CYBER HORIZON 2025

Flagship Report

September 2025

GLOBAL CYBERSECURITY FORUM | Site

Foreword

Dr. Hesham Altaleb
Chairman, Future of Cybersecurity
Knowledge Community
Saudi Information Technology
Company (SITE)

As technological innovation accelerates, cybersecurity is no longer just a technical concern. It has become a defining challenge for economies, societies, and governance systems worldwide. The rise of agentic AI, synthetic identities, and concentrated digital power are reshaping the frontiers of trust, resilience, and autonomy. These shifts demand more than incremental defense; they call for foresight, coordination, and leadership on a new scale.

This flagship report, Cyber Horizon 2025, reflects the collective effort of the Future of Cybersecurity Knowledge Community. Grounded in a global survey of 870 cybersecurity leaders and enriched by structured expert dialogues, roundtables, and comparative research on national and organizational practices, it offers a unique, evidence-based view of the forces redefining digital risk.

From this work, five key trends have been identified as the most urgent and systemic challenges. These are threats that span political, economic, and societal domains and that will shape the digital ecosystem for years to come. Beyond describing risks, the report highlights where leading nations and organizations are already responding. It also sets out practical recommendations to strengthen resilience and safeguard trust.

I would like to extend my gratitude to the many contributors whose insights and dedication made this report possible. Together, we provide decision-makers with a forward-looking framework that equips them to anticipate disruption, prioritize investment, and act decisively in securing a more resilient digital future.

Knowledge Community: The Future of Cybersecurity

The Future of Cybersecurity Knowledge Community is committed to exploring the potential opportunities and threats presented by an ever-evolving Cyberspace. By bringing together a diverse array of expertise from various stakeholder groups, it seeks to develop mechanisms that maximize the benefits and address the risks of this new and challenging dimension.

The community welcomes leading technology companies, global cybersecurity organizations, cybersecurity research centers, reputable think tanks, academic institutions, and other stakeholders with a vested interest in exploring and acting upon the future of cybersecurity.

Leading Authors

- **Dr. Manar Alohaly,** Saudi Information Technology Company (SITE)
- **Heelah Alraqiba,** Saudi Information Technology Company (SITE)
- **Shoaib Yousuf,** Boston Consulting Group (BCG)
- **Alberto Pardo,** Boston Consulting Group (BCG)
- **Duna Alghamdi,** Boston Consulting Group (BCG)
- **Chaimae Haska,** Boston Consulting Group (BCG)

Contributors

- **Dr. Bushra Alahmadi,** Saudi Information Technology Company (SITE)
- **Dr. Nasser Aldaghri,** Saudi Information Technology Company (SITE)
- **Hessah Almajhad,** Saudi Information Technology Company (SITE)
- **Dr. Stefan Deutscher,** Boston Consulting Group (BCG)
- **Hugh Eaton,** Boston Consulting Group (BCG)
- **Radu Balanescu,** Boston Consulting Group (BCG)
- **Dr. Amira Khattab,** Deloitte
- **Dr. Mohammed Alenezi,** National Company of Telecommunications and Information Security (NTIS)
- **Sulaiman Almohsen,** National Company of Telecommunications and Information Security (NTIS)
- **Ed Sleiman,** Microsoft
- **Thamer AlDhafiri,** Cipher
- **Abdulmalik Banaser,** Cipher
- **Naif Al Shaban,** Cipher
- **Jorge Martinez,** Axon
- **Abdulrahman AlManea,** Sirar
- **Bilal Baig,** Trend Micro
- **Mohammed Alomar,** CNTXT
- **Fahad Almobark,** CNTXT
- **Riku Valpas,** Fortinet
- **Neil Ginns,** International Business Machines Corporation (IBM)
- **Abdulrahman Aloasimi,** International Business Machines Corporation (IBM)
- **Haitham Al-Jowhari,** PwC

Contents

Useful Acronyms

Acronym	Definition
AI	Artificial Intelligence
API	Application Programming Interface
BEC	Business Email Compromise
CISO	Chief Information Security Officer
CT	Communications Technology
GBP	British Pound
GPT	Generative Pre-Trained Transformer
ICT	Information and Communications Technologies
ID	Identity
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
OT	Operational Technology
R&D	Research and Development
US	United States
USD	United States Dollar

Executive Summary

Cybersecurity is undergoing a profound transformation. The acceleration of artificial intelligence (AI), the proliferation of synthetic identities, and pressures on public trust are pushing organizations into uncharted territory. In this new era, threats extend far beyond technical codes; they are structural, systemic, and deeply impactful across political, economic, and societal domains.

The Future of Cybersecurity Knowledge Community, a Global Cybersecurity Forum (GCF) platform, brings together leaders from across the public and private sectors to co-develop practical, evidence-based guidance on these emerging challenges.

Cyber Horizon 2025, produced in collaboration with leading cybersecurity companies and community members, was designed with a clear purpose: to scan the horizon for future trends with the greatest transformative potential in Cyberspace, and to translate those signals into actionable insights for decision-makers.

Our analysis identifies five transformative trends with the greatest potential to reshape the future cybersecurity landscape:

- **Erosion of public trust through AI-powered disinformation**
- **Rising concentration of technological power**
- **Proliferation of synthetic identities**
- **Growth of autonomous AI-powered attacks**
- **Emergence of shutdown risks from interconnected autonomous systems**

These trends are not isolated disruptions; they are interconnected shifts. Drawing on insights from 870 cybersecurity professionals, the report examines each trend in a dedicated section, combining survey findings and expert commentary to identify key national and organizational recommendations to guide both immediate and long-term action for decision makers.

As these challenges accelerate, they demand more than reactive defense. They call for anticipation, cross sector co-ordination, and a new model of cyber leadership that treats trust, identity, and autonomy as core battlegrounds of the digital age, equipping organizations to act decisively in securing a resilient digital future.

Introduction

The cybersecurity landscape has evolved dramatically over the last decade, with 2025 marking a profound inflection point. Technologies once considered experimental are now embedded in our infrastructure, economies, and daily lives.

From generative AI to post-quantum cryptography, the rules that govern cyber risk, resilience, and trust are being rewritten in real time.

Cybersecurity is no longer a siloed technical concern. It has become a foundational pillar of cybersociety, with the potential for attacks to disrupt not only systems but also economies, social cohesion, and human safety. The scale, speed, and complexity of these changes demand a new kind of strategic awareness.

Cyber Horizon 2025 is an initiative of the GCF Future of Cybersecurity Knowledge Community, designed to equip decision makers to navigate what comes next. The report presents a Trend Impact Radar that maps 20 transformative trends which will reshape the future of cybersecurity across domains from artificial intelligence (AI) to global governance. It executes a deep dive into five key trends with the greatest potential to reshape the cybersecurity landscape. The analysis builds on a structured methodology enriched by expert consultations and global surveys, ensuring its findings are grounded in diverse perspectives and practical insights. Together, these offer a forward-looking perspective on the challenges and opportunities shaping the future of Cyberspace.

Cyber Horizon and The Trend Impact Radar

The Trend Impact Radar builds on our effort to systematically scan the transformative shifts that will reshape Cyberspace in the years ahead. The goal was not simply to catalog isolated risks, but to identify the structural forces – economic, societal, and political – that are redefining how digital security and resilience will evolve.

The Trend Impact Radar offers a strategic lens into 20 emerging trends (detailed in Appendix A) that will reshape the global cybersecurity landscape. It serves not only as a horizon-scanning tool, but also as a planning map designed to help policy makers and organizations anticipate future disruption, prioritize efforts and cybersecurity investments, and align stakeholders across Cyberspace.

Each trend in the radar was assessed through an expert survey based on its anticipated impact, time to maturity, and domain of influence – whether economic, societal or political. Together, these trends reflect the complexity and acceleration of change in cyber risk environments.

The radar is also a decision-support tool that enables stakeholders to continuously re-evaluate how emerging trends affect their specific zones of interest. Regulators may concentrate on issues such as digital identity, AI oversight, or information integrity; chief information security officers (CISOs) may prioritize autonomous defense, supply chain exposure, and the expansion of attack surfaces; while national security leaders may focus on questions of sovereignty, systemic risks, and cross-border co-ordination. The radar also makes it possible to re-evaluate these impacts over time, ensuring that priorities remain aligned as conditions evolve.

