The 2025 Cybersecurity Pulse Report

AI, Identity, and Risk: A Comprehensive Guide to Key Trends and Expert Insights from the RSAC 2025 Conference

RSAC 2025 Conference

ISMG

TABLE OF CONTENTS

INTRODUCTION

The *The 2025 Cybersecurity Pulse Report* represents a comprehensive synthesis of cybersecurity's most pressing challenges and emerging opportunities, distilled from four intensive days of expert interviews at the industry's premier annual gathering.

ISMG's editorial team, supported by our broadcast and content studios, conducted more than 150 in-depth interviews with industry executives, practitioners, thought leaders and policymakers across the cybersecurity ecosystem. These conversations - spanning vendors, investment firms, government agencies and global enterprises - form the foundation of this report, complemented by ISMG's Apollo AI platform.

Building on last year's approach, our Content Intelligence & AI Innovation Department employed multiple complementary approaches to ensure comprehensive coverage of the RSAC Conference. The research began with an AI-powered analysis of the RSAC Conference event agendas and sessions, supplemented by expert perspectives gathered and recorded during the event. We then conducted cross-session and cross-interview synthesis to detect patterns, reconcile conflicting viewpoints and highlight strategic priorities. We then mapped these expert insights to the eight predefined event themes while identifying areas of consensus, debate and divergence.

These findings were validated against ISMG's proprietary *Apollo Cybersecurity Reference Desk,* an AI agent trained on millions of pages of vetted knowledge from global industry frameworks, best practices, regulations, risk models and real-world case studies. And for the first time, we are able to train our models on prior RSAC Pulse Report content to discern changes in sentiment and topical trends at scale.

This multilayered approach, combining cutting-edge AI tools with expert-driven insights and human editing oversight, produces a holistic view of the cybersecurity landscape with actionable takeaways for security leaders navigating current AI challenges.

The resulting analysis revealed a notable evolution in the industry's focus compared to 2024, as reflected in our topical categorization.

Key Shifts From 2024 to 2025

01

AI and machine learning security has emerged as the dominant category, with topic coverage doubling from 18 sessions in 2024 to 36 in 2025, reflecting both widespread adoption and growing security concerns;

02

Cloud security continues its expansion with greater emphasis on multi-cloud environments and cloud-native security approaches;

03

Zero trust security saw a decline in dedicated sessions - from 8 to 5, suggesting its maturation and integration into broader security frameworks rather than diminished importance;

04

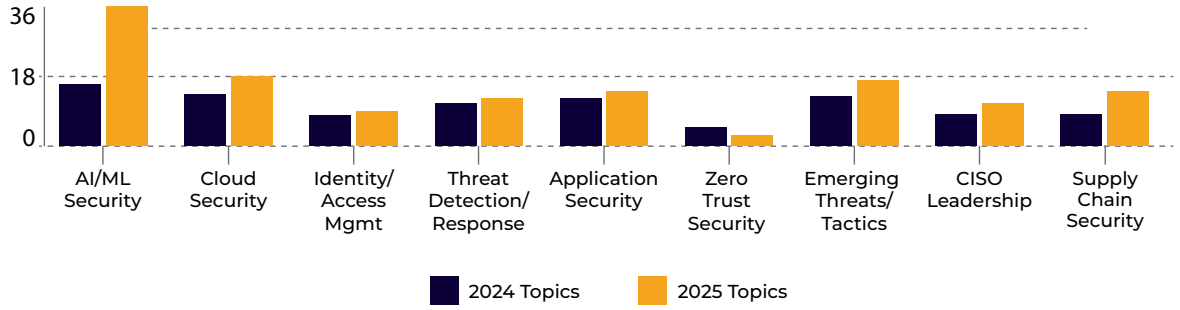
Emerging threats/tactics gained significant attention, particularly those leveraging AI capabilities for sophisticated attacks;

05

New dedicated tracks emerged for **fraud prevention and digital identity,** highlighting growing concerns about deepfakes and AI-powered impersonation.

RSAC Topic Focus Evolution: 2024 to 2025

Category Comparison | New Focus Areas | Key Trends



RSAC Topic Focus Evolution: 2024 to 2025

Category Comparison | New Focus Areas | Key Trends

Notable New/Expanded Categories in 2025:

AI and Machine Learning Security
Significant expansion with 36 themes in 2025, focusing on AI safety, LLM security, AI-powered threats, and secure AI development.

Fraud Prevention and Digital Identity
New dedicated category with 11 themes covering deepfakes, AI-powered fraud, and digital identity protection.

Critical Infrastructure Protection
Expanded focus with 13 themes addressing security for essential services, democracy protection, and industrial systems.

Disappeared or Diminished Categories:

Zero Trust security saw a decline from 8 presentations in 2024 to 5 in 2025, suggesting a possible maturation of this approach or its integration into other security domains.

RSAC Topic Focus Evolution: 2024 to 2025

Category Comparison | New Focus Areas | Key Trends

Key Trends in RSAC 2025:

AI Integration
Massive increase in AI-focused security topics, moving from a subset of themes to the dominant category

Identity-Centric Security
Continued emphasis on identity as the new perimeter, with particular focus on non-human identities in AI/ML systems

Secure by Design
Growing focus on building security into systems from the beginning, rather than adding it later

AI-Powered Threats
Increasing concern about AI being used by threat actors for more sophisticated attacks

Critical Infrastructure Focus
Greater attention to protecting essential services and critical infrastructure

Evolution from 2024 to 2025:

The 2025 program shows a clear shift from theoretical AI security discussions to practical implementation challenges, as organizations increasingly deploy AI systems in production environments. There's also greater attention to the interconnected nature of security domains, especially the convergence of identity, cloud, and AI security.

Dan Verton
Vice President, Content Intelligence & AI Innovation

PURPOSE AND STRUCTURE

This report is organized into eight chapters, each addressing a critical domain of cybersecurity strategy and operations. Together, they form a blueprint covering the most pressing issues facing security leaders in 2025, directly informed by the industry's leading voices.

The The 2025 Cybersecurity Pulse Report is designed to be an essential resource for the upcoming year - guiding planning, investment and operational effectiveness decisions for organizations navigating an increasingly complex threat landscape.

We extend our sincere appreciation to the hundreds of security leaders who shared their insights and experiences, as well as the ISMG Editorial and Studio teams for making this report possible. We look forward to continuing our mission of providing unparalleled insights and thought leadership to support your cybersecurity efforts.

Sincerely,

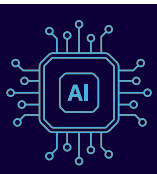
Daniel Verton

Dan Verton
Vice President, Content Intelligence & AI Innovation

EXECUTIVE SUMMARY

The *2025 Cybersecurity Pulse Report* synthesizes insights from research conducted by ISMG's Content Intelligence & AI Innovation Department as well as more than 150 Editorial interviews with subject matter experts at the annual RSAC 2025 Conference held from April 28-May 1, 2025. This report captures the current state of cybersecurity across eight critical domains, revealing both emerging threats and strategic opportunities.

Key Findings



AI's Dual-Edge Impact

AI has become the defining disruptive force in cybersecurity. While defenders leverage AI to scale response capabilities and automate threat detection, adversaries are using the same technologies to enhance phishing, generate polymorphic malware and conduct identity fraud with unprecedented precision. Organizations have faced a 250% increase in attack speed over the past four years, with 20% of breaches progressing from compromise to exfiltration in less than an hour. The convergence of AI and quantum computing further signals a critical shift requiring crypto-agility and forward planning.

The Collapse of Traditional Security Models

The perimeter-based security model is obsolete. Today's decentralized enterprise - characterized by cloud adoption, SaaS integration and remote work - demands a fundamental shift where identity, not infrastructure, forms the frontline of defense. Organizations struggle with proliferating tools, shadow IT and configuration drift while facing accelerating AI-assisted threats. Zero trust adoption remains uneven, with 63% of organizations implementing it but many facing integration challenges and incomplete coverage.

The Identity Crisis

Digital identity has become the primary battleground, with compromised credentials now a leading cause of breaches. Organizations are shifting from passwords to biometric and passwordless solutions while contending with synthetic personas, AI agents and deepfakes that challenge traditional authentication models. The rise of generative AI has magnified the risk to identity authenticity, enabling highly customized social engineering attacks while compelling a rethinking of access control for non-human entities operating at machine speed.

Proactive Detection and Response

Alert-centric security operations are giving way to proactive threat hunting and intelligence-informed defense. Organizations are moving from reactive models to hypothesis-driven investigation, leveraging real-time telemetry and agentic AI while embedding threat hunting into fusion teams. This shift demands analysts who understand scripting, telemetry correlation and adversary tactics rather than simply managing alerts.

Security as a Business Strategy

Cybersecurity has evolved from a technical function to a strategic business driver. Forward-looking enterprises integrate security into executive decision-making, treating it on par with financial and operational risks. Security maturity has become a market differentiator, with investors viewing it as a signal of operational excellence. Organizations are adopting value-focused metrics that quantify security in terms of operational efficiency, revenue enablement and risk reduction rather than compliance alone.

Critical Infrastructure Vulnerabilities

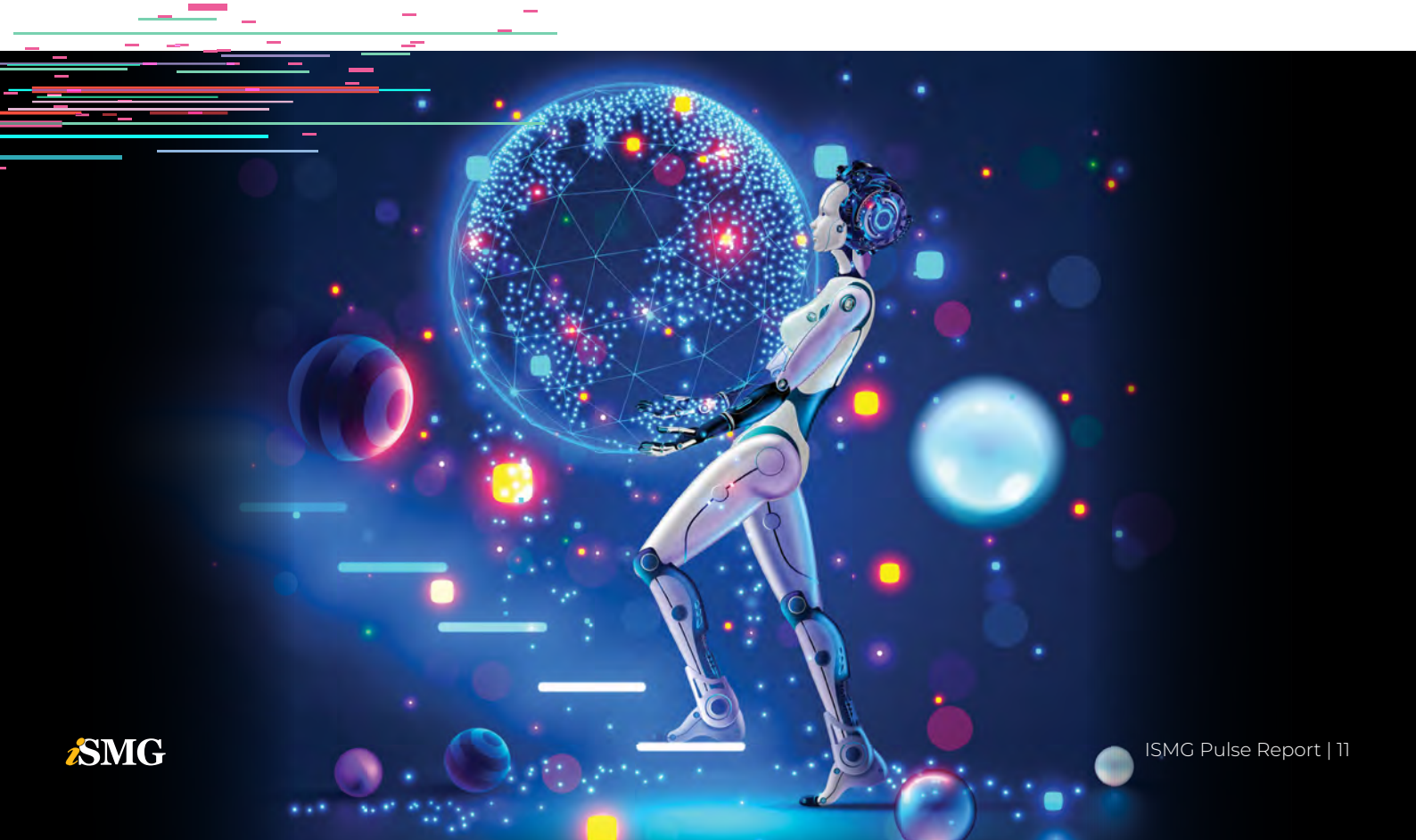
Critical infrastructure faces unprecedented systemic risk from converging IT/OT environments and the rapid evolution of renewable energy systems. The interdependence of sectors means that a breach in one domain can cascade across multiple systems. Energy infrastructure particularly faces an alarming security gap, with only 1% of cybersecurity focused on renewables despite their growing importance. This systemic fragility is prompting regulatory shifts from voluntary frameworks to enforceable obligations.

