Cyberstarts

2026

Cybersecurity Trends Report

AUTHOR

Career CISO, Operating Partner, Cyberstarts

PETE CHRONIS

CONTRIBUTORS

Chief Strategy Officer, Cyera

JASON CLARK

Chief Information Security Officer, Surf

DR. YONESY NÚÑEZ

Chief Trust Officer, Cyera

LAMONT ORANGE

Chief Strategy Officer, Gambit

CURTIS SIMPSON

Chief Strategy Officer and Chief Information Security Officer, Upwind

RINKI SETHI

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report blends insights from the world's most influential cybersecurity research bodies to create a unified, forward-looking view of the threat landscape and enterprise priorities for 2025–2027. It draws on empirical breach data from the Verizon DBIR, IBM Cost of a Data Breach Report, Mandiant M-Trends, CrowdStrike's Global Threat Report, and the ENISA Threat Landscape; global-scale telemetry from the Microsoft Digital Defense Report; strategic market forecasting from Gartner and Forrester; and macro-economic and governance perspectives from the World Economic Forum Global Cybersecurity Outlook and leading advisory firms. Each source offers a distinct vantage point, and the synthesis elevates only those patterns confirmed across multiple independent datasets.

> **Together, these reports point to a cybersecurity environment defined by rising operational pressure, accelerating AI-driven risk, and expanding regulatory expectations.**

Data has become the fastest-growing attack surface, with identity remaining the dominant vector for initial compromise. Attackers are increasingly leveraging automation and AI to scale targeting, social engineering, and exploitation, while defenders struggle to govern the rapid adoption of generative AI inside their organizations. Cloud and edge infrastructure continue to present reliability and resilience challenges, as ransomware and availability attacks remain persistent worldwide. Meanwhile, credential compromise and identity abuse are among the most common vectors leading to breaches and data theft. At the same time, budgets are tightening and talent shortages endure, forcing organizations to shift from reactive controls toward automation, intelligence-driven operations, and measurable resilience outcomes.

A survey of 84 senior security and technology leaders from the Cyberstarts advisor community reveals that cybersecurity is entering a phase defined by continuous, machine-speed conflict rather than episodic attacks. Sixty percent of leaders report rising attack velocity and incident data shows the time from initial access to data theft collapsed from nearly five hours to just over one hour in a single year signaling that traditional human-driven response models are struggling to keep pace. At the same time, confidence in resilience remains limited, with only 17% of CISOs highly confident they can avoid a material cyber event, as risk increasingly concentrates around ransomware, identity compromise, and data exposure in environments that are now nearly 60% cloud-dominant. While only 7% currently rank AI-driven attacks as their top immediate risk, leaders overwhelmingly acknowledge that AI is accelerating both attacker capability and enterprise adoption faster than governance can keep up.

> **The key lesson is that cybersecurity strategy is shifting toward a new operating model centered on data and identity control, automation that can operate at machine speed, and resilience across distributed cloud environments, as CISOs prepare for a future where AI shapes both how attacks are executed and how defenses must respond.**

The resulting picture of 2025–2027 is one where enterprise security programs succeed only if they treat data, AI, and identity as a unified security fabric, modernize cloud and edge foundations for continuity, and use automation to overcome the scale of modern telemetry. For CISOs, this translates into a shift from traditional detection models to architectures anchored in data posture, AI governance, identity integrity, and operational resilience. For investors, the same trends reveal durable growth categories in AI-native data security, identity and autonomy controls, AI governance orchestration, and intelligence-driven operational platforms, while putting pressure on legacy tools that cannot show measurable reductions in risk or response time.

Grounded in the convergence of the industry's most credible research and reinforced by direct insight from experienced CISO thought leaders, this report provides a clear, evidence-backed and practitioner-informed view of where cybersecurity is heading and what enterprises, vendors, and investors must do to stay ahead of the next three years of disruption.

2025–2027 CYBERSECURITY TRENDS

Across the major reports, the picture for the next three years is pretty consistent: risk is up, budgets are choppy, AI is amplifying both attackers and defenders, and resilience is becoming the real metric of success.

The cybersecurity risk landscape between now and 2027 will be shaped as much by geopolitics, regulation, and macro-infrastructure stress as by technical innovation. Geopolitical conflict is increasingly expressed through cyber operations that target civilian infrastructure, financial systems, energy grids, media networks, and global connectivity. At the same time, the fragmentation of global technology supply chains is introducing new dependencies, vulnerabilities, and concentration risks that amplify systemic exposure across industries.