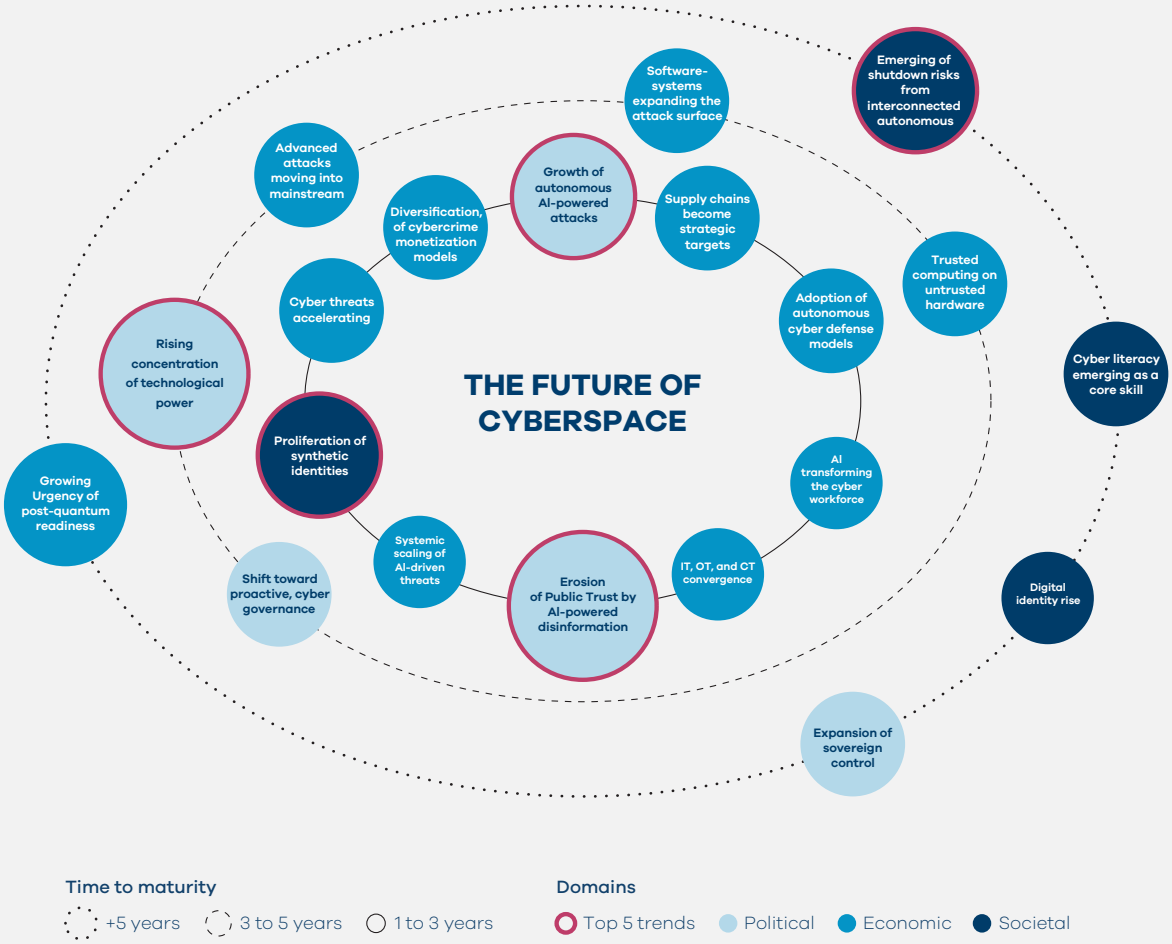


Figure 1: Trend Impact Radar*

* Some trend names have been shortened for visibility.

How to read the Trend Impact Radar

- **Each trend represents a forward-looking shift. It therefore shows not just what is happening now, but what could soon reshape digital risk, resilience, and trust**
- **The positioning of each trend on the radar reflects the expected time to maturity of each trend (one-to-three years, three-to-five years, or five years). Trends located near the center are already taking shape and require immediate strategic attention. Trends on the outer rings may still be emerging, but if realized, they hold the potential to be deeply disruptive, demanding early foresight and monitoring**
- **The size of each trend in the radar represents the expected level of impact that the trend will have in the future of Cyberspace**
- **The color of each trend shows which domain will be impacted the most among political, economic, and societal domains**

Out of the 20 trends identified, more than half (55%) are expected to mature within the next one-to-three years, underscoring the urgency for policy makers, business leaders, and cybersecurity professionals to act before these risks become deeply embedded.

Although all 20 trends influence political, economic and societal domains, their impact is asymmetrical. For instance, 20% of the trends were categorized as predominantly impactful in the political domain. These were ranked among the most disruptive overall, suggesting that governance and regulatory systems will be under significant pressure to adapt to the accelerating evolution of cyber threats.

1. Erosion of Public Trust Through AI-Powered Disinformation

1.1 Nature of the trend

The erosion of trust caused by AI-enabled disinformation represents a highly destabilizing trend in Cyberspace.

Disinformation – content deliberately crafted to deceive – and misinformation – false information spread without malicious intent – are amplified by powerful generative AI tools capable of creating synthetic voices, highly realistic deepfakes, and fabricated digital personas.

These technologies flood the information environment with persuasive falsehoods, making it increasingly difficult for citizens, institutions, and organizations to distinguish fact from fabrication. The result is a structural weakening of information integrity that threatens the foundations of democratic governance, social cohesion and interpersonal trust.

1.2 Drivers and acceleration signals

Enabled disinformation tactics are evolving rapidly. Generative AI has lowered the barrier to producing highly convincing synthetic content, enabling a wide range of actors to flood the information space with false narratives that erode public trust.

Clear signals of this acceleration can be seen in the industrialization of disinformation campaigns. CrowdStrike has documented how the Green Cicada Network deployed thousands of AI-generated social media accounts to amplify manipulated narratives around elections, illustrating how operations that once relied heavily on human effort can now be scaled and automated at unprecedented levels.[1] Since the release of generative pre-trained transformer (GPT)-powered tools, successive years have seen both state-linked and non-state actors expanding their use of synthetic personas and automated content farms.

As of 2025, the sophistication of these tactics has advanced even further. Cybercriminal groups are now routinely leveraging platforms such as FraudGPT and similar tools to generate deepfake audio for extortion, synthetic video impersonations of executives for fraud, and AI-crafted phishing campaigns that achieve success rates more than four times higher than those written by humans.

The weight of these developments is falling on sectors where the credibility of information is central to their functioning, such as central government, media, and education. These domains are particularly vulnerable because false narratives, even when short-lived, can rapidly destabilize public confidence. Survey findings confirm this dynamic: respondents identified government (36%), media (33%), and education (29%) as the top three sectors most exposed to the accelerating spread of AI-driven disinformation.

1.3 Implications and systemic consequences

The impacts of this trend are multidimensional and increasingly costly. Societies are experiencing deepening polarization, declining trust in journalism, and greater vulnerability to misinformation on health and finance. False narratives around vaccines, climate policy, and economic security continue to spread rapidly online, creating measurable consequences for public systems. In the United States, misinformation and disinformation around COVID-19 vaccination decisions have been estimated to cost between 50 million to USD 300 million per day in healthcare expenses, productivity losses, and excess morbidity and mortality.[2] These dynamics illustrate how disinformation directly undermines public health, challenges social cohesion, and weakens overall societal resilience.

Organizations are also carrying rising costs as disinformation schemes become more convincing.[3] For instance, a recent U.K. AI-powered disinformation campaign simulation found that for every GBP 10 spent on AI-driven ads, as much as GBP 1 million in deposits could be shifted, showing just how cost-effective influence operations can be in triggering bank runs. Beyond direct fraud, organizations also contend with reputational erosion, as manipulated narratives and impersonations undermine stakeholder confidence.[4]

Together, these impacts show how disinformation has moved well beyond reputational harm, creating systemic risks with political, societal, and economic dimensions. The scale of investment, the measurable costs to public health systems and the destabilizing effect on financial markets all underscore that the consequences are real, significant, and escalating.

1.4 National-level strategic responses

Governments worldwide are beginning to recognize AI-driven disinformation as a matter of national resilience. The European Union has invested heavily in election monitoring and resilience programs[5], while several countries—including Canada[6], Japan[7], and India[8]—have launched national task forces dedicated to countering synthetic media and deepfake campaigns. These early actions reflect a growing consensus: defending information integrity requires proactive, government -led intervention on par with other critical infrastructure challenges.

Building on these developments, insights from our global survey provide further perspectives on which national-level measures are viewed as most effective by cybersecurity leaders. **Figure 2** presents the full set of national-level actions identified by respondents, with the top three priorities highlighted.

AI is enabling misinformation and disinformation, weakening public trust. Which top three national-level actions do you think should be prioritized to counter the rise of AI-generated misinformation or disinformation?

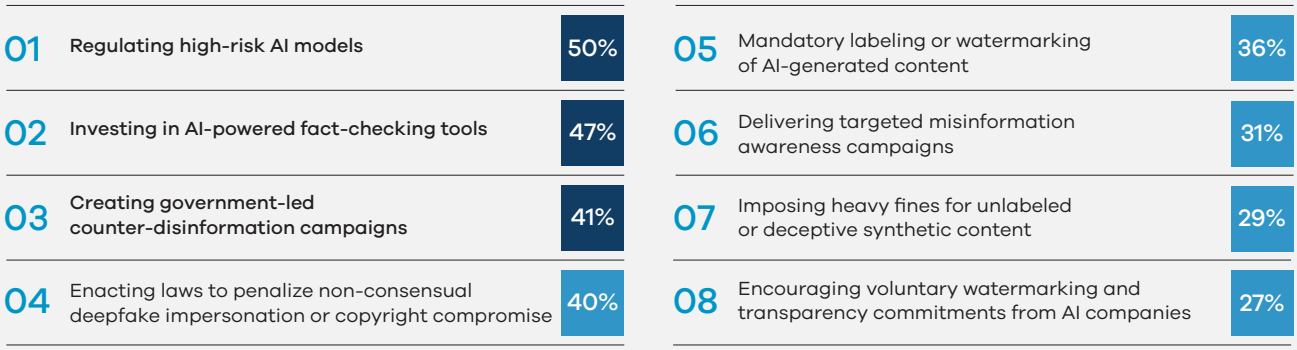


Figure 2: Survey results: National-level actions towards AI-driven misinformation

Survey respondents identified three 'most-effective' national-level measures to counter AI-driven misinformation: 1) regulating high-risk AI models (50%); 2) investing in AI-powered fact-checking tools (47%); and 3) implementing government-led counter-disinformation campaigns (41%). These preferences reflect the view that governments must take a proactive role in shaping policy, investing in technological safeguards, and leading coordinated efforts to strengthen societal resilience against disinformation.

1. The regulation of high-risk AI models emerged as the most widely supported measure. This reflects a recognition that technologies capable of enabling large-scale deception require stronger oversight before they are deployed. Certification processes, independent safety testing, and red-teaming protocols that identify misuse pathways prior to release could provide a structured way to manage risks. In practice, implementation might involve specialized national oversight bodies – similar in scope and authority to regulators in sectors such as pharmaceuticals or food safety – with the capacity to monitor AI developers, enforce penalties in cases of misuse, and ensure compliance with evolving standards designed to safeguard information integrity.

2. Investing in AI-enabled verification and fact-checking capacity emerged as a key priority. Traditional fact-checking processes are too slow to match the speed and scale of synthetic disinformation, and respondents emphasized the importance of embedding automated systems that can provide real-time verification, detect manipulated content, and support the circulation of counter-narratives. Such systems could be integrated into national media infrastructures, supported by independent broadcasters and civil society organizations. This would ensure that verified information reaches the public as quickly as falsehoods. Effective implementation is likely to require sustained research partnerships with universities and technology firms, alongside the adoption of transparency standards and open auditability of the models used to preserve credibility.