The Human Element

Cybersecurity is fundamentally a human endeavor, with emotional resilience, behavior patterns and mental well-being emerging as essential dimensions of security posture. The industry faces a burnout crisis, with 50% of professionals expecting burnout in the coming year, rising to 85% in the Asia-Pacific region. Progressive organizations are responding by automating pain points, institutionalizing recovery periods and building mental health support into security operations.

The Evolution of Cybercrime

Cybercrime has matured into an industrialized ecosystem with clear ROI models, automation and robust criminal supply chains. Ransomware tactics have shifted from encryption to data exfiltration, with 50% of recent attacks involving only data theft. AI-driven attacks using deepfakes and voice cloning have increased 442%, while supply chain compromises enable threat actors to pivot from a single vulnerability to mass exploitation in under an hour. No industry is immune, with 86% of cases resulting in business disruption.



The cybersecurity landscape of 2025 demands not just better tools, but integrated thinking across disciplines, borders and business units. Organizations that balance innovation with transparency, agility with governance, and technology with human factors will be best positioned to navigate this evolving threat environment.

This *The 2025 Cybersecurity Pulse Report* is the fifth such report in the Pulse Report series and is an essential addition to our ongoing effort to capture and disseminate expert-driven cybersecurity intelligence from the massive volume of content generated at ISMG events worldwide, ensuring decision-makers stay ahead in an increasingly complex threat environment.

STRATEGIC IMPERATIVES

1. **Invest in AI-powered defenses:** leverage AI not just for efficiency but as a core component of threat detection, while implementing governance frameworks to mitigate AI risks.
2. **Adopt identity-centric security:** Move beyond perimeter-based models to focus on authenticating and continuously validating identities, treating SaaS applications as platforms rather than endpoints.
3. **Prioritize visibility and integration:** Combat fragmentation by unifying telemetry across environments and breaking down silos between security tools.
4. **Embed resilience into design:** Build systems capable of sustaining operations through attacks, not just preventing them, with a particular focus on critical infrastructure.
5. **Quantify security value:** Shift metrics from compliance to business enablement, demonstrating how security investments directly support strategic objectives.
6. **Humanize security operations:** Invest in the psychological safety and well-being of security teams to enhance decision-making and reduce attrition.
7. **Accelerate detection and response:** Move from alert triage to hypothesis-driven hunting and intelligence-informed defense.
8. **Prepare for emerging threats:** Develop strategies for autonomous AI agents, post-quantum cryptography and decentralized threats operating at machine speed.

CHAPTER 1

AI's Disruption of Security: Risks, Defenses and New Frontiers

Artificial intelligence has become the defining force of disruption across cybersecurity, physical security and national defense. While defenders race to harness AI for detection, response and mitigation, threat actors are equally leveraging it to exploit scale, speed and deception.

01

AI-Enhanced Threats in Cybersecurity

The cybersecurity community is grappling with a new kind of asymmetry. Adversaries can now automate phishing, generate polymorphic malware and conduct identity fraud with alarming precision. “We’ve seen a 250% increase in the speed of attacks over the past three or four years,” said Danny Milrad, director of product marketing - Unit 42 at Palo Alto Networks. “Twenty percent of our cases, from the time of compromise to exfiltration, were within less than an hour.”

This trend echoes warnings from the European Union Agency for Cybersecurity (ENISA), which described AI as a catalyst for increasingly adaptive and evasive threats, including generative phishing, deepfakes and adversarial attacks.[1]

But defenders are not powerless. AI is proving vital to scaling response. “Defenders are using AI. But they’re not using AI enough,” Milrad said. His team found that “in 75% of the cases, the data was in the logs that indicated there was an

> “We’ve seen a 250% increase in the speed of attacks over the past three or four years.”
>
> *Danny Milrad, director of product marketing - Unit 42 at Palo Alto Networks.*

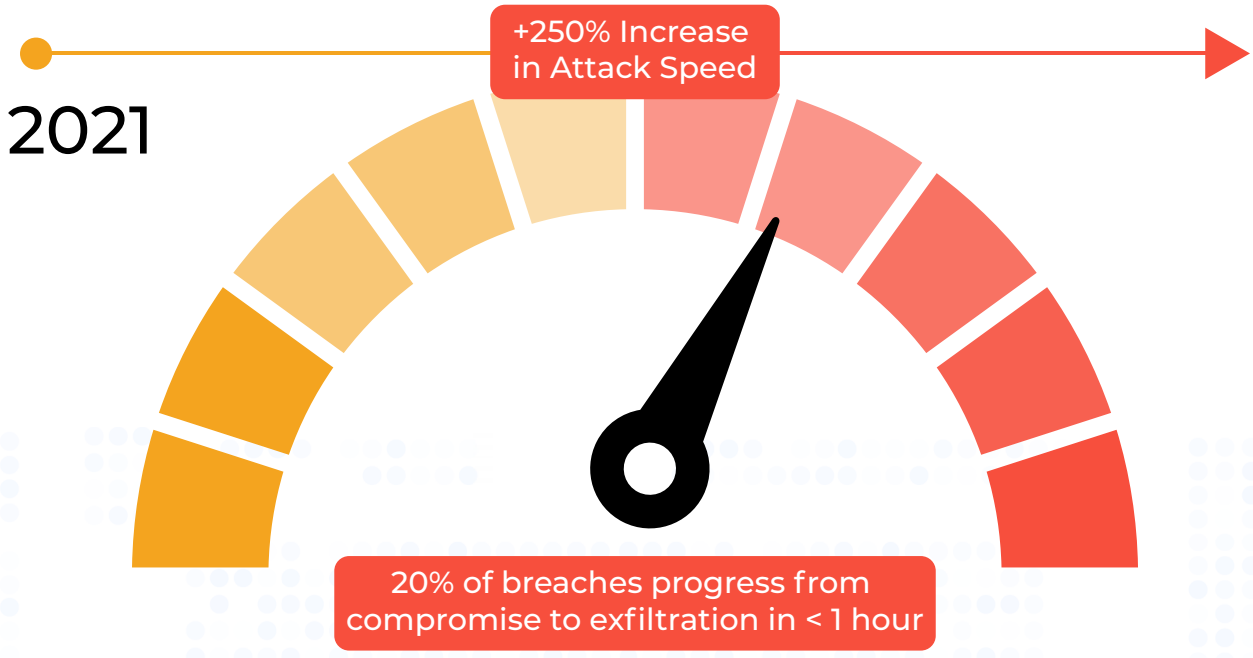
attack," but signals were missed due to "silos, complexity and just all the signal noise coming through."

The AI vs. AI paradigm comes with its own set of risks, especially adversarial machine learning (ML). NIST's AI Risk Management Framework underscores the need for robust, explainable and monitored models to counter these threats by developing a taxonomy addressing such adversarial ML threats.[2]

"We don't see new crimes being done," said Cynthia Kaiser, deputy assistant director at the FBI. "What we see are actors using AI to be able to do some crimes a little bit better." This subtle yet powerful insight defines the current landscape: AI is not inventing new cybercrimes, but it is amplifying the effectiveness of existing ones.

> **We don't see new crimes being done," said. What we see are actors using AI to be able to do some crimes a little bit better.**
>
> *Cynthia Kaiser, deputy assistant director at the FBI.*

AI's Dual-Edge Impact: The Acceleration of Cyber Attacks



02

National Security and the AI Arms Race

AI is not just reshaping corporate defense - it is redefining military doctrine.

Armed forces are integrating autonomous drone swarms, AI-enhanced missile guidance and predictive intelligence systems into their strategic operations. The Congressional Research Service has warned that this shift compresses decision-making timelines, increasing the risk of unintended escalation - reshaping not just capabilities but doctrine.[3]

> AI in cyber is a double-edged sword..
>
> *Peter McKay, CEO of Snyk*

Kaiser underscored how adversaries are already weaponizing AI. “We were able to disrupt a Russian tool in advance of the 2024 elections [that used] AI-generated images,” she said. “North Korean IT workers, hide who they are, try to get a job … so they can bring that money back overseas.” These examples highlight how generative models are being leveraged in covert operations, blending cyberwarfare with social manipulation.

Peter McKay, CEO of Snyk, warned of AI's dual-use nature. "AI in cyber is a double-edged sword. The same models we use to detect intrusions can be flipped to identify system vulnerabilities," he said. "You've got rogue states, cyber gangs and militaries - all incentivized to abuse the same tools we rely on for defense." This dynamic is especially troubling given that language models are already capable of identifying vulnerabilities and generating exploit code.

Calls for international regulation are growing, particularly around lethal autonomous weapons. The United Nations Institute for Disarmament Research has emphasized the urgency of agreements to control these systems,[4] while NIST notes the "expanded attack surface" and risks such as prompt injection and data poisoning.[5] "Speed is the danger," McKay warned. "AI collapses the time you have to react - and that's when mistakes get made."

> **"You've got rogue states, cyber gangs and militaries - all incentivized to abuse the same tools we rely on for defense."**
>
> *Peter McKay, CEO of Snyk*

03

The Deepfake Dilemma: AI's Expanding Threat to Enterprise Security

As generative AI becomes cheaper, more powerful and easier to access, organizations must face a new reality - one where fake audio, video and identities infiltrate enterprises with alarming ease and frequency.

Hany Farid, Professor at UC Berkeley and co-founder and chief science officer at GetReal, emphasized that deepfakes are not speculative threats - they are already embedded in the operational fabric of cyberattacks. "For every one of those stories you read, there are 10 to 20 that you don't read about," he said. "These attacks are happening to enterprises on a daily basis."

With tools now capable of cloning a voice from a 15-second sample or altering appearance in real-time video calls, threat actors can exploit virtual meeting platforms and hiring processes at scale. In enterprise environments, real-time video impersonation demands an instantaneous response. "In real time, you have to detect this thing within 10 to 15 seconds - you don't have an hour or two," Farid said.

> "In real time, you have to detect this thing within 10 to 15 seconds - you don't have an hour or two."
>
> *Hany Farid, Professor at UC Berkeley and co-founder and chief science officer*

Milrad expanded on this, flagging a disturbing rise in the use of generative AI for social engineering and insider threats. “We’re also seeing another trend … the use of deepfake technology to bypass measures from an insider threat perspective.” In some instances, attackers “send somebody in for an interview and send somebody else in to take the job,” exploiting disjointed HR and InfoSec processes. His recommendation? Cross-functional vigilance: “We are advocating for HR to work with InfoSec, to work with the SecOps team.”

Adding to the complexity is the legal ambiguity surrounding AI-generated content. Deepfakes and synthetic media often fall outside clear statutory definitions. Kaiser said, “Just because you’re lying, it doesn’t mean it’s not free speech. There has to be something else there.” This nuance requires entities like the FBI to assess deeper contextual cues - such as impersonation, fraud or foreign origination - before legal action can be pursued.

04

AI for Good: Security Operations Center Augmentation and Standards

While AI poses undeniable risks, it is also being harnessed to reinforce cyber defenses and streamline operations. Organizations are deploying machine learning models for threat detection, deepfake analysis and behavioral anomaly recognition - enhancing capabilities far beyond manual methods.

The SANS Institute's 2024 Detection & Response Survey and the NIST AI Risk Management Framework both spotlight AI's growing role in powering zero trust architectures and improving operational resilience.[5,6]

Daniel Kennedy, principal research analyst - information security channel at S&P Global Market Intelligence, explored behavioral differences between ransomware victims and non-victims. His team uncovered a sobering disconnect between expectations and reality. "The number of people who think they'll pay the ransom is a much lower percentage than people who actually do," he said.

> **"The number of people who think they'll pay the ransom is a much lower percentage than people who actually do."**
>
> *Daniel Kennedy, principal research analyst - information security channel at S&P Global Market Intelligence GetReal*

"The percentage of people who said they were a victim of ransomware attacks has gone down, but the percentage of people who have paid the ransom has gone up significantly." Kennedy labeled this trend as a form of "overconfidence," noting that improved tooling hasn't translated into fewer breaches.

"The tools have gotten better, but the overconfidence in the tools has kept up with the tools getting better," Kennedy said. Compounding the issue, he warned that 40% of alerts still fall through the cracks due to analyst fatigue.