01. Critical infrastructure is no longer limited to data centers and networks

Satellite systems, undersea cables, cloud control planes, and cross-border data exchange corridors have become strategic assets and adversarial targets. Disruption or compromise of these systems has cascading economic and security consequences that no single enterprise can mitigate alone.

Regulatory pressure is accelerating in parallel. The EU AI Act, growing adoption of the NIST AI Risk Management Framework, and emerging U.S. AI safety and governance rules are rapidly hardening security requirements for cloud providers, AI vendors, and enterprises. These forces will directly influence security budgets, architectural decisions, vendor selection, and operational readiness, particularly for highly regulated sectors such as financial services, healthcare, energy, media, and critical infrastructure. Any assessment of cybersecurity trends that excludes these forces underestimates the speed and magnitude of structural change now underway.

The data shows that the volume and cost of incidents are still heavy. Verizon's latest DBIR analyzed more than 30,000 incidents and over 10,000 confirmed breaches, with the "human element" involved in roughly two thirds of them, and ransomware among the top threats in almost every industry. IBM's 2024 breach report puts the average cost of a breach at about 4.88 million dollars, up around ten percent from the previous year, the largest jump since the pandemic, driven mostly by lost business and post-breach response costs. The 2025 edition then shows a slight pullback toward 4.4 million, attributing it to faster detection and containment, but highlights that AI systems without proper oversight drive higher breach likelihood and cost. The net of it: risk remains elevated through 2026, and efficiency gains from AI only show up if governance keeps pace.

On the threat side, three surfaces dominate: data, identity, and availability. ENISA's latest Threat Landscape calls out seven prime threats, with attacks on availability, ransomware, and data threats as the top three, based on more than eleven thousand analyzed incidents in Europe. These match what other syntheses of threat reports are seeing: rising breach costs, vulnerability exploitation, DDoS, supply chain abuse, and steady pressure on misconfigured cloud and edge infrastructure. Microsoft's Digital Defense Report describes a 2.75 times increase in human-operated ransomware encounters, yet a threefold decrease in successful "ransom stage" attacks, which it attributes to stronger controls, while also reporting 78 trillion security signals observed per day across its ecosystem. That points to a world where defenders can win specific battles but are constantly outnumbered.

02. AI is the real hinge

The World Economic Forum's 2025 Global Cybersecurity Outlook reports that about seventy two percent of leaders see cyber risk increasing, ransomware still sits atop concern lists, and sixty six percent say AI will have the most significant impact on cybersecurity in the coming year. Only thirty seven percent, though, report having

processes to evaluate and govern generative AI risk. WEF's coverage notes that budgets are tightening, growth in cyber spend slowing to low single digits, while both criminals and defenders lean into AI agents and automation. In parallel, ENISA and WEF both highlight "cyber inequity": a growing gap between highly resilient, well-resourced organizations and everyone else. That inequity will matter a lot by 2027, because attackers are using AI to scale into weaker ecosystems that are interconnected with stronger ones.

As enterprises industrialize generative AI, the threat surface is expanding beyond traditional infrastructure into the AI lifecycle itself. Training data poisoning, model inversion, unauthorized fine-tuning, shadow models, and the emergence of autonomous AI agents introduce new classes of systemic risk. The security challenge is no longer limited to protecting prompts and outputs. It now encompasses data sourcing, feature engineering pipelines, model training, deployment, agent permissions, inter-model dependencies, and post-deployment monitoring.

Autonomous AI agents represent a particularly disruptive shift. These agents increasingly operate across business workflows, infrastructure, and decision systems with limited human oversight. Cross-model dependency chains and agent-to-agent interactions create opaque risk paths that traditional security tooling was never designed to observe or govern. Securing AI therefore requires end-to-end visibility, continuous validation of model integrity, strict control of agent permissions, and persistent monitoring for behavioral drift, misuse, and compromise.

03. Cloud concentration is creating a new class of systemic cyber risk

Hyperscaler outages, control-plane compromises, identity federation failures, shared machine-learning infrastructure weaknesses, and cross-tenant escape vulnerabilities now represent failure modes with economy-wide consequences. These risks resemble financial-sector contagion more than traditional enterprise security incidents.

As enterprises consolidate critical operations onto a small number of global platforms, localized failures increasingly propagate across entire industries. No single organization can fully mitigate these exposures in isolation. This reality elevates the importance of resilience engineering, architectural diversification, identity integrity, and tested recovery strategies as primary board-level risk controls.