3. The deployment of government-led counter-disinformation campaigns were viewed as critical not only for debunking falsehoods, but also for strengthening long-term societal resilience. By promoting digital literacy, encouraging critical consumption of media, and reinforcing the visibility of credible sources, such campaigns can help inoculate populations against manipulation. Successful initiatives could borrow methods from public health campaigns, in which trusted voices and local networks play a key role in reinforcing protective behaviors. Implementation would likely require coordinated strategies across ministries of education and information and technology, supported by partnerships with civil society and local media to extend outreach and impact.

In addition to the top-ranked actions, several other national-level measures identified from leading nations' benchmarks were explored but ultimately given lower prioritization. These included enacting laws to penalize non-consensual deepfake impersonation or copyright compromise (40%), mandatory labeling or watermarking of AI-generated content (36%), delivering targeted misinformation awareness campaigns (31%), imposing heavy fines for unlabeled or deceptive synthetic content (29%), and encouraging voluntary watermarking and transparency commitments from AI companies (27%).

Going forward, governments must treat AI-driven disinformation as a systemic resilience challenge, rather than a narrow communications issue. Policy makers need to act quickly, assessing the full range of tools within their mandate to confront the threat.

This will require a balanced mix of regulation, technological safeguards, and public awareness initiatives. Legal frameworks can establish accountability, but they must be complemented by investment in verification technologies and education efforts that strengthen societal resilience. Only by combining regulatory action with innovation and outreach can governments restore public trust and stay ahead of rapidly evolving AI-powered disinformation.

1.5 Organizational-level strategic responses

Increasingly, these efforts are integrated into security operations centers and crisis-management playbooks, reflecting a shift from treating synthetic media as a reputational nuisance to addressing it as a core operational risk.

Building on these developments, insights from our global survey provide further perspective on which organizational-level measures are viewed as most effective by cybersecurity leaders. **Figure 3**, below, presents the full set of organizational-level actions identified by respondents, with the top three priorities highlighted.

AI is enabling misinformation and disinformation, weakening public trust. Which top three actions do you think organizations should prioritize to reduce exposure to misinformation or disinformation?

01	Investing in AI content authentication tools	42%
02	Upskilling cyber workforce	42%
03	Monitoring for misinformation and disinformation	42%
04	Collaborating and partnering with trusted information platforms	41%
05	Reviewing and updating internal policies	37%
06	Ensuring compliance with emerging laws and regulations	35%
07	Providing employee training to improve media literacy	32%
08	Developing and rehearsing strategic response plans	29%

Figure 3: Survey results: Organizational-level actions towards AI-driven misinformation

At the organizational level, survey respondents prioritized three key measures: 1) investing in AI content authentication tools (42%); 2) upskilling the cyber workforce to identify and respond to misinformation/disinformation (42%); and 3) monitoring for misinformation and disinformation (42%). These preferences reflect the recognition that organizations must combine advanced tools, skilled people, and proactive monitoring to strengthen resilience against synthetic media and disinformation.

1. Investing in AI content authentication tools emerged as the most frequently chosen measure (tied with workforce upskilling). This reflects the recognition that technical safeguards – such as watermarking, blockchain-based verification and real-time provenance tracking – are essential to ensure that organizational communications and digital assets can be verified as authentic. Implementation might include embedding these tools directly into workflows, ensuring that press releases, executive communications, and customer-facing content carry verifiable markers that protect trust and reduce the risk of manipulation.

2. Upskilling the cyber workforce was equally prioritized, signaling that technology alone is not enough. Organizations see the need to equip their teams with the ability to detect, analyze, and respond to synthetic disinformation campaigns. Training initiatives may involve simulation exercises, detection workshops, and ongoing awareness programs, ensuring that staff can identify manipulated content quickly and respond effectively. This builds organizational resilience by reinforcing the human layer of defense alongside technical safeguards.

3. Monitoring for misinformation and disinformation was the third key action area. Respondents highlighted the importance of continuous surveillance of information ecosystems to detect falsified or harmful narratives early. Implementation could involve investing in monitoring tools, establishing dedicated rapid-response teams, and participating in industry-wide sharing networks to exchange intelligence on emerging synthetic threats. These measures allow organizations to move beyond reactive crisis management and toward proactive, real-time detection and response.

In addition to the top-ranked actions, several other organizational-level levers identified from leading organizations' benchmarks were explored but ultimately given lower prioritization. These included collaborating and partnering with trusted information platforms (41%); reviewing and updating internal policies (37%); ensuring compliance with emerging laws and regulations (35%); providing employee training to improve media literacy (32%); and developing and rehearsing strategic response plans (29%).

Going forward, organizations must recognize that information integrity is a core operational risk, not merely a reputational concern.

Leaders should act quickly to embed safeguards that address the growing threat of synthetic content.

This means deploying robust technical defenses, equipping staff with the skills to detect and analyze manipulation, and establishing continuous monitoring systems. By combining technological, organizational and cultural measures, companies can strengthen their resilience and protect both their operations and the broader trust of their stakeholders.

2. Rising Concentration of Technological Power

2.1 Nature of the trend

The growing concentration of technological power in the hands of a few firms is reshaping digital governance and creating systemic vulnerabilities.

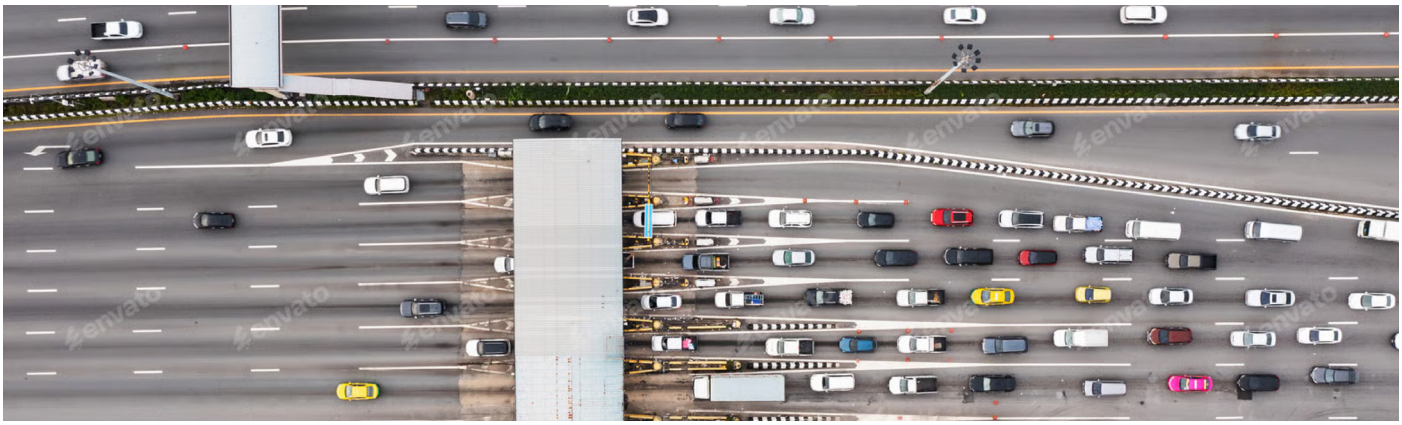
A small number of platforms now control critical infrastructure, cloud environments, and AI capabilities that underpin the global economy. This concentration blurs the boundaries between public governance and private enterprise and impacts accountability, transparency, and resilience. As reliance on these providers grows, states, organizations and societies are becoming more closely tied to the performance and decisions of a limited set of actors.

2.2 Drivers and acceleration signals

The consolidation of digital infrastructure is being accelerated by several key drivers. One important factor is the rise of so-called "shadow AI" – AI embedded invisibly into enterprise tools without formal oversight – which demonstrates how deeply organizations are becoming dependent on a small number of dominant technology providers.

These providers exert increasing influence over access and standards, as governments seek to adapt in a rapidly evolving and fragmented governance environment. This growing dependency amplifies systemic risk and is reinforced by high-profile incidents that reveal the scale of potential disruption. One recent example involved a faulty software update that cascaded across critical systems, triggering approximately 8.5 million crashes worldwide and simultaneously affecting airlines, banks, hospitals, and government services.[9] The economic fallout was immense, exceeding USD 10 billion globally, with losses in the UK alone ranging from GBP 1.7 to GBP 2.3 billion.[10] The top 500 U.S. companies reported nearly USD 5.4 billion in damages, of which only a fraction — between USD 540 million and USD 1.08 billion — was insured.[11] Beyond the incident itself, what matters is the signal: concentrated digital infrastructures magnify the speed, scale, and reach of disruption, turning localized failures into global shocks within hours.

Importantly, this acceleration is not affecting all domains equally; some sectors are disproportionately exposed. Survey respondents identified government (33%), financial services (31%), and healthcare (29%) as the top three most vulnerable sectors, reflecting how reliance on a narrow set of technology providers creates systemic exposure in the very sectors that underpin national resilience.



2.3 Implications and systemic consequences

The costs and implications of techno concentration are both vast and varied. Businesses face systemic exposure: a cloud outage could halt operations, disrupt supply chains, or incapacitate critical services, leading to severe financial losses. A 2024 major failure in one cybersecurity vendor costed Delta Air Lines alone around USD 500 million in lost revenue and expenses, affecting 1.3 million passengers across 7,000 canceled flights.[12]

More broadly, sustained market concentration carries the risk of reduced competition, slower innovation, and fewer choices for consumers. These risks are magnified by the scale of investment at stake: global spending on cloud services, driven by the growth of agentic AI-enabled applications and systems, is projected to reach USD 1.3 trillion by 2029.[13] Such massive concentration of infrastructure and financial commitment makes the need for resilience and oversight more critical than ever.

For governments, the consolidation of digital infrastructure raises fundamental questions of accountability and resilience. When critical systems and national data flows depend on a handful of providers, states have reduced visibility over security standards, incident response, and even strategic decision-making. The concentration of market power creates asymmetries of information and bargaining leverage that leave governments reacting to failures rather than shaping the rules of engagement. As reliance deepens, the absence of diversified infrastructure increases systemic exposure, underscoring the urgent need for proactive regulation and development of national capabilities.

2.4 National-level strategic responses

National policy discussions increasingly focus on the concentration of digital power as a systemic dependency, with parallels to financial stability and critical infrastructure resilience.