From a productivity standpoint, AI is also reshaping security operations centers (SOCs). "Our internal cybersecurity teams [are] leveraging AI to respond to threats, manage our SIEM and help create a more secure organization," said Collin Gallagher, senior vice president at Thoma Bravo.

> "Our internal cybersecurity teams [are] leveraging AI to respond to threats, manage our SIEM and help create a more secure organization."
>
> *Collin Gallagher, senior vice president at Thoma Bravo Market Intelligence GetReal*

By offloading repetitive tasks, AI allows analysts to prioritize high-value threat hunting. Gallagher cited Proofpoint, a Thoma Bravo portfolio company, as a leading example: "They did leverage large language models … to detect what the intent of a message was," Gallagher said.

Frameworks are advancing in lockstep with these technical gains. NIST's AI RMF and the SANS 2024 report emphasize the importance of governance and dynamic trust modeling, particularly as AI tools become foundational to threat detection and SOC workflows.[6]

05

The Quantum Horizon

The convergence of AI and quantum computing marks a major shift in cybersecurity. As quantum capabilities evolve, traditional cryptographic standards face obsolescence. “Quantum computers can break current cryptography,” said Jon France, CISO at ISC2. “We’ve got to be thinking about being crypto-agile,” as quantum timelines accelerate. He warned that teams “need to build road maps and strategies now to be ready to migrate as soon as standards are ratified.”

In response, national and international efforts are intensifying. The National Cybersecurity Center of Excellence, part of NIST, has articulated the importance of preparing for the post-quantum era.[7]

Preparing for the post-quantum era requires global coordination across vendors, standards bodies and implementers. AI, meanwhile, will play a dual role - both aiding in real-time threat detection and complicating cryptographic transitions.

> “We’re going to go through a phase where things will break before they get better.
>
> *Jon France, CISO at ISC2*

As France concluded, “We’re going to go through a phase where things will break before they get better.” Managing this transition demands not just innovation but also foresight, collaboration and strong cyber hygiene.

Conclusion

AI’s disruption of security is not a temporary phase - it is a permanent shift. It brings speed, complexity and autonomy that challenge existing defense paradigms. But it also enables new forms of resilience and innovation.

Alberto Yépez, managing director at Forgepoint Capital, described the current moment as a “massive wave of innovation with AI” that mirrors the early internet era - but on steroids.

The path forward lies in balancing innovation with transparency and agility with governance. Those choices will shape whether AI becomes a stabilizing force or a strategic vulnerability.

Yépez advocated for a tempered optimism - one that embraces AI innovation but insists on ethical design and decision-making oversight. “You let machines make decisions … you may be sorry about that,” he warned. “It’s always the human in the loop.”

Footnotes

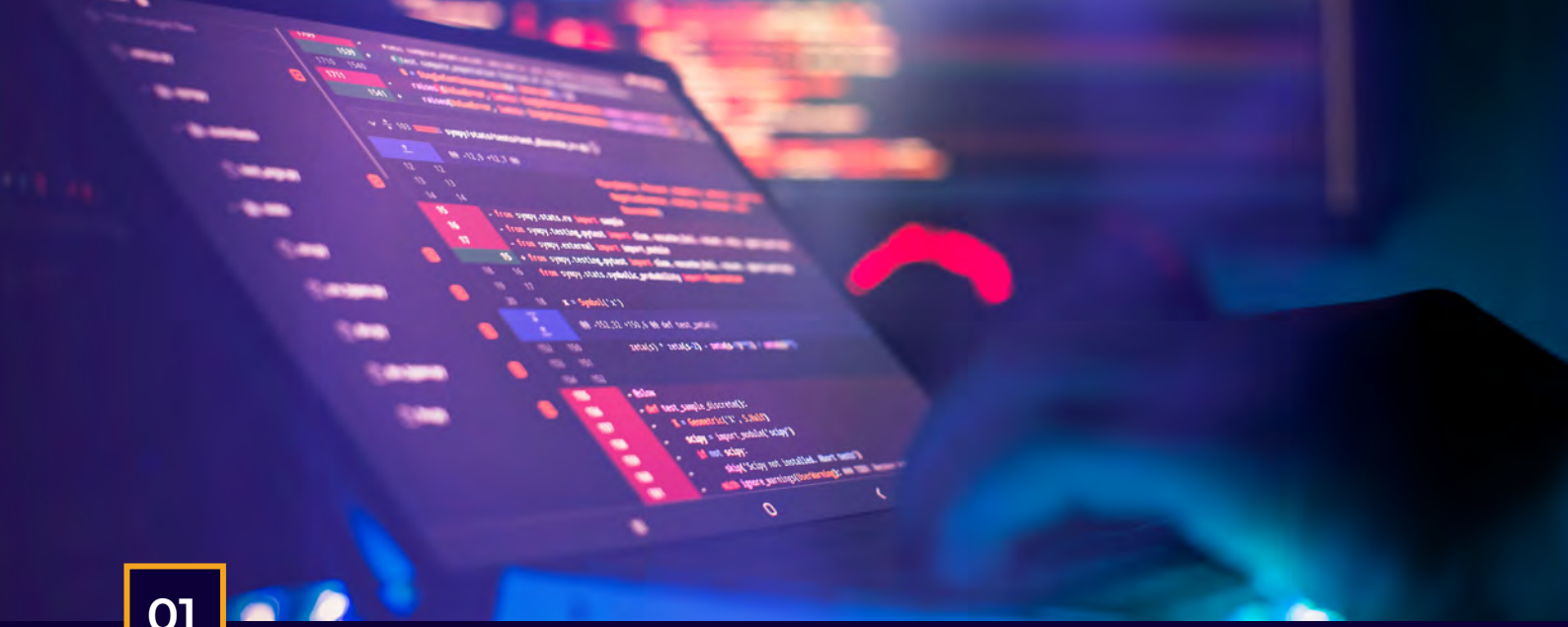
1. NISA. (2023). AI threat landscape report unveils major cybersecurity challenges. https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges
2. NIST. (2023). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations. https://csrc.nist.gov/pubs/ai/100/2/e2023/final
3. Congressional Research Service. (2023). Artificial intelligence and national security. https://www.congress.gov/crs-product/R45178
4. Council on Foreign Relations. (2024). Election 2024: The deepfake threat to democracy. https://www.cfr.org/blog/election-2024-deepfake-threat-2024-election
5. NIST. (2023). AI risk management framework (RMF) 1.0. https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems
6. SANS Institute. (2024). 2024 detection & response survey: Transforming cybersecurity operations https://www.sans.org/white-papers/sans-2024-detection-response-survey/
7. National Cybersecurity Center of Excellence (NCCoE). (2023). The quantum threat to cybersecurity. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

CHAPTER 2

The Collapse of Traditional Security Models: How Cloud, SaaS and Identity Are Reshaping Cybersecurity

For decades, cybersecurity strategy was grounded in a simple premise: build a strong perimeter and monitor what enters and exits. Firewalls, VPNs and intrusion prevention systems (IPSs) were designed to secure a clearly defined network boundary. That boundary, however, no longer exists. In today's decentralized enterprise - shaped by rapid cloud adoption, widespread SaaS integration and remote work - the idea of a network perimeter is largely obsolete.

The collapse of traditional security models is not just a matter of dissolving borders - it's a radical reordering of priorities. Identity, not infrastructure, is now the frontline. Visibility, not control, is the new imperative.



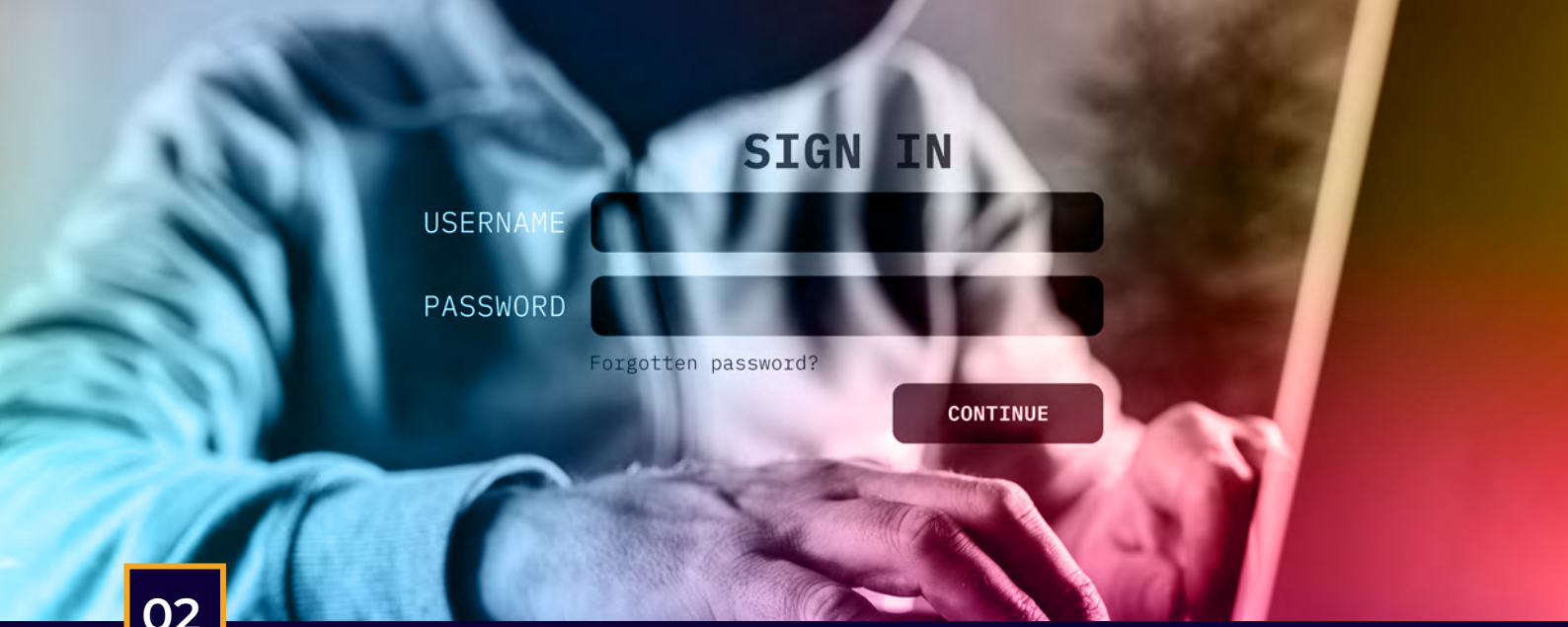
01

Perimeter Defenses Are Crumbling

One of the clearest signs that perimeter-based models no longer suffice is the shifting role of the browser. Once treated as a passive portal, the browser is fast becoming a focal point of enterprise security architecture - and a source of both opportunity and risk.

"The browser we all use every single day, it's consumer-grade technology ... it wasn't built for the rigors of the enterprise," Rogers said. He likens deploying legacy browsers in modern business environments to "taking the family sedan racing in the Indianapolis 500."

> "The browser we all use every single day, it's consumer-grade technology ... it wasn't built for the rigors of the enterprise."
>
> *Bradon Rogers, head of product at Island*



02

Identity Is the New Battlefield

Cybercriminals increasingly favor exploiting identities rather than breaking through network defenses. Phishing remained the most common cybercrime in 2024,[8] and compromised credentials are now a leading cause of breaches. There is a significant year-over-year increase in the sale of stolen credentials, with a sharp rise in VPN and enterprise login offerings, underscoring how attackers capitalize on human error and weak access controls.[9]

In short, if they can log in, they don't have to hack in.

Credential phishing, token theft and session hijacking are among the most common entry points. "We have really good controls... on how you get in the front door, but we need a lot more work on what you could do once you're inside," said Mike Towers, chief security and trust officer at Veza. He likens the industry's current approach to identity to TSA security at an airport - great at screening but blind to behavior inside the terminal.

> "We have really good controls... on how you get in the front door, but we need a lot more work on what you could do once you're inside."
>
> *Mike Towers, chief security and trust officer at Veza*

Most legacy systems were designed "to meet service levels, to tick compliance checkboxes and to run workflows. So none of those things help with security," Towers said. This service-first orientation means organizations are "really good at granting access. They're really poor at taking it away."