Gartner's 2025 cybersecurity trends wrap this into a program view. They emphasize preemptive security, generative AI's impact, digital decentralization, supply chain interdependence, talent shortages, and regulatory expansion as the structural drivers of change. Others echo this: multiple analyses project global IT spend passing five trillion dollars, with the vast majority of CIOs either maintaining or increasing security budgets but shifting dollars toward AI-enabled detection, resilience engineering, and risk-aligned controls rather than more of the same point tools.

PUT TOGETHER, THE 2025 TO 2027 NARRATIVE LOOKS LIKE THIS:

- Threat volume, complexity, and cost stay high, but the marginal payoff of traditional perimeter and detection tools flattens.
- Attackers weaponize AI for better phishing, deeper identity fraud, more precise vulnerability targeting, and convincing deepfake-driven social engineering.
- Defenders apply AI for triage, correlation, hunt, attack surface management, and data discovery, but struggle with AI governance, data protection, and model integrity.
- Regulation, geopolitical tension, and supply chain fragility push cyber from "IT problem" to systemic risk.
- The winners by 2027 have shifted their programs toward resilience, with measurable improvements in dwell time, containment, and business continuity, especially around data and AI systems.

2026 EXECUTIVE SURVEY

We surveyed 84 senior security and technology leaders from the Cyberstarts advisor community, providing a practitioner view into real enterprise priorities. With this sample size, the findings carry an approximate margin of error of ±6%, offering a reliable snapshot of how security leaders are experiencing the current threat environment.

60% of security leaders report that attack velocity increased over the past year, including 22% who say it increased significantly.

But the real story is not simply that attacks are increasing. The deeper change is that three constraints that historically limited attackers are disappearing at the same time. Human labor, human expertise, and human speed once acted as natural friction in cyber conflict. Those constraints are now dissolving as automation and AI expand attacker capability. What is emerging is a new dynamic defined by machine speed conflict.

Independent data gathered on cybersecurity incidents further illustrates this shift. The time for attackers to move from initial access to data theft collapsed from roughly 285 minutes in 2024 to about 72 minutes in 2025, a fourfold acceleration in a single year.

This compression fundamentally changes the equation for security operations. If attackers can move from entry to exfiltration in just over an hour, the traditional SOC model built around human triage and containment struggles to keep pace. The attack window is collapsing faster than defenders can react.

The survey results also reveal that CISOs recognize security is being reshaped by structural forces that extend well beyond traditional threat dynamics. Risk is becoming systemic as technological acceleration, expanding digital ecosystems, and growing regulatory expectations converge.

55% of security leaders describe themselves as only moderately confident in their ability to avoid a material cybersecurity event, while just 17% report high confidence and roughly one in five report low confidence.

This gap between moderate and high confidence reflects a broader reality. Many organizations have deployed controls, but fewer trust those controls to perform reliably under real attack conditions.

When leaders describe what most undermines their confidence, several risks appear consistently.

Ransomware and extortion lead at 26%, followed closely by identity compromise at 25% and data exposure at 22%.

These results reinforce that enterprise risk is now multi dimensional. Identity, data, and operational resilience increasingly intersect as the core battlegrounds for modern security.

Operational pressure is also visible in the daily challenges teams face.

35% of leaders cite phishing and social engineering as the most persistent operational challenge, while 27% point to cloud misconfigurations.

Even in an era of advanced technology, human behavior and configuration complexity remain powerful drivers of risk.

At the same time, the infrastructure environment continues to evolve rapidly.

Nearly 60% of enterprises report environments that are at least 75% cloud based or fully cloud native.

As traditional network perimeters dissolve, security strategy is shifting toward identity systems, data controls, and platform level governance that operate across distributed environments.

Artificial intelligence adds a new dimension to this transformation.

7% represents only about the share of security leaders who currently rank AI-driven attacks as their top immediate risk.

Yet almost every conversation with CISOs points to AI influencing decisions around data visibility, automation, and governance. In other words, AI adoption is accelerating faster than our ability to govern it.

This creates a familiar pattern seen during previous technology transitions. Organizations deploy new capabilities quickly to capture competitive advantage. Governance and control mechanisms follow later.

The implication is that security leaders are already rethinking how people, process, and technology must evolve together to operate safely in AI driven environments.

Across the Cyberstarts community, three strategic questions repeatedly emerge when leaders discuss how AI will reshape cybersecurity.

The first question centers on how enterprises will secure and govern AI itself.

Data security, identity security, and application security are all being reimagined as organizations attempt to control how models access information, how decisions are made, and how outputs are validated.