The European Union (EU) has advanced its Digital Markets Act and Digital Services Act to curb dominant platforms and impose stricter accountability for outages and misuse.[14] The United States has intensified antitrust investigations into major cloud and AI providers while exploring federal incident reporting mandates. Meanwhile, countries such as India[15] and Australia[16] are investing in sovereign cloud initiatives to reduce dependency on a handful of foreign vendors. These early steps illustrate a growing recognition that unchecked concentration can undermine cyber resilience and market fairness.

Building on these developments, insights from our global survey provide further perspective on which national-level measures are viewed as most effective by cybersecurity leaders. **Figure 4**, below, presents the full set of national-level actions identified by respondents, with the top three priorities highlighted.

A small number of technology platforms now control core infrastructure and capabilities, resulting in an unbalanced concentration of technological power. Which top three national-level actions do you think should be taken to mitigate the risks of technological concentration?

01	Establishing a global cyber governance body	40%
02	Promoting the use of open-source technologies	35%
03	Mandating interoperability across platforms/data	35%
04	Strengthening antitrust enforcement and merger scrutiny	34%
05	Investing in digital sovereignty through local infrastructure	31%
06	Introducing targeted competition rules for AI-heavy sectors	27%
07	Regulating tech platforms as essential critical infrastructure	27%
08	Implementing proactive regulation of dominant "gatekeeper" platforms	25%
09	Coordinating through international bodies	24%
10	Expanding investigative powers of national competition authorities	21%

Figure 4: Survey results: National-level actions towards techno power concentration

Survey respondents identified three measures as most effective for addressing the risks of concentrated technological power: 1) establishing a global cyber governance body to ensure co-ordination and accountability (40%); 2) promoting the use of open-source technologies within critical infrastructures (35%); and 3) mandating interoperability across platforms and data systems (35%). These preferences reflect the recognition that concentration risk is not solely an economic issue, but also a systemic challenge that benefits from structured oversight and coordinated responses.

1. Establishing a global cyber governance body was the most widely supported option. Respondents emphasized that the concentration of technological power requires co-ordination beyond national boundaries, with international governance structures that can monitor systemic risks, set resilience standards, and enforce accountability. Implementation could involve the creation of multilateral oversight bodies modeled on organizations like the International Atomic Energy Agency. These would provide transparency, ensure compliance across borders, and align rules to reduce systemic dependency on a small set of dominant firms.

2. Promoting open-source technologies was the second priority. Respondents highlighted the importance of encouraging the adoption of open, transparent, and community-driven solutions as a counterbalance to concentration risks. Open-source adoption reduces dependency on a handful of providers while strengthening resilience and innovation across industries. Implementation could involve government investment in open-source development, policies favoring open standards in procurement, and incentives for critical sectors (e.g., healthcare or finance) to integrate open-source alternatives into their core systems.

3. Mandating interoperability across platforms and data systems was the third measure prioritized by respondents. This reflects the recognition that concentration risks are amplified when systems are locked into proprietary standards, limiting competition and resilience. By mandating interoperability, governments can force providers to ensure compatibility, facilitate switching, and reduce systemic exposure to single points of failure. Implementation could involve legislation requiring open application programming interfaces (APIs), common data standards and technical certification for critical infrastructure providers.

In addition to the top-ranked actions, several other national-level measures identified from leading nations' benchmarks were explored but ultimately given lower prioritization. These included strengthening antitrust enforcement and merger scrutiny (34%); investing in national cyberinfrastructure (31%); introducing targeted competition rules for AI-heavy sectors (27%); regulating tech platforms as essential critical infrastructure (27%); implementing proactive regulation of dominant "gatekeeper" platforms (25%); coordinating through international bodies (24%),; and expanding the investigative powers of national competition authorities (21%).

Going forward, the growing concentration of technological power must be treated as a systemic dependency risk, comparable to financial stability. Policy makers cannot afford to delay; urgent action is required to reduce vulnerabilities and prevent overreliance on a handful of dominant players.

This calls for a combination of international co-ordination and strong national policies that foster competition, mandate interoperability and diversify critical infrastructure. By addressing techno-concentration with both regulatory and market-based measures, governments can build resilience, protect sovereignty and ensure that technological progress remains aligned with public interest.

2.5 Organizational-level strategic responses

Leading organizations are already adapting their resilience strategies to account for the risks of concentration.

Many firms are investing in joint industry alliances to share intelligence on vendor exposures and negotiate stronger contractual safeguards with technology providers. These efforts signal a shift from viewing outages as isolated information technology (IT) problems to treating them as enterprise-wide risks requiring board-level oversight.

Building on these developments, insights from our global survey provide further perspectives on which organizational-level measures are viewed as most effective by cybersecurity leaders. **Figure 5** presents the full set of organizational-level actions identified by respondents, with the top three priorities highlighted.

A small number of technology platforms now control core infrastructure and capabilities, resulting in an unbalanced concentration of technological power. What do you think organizations should do now to safeguard against the risks of dominant tech companies?

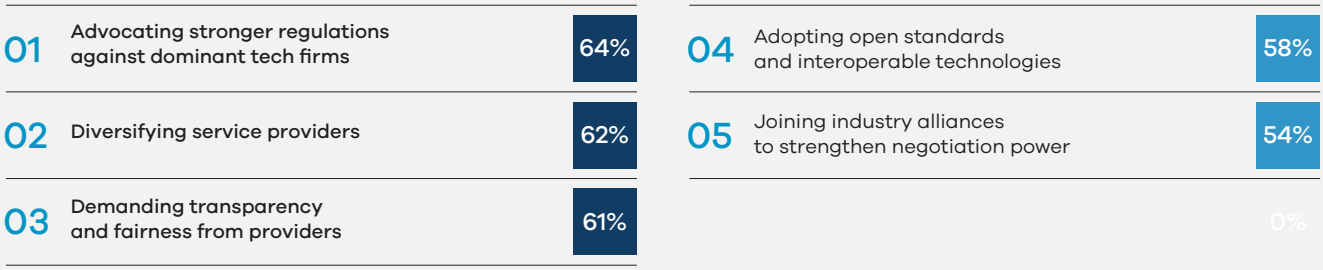


Figure 5: Survey results: Organizational-level actions towards techno power concentration

At the organizational level, survey respondents emphasized three main priorities: 1) advocating stronger regulations against dominant tech firms (64%); 2) diversifying service providers (62%); and 3) demanding transparency and fairness from providers (61%). These results reflect the recognition that organizations are not only consumers of technology, but also stakeholders who can actively influence the governance and accountability of dominant providers, thereby reducing systemic risks.

1. Advocating for stronger regulations against dominant tech firms was the most frequently chosen response. Respondents underscored that organizations should push for stricter rules to hold large technology providers accountable for outages, misuse, and practices that limit transparency or competition. Implementation could involve industry coalitions lobbying regulators, publishing transparency requirements, and creating market pressure that compels dominant firms to adopt higher resilience and accountability standards.

2. Diversifying service providers was another major concern, reflecting the importance of reducing dependency on a handful of dominant platforms by spreading risk across multiple vendors. Implementation may include adopting multi-cloud strategies, maintaining backup providers for critical services, and incorporating vendor diversification into enterprise risk management frameworks. Such approaches reduce exposure to single points of failure and increase organizational resilience in the face of systemic disruptions.

3. Demanding transparency and fairness from providers was the third key action. Respondents emphasized that organizations must insist on visibility in service performance, data practices, and contractual safeguards. Implementation could include negotiating stronger transparency clauses, requiring providers to publish audit results, and participating in industry alliances that collectively push for higher standards. By demanding fairness, organizations not only protect themselves, but also help shape a more balanced and resilient digital ecosystem.

In addition to the top-ranked actions, several other organizational-level levers identified from leading organizations' benchmarks were explored but ultimately given lower prioritization. These included adopting open standards and interoperable technologies (58%) and joining industry alliances to strengthen negotiation power (54%).

Going forward, organizations must recognize that their role extends beyond being passive technology users to active stakeholders in governance.

Firms should act quickly to diversify their providers, reduce dependency on dominant vendors, and support measures that enhance transparency and accountability across the ecosystem. By advocating for higher standards and aligning with regulatory interventions, leaders can help rebalance market power, mitigate systemic risks, and contribute to a healthier and more resilient technological landscape.

3. Proliferation of synthetic identities

3.1 Nature of the trend

The rise of synthetic identities marks a profound shift in how digital trust is established and maintained. Traditionally, verification relied on static anchors such as official documents, biometric markers, or recognizable behavioral patterns. With the advent of generative AI, however, these long-standing verification mechanisms are increasingly vulnerable.

Synthetic personas – once used sparingly in research or niche applications – are now proliferating across digital ecosystems. These personas appear in automated customer service systems, onboarding pipelines, and even professional networks, where they blur the line between real and fabricated users. As these fabricated identities become more indistinguishable from authentic ones, the very foundation of identity-based trust is being challenged.

3.2 Drivers and acceleration signals

Several factors are accelerating the spread of synthetic identities. Advances in generative AI make it possible to create high-quality deepfakes, synthetic voices, and fabricated documents at low cost.

Fraud-as-a-service offerings now enable even low-skilled actors to bypass authentication systems with off-the-shelf tools. According to Javelin Research, identity fraud losses in the United States alone reached USD 52 billion in 2021, impacting more than 42 million adults; synthetic identity fraud is considered the fastest-growing segment of this threat.[17]

Another driver is targeting high-trust environments. Criminal groups increasingly use AI-generated profiles or deepfake video interviews to infiltrate companies under the guise of legitimate employees.[18] There are documented cases of attackers securing remote developer roles to embed backdoors into organizational systems. Financial services, government portals and healthcare systems are particularly vulnerable. Survey respondents in our study echoed this trend, identifying financial services (30%) and government (30%) as the most exposed sectors, followed by healthcare (22%) and information and communications technologies (ICT) (21%). These results signal both the scale of adoption and the pace at which synthetic identities are destabilizing verification systems.

3.3 Implications and systemic consequences

The impacts of synthetic identities extend across governments, societies, and organizations, generating both financial costs and systemic risks.