Zero trust has emerged as the leading response to this identity crisis. But despite its promise, real-world adoption remains uneven. A 2024 Gartner survey found that while 63% of organizations had begun implementing zero trust, many struggled with integration challenges, cost overruns and incomplete coverage.[10]

> "This service-first orientation means organizations are "really good at granting access. They're really poor at taking it away."
>
> *Mike Towers, chief security and trust officer at Veza*

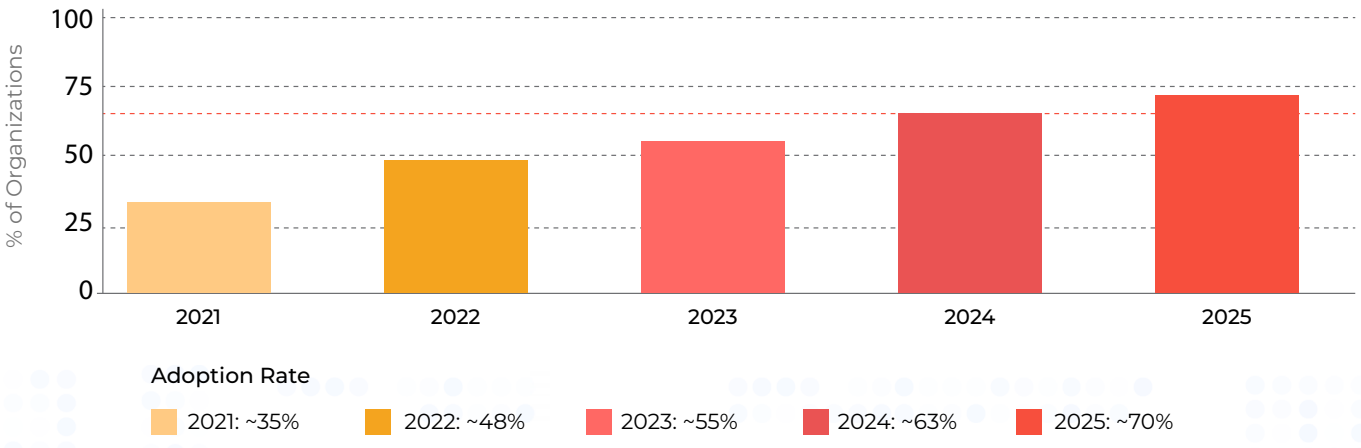
The Collapse of Traditional Security Models

Zero Trust Implementation Analysis

"63% of organizations have begun implementing zero trust, but many struggle with integration challenges, cost overruns, and incomplete coverage."

Zero Trust Adoption Rates (2021-2025)

Percentage of organizations that have begun implementing zero-trust security approaches



Source: 2024 Gartner Zero Trust Adoption Survey

03

The Limitations of Identity-Only Strategies

While identity has become central to modern security models, relying on it alone can create dangerous blind spots. “Organizations had a very fragmented infrastructure … many different products, many different controls … but they don’t talk to each other, and they don’t understand each other,” said Dean Sysman, CEO and co-founder of Axonius. The result is a critical loss of visibility that adversaries quickly exploit.

“Most breaches … don’t happen because of a very flashy zero-day,” Sysman said. “They’re just taking advantage of open opportunities.”

> **Most breaches … don’t happen because of a very flashy zero-day. They’re just taking advantage of open opportunities.**
>
> *Dean Sysman, CEO and co-founder of Axonius*

04

SaaS Sprawl and the Challenge of Shadow IT

As cloud and SaaS adoption skyrockets, organizations face mounting challenges in managing the resulting sprawl and shadow IT. “Clients are purchasing SaaS from multiple vendors, and those vendors are not staying ahead of the curve on security and compliance,” said Dean Fantham, founder, managing partner and CTO at Edgile. “Those end up with risk [to] the customers.”

Fantham also emphasized a leading cause of breaches. “One of the biggest challenges in the shift to the cloud and one of the greatest causes of breaches are misconfigurations,” he said. Configuration drift, especially in teams adjusting to cloud environments, represents a silent yet potent threat.

Tool proliferation continues unchecked, creating blind spots, increasing cost and forcing teams into fragmented silos. Meanwhile, even foundational concepts such as “network” and “access” are evolving. “The definition of what the network is changes. The definition of what access means changes,” said PJ Hamlen, worldwide leader for the Global Partner Security Initiative at Amazon Web Services. This shift demands a rethinking of legacy mental models.

> “Clients are purchasing SaaS from multiple vendors, and those vendors are not staying ahead of the curve on security and compliance.”
>
> *Dean Fantham, founder, managing partner and CTO at Edgile*

05

The AI Disruption: Threat and Opportunity

AI is both a disruptor and an enabler. On one hand, it provides organizations with new automation and decision-making capabilities. On the other hand, it equips threat actors with faster and more intelligent tools.

"In a world of SaaS sprawl, unmanaged devices and AI-assisted threats, organizations are recognizing that securing the application interface layer - not the device or network - is the new frontier," said Bradon Rogers, head of product at Island.

This reality demands a mindset shift. Security leaders must now defend against AI-generated threats while responsibly integrating AI into their own operation.

> "In a world of SaaS sprawl, unmanaged devices and AI-assisted threats, organizations are recognizing that securing the application interface layer - not the device or network - is the new frontier."
>
> *Bradon Rogers, head of product at Island*

06

Redefining Security in a World Without Perimeters

The evolution of work and technology has rendered the traditional network perimeter obsolete. “The cloud has moved from being an add-on to the data center … now the data center has started to become the add-on to the cloud,” Hamlen observed. This inversion forces a fundamental shift in how cybersecurity is architected.

Legacy endpoint and VPN-based controls are ill-equipped for today’s device diversity and decentralized workforces. “My favorite use cases are often BYO,” said Rogers. “You’re dealing with a wide variety of different form factors … but the browser still exists on all those devices. If the browser is the enterprise browser for delivering applications, it can be ubiquitous.”

This evolution is not merely technological - it’s architectural and strategic. “Ultimately, the transformation reflects a broader move away from rigid perimeters toward adaptive, identity-aware models,” Rogers said.

> “Clients are purchasing SaaS from multiple vendors, and those vendors are not staying ahead of the curve on security and compliance.”
>
> *Dean Fantham, founder, managing partner and CTO at Edgile*

As organizations move toward zero trust and identity-centric strategies, the challenge lies in stitching together disparate pieces into a cohesive security fabric - one that can operate effectively in a cloud-native, perimeterless world.

Conclusion: Principles for the Future

- Identity is critical, but not sufficient. Authentication is the starting point, not the finish line.
- SaaS is a security domain. Treat SaaS apps as platforms, not endpoints.
- Visibility must be unified. Fragmented telemetry undermines threat detection.
- AI must be governed. Automation without oversight invites new risks.
- Zero trust is a journey. Architecture matters, but culture and process are what make it stick.

The collapse of traditional models isn't a crisis; it's a catalyst. Those who adapt will find themselves not just protected but empowered in the digital era.

Footnotes

8. Mandiant. (2025, March). AI in cyber threats: 2025 outlook. https://cloud.google.com/blog/topics/threat-intelligence/mandiant-leveraging-ai/
9. Palo Alto Networks Unit 42. (2024, February). Cloud threat report: Volume 7. https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research
10. Gartner. (2024, April). Zero trust adoption survey 2024. https://www.cybersecuritydive.com/news/majority-businesses-zero-trust-gartner/713856/

CHAPTER 3

The Evolving Identity Crisis: Trust, Authentication and Digital Persona Risk

The question of identity in today's digital world is no longer just "Who are you?" - it's "Who's authorized?" and "Can I trust this interaction?" Digital identity has become the new battleground of cybersecurity, as synthetic personas, AI agents and compromised infrastructure stretch traditional models of authentication and trust to their breaking point.

"Identity is the security perimeter that kind of gates everything else," said Alex Weinert, chief product officer at Semperis. If this perimeter is breached, "they've got everything, regardless of what second line security you might have." It's a paradigm shift security leaders are only beginning to address.

01

Trust in Digital Identity Is Fracturing

The breakdown of trust in digital identity is accelerating, fueled by the widespread compromise of legacy identifiers such as passwords, Social Security numbers and security questions. This erosion of trust has invited a surge in fraud. In 2023, over 1.4 million identity theft cases were reported in the U.S., leading to billions in financial losses.[11]

"Fraud is becoming more automated, it is becoming more pervasive and the financial impact on individuals is higher," said James Lee, president of the Identity Theft Resource Center. But it's not just financial. "With higher financial impact comes higher emotional impact, which is an often overlooked part of any of these scams."

> **Fraud is becoming more automated, it is becoming more pervasive and the financial impact on individuals is higher.**
>
> *James Lee, president of the Identity Theft Resource Center*

02

Biometric and Passwordless Authentication Gain Ground

As digital trust becomes more complex, organizations are steadily shifting away from traditional, knowledge-based authentication. Passwords are giving way to biometric and passwordless solutions as enterprises contend with an expanding access surface and users operating across personal and work devices. “People can work from anywhere. They can work on both personal devices as well as work devices, and they work on all types of apps, not just apps that IT has deployed,” said Jeff Shiner, co-CEO of 1Password.

This shift creates what Shiner terms an “access trust gap,” where the tools IT expects to manage no longer align with actual user behavior. Instead of enforcing blanket controls, modern systems are leaning into user agency: “We can give visibility into where that device is insecure … but we don’t force it onto that device,” Shiner said. “You, as the owner, can sit there and see, oh, in order to use a business app, I need to put this patch on. But you still get that choice.”

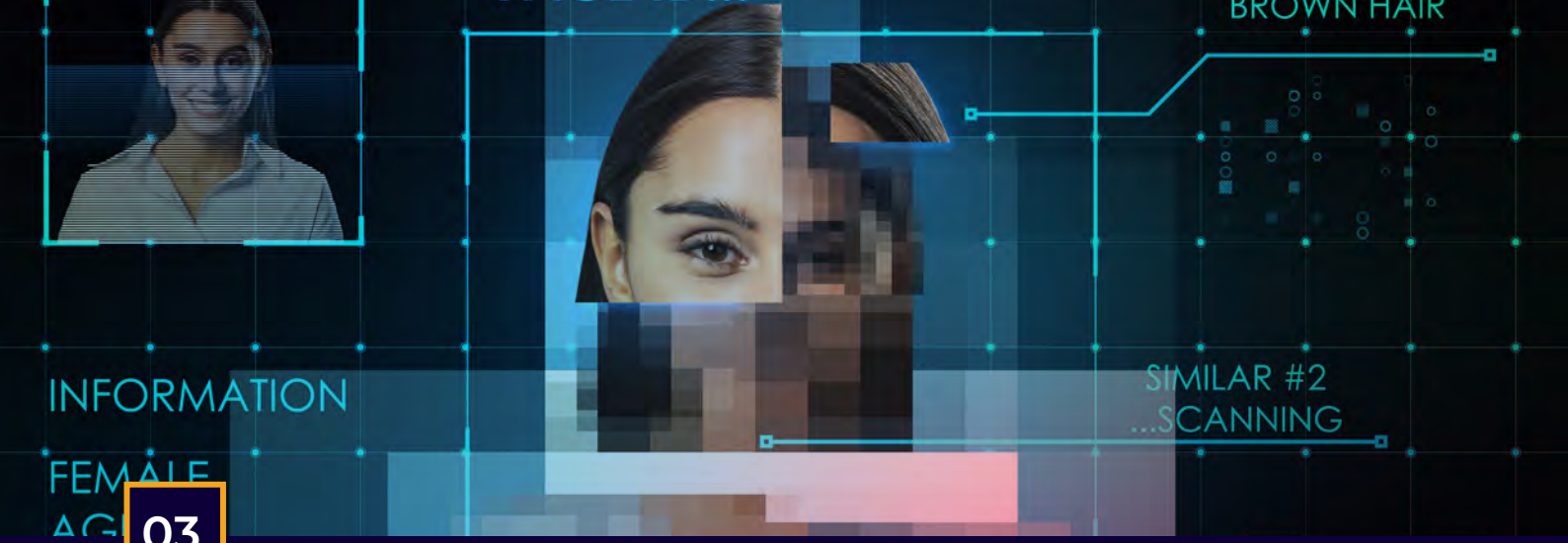
> “People can work from anywhere. They can work on both personal devices as well as work devices, and they work on all types of apps, not just apps that IT has deployed.”
>
> *Jeff Shiner, co-CEO of 1Password*

Passkeys - cryptographic alternatives to passwords - are gaining momentum.[12] Apple, Google and Microsoft have backed them as a secure, user-friendly standard. They fit naturally into this paradigm of "honest security," which balances control with user autonomy. But the technology challenge escalates when non-human entities - such as AI agents - enter the identity ecosystem.

These agents don't carry smartphones or perform human behaviors that traditional MFA relies on. "They make decisions. They make choices. They need access to data … but they're not a person," Shiner said. For them, identity must be encoded into service accounts with "just-in-time access … for a limited period of time."

> **"They make decisions. They make choices. They need access to data … but they're not a person."**
>
> *Jeff Shiner, co-CEO of 1Password*

Even with MFA in place, social engineering remains a primary threat vector. As Weinert noted, attackers increasingly exploit behavioral fatigue. "We saw, regularly, attacks where people would simply send a message saying, 'Hey, please send me the code on your authenticator.'"