THE SECOND QUESTION REFLECTS THE REALITY THAT ADVERSARIES ARE ALREADY ADOPTING AI. WE KNOW FROM INDEPENDENT RESEARCH THAT:

- 87% of organizations report experiencing an AI driven attack in the past year.
- 82% of phishing campaigns now involve AI generated content.
- 80% of ransomware campaigns use AI tools for code generation or automation.

These capabilities dramatically increase attacker scale and precision, amplifying the same machine speed dynamics already visible in incident response data.

The third strategic question focuses inward on how defenders will leverage AI themselves.

Security leaders are exploring how AI can help streamline and optimize security operations in areas such as risk assessment, SOC investigations, and automated remediation. If attackers are operating at machine speed, defensive operations will need to evolve toward the same tempo.

Taken together, the survey results point to a profession that understands the ground is shifting beneath it. CISOs are managing environments that are more cloud concentrated, more data intensive, and increasingly shaped by automation and AI. Attack velocity is rising, incident timelines are compressing, and confidence in existing controls remains cautious. At the same time, investment patterns and leadership conversations reveal where attention is moving next. Security leaders are beginning to converge around a new operating model that prioritizes control over data and identity, resilience across digital infrastructure, and automation that can keep pace with machine speed threats. When we step back and translate these signals into how the CISO role will evolve over the next several years, a clear set of priorities begins to emerge.

CISO PRIORITIES AND OPERATING AGENDA

If you evaluate cybersecurity trends and results from the executive survey into a modern CISO playbook, priorities for the next three years line up around a few themes: securing AI and data, consolidating identity and access, modernizing cloud and edge controls, scaling intelligent and autonomous operations, and embracing resilience.

01. AI and data become a single, inseparable problem.

Every major report is converging on data as the dominant attack surface and AI as the dominant consumer of that data. Verizon and ENISA show that data theft, extortion, and double-extortion ransomware are now more common than pure encryption lockups. IBM's breach cost numbers are driven heavily by data-heavy industries and lost business after trust is broken. For a CISO, that means data classification and DSPM, AI model and agent governance, and end-to-end lineage and access control become "table stakes," not nice to have. In the 2025 to 2027 window, securing gen AI use cases is not just about prompts and tokens, it is fundamentally about making sure sensitive data is visible, minimized, and wrapped in policy before it ever touches a model.

02. Identity and access become the practical perimeter.

Both Microsoft and Verizon continue to show that phishing, credential abuse, and identity-centric attacks dominate initial access. The next three years likely belong to programs that fully commit to strong identity foundations: risk-based authentication, privileged access management, continuous verification, and real-time anomaly detection across users, machines, and AI agents. In an AI-saturated environment, you are treating identities as both human and non-human, and you are committing to visibility into where those identities can touch data and critical systems.

03. Cloud, edge, and availability need to be treated as one continuity fabric.

ENISA's focus on availability attacks, plus growing evidence of exploitation across VPNs, remote management tools, and hypervisors, shows how fragile hybrid foundations still are. Over 2025 to 2027, CISOs will be judged on their ability to keep core services up through ransomware, DDoS, and cloud outages. That drives investment into resilient architectures, immutable backups, segmentation, zero trust network design, and tested incident and recovery playbooks, not just more alerting.

04. Intelligent, autonomous operations become mandatory.

Microsoft's data on trillions of security signals per day is a proxy for what every enterprise is feeling. SOCs cannot hire their way out of that. WEF's 2025 report notes that cyber risk is rising faster than budgets and talent, which forces a pivot to automation and decision support. Over the next three years, the most advanced CISOs will use AI copilots and automation not as side projects but as core operating model changes: automated triage and enrichment, policy as code, closed-loop response for common incidents, and AI-assisted investigations that compress mean time to detect and respond.

In addition, a new offensive model is emerging in the form of AI swarm attacks that makes automated prevention, detection and response an absolute necessity. Attackers deploy large numbers of autonomous or semi-autonomous AI agents that coordinate in real time to conduct sustained, adaptive, and highly scalable campaigns. Unlike traditional attacks driven by fixed playbooks, swarms continuously learn, optimize, and redistribute effort across the kill chain. They generate massive parallel experimentation, converging rapidly on the most effective compromise paths.

This shift breaks many foundational defensive assumptions. Rate limiting, signature detection, manual triage, and sequential response models cannot operate at the speed or scale required to counter adaptive swarms. Effective defense now depends on automation, identity-centric controls, continuous risk assessment, and resilience engineering. Against swarms, the objective is not perfect prevention but faster detection, containment, and recovery than the attacker's rate of adaptation.

