-niche-policy-to-strategic-risk-tool
7. https://thecgp.org/what-federal-contractors-need-to-know-about-cmmc
8. https://www.hipaajournal.com/yale-new-haven-health-system-data-breach/
9. https://www.hipaajournal.com/hipaa-updates-hipaa-changes/
10. https://www.helpnetsecurity.com/2025/07/31/vciso-services-adoption-2025
11. https://www.n-ix.com/it-staff-augmentation-trends

State of the Industry

© 2025 Securance LLC. All Rights Reserved.

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com