03

Deepfakes, AI Agents and Synthetic Identity Risk

The rising sophistication of gen AI has magnified risks to identity authenticity. AI agents - non-human entities that make autonomous decisions - are not just executing tasks at machine speed but also reshaping the way organizations think about access and control.

"They're not actually behaving like humans, even though they might have privileged access," warned Matt Cohen, CEO of CyberArk. "We have to know where they are, who they are, we have to know what access rights they have, put that in context, and we actually have to be watching them all the time."

This monitoring imperative grows more complex in the face of AI-enabled fraud. "Generative AI gives you this ability to tightly customize the message," Weinert said. "The average human's ability to withstand an attack like this ... is going to plummet."

Synthetic identities, which blend real and fabricated information, further blur the line between real and fake. Victims of identity compromise often don't

> **Almost 80% of all cyberattacks ... begin with identity. It begins with information that's been stolen in another data breach.**
>
> *James Lee, president of the Identity Theft Resource Center*

realize they've been targeted until long after the fact. "Almost 80% of all cyberattacks … begin with identity. It begins with information that's been stolen in another data breach," Lee said. Yet many victims remain silent, internalizing blame: "They feel shame. 'I am too smart. I can't believe I fell for this.' So they keep it to themselves," he said.

Defensive AI tools are essential to push back against these threats. "You can use robots to fight robots," Weinert said, who emphasized the need for AI that can "detect non-human mails" and hunt threats more dynamically than human analysts ever could.

> **You can use robots to fight robots.**
>
> *Alex Weinert, chief product officer at Semperis*

04

Governments' Race to Regulate Identity and AI

In response to mounting digital identity and AI threats, governments worldwide are advancing policy at pace. While Europe leads with sweeping frameworks such as the eIDAS 2.0 and the AI Act, other regions are catching up with targeted regulations and public-private partnerships.[13,14]

Meanwhile, within the U.S., the policy landscape is defined more by federal guidance and state-level initiatives than national mandates. "With the modern enterprise, where we have everything moving to the cloud, remote work and everything else … identity has become the first, and in many cases, the last line of defense," said Mickey Bresman, CEO and co-founder of Semperis. But this prioritization has also made identity systems a singular point of failure. "If the identity system goes down … you cannot log in to your applications. Basically, everything stops immediately."

Across both democratic and authoritarian regimes, there is growing recognition that AI agents and machine-generated personas will require a rethinking of not just digital ID frameworks but also cross-border standards for content provenance, behavioral analysis and risk adjudication.

> "Almost 80% of all cyberattacks … begin with identity. It begins with information that's been stolen in another data breach.
>
> *James Lee, president of the Identity Theft Resource Center*

Conclusion: Principles for the Future

In a world of deepfakes, data breaches and synthetic personas, digital identity can no longer be taken at face value. Security leaders must prioritize:

- Frictionless but verified identity experiences;
- Privacy-preserving authentication by default;
- Defense against emerging threats such as AI impersonation.

Trust is no longer a binary. It's dynamic, contextual and shaped by design. If you can't verify who or what you're interacting with, you can't secure anything. Identity isn't just a feature anymore. It's the foundation.

Footnotes

11. Federal Trade Commission. (2023). Consumer Sentinel Network data book 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023
12. FIDO Alliance. (n.d.). Passkeys. https://fidoalliance.org/passkeys/
13. European Commission. (n.d.). eIDAS regulation. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
14. European Parliament. (2023). Artificial Intelligence Act. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

CHAPTER 4

Detection and Response Reinvented: How Enterprises Are Shifting From Alerts to Proactive Hunting

The alert-centric detection model, once foundational to SOCs, is nearing obsolescence. As attackers grow more agile and attack surfaces expand, reactive security is buckling under the pressure of alert fatigue and delayed response. In its place, enterprises are embracing a forward-leaning model: one fueled by real-time telemetry, agentic AI and human-led threat hunting that is deeply embedded into modern cyber resilience strategies.

01

The Fatigue of the Reactive Model

Legacy SOC models built on static detections and layered triage are increasingly being outpaced by adversaries who leverage stealth and speed. “Security today is very reactive,” said Martin Zugec, technical solutions director at Bitdefender. “We usually let this stuff happen, and then later the security operations are going to investigate based on EDR XDR incidents.”

Zugec highlighted how attackers exploit native tools in the environment to evade detection. “All these attacks have been the use of ‘living off the land’ attack components … they just use the tools that already exist on the network,” he said. In one case, the attack left no malware trace. “It was 100% ‘living off the land’ attack, no malware … data encryption was using BitLocker.”

Zugec argued this situation is no longer sustainable. The outcome is a detection surface too noisy to act on and too blind to catch subtle intrusions.

> “All these attacks have been the use of ‘living off the land’ attack components … they just use the tools that already exist on the network.
>
> *Martin Zugec, technical solutions director at Bitdefender*

02

The Rise of Threat Hunting as a Strategic Discipline

Proactive threat hunting is emerging as the antidote to alert fatigue. A fundamental shift is underway - from waiting for alerts to actively hunting for adversaries. Luckily, agentic AI can help with threat hunting in a big way. "Threat hunting is one area where we intend to leverage the agentic AI in a big way," said Sameer Ratolikar, CISO of HDFC Bank.

"You're not going to be able to respond to attacks if you're constantly switching between different avenues," said John Pirc, vice president and head of product management at NetWitness. He emphasized that legacy detection is focused too heavily on external ingress traffic. "Many tools still focus on 'north-south traffic ... traffic that's coming from the internet into the organization,' while the real threats often move laterally ... going east-west."

> **Almost 80% of all cyberattacks ... begin with identity. It begins with information that's been stolen in another data breach.**
>
> *James Lee, president of the Identity Theft Resource Center*

The convergence of threat hunting and incident response is reinforcing the need for hypothesis-led analysis over rule-based triage.

Moreover, threat hunting isn't an isolated practice; it's becoming embedded in fusion teams that combine detection engineering, response and intelligence. This architectural change is driving a cultural shift, where analytical curiosity and domain context outweigh rote alert triage.

03

Reinventing the Analyst Experience

The modern analyst is expected to go beyond rule creation to behavioral modeling and lateral thinking.

According to Sumit Dhawan, CEO of Proofpoint, today's SOC demands understanding scripting, telemetry correlation and adversary TTPs - not just managing alerts.

Marty Momdjian, general manager of Ready1 at Semperis, reinforced the strategic imperative. "Incidents happen 24 hours a day," he said. "The problem isn't just in the detection tooling - it's in the fragmentation of response."

Momdjian stressed the value of preparedness as an organizational imperative. "Start small. Start with tabletop exercises … in 30 minutes, you can be online in the platform and build your incident response team within seven days."

> **Start small. Start with tabletop exercises … in 30 minutes, you can be online in the platform and build your incident response team within seven days.**
>
> *Marty Momdjian, general manager of Ready1 at Semperis*

04

Strategic Outcomes and Organizational Maturity

The reinvention of detection and response has cascading strategic implications:

- Faster time to detect: Hypothesis-driven hunting reduces dwell time and tightens containment windows.
- Smarter investment: Budgets are shifting from perimeter controls to capabilities that prioritize resilience and adaptability.
- New metrics: KPIs now include mean time to detect, mean time to hunt and hypothesis-to-containment velocity.
- Collaborative intelligence: Participation in ISACs and threat intelligence exchanges is no longer optional for mature security programs.[15]

Conclusion

Detection and response are undergoing a seismic shift. The age of dashboards and delayed responses is giving way to real-time analysis, proactive engagement and intelligence-informed defense. In this new era, success belongs to the organizations that can unite the speed of AI with the insight of human analysts.

Footnotes

15. FS-ISAC. (2024). 2024 year in review. https://www.fsisac.com/2024-year-in-review

CHAPTER 5

Security as a Business Strategy: How Leadership, Risk and Resilience Drive Competitive Advantage

Cybersecurity has shifted from a technical silo to a central pillar of business strategy. In 2025, forward-looking enterprises no longer see security merely as compliance or overhead - they see it as the foundation for trust, adaptability and sustained growth. This chapter explores how executives are reframing cybersecurity as a strategic advantage, not just a defensive necessity.

01

Leadership: Security at the Executive Level

Cybersecurity leadership is no longer relegated to the back office - it's at the boardroom table.

By 2026, more than 60% of threat detection, investigation and response capabilities will leverage exposure management data to validate and prioritize threats - up from less than 5% today.[16] This shift underscores the growing importance of cybersecurity in strategic decision-making.

Executives are integrating security into every major decision - from digital transformation to mergers and acquisitions. Deloitte's 2023 Global Future of Cyber Survey found that cyber is more than just technology-focused - it is foundational to an organization's growth strategy.[17]

"The opportunity now is to own and lead the change into an AI world ... because if you don't as a security professional, you may get left behind," said Kevin Mandia, co-founder and strategic partner at Ballistic Ventures and former CEO of Mandiant. He described how evolving

> **The CISO has become a super significant, important role within any enterprise. They also have the challenge of communicating a very technical risk in the language that a board can understand - in risk terms and in dollar terms.**
>
> *Liran Grinberg, co-founder and managing partner at Team8*

threats have created “jump balls” in areas such as AI, supply chain and resilience - contested domains where security-savvy leaders must compete. “My CISO got almost every jump ball because I wanted a security-minded person to be the gatekeeper … but it goes to the best exec, usually,” Mandia said.

This demand for business fluency is reshaping the CISO role. Liran Grinberg, co-founder and managing partner at Team8, put it bluntly: “The CISO has become a super significant, important role within any enterprise. They also have the challenge of communicating a very technical risk in the language that a board can understand - in risk terms and in dollar terms.”

Brian Essex, executive director of U.S. Software Equity Research at J.P. Morgan, highlighted how investors view security as a leading indicator of maturity. “Investors want to see profitable growth … They need to see the cash flow. They need to see the fundamental quality that affords for a better investment,” he said. The message is clear - cyber maturity signals operational excellence.

> **Investors want to see profitable growth … They need to see the cash flow. They need to see the fundamental quality that affords for a better investment**
>
> *Brian Essex, executive director of U.S. Software Equity Research at J.P. Morgan*

02

Risk: From Reactive Defense to Strategic Risk Integration

Security is being fully integrated into enterprise risk frameworks, treated on par with financial, operational and geopolitical risks. McKinsey emphasizes that cybersecurity teams must improve risk management by applying quantitative risk analytics and aligning with business goals.[18]

"You have to talk in business speak," said Matt Kunkel, CEO and co-founder of LogicGate. "You can't talk in bits and bytes or vulnerabilities and assets. You have to talk in dollars and cents."

He elaborated on LogicGate's own journey. "We just introduced ... the first ever value realization application and framework that is embedded into the Risk Cloud platform," he said. This helps organizations measure GRC outcomes not just in terms of compliance but also "operational efficiency, revenue enablement and risk reduction."

Jeff Pollard, vice president and principal analyst at Forrester, emphasized the value of preemptive

> **"You have to talk in business speak. You can't talk in bits and bytes or vulnerabilities and assets. You have to talk in dollars and cents."**
>
> *Matt Kunkel, CEO and co-founder of LogicGate*

planning in an unstable world. “Once you give up the money, you don’t get it back.” He warned against “expense in depth” - spending on overlapping tools - and encouraged optimization instead. “Twenty percent of our customers are demanding this, and they’re responsible for 80% of our revenue,” he said, advising security leaders to align risk priorities with business value.

“More and more conversations are now coming up in terms of how do you align the work that we are doing in cybersecurity to how much risk we are reducing,” said Sumedh Thakar, president and CEO of Qualys, underscoring the shift to measurable risk reduction.

> “More and more conversations are now coming up in terms of how do you align the work that we are doing in cybersecurity to how much risk we are reducing.”
>
> *Sumedh Thakar, President and CEO of Qualys*

03

Resilience: Cyber Maturity as a Market Differentiator

In today's threat landscape, resilience isn't optional - it's a market differentiator.

Organizations with high cyber maturity recover faster, protect revenue and maintain trust during incidents. Those lacking resilience risk falling behind. The World Economic Forum reports a growing divide: the number of companies maintaining even a "minimum viable level of cyber resilience" has decreased by 30% in the last year.[19]

As Paul Zimmerman, director of technology at Blaine County School District, said after leading a rapid six-day ransomware recovery, "There is no way we would have been able to recover in six days without Cohesity as a part of that process."

Zimmerman stressed the importance of both tools and preparation. "It's a very good plan. However, I need the tools that let me implement that plan," he said. "Now, I have the technology and tools that let me actually do this plan as described."