CISOs will increasingly be judged not by control coverage but by measurable shifts in risk outcomes. AI-driven automation is already compressing mean time to detect and respond, reducing dwell time, lowering breach probability, and materially altering loss distributions. While precise figures vary by industry and maturity, early evidence indicates that organizations with automated triage, identity-centric controls, and continuous risk assessment consistently achieve double-digit improvements in MTTD and MTTR, with corresponding reductions in breach impact and recovery costs.

Without quantitative benchmarks, security programs struggle to prioritize investment and demonstrate return. Over the next three years, directional metrics tied to detection speed, containment efficiency, cost avoidance, and resilience performance will become core governance instruments for boards and regulators.

05. Governance, regulation, and cyber inequity reshape the board conversation

WEF's 2024 and 2025 outlooks highlight shrinking "minimum viable cyber resilience" and growing gaps between top and bottom performers, while pointing to emerging tech and regulation as key drivers. For CISOs, that means the board story from 2025 to 2027 is about alignment with AI and cyber regulations, demonstrable resilience metrics, and clear risk appetite definitions. You will be expected to show how AI is governed, how third parties are managed, and how your program maintains resilience under plausible worst-case scenarios, not just how many vulnerabilities you patched.

Technology alone will not determine cybersecurity outcomes over the next three years. Structural economic and organizational constraints will increasingly shape what enterprises can realistically achieve. The global cyber workforce shortage, widespread practitioner burnout, rising cyber insurance premiums, and the shrinking pool of affordable reinsurance are exerting growing pressure on security programs. These forces are producing a widening resilience gap between highly resourced enterprises and the broader economy.

This gap matters because attackers are already exploiting weakly defended ecosystems that are deeply interconnected with stronger ones. Capital availability, talent distribution, regulatory burden, and insurance constraints will distort adoption patterns and risk exposure far more than individual product capabilities. Effective cyber strategy must therefore integrate organizational design, financial planning, and human capital development alongside technical controls.

In short, the CISO operating model that fits these trends is one where AI, data, and identity are managed as a unified fabric, where the SOC is augmented with intelligent automation, and where resilience and regulatory readiness become the main yardsticks of success.

CONCLUSION

The next three years mark a transition point where cybersecurity moves from a fragmented collection of controls to an integrated resilience discipline shaped by data gravity, AI acceleration, and identity-centric risk. The research consensus behind this report makes it clear that no single technology, framework, or operating model is sufficient on its own. Enterprises that thrive in this period will be the ones that treat data sensitivity, AI autonomy, and identity integrity as inseparable forces driving both opportunity and exposure. The organizations that cling to legacy perimeter thinking or incremental detection tooling will find themselves overwhelmed by volume, complexity, and the speed at which attackers adapt.

At the same time, this landscape creates new clarity for how CISOs and boards chart the path forward. The reports all point toward a future where operational effectiveness is defined by faster containment, stronger continuity, and disciplined AI governance rather than by the number of alerts processed or tools deployed. Security leaders who modernize identity foundations, build resilient cloud and edge architectures, and adopt automation as an operating necessity — rather than as an experiment — will be best positioned to manage rising expectations from regulators, customers, and executive teams. What emerges is a model of cybersecurity where trust, transparency, and measurable impact matter as much as technology choice.

> **Looking ahead, CISOs should rebalance portfolios toward AI-native data protection, identity modernization, agent and model security, and automation-driven operations. Architectural priorities must shift from incremental tooling to integrated security fabrics that unify data, AI, identity, cloud, and operations. Boards must evolve oversight models to focus on measurable resilience, AI governance, and systemic risk exposure rather than control inventories.**

For innovators and investors, the trends surface both the opportunities worth pursuing and the categories likely to contract. Durable growth sits in AI-native data protection, agent and model security, identity modernization, and intelligent operations. Platform consolidation will continue, and solutions that cannot demonstrate real-world outcome improvement will fade. When viewed together, the combined intelligence behind this report delivers a unified message: the winners in 2025–2027 will be those who adapt early to the convergence of data, AI, and identity; who design for resilience rather than reaction; and who treat cybersecurity not as a defensive cost but as an essential enabler of digital ambition.

For investors, the next phase will bring accelerated consolidation in mature categories and category creation around AI security, autonomous agent governance, and resilience platforms. Solutions that cannot demonstrate real-world outcome improvement will be absorbed or displaced. Strategic advantage will accrue to those who align early with the convergence of data, AI, and identity and who design for resilience rather than reaction.