For governments, the integrity of national identity (ID) systems and border management is at stake. Europol has warned that synthetic passports and forged biometric data are already being sold on darknet markets, creating vulnerabilities for immigration control and national security.[19] The costs are significant: a recent study in the UK estimated that synthetic identity fraud could cost businesses around GBP 4.2 billion if appropriate steps are not taken.[20]

For societies, the proliferation of synthetic identities undermines trust in digital interactions. When everyday users cannot distinguish between authentic and fabricated individuals, social cohesion suffers. The risk is particularly acute in healthcare, where falsified identities have been used to obtain prescription drugs or access benefits, distorting public health systems and diverting resources from legitimate patients.

Organizations also face severe operational and reputational consequences. Fraudulent onboarding, insider threats disguised under synthetic profiles, and executive impersonations not only expose sensitive data but also erode stakeholder confidence. Beyond direct fraud losses, companies experience hidden costs: Gartner predicts that by 2026, 30% of enterprises will no longer consider standalone identity verification and authentication solutions reliable due to AI-generated deepfakes.[21]

3.4 National-level strategic responses

Governments worldwide are beginning to recognize synthetic identity fraud as a national security and economic stability issue. Several countries are piloting advanced identity protection measures. India's Aadhaar program has been upgrading its biometric systems to counter AI-driven forgery[22], while the EU has launched the European Digital Identity Wallet to enable secure, verifiable cross-border transactions.[23] These early initiatives show that governments are already moving to reinforce digital identity frameworks before synthetic identities undermine them completely.

Building on these developments, insights from our global survey provide further perspective on which national-level measures are viewed as most effective by cybersecurity leaders. **Figure 6**, below, presents the full set of national-level actions identified by respondents, with the top three priorities highlighted.

AI-generated content is undermining identity verification by making it harder to trust visual cues like faces, voices, and signatures. Which top three national measures would help the most in being prepared for synthetic identity fraud?

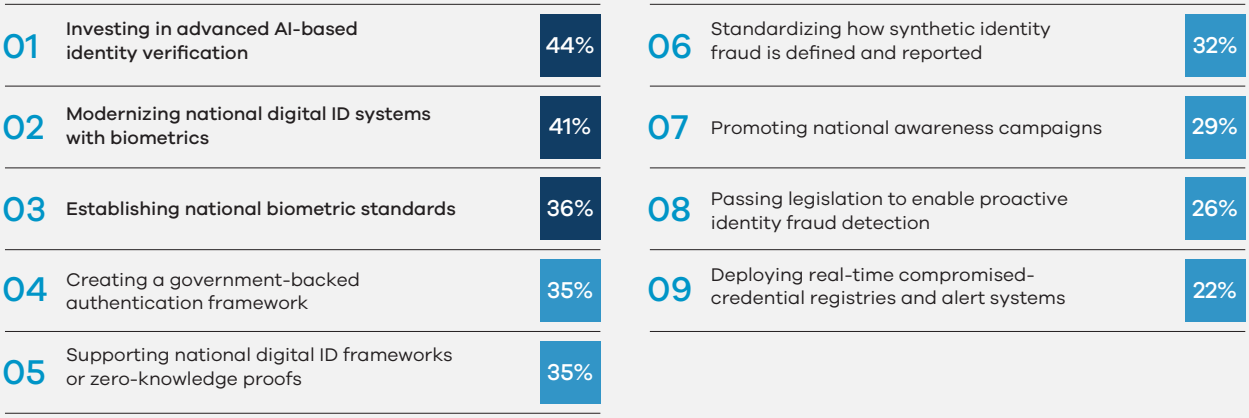


Figure 6: Survey results: National-level actions towards synthetic identities threats

Survey respondents identified three 'most-effective' national-level measures to counter synthetic identity threats: 1) investing in advanced AI-based identity verification (44% of respondents); 2) modernizing national digital ID systems with biometrics (41%); and 3) establishing national biometric standards (36%). These preferences reflect the recognition that safeguarding digital identity requires governments to modernize infrastructure, adopt advanced verification technologies, and harmonize standards to ensure trust and resilience across sectors.

1. Investing in advanced AI-based identity verification was the most supported measure, reflecting the urgent need to strengthen detection capabilities. AI-based systems analyze behavioral signals, device fingerprints, and cross-channel data to spot anomalies that static methods often miss. Implementation could involve governments working with regulators and technology firms to deploy adaptive verification across critical sectors such as banking, border control, and healthcare, ensuring that fraudulent identities are intercepted before they cause systemic harm.

2. Modernizing national digital ID systems with biometrics was the second most supported response, underscoring the recognition that traditional ID infrastructures are insufficient in the face of synthetic forgeries. Biometric frameworks that combine multiple markers – such as facial, iris, and gait recognition – are far less vulnerable to manipulation than single-factor systems. Implementation could include phased rollouts of multi-modal biometric ID programs, integration with smartphones and e-government services, and collaborative pilot projects with private sector partners to test resilience against advanced identity forgeries.

3. Establishing national biometric standards was the third most frequently chosen option, highlighting the risks created by fragmented systems. Without harmonization, inconsistent data collection and storage practices create exploitable gaps for adversaries. Implementation could involve governments working with international bodies such as the International Organization for Standardization (ISO) or International Telecommunication Union (ITU) to set shared standards for biometric data collection, encryption, and interoperability, balancing security objectives with privacy safeguards.

In addition to the top-ranked actions, several other national-level measures identified from leading nations' benchmarks were explored but ultimately given lower prioritization. These included creating a government-backed authentication framework (35%); supporting national digital ID frameworks based on verifiable credentials or zero-knowledge proofs (35%); standardizing how synthetic identity fraud is defined, detected, and reported (32%); promoting national awareness campaigns (29%); passing legislation to enable proactive identity fraud detection (26%); and deploying real-time compromised-credential registries and alert systems (22%).

Going forward, governments must treat the protection of digital identity as a cornerstone of both national security and economic stability. Policy makers should act swiftly to modernize outdated infrastructure, strengthen verification technologies, and reduce vulnerabilities that malicious actors can exploit.

At the same time, aligning international frameworks and harmonizing standards will be essential to safeguard identity systems across borders. By combining regulatory action with technological upgrades and global co operation, leaders can build resilient identity ecosystems and maintain public trust.

3.5 Organizational-level strategic responses

Organizations are also beginning to adapt to the challenge of synthetic identities, moving beyond static authentication and experimenting with layered, dynamic solutions.

Leading banks have introduced continuous authentication systems, in which user behavior is monitored throughout an interaction rather than just at log-in. Technology firms are rolling out liveness detection tools that make it harder for deepfakes to bypass video[24] verification, and telecommunications providers are joining cross-industry fraud intelligence networks to share insights about synthetic identity tactics.[25]

Building on these developments, insights from our global survey provide further perspectives on which organizational-level measures are viewed as most effective by cybersecurity leaders. **Figure 7** presents the full set of organizational-level actions identified by respondents, with the top three priorities highlighted.

AI-generated content is undermining identity verification by making it harder to trust visual cues like faces, voices, and signatures. What should organizations do to effectively address synthetic identity threats?

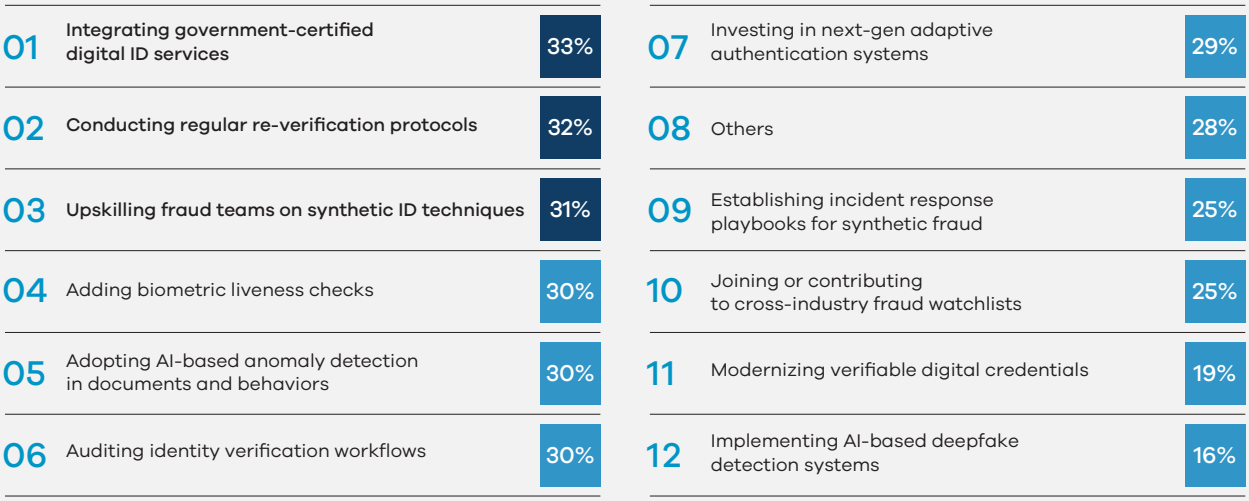


Figure 7: Survey results: Organizational-level actions towards synthetic identities threats

Survey respondents identified three 'most-effective' organizational-level measures to counter synthetic identity threats: 1) integrating government-certified digital ID services (33%); 2) introducing regular re-verification protocols (32%); and 3) upskilling fraud teams on synthetic ID techniques (31%). These results reflect the recognition that safeguarding against synthetic identities requires organizations to strengthen trust frameworks, implement ongoing validation processes, and equip their workforce with the skills needed to detect and respond to emerging fraud tactics.

1. Integrating government-certified digital ID services was the most frequently chosen measure. Respondents emphasized that aligning with nationally recognized ID frameworks provides a higher level of assurance and resilience against identity fraud. Implementation could involve integrating digital ID wallets, government-issued verification mechanisms, and trusted authentication services into onboarding, access management and, transaction systems. This creates a stronger trust foundation that synthetic identities find more difficult to bypass.

2. Introducing regular re-verification protocols was the second priority. This measure recognizes that one-time identity checks are insufficient in a fast-evolving threat landscape. Organizations can improve resilience by periodically re-validating the identities of customers, employees, or partners. Implementation could include annual re-verification for high-value accounts, random spot checks for sensitive systems, or industry-specific requirements such as ongoing credential verification in financial services.