> "If you don't have a plan, and if you don't have everybody on the same hymnal sheet ... now you have to deal with all sorts of other issues internally - egos, jockeying around."
>
> *Dale Zabriskie, Field CISO at Cohesity*

Dale Zabriskie, field CISO at Cohesity, explained the operational dynamics of resilient organizations. “If you don’t have a plan, and if you don’t have everybody on the same hymnal sheet … now you have to deal with all sorts of other issues internally - egos, jockeying around,” he said. Zabriskie also emphasized the value of “minimal viable business” planning. “What would you bring up first? What order? When? What data, what people, what processes does that include?”

Harry Coker, secretary of Maryland Department of Commerce, added a macro view: “America cannot be as strong as it needs to be without a strong cybersecurity posture … We cannot strengthen our economic prosperity until we sufficiently secure cyberspace.”

Finally, John Kindervag, chief evangelist at Illumio, brought it full circle. “Zero trust is really about protecting things that matter to an organization,” he said. For Kindervag, resilience isn’t just a design principle - it’s a business imperative. “Now they have a strategy that they can apply, not just a product, but a strategy.”

> **America cannot be as strong as it needs to be without a strong cybersecurity posture … We cannot strengthen our economic prosperity until we sufficiently secure cyberspace.**
>
> *Harry Coker, Secretary of Maryland Department of Commerce*

04

Final Word: Security Is Strategy

The competitive edge in 2025 lies in security maturity. Security-minded leadership wins boardroom trust, integrated risk strategy earns investor confidence and operational resilience defines market winners.

"It's not a question of if you're going to have a ransomware event, it's just a question of when - and you need to be prepared," Zimmerman said.

> **It's not a question of if you're going to have a ransomware event, it's just a question of when - and you need to be prepared.**
>
> *Paul Zimmerman, Director of technology at Blaine County School District*

Footnotes

16. CyberMagazine. (2023). Top cybersecurity predictions for 2023–2026. Cyber Magazine. https://cybermagazine.com/articles/gartner-unveils-top-cybersecurity-predictions-for-2023-2024
17. Deloitte. (2023). Global future of cyber survey. https://www.deloitte.com/global/en/services/consulting-risk/content/future-of-cyber.html
18. McKinsey & Company. (2018). Cyber risk strategy for cybersecurity. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-and-the-risk-function
19. World Economic Forum. (2024). 4 ways to advance equity in cyberspace. https://www.weforum.org/stories/2024/12/4-ways-to-advance-equity-in-cyberspace/

CHAPTER 6

Critical Infrastructure and Systemic Cyber Risk: Fragile Interconnected Worlds

As the backbone of national stability, critical infrastructure is increasingly under siege from sophisticated cyberthreats. What were once isolated incidents or cybercriminal nuisances have evolved into sustained campaigns with the capacity to paralyze entire sectors. From energy and water to aviation and telecommunications, modern interconnected systems reveal an alarming systemic fragility.

"In an OT cyberattack scenario, it's not just money, it's not just data, but it's safety, it's lives and its health at risk," said Burgess Cooper, CEO of Cybersecurity Division, Adani Enterprises.

01

Systemic Cyber Risk: The Expanding Threat Surface

The concept of systemic cyber risk is no longer academic. Events such as the Colonial Pipeline ransomware attack in 2021 underscored the real-world impact, with fuel shortages cascading across the U.S. East Coast.[20] Meanwhile, software vulnerabilities such as Log4j have demonstrated how a single flaw can ripple through multiple sectors, highlighting the interconnected nature of digital infrastructure.[21]

The convergence of digital operations and physical systems exposes entire ecosystems to cascading disruption, said Eric Trexler, senior vice president of U.S. Public Sector at Palo Alto Networks. "Visibility is one of the key aspects that we always look at ... getting sensors on the ground and understanding where the cyber challenges might be."

Colin Soutar, managing director at Deloitte, warned that "fragility in one domain could destabilize others," citing the vast scale of transportation infrastructure as a risk multiplier. "We know the

> **Countries say what's happening with our data? Where's our data going? Who's accessing it? As soon as it goes into that state-on-state activity, they can't use Interpol platforms anymore.**
>
> *Craig Jones, former director of cybercrime at Interpol*

adversary is in the critical infrastructure … What happens in time of conflict? How is that used against us?"

International fragmentation also complicates systemic risk management, said Craig Jones, former director of cybercrime at Interpol. "We've seen the geopolitics shrinking," Jones said. "Countries say, what's happening with our data? Where's our data going? Who's accessing it?" He added, "As soon as it goes into that state-on-state activity, they can't use Interpol platforms anymore," referencing the limits of legal cooperation under geopolitical tension.

02

The Reckoning of OT Security: From Visibility to Resilience

Legacy systems, converging with modern IT networks, create new attack surfaces with poor visibility. Robert M. Lee, CEO of Dragos, stressed the need for forensic readiness. "There's no way to know yet," he said in reference to power outages that lack proper instrumentation for root-cause analysis. "This is what a bad day looks like," describing his model for planning from worst-case scenarios backward.

"Back in the day, 10 years back, these manufacturing plants were not connected to the central systems ... they were actually pods and islands," said Rajesh Khazanchi, CEO and co-founder of ColorTokens. But now, "they are also becoming big threat vectors." He emphasized the speed at which lateral threats can propagate, referencing a conversation with a logistics executive: "Almost all of them can be compromised within 15 minutes." His recommendation: building containment strategies grounded in zero trust.

> **"Back in the day, 10 years back, these manufacturing plants were not connected to the central systems ... they were actually pods and islands."**
>
> *Rajesh Khazanchi, CEO and co-founder of ColorTokens*

03

Zero Trust in Critical Environments: Theory Meets Practice

Zero trust is gaining traction in critical infrastructure sectors, but implementation is uneven. The principle of "never trust, always verify" can be difficult to execute in OT environments where downtime is unacceptable and legacy systems dominate. Yet progress is happening.

Lee advocated for a risk-tiered triage model. "Only about 4% to 6% [of OT vulnerabilities] require urgent patching," he said, proposing a pragmatic, risk-based approach instead of blanket defenses.

Khazanchi echoed this thinking with a focus on critical asset isolation. "You want to make sure your most important assets are completely safe … quarantined, isolated from the rest of the systems," he said.

> "Only about 4% to 6% [of OT vulnerabilities] require urgent patching"
>
> *Robert M. Lee, CEO of Dragos*

04

Renewables: The New Frontline of Critical Risk

The rapid transformation of global energy infrastructure presents an alarming security blind spot that few are addressing. As power generation shifts from centralized plants to distributed renewable networks, cybersecurity measures have failed to evolve at the same pace.

"Only 1% of cybersecurity is involved in renewables," said Rafael Narezzi, managing director at Cyber Energia, warning that legacy tech and fragmented ownership make defense difficult. "In the renewables industry, you might have four different owners ... each one has different responsibilities," he said. "Energy becomes digital. However, protecting what is digital means actually acting to ensure the legacy system is not there." He added that regulators are finally responding: "Directors will be personally liable for not having the cybersecurity ... The time has come."

05

Global Response: Regulation and Policy Momentum

Governments are beginning to address systemic cyber risk through policy. The U.S. National Cybersecurity Strategy (2023) calls for shared responsibility, placing more onus on software providers and mandating robust incident reporting.[22] Europe's NIS2 Directive and Cyber Resilience Act signal a move from voluntary frameworks to enforceable obligations.[23]

Australia's updates to the SOCI Act go even further, enabling government intervention in private-sector operations during major incidents.[24] These shifts acknowledge that the market alone cannot resolve systemic vulnerabilities.

European and Australian efforts reflect a global regulatory awakening. Hans de Vries, chief cybersecurity and operations officer at ENISA, assessed Europe's readiness:

> **If we get a C+, that would be okay for Europe. I mean, we need to get to the A level.**
>
> *Hans de Vries, chief cybersecurity and operations officer at ENISA, assessed Europe's readiness*

"If we get a C+, that would be okay for Europe. I mean, we need to get to the A level," he said. The region's cyber blueprint aims to fast-track coordinated responses.

"You have to act fast," de Vries said. He also stressed planning for offline continuity. "When there is no power … you have to have the blanket and water to really save yourselves for a few days."

06

Defining Systemic Risk: Still Murky Waters

Even as these threats mount, the industry lacks a clear consensus on what constitutes a systemic cyber event. Is it about the scale of disruption, cross-sectoral impact or the triggering mechanism?

“We’re trying to define a moving target,” said Stacy Bostjanick, deputy CIO for cybersecurity at U.S. Department of Defense. “But the important part is recognizing the interdependencies. No entity exists in a vacuum anymore.”

Conclusion

The convergence of digital systems with physical infrastructure has transformed energy security into a complex battlefield where cyberthreats can have real-world consequences. This new landscape demands a fundamental rethinking of protection strategies at the intersection of national security, technological vulnerability and public safety. As Robert M. Lee concluded, "Securing OT demands visibility, specialized expertise, and a shift from reactive defense to systemic resilience."

The path forward requires not merely better defenses, but deliberately engineered resilience: systems designed to withstand attacks, contain breaches when they occur, and maintain essential operations even under duress. The energy sector must evolve from incident response to strategic preparedness - building capacity not just to react to threats, but to sustain critical functions through them.

Footnotes

20. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Colonial Pipeline ransomware attack impact. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

21. Cybersecurity and Infrastructure Security Agency (CISA). (2022). Log4j vulnerability systemic risk. https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance

22. The White House. (2023). U.S. National Cybersecurity Strategy 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

23. International Association of Privacy Professionals (IAPP). (n.d.). European Union's NIS2 Directive and Cyber Resilience Act. https://iapp.org/news/a/navigating-the-new-eu-cybersecurity-standards-the-nis2-directive-and-cyber-resilience-act/

24. Herbert Smith Freehills. (2023, March). Australia's SOCI Act updates. https://www.herbertsmithfreehills.com/insights/2023-03/demystifying-australias-recent-security-of-critical-infrastructure-act-reforms

CHAPTER 7

Human-Centric Cyber Operations: Why Behavior, Resilience and Mental Health Matter More Than Ever

In an age dominated by gen AI, zero-day exploits and relentless ransomware attacks, cybersecurity conversations often orbit around tools, frameworks and technological firepower. Yet, beneath the surface of all the software and systems lies an undeniable truth: cybersecurity is, at its core, a human endeavor.

Over the last two years, industry voices have grown louder on this point, arguing that emotional resilience, behavior patterns and mental well-being are now essential dimensions of security posture. The evidence is no longer anecdotal - burnout, workforce fatigue and culture-driven failure points are creating measurable risk.

01

Defining Systemic Risk: Still Murky Waters

For years, cybersecurity awareness campaigns positioned humans as the "weakest link." Mistakes such as clicking phishing links or using poor passwords were treated as user failings. But today's most progressive security leaders reject this view. Instead, they frame people as the first line of defense - assets to be empowered, not blamed.

Global institutions are following suit. In 2024, ENISA launched initiatives advocating behavioral-first security design and empathy-led leadership training for executives.25 Similarly, former CISA Director Jen Easterly's campaign emphasized designing security "for humans, not in spite of them."[26]

Security culture, then, becomes a leadership responsibility. "Culture doesn't just happen. It's a structure designed not just for skill-building but for confidence and psychological safety," said Bruce Johnson, senior director of enterprise security at TekStream. "We have recruiters that work with them on a monthly basis to see how they're doing, what their proclivities are and give them career guidance."

> **Culture doesn't just happen. It's a structure designed not just for skill-building but for confidence and psychological safety**
>
> *Bruce Johnson, senior director of enterprise security at TekStream*

02

Inside the Cybersecurity Burnout Crisis

While end-user behavior remains critical, another human concern is creating deeper systemic risk: burnout among cybersecurity professionals.

The numbers are staggering. A 2024 global survey found that 50% of security professionals expected to experience burnout in the coming year.[27] In Asia-Pacific, that figure soared to 85%. A CISO-focused report revealed that 60% of cyber leaders ranked stress as their top personal risk - surpassing even the breach of their own systems.[28]

Fatigue in cybersecurity isn't just a workplace issue - it's a vulnerability. Constant incident response, staff shortages and alert overload lead to errors, missed threats and mental shutdown. According to Centripetal Networks, more than 90% of professionals check messages during vacation and over 30% are interrupted every night.[29]

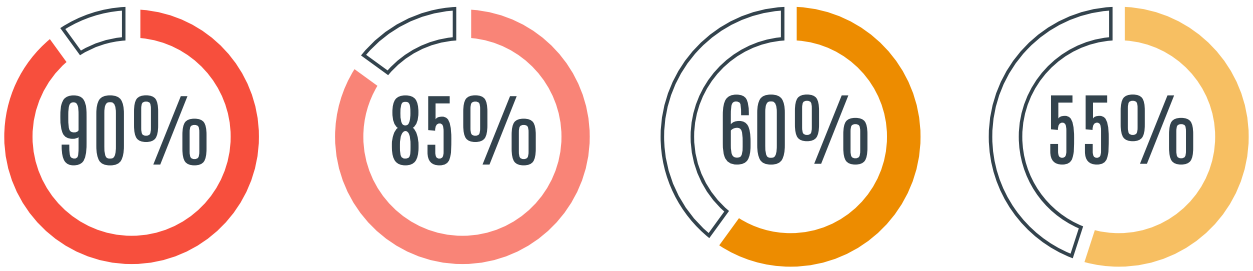
> **They don't have to spend as much time doing that manual cleanup, that manual work of going to hunt for the data.**
>
> *Robin Das, executive director of market growth strategy at DataBee*

We're dealing with a field that has existential implications - where the cost of failure is massive. That kind of weight can break people if we're not proactive about supporting them.

"We've kind of alleviated the burden on those audit teams," said Robin Das, executive director of market growth strategy at DataBee, describing how continuous controls monitoring helps replace reactive, high-stress cycles with proactive insight. "They don't have to spend as much time doing that manual cleanup, that manual work of going to hunt for the data."

The Cybersecurity Burnout Crisis

Burnout Risk Indicators



- **Check Messages on Vacation** 90 (innermost red circle)
- **APAC Professionals Expecting Burnout** 85% (pink/salmon circle)
- **Cyber Leaders with Stress as Top Risk** 60% (yellow circle)
- **Global Professionals Expecting Burnout** purple outermost circle, 50%

03

Reinventing Security Culture Through Support and Systems

The response from leading organizations reflects a growing recognition that psychological safety is a foundation for performance - not a perk. The goal: reduce cognitive load, build emotional stamina, and re-engineer operations to protect both networks and the people who defend them.

1. **Automating the right pain points:** AI and SOAR technologies are being deployed not just for efficiency but for human relief. “We’re focused on reducing manual pain,” Das said. “The less time people spend on toil, the more space they have to think creatively and recover psychologically.”
2. **Institutionalizing recovery:** Work-life policies are becoming codified into operations: shift rotations, mandatory rest after incidents and protected downtime. ISACA’s 2024 report emphasized this trend, noting rising adoption of “no-alert-after-hours” protocols.[30]
3. **Building mental health into security operations:** Companies are rolling out therapy stipends, in-house wellness coaches and stress management training. “It’s not just about burnout prevention - it’s about building the muscle of resilience,” Johnson said. Organizations such as Mental Health Hackers and ISSA now offer field-specific programs aimed at tech mental health.

4. **Training leadership for psychological literacy:** The tone from the top matters. Security leaders are being trained to recognize stress signals and intervene early. Karen Worstell, former Microsoft CISO, reflected on her own sabbatical from burnout and now champions psychological safety in leadership circles.[31]

Conclusion

The future of cybersecurity is not just code and threat intel. It's also emotional regulation, trust-driven collaboration and adaptive capacity in the face of crisis.

Organizations that prioritize human resilience will outperform those that ignore it - not because it's nice, but because it's necessary. Reduced turnover, faster incident response and better decision-making under pressure downstream benefits of a supported team.

It's time to retire the "weakest link" narrative. People are not the flaw in the system - they are the firewall. When trained, trusted and protected, they're the most adaptive and intelligent defense a company has.

As Easterly wrote in her open letter: "You are not alone … We all need help sometimes."[25]

Footnotes

25. ENISA. (2024). Cybersecurity culture for C-level executives. https://www.enisa.europa.eu/publications/security-awareness-for-c-level-management

26. Easterly, J. (2023). You are not alone. CISA.gov. https://www.cisa.gov/news-events/news/you-are-not-alone

27. Security Management Magazine. (2024). Cybersecurity burnout report. https://www.asisonline.org/security-management-magazine

28. Sophos. (2024). Cybersecurity burnout in Asia-Pacific: APJ survey. https://www.sophos.com/en-us/content/burnout-report-apj

29. Centripetal Networks. (2023). Work-life balance survey. https://www.centripetal.ai/newsroom/work-life-cybersecurity

30. ISACA. (2024). State of cybersecurity report. https://www.isaca.org/resources/state-of-cybersecurity

31. Worstell, K. (2024). Reflections on burnout. https://www.linkedin.com/in/karenworstell

CHAPTER 8

The Rise of Cybercrime Innovation: Adversaries, Tactics and Dark Market Dynamics

Over the past two years, cybercrime has matured into a fast-moving, industrialized ecosystem, shaped by professionalized actors and turbocharged by gen AI. Today's threat actors resemble lean startups - operating with clear ROI models, leveraging automation and sharing tools in robust criminal supply chains.

Adam Meyers, senior vice president of counter adversary operations at CrowdStrike said, "Adversaries don't want to work harder. They want to work less and easier and faster." This ethos is reshaping every layer of the cybercriminal stack, from initial compromise to financial laundering.

01

Ransomware Reinvented: Multi-Extortion and Market Maturation

While ransomware remains a core tactic, the economic dynamics have changed. Threat actors are increasingly shifting away from encryption-only strategies to pure data exfiltration and extortion. “In the first quarter, as high as 50% of the ransomware attacks that we at Recorded Future saw were data theft only, no encryption,” said Allan Liska, senior security architect at Recorded Future.

In some cases, affiliates have doubled back to previously extorted victims to demand second payments - a bizarre new turn in the criminal monetization cycle. Despite broad victim impact in campaigns such as MOVEit, “we just don’t see that many payments,” Liska said, signaling a potential inflection point. “Honestly, we’re going to start to see a fall in ransomware … because I think it’s going to become less profitable.”

Groups such as LockBit and BlackCat exemplify how ransomware-as-a-service models have industrialized this threat, making sophisticated ransomware accessible to low-skill affiliates for a share of the ransom haul.[32]

In 2023 alone, ransomware attacks caused estimated global losses exceeding $20 billion.[33]

> “In the first quarter, as high as 50% of the ransomware attacks that we at Recorded Future saw were data theft only, no encryption.”
>
> *Allan Liska, senior security architect at Recorded Future*

02

AI-Driven Attacks: Deepfakes, Voice Cloning and Adaptive Malware

Threat actors are now wielding AI not only for efficiency but to enhance deception at scale. "We saw a 442% increase in voice-based phishing attacks," Meyers said, describing how actors manipulate help desk agents using impersonation and urgency. One common tactic includes launching "spam bombs" to overwhelm inboxes, followed by a fake IT call. "The user is annoyed … and so then the threat actor says, 'Oh, well, I could help you with that. Just click on this link and we'll get that sorted out,'" he said.

> "We saw a 442% increase in voice-based phishing attacks.
>
> *Adam Meyers, senior vice president of counter adversary operations at CrowdStrike*

Deepfake fraud is emerging as another frontier. "We're seeing threat actors send somebody in for an interview and send somebody else in to take the job," said Danny Milrad, director of product marketing - Unit 42 at Palo Alto Networks. This fusion of AI-generated personas and real-world credentials is creating unprecedented identity manipulation risks, particularly during onboarding processes.

A notable case in 2023 involved a deepfake video call used to convince a finance employee to transfer $25 million.[34] Meanwhile, AI-powered malware is becoming more evasive, adjusting behavior in real time to avoid endpoint detection systems.[35]

03

Dark Market Dynamics: Cybercrime-as-a-Service and Shifting Platforms

The underground economy has matured into a distributed, commoditized landscape, with services available à la carte. "It's a commodity. It is a low investment and also a low barrier of entry," said Derek Manky, chief security strategist and global vice president of threat intelligence at Fortinet. Vendors on the darkweb operate like agile micro-businesses, adapting offerings to demand signals.

Moreover, attackers are coordinating across multiple attack surfaces. "We saw in 70% of our cases, the attacks happened on three or more attack surfaces," Milrad said. Despite visibility in the logs, defenders often miss these signals due to alert fatigue and siloed systems. "In 75% of the cases, the data was in the logs that indicated that there was an attack," he said.

> "We saw in 70% of our cases, the attacks happened on three or more attack surfaces. In 75% of the cases, the data was in the logs that indicated that there was an attack."
>
> *Danny Milrad, director of product marketing - Unit 42 at Palo Alto Networks*

04

Supply Chain Attacks: The Domino Effect of Trust

Supply chain compromise remains a highly efficient strategy. “We’ve seen a 250% increase in the speed of attacks over the past three or four years,” Milrad said. The MOVEit-style exploits demonstrate how threat actors can pivot from a single vulnerability to mass compromise in under an hour. “About four years ago … exfiltrated data was about five or six days … [now] 20% of our cases … from compromise to exfiltration were within less than an hour,” he said.

From SolarWinds to MOVEit, supply chain attacks have become a favored strategy for attackers seeking exponential access. By compromising a single trusted vendor, adversaries can infiltrate hundreds or thousands of downstream clients.

The 2023 Clop ransomware campaign, which exploited a vulnerability in MOVEit file transfer software, impacted over 2,500 organizations globally - including government agencies and healthcare providers.[36]

> “We’ve seen a 250% increase in the speed of attacks over the past three or four years. About four years ago … exfiltrated data was about five or six days … [now] 20% of our cases … from compromise to exfiltration were within less than an hour.”
>
> *Danny Milrad, director of product marketing - Unit 42 at Palo Alto Networks*

05

Cryptocurrency and Financial Obfuscation

Cryptocurrency remains the lifeblood of cybercriminal financial operations. While Bitcoin is still common, privacy coins such as Monero and tools such as coin mixers are favored for their enhanced anonymity.

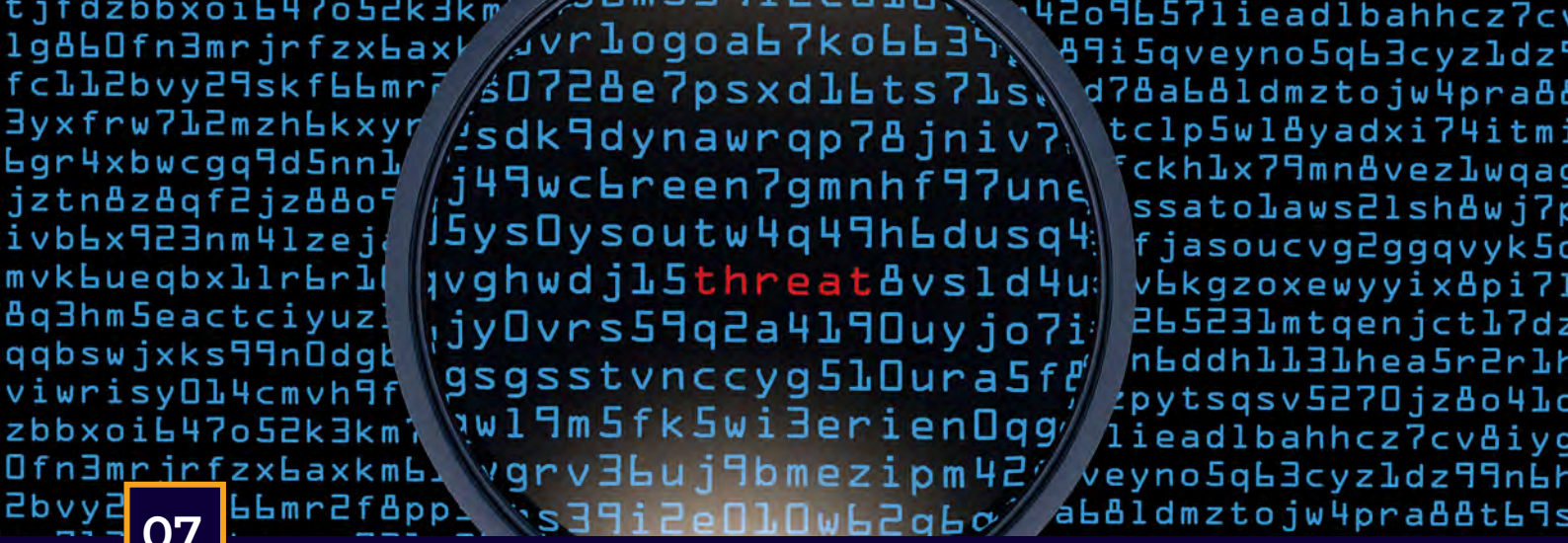
Though less emphasized directly, Milrad pointed to increasing use of anonymized infrastructure and cloud for rapid exfiltration - tactics consistent with the laundering of stolen data through cryptocurrency mixers and decentralized platforms. “They’re using the cloud to accelerate the exfiltration of their data,” he said, reinforcing the connection between infrastructure decentralization and financial laundering resilience.