3. Upskilling fraud teams on synthetic ID techniques was the third key measure. Fraud detection teams require new expertise to keep pace with adversaries. Training programs can cover deepfake detection, forensic document analysis, and behavioral anomaly monitoring. Implementation may involve partnerships with cybersecurity training providers, simulation exercises to mimic real-world synthetic identity fraud, and participation in cross-sector fraud intelligence networks.

In addition to the top-ranked actions, several other organizational-level levers identified from leading organizations' benchmarks were explored but ultimately given lower prioritization. These included adding biometric liveness checks (30%); adopting AI-based anomaly detection in documents and behaviors (30%); auditing identity verification workflows (30%); investing in next-gen adaptive authentication systems (29%); establishing incident response playbooks for synthetic fraud (25%); joining or contributing to cross-industry fraud watchlists (25%); modernizing verifiable digital credentials (19%); and implementing AI-based deepfake detection systems (16%).

Going forward, organizations must recognize that static, one-time authentication methods are no longer sufficient to guard against increasingly sophisticated AI-driven forgeries.

Leaders should act quickly to adopt dynamic, layered verification approaches that combine certified ID systems with continuous re-verification processes. At the same time, investing in both advanced technical tools and highly trained fraud teams will be essential to sustain resilience. By embedding these measures, organizations can strengthen protection against identity fraud and maintain trust in digital interactions.

4. Growth of Autonomous AI-powered Attacks

4.1 Nature of the trend

The nature of cyberattacks is undergoing a structural shift. What were once opportunistic, one-off intrusions are increasingly being replaced by persistent, goal-driven operations shaped by the integration of AI. Adversaries are beginning to deploy AI to automate reconnaissance, decision-making and execution across the attack lifecycle.

This creates attacks that are adaptive, coordinated and less reliant on human intervention. Unlike earlier waves of cyber conflict, these operations are characterized by autonomy and intent: systems that probe, learn, and exploit at machine speed, with limited need for human operators.

4.2 Drivers and acceleration signals

The drivers of this trend lie in both the capabilities of AI technologies and the way adversaries are operating them. One critical signal is the dramatic reduction in the time between the disclosure of vulnerabilities and their exploitation. Fortinet has noted that this window has narrowed to hours in some cases, leaving defenders little time to act. Generative AI tools are being used to produce malicious scripts, polymorphic malware, and payloads that adapt dynamically to the environment they encounter.[3]

Building on these drivers, another acceleration signal comes from adversary behavior. CrowdStrike reports that the average breakout time for attackers has dropped to 48 minutes, with the fastest intrusion recorded at just 51 seconds.[1] At the same time, the proliferation of tools such as FraudGPT, BlackmailerV3, and EvilProxy make scalable credential theft and extortion accessible even to less-experienced actors.[3] What was once the domain of elite cyber groups is becoming democratized, enabling a wider base of adversaries to launch advanced attacks.

Taken together, these developments show that signals of convergence are also emerging. Information stealers like Redline and Vidar are now being enhanced with AI modules that extract multifactor authentication tokens, browser sessions and cloud credentials.[3]

This points to the rise of a fully autonomous attack chain, where reconnaissance, exploitation, lateral movement, and data exfiltration are orchestrated automatically, with real-time adaptation and layered deception, such as adversary-in-the-middle techniques.

This rapid acceleration is not affecting all domains equally; some sectors are disproportionately exposed. Survey respondents identified financial services (37%), ICT (33%), and healthcare (30%) as the most vulnerable sectors, underscoring how disruption in these areas could cascade across economies and societies if adversaries harness AI at scale.

4.3 Implications and systemic consequences

The systemic consequences of autonomous AI-powered attacks are profound. For governments, the national security risks are immediate. Attacks on critical infrastructure, defense networks or electoral systems can now be launched and scaled faster than existing defensive frameworks can respond.

The World Economic Forum has warned that without coordinated oversight, AI-driven threats will continue to outpace safeguards, creating an imbalance between attackers and defenders.[26]

For organizations, the cost implications are already visible. IBM's Cost of a Data Breach report estimated the global average cost of a breach at USD 4.4 million[27], highlighting that AI is greatly outpacing security and governance in favor of do-it-now adoption. The findings show that ungoverned AI systems are more likely to be breached and more costly when they are beyond financial loss, reputational damage and regulatory penalties exacerbate the burden.

Societies are already exposed to the risk of service disruptions, and the potential consequences highlight how severe such failures could become. An autonomous attack on healthcare providers or utilities, for example, has the potential to halt access to essential services, triggering cascading effects on public safety. Given the growing interconnection of these systems, a disruption in one sector could quickly ripple across supply chains and entire communities. These dynamics reinforce the urgency of building defenses that operate at machine speed and adapt as rapidly as the threats themselves.

4.4 National-level strategic responses

Governments are beginning to recognize that traditional, signature-based detection and reactive models are insufficient against AI-powered threats. Several states have launched task forces on AI in cybersecurity[28], while others are piloting certification standards for AI systems used in sensitive domains.[29]

The EU is exploring regulatory requirements for explainability in AI-driven systems[30], while the United States has convened industry and defense leaders to draft accountability frameworks for AI deployment in both civilian and military applications.[31] These early measures show that governments are beginning to treat autonomous attacks as systemic national risks.

Building on these developments, insights from our global survey provide further perspectives on which national-level measures are viewed as most effective by cybersecurity leaders. **Figure 8**, below, presents the full set of national-level actions identified by respondents, with the top three priorities highlighted.

AI is changing how threats are developed and deployed, prompting new challenges in cyber defense. Which top three national-level actions do you think should be taken to counter AI-enabled cyber threats?

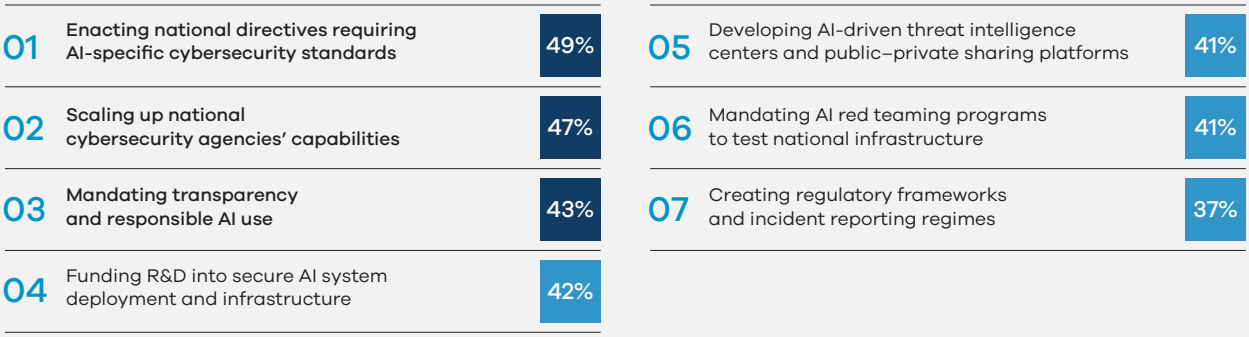


Figure 8: Survey results: National-level actions towards autonomous AI-powered attacks

Survey respondents identified three 'most-effective' national-level measures to counter autonomous AI-powered attacks: 1) enacting national AI-specific cybersecurity directives (49%); 2) scaling up national cybersecurity agencies' capabilities (47%); and 3) mandating transparency and responsible AI use (43%). These results reflect the growing consensus that autonomous AI-driven threats require governments to strengthen regulation, enhance institutional capacity, and enforce accountability standards at scale.

1. Enacting national AI-specific cybersecurity directives was the most widely supported measure. Respondents emphasized the need for governments to set binding rules that specifically address the use of AI in cybersecurity contexts. Implementation could involve developing regulations that establish clear technical standards, minimum resilience requirements, and oversight mechanisms tailored to AI-enabled systems. Such directives would provide governments with the tools to anticipate risks and respond more effectively when AI systems are deployed in critical domains.

2. Scaling up national cybersecurity agencies' capabilities was the second priority. Respondents highlighted the importance of building state capacity to match the speed and sophistication of AI-driven attacks. Implementation might include expanding budgets for national cyber agencies, recruiting specialized AI expertise, and creating advanced operational centers capable of continuous monitoring, rapid response, and cross-sector co-ordination. These investments would ensure that national defenses evolve in parallel with adversarial capabilities.

3. Mandating transparency and responsible AI use was the third key measure. Respondents recognized that AI systems introduce an opacity that undermines accountability and resilience. Implementation could involve requiring AI developers and operators to document decision-making processes, provide audit trails of system actions, and publish compliance reports addressing issues such as bias, explainability and security safeguards. By enforcing transparency, governments could reduce systemic risks while fostering trust in AI-enabled cybersecurity practices.

In addition to the top-ranked actions, several other national-level measures identified from leading nations' benchmarks were explored but ultimately given lower prioritization. These included funding research and development (R&D) into secure AI system deployment and infrastructure (42%); developing AI-driven threat intelligence centers and public-private sharing platforms (41%); mandating AI red-teaming programs to test national infrastructure (41%); and creating regulatory frameworks and incident reporting regimes (37%).

Going forward, governments must recognize autonomous AI-powered attacks as systemic national risks that demand both regulation and institutional capacity.

Policy makers should act with urgency to establish strong legal guardrails while simultaneously expanding the capabilities of cyber agencies to operate at machine speed. A balanced approach that combines regulatory frameworks with operational readiness will be essential to contain threats, deter malicious actors, and safeguard national security in an era of increasingly autonomous AI-driven attacks.

4.5 Organizational-level strategic responses

Organizations are also beginning to adapt to the new threat environment. Large enterprises are running AI-driven simulation environments to model autonomous attack vectors, while sectors such as finance and energy are increasingly investing in predictive defenses that use machine learning to detect anomalies before they escalate.

Technology firms are collaborating to share intelligence on AI-driven threat tactics, reflecting a shift toward collective defense. Building on these developments, insights from our global survey provide further perspective on which organizational-level measures are viewed as most effective by cybersecurity leaders. **Figure 9**, below, presents the full set of organizational-level actions identified by respondents, with the top three priorities highlighted.

AI is changing how threats are developed and deployed, prompting new challenges in cyber defense. What do you think should be the top three priorities for mitigating AI-powered cyber threats at an organizational-wide level?

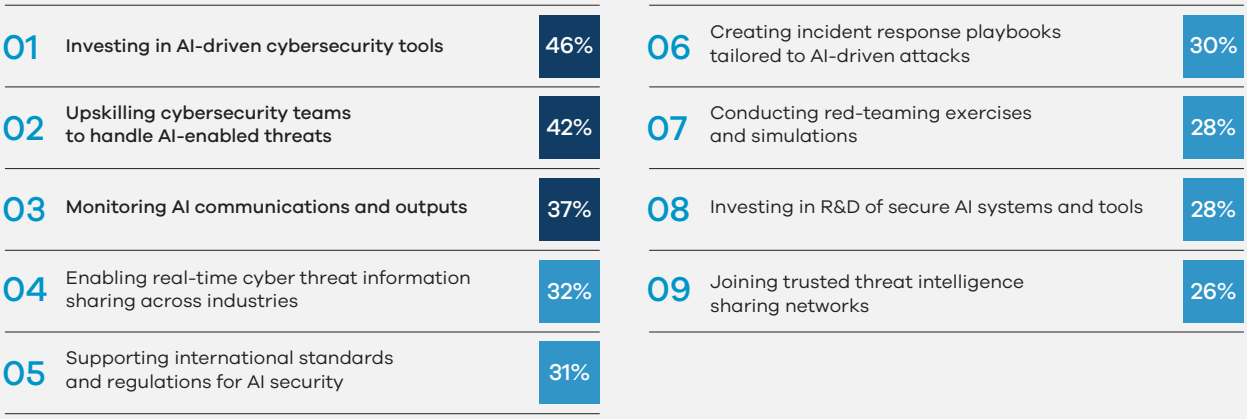


Figure 9: Survey results: Organizational-level actions towards autonomous AI-powered attacks

Survey respondents identified three 'most-effective' organizational-level measures: 1) investing in AI-driven cybersecurity tools (46%); 2) upskilling cybersecurity teams to handle AI-enabled threats (42%); and 3) monitoring AI communications and outputs to prevent misuse (37%). These results reflect the emphasis organizations place on combining advanced technological defenses with stronger human capabilities and proactive monitoring to keep pace with rapidly evolving AI-driven attacks.

1. Investing in AI-driven cybersecurity tools was the most frequently chosen organizational response. Respondents highlighted the importance of equipping organizations with defensive capabilities that operate at the same speed and scale as attackers. Implementation could involve deploying AI-enabled monitoring systems, anomaly detection tools, and automated response platforms, while ensuring that these are integrated across enterprise risk management frameworks. By adopting such tools, organizations can strengthen visibility into complex environments and react quickly to new attack vectors.

2. Upskilling cybersecurity teams to handle AI-enabled threats was the second priority. Respondents underscored the need for human expertise to complement automated defenses, ensuring that staff are prepared to interpret AI-generated intelligence and manage advanced attack scenarios. Implementation may include targeted training programs, simulation exercises, and continuous education on adversarial AI techniques. By improving workforce readiness, organizations increase their resilience against both the technical and strategic aspects of AI-driven threats.

3. Monitoring AI communications and outputs to prevent misuse was the third measure. Respondents recognized that attackers increasingly exploit AI models and platforms themselves. Implementation could involve embedding monitoring processes within organizations to track unusual outputs, detecting adversarial behaviors, and identifying instances of synthetic content generation that could be weaponized. Establishing oversight mechanisms ensures that organizations can mitigate risks at the source and reduce exposure to misuse of AI within their operational environments.

In addition to the top-ranked actions, several other organizational-level levers identified from leading organizations' benchmarks were explored but ultimately given lower prioritization. These included enabling real-time cyber threat information sharing across industries (32%); supporting international standards and regulations for AI security (31%); creating incident response playbooks tailored to AI-driven attacks (30%); conducting red-teaming exercises and simulations (28%); investing in the R&D of secure AI systems and tools (28%); and joining trusted threat intelligence sharing networks (26%).

Going forward, organizations must recognize that defending against AI-powered threats requires adopting the same technologies that adversaries exploit.

Leaders should act quickly to integrate AI-enabled defense tools into enterprise security strategies, while ensuring human oversight remains central to interpreting AI-generated intelligence and managing emerging risks. By combining technological innovation with skilled cybersecurity teams and proactive monitoring, firms can strengthen resilience and maintain a decisive edge against evolving AI-driven attacks.

5. Emerging Shutdown Risks from Interconnected Autonomous Systems

5.1 Nature of the trend

Autonomous systems are increasingly embedded as decision-makers within critical infrastructures such as energy, finance, healthcare, and transportation. Once peripheral, they now determine access, routing, and optimization in real time. While this brings efficiency and scale, it also creates fragility: failures in one domain can cascade rapidly across others.

As these systems govern not just processes, but also interdependence, their malfunction or misalignment risks large-scale shutdowns that disrupt social and economic continuity.

5.2 Drivers and acceleration signals

First, autonomy is amplifying the risk concentration within control environments. Automation orchestration tools, widely used in cloud and enterprise systems, concentrate enormous authority in control planes.

When misused, whether through malicious escalation of privileges or flawed updates, these control planes can trigger large-scale failures. The potential for a single point of failure is heightened by the degree of automation: what once required human intervention can now propagate automatically across thousands of systems within minutes.

In addition, opacity and interconnection magnify disruption. Autonomous systems increasingly mediate essential infrastructure: credit scoring governs lending and insurance, logistics systems optimize supply chains, and triage AI platforms manage healthcare access. With these systems often operating as black boxes, oversight is limited. Recent disruptions illustrate the stakes: as recently as June 2025, a cloud outage rapidly cascaded through platforms, exposing how disruptions in centralized infrastructure can instantly cascade across sectors.[32] These events emphasize that lack of visibility and tight interdependence convert localized failures into systemic shutdowns.

This rapid acceleration is also not affecting all domains equally; certain sectors are disproportionately exposed. Survey respondents highlighted ICT and telecommunications (35%), financial services (32%), and healthcare (29%) as the most vulnerable, pointing to the danger of localized failures propagating quickly into multiple sectors essential for economic and social stability.

5.3 Implications and systemic consequences

For governments, shutdowns threaten the continuity of essential public services, ranging from healthcare delivery and emergency communications to transportation and energy supply.

When autonomous systems or centralized platforms fail, government agencies often have limited visibility into root causes, leaving them reliant on external vendors for diagnosis and recovery. This creates risks, where critical national functions are effectively dependent on the operational resilience of a handful of technology providers. Cross-border interdependencies further complicate accountability: when a failure originates in one jurisdiction but cascades globally, tracing liability and coordinating responses across governments becomes enormously challenging.

For organizations, financial and operational exposure continues to escalate. EMA Research estimates the average cost of IT downtime at USD 12,900 per minute per minute, with large-scale incidents easily crossing into hundreds of millions of dollars in lost revenue, remediation, and customer compensation[33]. Beyond direct costs, outages can erode customer trust, disrupt supply chains, and trigger regulatory scrutiny, amplifying the damage long after systems are restored. For sectors that rely on just-in-time operations – such as airlines, logistics, and healthcare – even short outages can cascade into weeks of disruption. As organizations adopt more autonomous systems, the attack surface grows more complex, making recovery slower and the risks of compounding errors far greater.

For societies, the consequences can be profound, affecting safety and stability. Outages in healthcare AI systems can delay medical services and put patient safety at risk. Failures in energy grids or transportation control systems can paralyze entire cities, halt economic activity, and create physical safety risks. Breakdowns in financial trading platforms can potentially shake confidence in institutions and create market volatility. Unlike traditional IT failures, the risks here are not isolated but systemic: interconnected autonomous systems mean that multiple domains – health, finance, transportation, communications – can fail simultaneously. This unpredictability magnifies the threat, making it harder for communities to prepare or adapt while deepening the sense of fragility in essential services.

5.4 National-level strategic responses

Governments are beginning to adapt their approaches from sector-specific oversight to systemic safeguards. The EU, for example, is advancing proposals for independent supervisory bodies to oversee critical AI systems[34], while Singapore[35] and Japan[36] have launched national initiatives to certify autonomous systems in healthcare and transport.

Some countries are also piloting public education campaigns on AI risk to build resilience and awareness among citizens. Building on these developments, insights from our global survey provide further perspectives on which national-level measures are viewed as most effective by cybersecurity leaders. **Figure 10**, below, presents the full set of national-level actions identified by respondents, with the top three priorities highlighted.

AI is changing how threats are developed and deployed, prompting new challenges in cyber defense. What do you think should be the top three priorities for mitigating AI-powered cyber threats at an organizational-wide level?

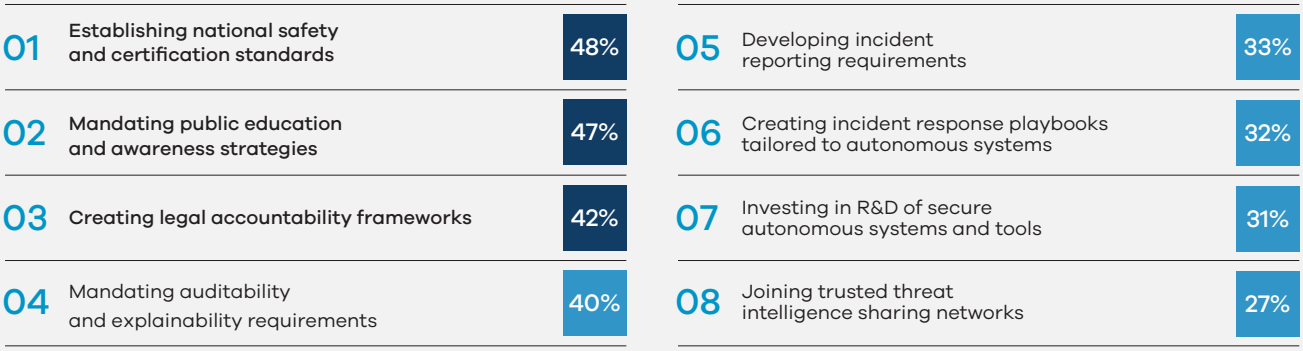


Figure 10: Survey results: National-level actions towards risks of autonomous decision making systems

Survey respondents identified three 'most-effective' national-level measures to address shutdown risks: 1) establishing national safety and certification standards for autonomous systems before deployment (48%); 2) mandating the development of national public education and awareness strategies (47%); and 3) creating legal accountability frameworks defining liability for autonomous system decisions and harm (42%). These results reflect recognition that the risks of interconnected autonomous systems cannot be left to technical operators alone, but require structured national policy responses to strengthen resilience and accountability.