06

Industry Impact: Every Sector Is a Target

No industry is immune from these threats. “In 86% of the cases that we worked at, there was business disruption,” Milrad said.

- **Financial services** remain a top target for credential theft and fraud.
- **Healthcare** faces catastrophic risk from ransomware - breaches now cost an average of $10.93 million per incident.[37]
- **Critical infrastructure** is increasingly targeted by geopolitically motivated actors.
- **Retail and e-commerce** endure constant pressure from account takeovers and bots.



07

What's Ahead: Emerging Threats on the Horizon

Looking forward, several trends signal even greater threats:

- **Autonomous AI agents:** Crafting exploits, social engineering scripts or even negotiating ransoms.
- **Post-quantum harvesting:** Stealing encrypted data today for decryption tomorrow.
- **Decentralized dark markets:** Migrating to blockchain-based platforms that resist takedowns.
- **AI-powered insider threats:** Hiring imposters or deploying bots into workforce pipelines.

Conclusion

From lone operators to AI-augmented criminal syndicates, the ecosystem is now vast, fast and increasingly decentralized. As Liska noted, “Why wait to get the ransom when you can just steal the cryptocurrency or something like that?” Future defense will require not only better tools but integrated thinking - across disciplines, borders and business units. The call to action is clear: move faster, see further and stay agile.

Footnotes

32. Chainalysis. (2024). Crypto crime report 2024. https://www.chainalysis.com/blog/crypto-crime-2024/

33. Cybersecurity Ventures. (2024). Official annual cybercrime report 2024. https://cybersecurityventures.com/annual-cybercrime-report-2024/

34. Franck, T. (2023, April 15). Scammers used AI to mimic voice in $25M heist. CNBC. https://www.cnbc.com/2023/04/15/scammers-used-ai-to-mimic-voice-in-25m-heist.html

35. McAfee Labs. (2024, January). Threats report: Q4 2023. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-january-2024.pdf

36. Cimpanu, C. (2023, July). Clop ransomware claims MOVEit attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-moveit-attacks/

37. IBM Security. (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach

CONCLUSION

The 2025 Cybersecurity Pulse Report captures a pivotal moment in the evolution of cybersecurity. Across eight deeply interwoven themes—from the disruption wrought by AI to the reconfiguration of identity and infrastructure, and the systemic vulnerabilities confronting critical sectors—the industry's top minds have illuminated the threats at hand as well as the strategic paths forward.

A central throughline of this year's insights is the transformation of cybersecurity from a purely technical challenge into a multidimensional business, societal, and even psychological imperative. AI emerged as both the industry's most formidable disruptor and its most promising defense mechanism. From enabling real-time threat detection and automating security operations to simultaneously fueling polymorphic malware and deepfake-driven attacks, AI has redefined the speed, scale, and complexity of the industry.

The collapse of traditional security perimeters, driven by cloud proliferation and identity-based access models, has forced organizations to rethink foundational assumptions. Trust and identity are no longer static constructs but dynamic, context-sensitive layers of control that must adapt to a new generation of risks posed by synthetic personas, machine-speed impersonations, and ubiquitous access points.

Yet, amid this technical upheaval, the human factor remains paramount. Burnout, behavioral fatigue, and the emotional toll of frontline defense have prompted leading organizations to invest in psychological resilience and mental health as integral components of operational security. Simultaneously, the rapid industrialization of cybercrime and the growing integration of criminal ecosystems demand equally agile, unified, and intelligence-led responses.

What is most evident from the breadth of interviews and expert perspectives in this report is that cybersecurity in 2025 is no longer about building higher walls—it is about building smarter, more adaptive, and interconnected systems. The convergence of AI, cloud, identity, and critical infrastructure resilience, paired with a renewed focus on human-centered design, signals a new era where cybersecurity is indistinguishable from enterprise strategy.

In this environment, success will belong to organizations that can balance innovation with integrity, agility with governance, and automation with empathy. This report serves not only as a record of where we are but as a strategic compass for where we need to go next.

CONTRIBUTORS

List of Experts Who Contributed to This Report

- **Adam MaGill -** Senior Vice President, Global Security (CISO), Concentrix
- **Alex Doll -** Founder and Managing General Partner, Ten Eleven Ventures
- **Alex Weinert -** Chief Product Officer, Semperis
- **Allan Liska -** Senior Security Architect and Ransomware Specialist, Recorded Future
- **Aly Shivji -** Global Vice President, Global Partner Sales, Splunk
- **Ami Luttwak -** Co-Founder and CTO, Wiz
- **Andrew Rubin -** Founder and CEO, Illumio
- **Andy Ellis -** Partner, YL Ventures
- **Anna Delaney -** Director, Productions, ISMG
- **Anne Neuberger -** Former Deputy National Security Advisor for Cyber and Emerging Tech, White House
- **Anupam Upadhyaya -** Vice President of Product Management, Palo Alto Networks
- **Arik Kleinstein -** Co-Founder and Managing Partner, Glilot Capital Partners
- **Arnab Bose -** Chief Product Officer, Workforce Identity Cloud, Okta
- **Arvind Nithrakashyap -** Co-Founder and CTO, Rubrik
- **Ash Kulkarni -** CEO, Elastic
- **Avivah Litan -** Distinguished Vice President Analyst, Gartner
- **Bob Ackerman -** Founder and Managing Director, AllegisCyber Capital
- **Bradon Rogers -** Chief Customer Officer, Island
- **Brett Leatherman -** Deputy Assistant Director, Cyber Operations, FBI
- **Bruce Johnson -** Senior Director, Enterprise Security, TekStream
- **Christiaan Beek -** Senior Director, Threat Analytics, Rapid7
- **Colin Soutar -** Managing Director, Deloitte
- **Collin Gallagher -** Senior Vice President, Thoma Bravo
- **Craig Jones -** Immediate Past Director Cybercrime, Interpol
- **Dale "Dr. Z" Zabriskie -** Field CISO, Cohesity

- **Dan Streetman -** CEO, Tanium
- **Daniel Kennedy -** Principal Research Analyst, Information Security Channel, S&P Global Market Intelligence
- **Danny Milrad -** Head, Product Marketing, Unit 42, Palo Alto Networks
- **Dave DeWalt -** Founder, Managing Director and CEO, NightDragon
- **Dave Merkel -** Co-Founder and CEO, Expel
- **Dean Fantham -** Founder, Managing Partner and CTO, Edgile
- **Dean Sysman -** Co-Founder and CEO, Axonius
- **Derek Manky -** Chief Security Strategist and Global Vice President, Threat Intelligence, Fortinet
- **Dimitri Sirota -** Co-Founder and CEO, BigID
- **DJ Sampath -** Senior Vice President, AI Software and Platform, Cisco
- **Dmitri Alperovitch -** Co-Founder and Chairman, Silverado Policy Accelerator
- **Eric Trexler -** Senior Vice President, U.S. Public Sector, Palo Alto Networks
- **Fergus Hay -** CEO and Co-Founder, The Hacking Games
- **Hans de Vries -** Chief Cybersecurity and Operations Officer, ENISA
- **Hany Farid -** Co-Founder and Chief Science Officer, GetReal
- **Harry Coker -** Secretary, Maryland Department of Commerce
- **Ian Tien -** CEO and Co-Founder, Mattermost
- **James Dempsey -** Managing Director, Cybersecurity Law Center, IAPP
- **Jamie Fitz-Gerald -** Vice President, Product Management - Access Management, Devices, Security and Risk, Okta
- **Jason Clinton -** CISO, Anthropic
- **Jay Chaudhry -** Founder, Chairman and CEO, Zscaler
- **Jeetu Patel -** Executive Vice President and Chief Product Officer, Cisco
- **Jeff Shiner -** Co-CEO, 1Password
- **Jim O'Boyle -** Vice Chairman, Sales, Varonis
- **John Fokker -** Head of Threat Intelligence, Principal Engineer, Trellix
- **John Pirc -** Head of Product Management and Threat Intelligence, NetWitness
- **Joshua Motta -** Co-Founder and CEO, Coalition
- **Julie Bernard -** Principal, Cyber and Strategic Risk, Deloitte & Touche LLP
- **Kabir Barday -** Founder, Chairman and CEO, OneTrust

- **Kayle Giroud -** Director, Common Good Initiatives, Global Cyber Alliance
- **Kelley Misata -** Founder and CEO, Sightline Security
- **Kelly Ahuja -** CEO, Versa Networks
- **Kevin Simzer -** COO, Trend Micro
- **Lingping Gao -** CEO and Chairman, NetBrain
- **Liran Grinberg -** Co-Founder and Managing Partner, Team8
- **Lisa Plaggemier -** Executive Director, National Cybersecurity Alliance
- **Mandy Andress -** CISO, Elastic
- **Manoj Srivastava -** Chief Technology and Product Officer, Blackpoint Cyber
- **Mark McClain -** Founder and CEO, SailPoint
- **Martin Zugec -** Technical Solutions Director, Bitdefender
- **Marty Momdjian -** Executive Vice President and General Manager - Ready1, Semperis
- **Matt Kunkel -** CEO and Co-Founder, LogicGate
- **Matt Muller -** Field CISO, Tines
- **Matt Turek -** Deputy Director, Information Innovation Office, DARPA
- **Matthew J. Schwartz -** Executive Editor, DataBreachToday and Europe, ISMG
- **Michael Novinson -** Managing Editor, Business, ISMG
- **Mickey Bresman -** CEO, Semperis
- **Mike Nichols -** Vice President, Product Management, Elastic
- **Mike Towers -** Chief Security and Trust Officer, Veza
- **Mo Aboul-Magd -** Vice President of Product, Cybersecurity, SandboxAQ
- **Nadir Izrael -** CTO and Co-Founder, Armis
- **Narayan Sundar -** Director, AI GTM, Palo Alto Networks
- **Ofer Ben-Noon -** CTO, SASE, Palo Alto Networks
- **Paul Zimmerman -** Director of Technology, Blaine County School District
- **Peter McKay -** CEO, Snyk
- **Phillip Wylie -** xIoT Security Evangelist, Phosphorus Cybersecurity
- **Pieter Danhieux -** Co-Founder and CEO, Secure Code Warrior
- **PJ Hamlen -** WW Leader, Global Partner Security Initiative, AWS
- **Rafael Narezzi -** Managing Director, Cyber Energia

- **Rahul Neel Mani -** Vice President, Community Engagement and Editorial, ISMG
- **Ray Heffer -** Field CISO, Veeam
- **Richard Bird -** Chief Security Officer, Singulr AI
- **Rick Grinnell -** Founder and Managing Partner, Glasswing Ventures
- **Robin Das -** Executive Director, Market Growth Strategist, DataBee
- **Ronald Raether -** Partner, Troutman Pepper Locke
- **Sam Curry -** Global Vice President, CISO in Residence, Zscaler
- **Sam Rubin -** Senior Vice President, Unit 42 Consulting and Threat Intelligence, Palo Alto Networks
- **Sandra Joyce -** Vice President, Threat Intelligence Group, Google Cloud
- **Sanjay Virmani -** Special Agent in Charge, FBI, San Francisco
- **Sean Atkinson -** CISO, Center for Internet Security
- **Sebastien Cano -** Senior Vice President, Cyber Security Products, Thales
- **Seemant Sehgal -** Founder and CEO, BreachLock
- **Sheetal Venkatesh -** Vice President, Product Management, Cohesity
- **Sidra Ahmed Lefort -** Director, Munich Re Ventures
- **Stacy Bostjanick -** Deputy CIO, Cybersecurity, U.S. Department of Defense
- **Stefano Zanero -** Professor, Politecnico di Milano
- **Suja Viswesan -** Vice President, Security and Runtime Products, IBM
- **Sumedh Thakar -** President and CEO, Qualys
- **Sumit Dhawan -** CEO, Proofpoint
- **Tamar Bar-Ilan -** Co-Founder and CTO, Cyera
- **Tim Brown -** CISO, SolarWinds
- **Todd Nightingale -** CEO, Fastly
- **Todd Weber -** Vice President, Professional Services, Semperis
- **Tom Field -** Senior Vice President, Editorial, ISMG
- **Travis Rosiek -** Public Sector CTO, Rubrik
- **Umesh Padval -** Managing Director, Thomvest Ventures
- **Yotam Segev -** Co-Founder and CEO, Cyera

About ISMG

IInformation Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of its 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800)944-0401 · sales@ismg.io

ISMG

BANK INFO SECURITY · CAREERS INFO SECURITY · GOV INFO SECURITY · HEALTHCARE INFO SECURITY

CU Just for Credit Unions INFO SECURITY · Data Breach Prevention. Response. Notification. TODAY · infoRisk TODAY · AIToday.io · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QG MEDIA