1. Establishing national safety and certification standards was the most widely supported measure. Respondents emphasized that autonomous systems must undergo rigorous evaluation before deployment in high-stakes environments such as healthcare, finance, and energy. Implementation could involve independent national regulators who are empowered to audit algorithms, test fail-safes, and enforce certification to ensure systems meet resilience benchmarks.

2. Mandating the development of national public education and awareness strategies was the second most supported measure. Respondents highlighted the need for societies to better understand both the risks and benefits of autonomous systems. Implementation could include: public campaigns, integration of AI literacy into education systems, and awareness programs for businesses and citizens, ensuring preparedness for potential disruptions and building trust in responsible adoption.

3. Creating legal accountability frameworks defining liability for autonomous system decisions and harm was the third key measure. Respondents underscored the importance of establishing clear liability when autonomous systems cause failures or damage. Implementation could include legislation assigning responsibility to developers, operators, or vendors, along with mechanisms for compensation and redress. By clarifying accountability, governments can close regulatory gaps and ensure trust in the governance of autonomous systems.

In addition to the top-ranked actions, several other national-level measures identified from leading nations' benchmarks were explored but ultimately given lower prioritization. These included mandating auditability and explainability requirements (40%); developing incident reporting requirements (33%); creating incident response playbooks tailored to autonomous systems (32%); investing in the R&D of secure autonomous systems and tools (31%); and joining trusted threat intelligence sharing networks (27%).

Going forward, governments must treat autonomous systems as critical national infrastructure requiring robust safeguards before widespread deployment.

Policy makers should move quickly to establish certification standards and liability frameworks that ensure accountability, while also launching public education initiatives to build resilience in society. By combining regulatory measures with awareness programs, leaders can reduce the risk of cascading systemic failures and strengthen national preparedness for the challenges posed by interconnected autonomous systems.

5.5 Organizational-level strategic responses

Organizations are already beginning to adjust to the risks of interconnected autonomy. Large cloud providers are implementing audit trails to increase visibility into AI decision-making, while hospitals and financial firms are developing incident response playbooks tailored to autonomous failures. Telecommunications operators and utilities are experimenting with dynamic detection pipelines that monitor system behavior continuously, aiming to catch harmful anomalies before they scale.

These efforts illustrate how industry pilots safeguards even before regulatory mandates arrive.

Building on these developments, insights from our global survey provide further perspectives on which organizational-level measures are viewed as most effective by cybersecurity leaders. **Figure 11**, below, presents the full set of organizational-level actions identified by respondents, with the top three priorities highlighted.

AI is changing how threats are developed and deployed, prompting new challenges in cyber defense. What do you think should be the top three priorities for mitigating AI-powered cyber threats at an organizational-wide level?

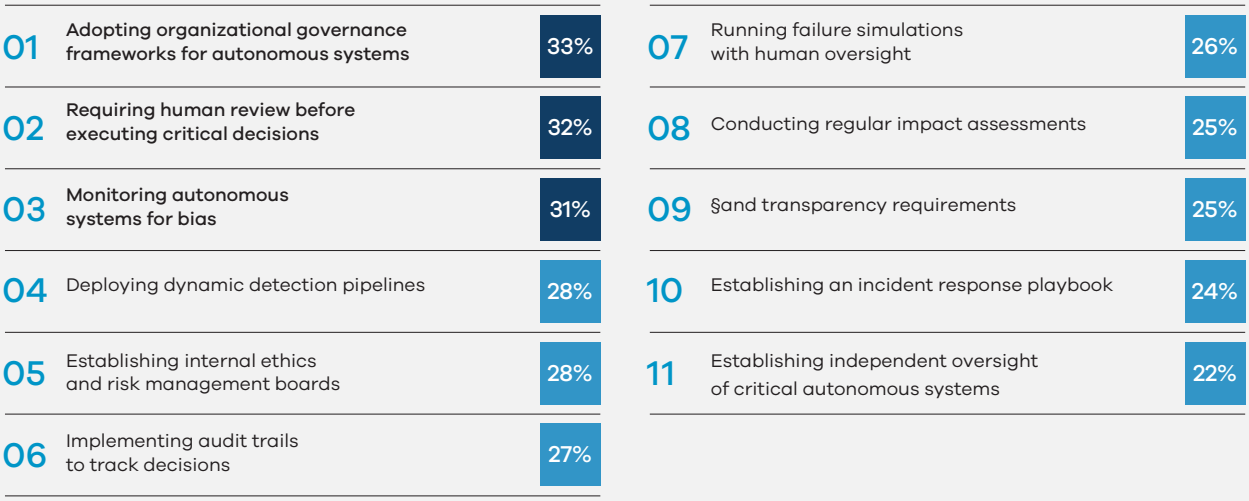


Figure 11: Survey results: Organizational-level actions towards autonomous decision making risks

Survey respondents identified the three 'most-effective' organizational-level measures: 1) adopt organizational governance frameworks for autonomous systems (33%); 2) require human review before executing critical decisions (32%); and 3) monitor autonomous systems for bias using benchmarking and continuous feedback loops (31%). These results highlight the importance of balancing governance, human oversight, and fairness when managing the risks posed by autonomous decision-making systems.

1. Adopting organizational governance frameworks for autonomous systems was the most frequently chosen measure. Respondents emphasized that organizations need structured principles, policies, and processes to guide safe deployment and oversight. Implementation could involve creating cross-functional governance boards, setting internal policies aligned with regulatory standards, and embedding risk management tools that ensure systems remain aligned with organizational values and objectives.

2. Requiring human review before executing critical decisions was the second most supported measure. Respondents noted that even highly advanced autonomous systems should not operate without human oversight when making decisions with significant safety, financial, or ethical implications. Implementation could include mandatory human-in-the-loop mechanisms for critical functions, escalation processes to human operators during anomalies, and clear accountability protocols for final decisions.

3. Monitor autonomous systems for bias was the third key measure. Respondents recognized that bias and fairness risks must be actively managed as systems scale. Implementation could involve benchmarking tools, continuous feedback loops, and monitoring dashboards that track outcomes across different populations and scenarios. By identifying and correcting biases, organizations can ensure fairer and more trustworthy use of autonomous technologies.

In addition to the top-ranked actions, several other organizational-level levers identified from leading organizations' benchmarks were explored but ultimately given lower prioritization. These included deploying dynamic detection pipelines (28%), establishing internal ethics and risk management boards (28%), implementing audit trails to track decisions (27%), running failure simulations with human oversight (26%), conducting regular impact assessments (25%), introducing explainability and transparency requirements (25%), establishing incident response playbooks (24%), and establishing independent oversight of critical autonomous systems (22%).

Going forward, organizations must recognize that automation cannot be trusted blindly; it requires structured accountability mechanisms.

Leaders should embed strong governance frameworks, maintain human oversight in critical decision-making processes, and establish continuous monitoring for bias and fairness. By taking these steps, firms can prevent disruptions, strengthen accountability, and ensure trust in the deployment of autonomous systems.

Conclusion

The trends explored in this flagship report highlight not only the scale of change underway in cybersecurity, but also the depth of its systemic implications. From the erosion of information integrity to the concentration of technological power, each trend illustrates that the challenges are no longer simply technical. They are strategic, societal and global.

What emerges is clear: safeguarding the future of Cyberspace requires more than incremental improvements. It demands anticipatory governance, resilient organizational capabilities, and deeper collaboration across public and private boundaries. Nations must set frameworks that are enforceable, adaptive and trusted; organizations must embrace proactive, operationally effective defenses that keep pace with adversarial innovation.

The key trends highlighted in this report demonstrate how the frontiers of trust, identity, and autonomy are being redefined. Addressing them effectively will shape not only the resilience of digital systems, but also the integrity of economies, societies, and institutions themselves. By acting decisively, stakeholders can transform these pressures into opportunities – and build a digital future that is secure, inclusive, and sustainable.

Appendix A: Horizon scan of all 20 trends

To identify the most critical developments shaping the future of cybersecurity, all 20 trends were evaluated using a structured scoring framework. Each trend was assessed across several dimensions: its expected time to maturity; its potential impact on political, societal, and economic domains; and its relevance as reflected in survey responses.

Survey input formed the core of this evaluation, with respondents indicating which trends they considered most urgent and consequential. These inputs were then translated into normalized percentage-based scores, allowing us to compare trends on a common scale. This process enabled us to rank all 20 trends systematically and highlight the top five – those that not only received the highest percentage of support from survey participants, but also demonstrated the strongest overall potential to reshape the cybersecurity landscape.

1. Erosion of public trust through AI-powered disinformation

Score: 100% – **Time to mature:** 1-3 years – **Most impacted domain:** Political

AI is being weaponized by adversaries to spread misinformation, destabilizing public discourse and trust in institutions. The trend is accelerating via rapid content generation and precision targeting.

2. Rising concentration of technological power

Score: 99% – **Time to mature:** 3-5 years – **Most impacted domain:** Political

A few tech platforms now hold concentrated technological power, shaping regulation, security, and infrastructure, as well as blurring public-private lines and challenging accountability.

3. Proliferation of synthetic identities

Score: 97% – **Time to mature:** 1-3 years – **Most impacted domain:** Societal

AI-generated personas and deepfakes are breaking classical ID-based authentication systems. The speed of adoption makes visual cues increasingly unreliable as trust anchors.

4. Growth of autonomous AI-powered attacks

Score: 95% – **Time to mature:** 1-3 years – **Most impacted domain:** Political

Adversaries are industrializing AI to deliver persistent, goal-oriented attacks. This marks a shift away from opportunistic attacks – short-term, low-effort exploits that take advantage of easy vulnerabilities – towards more strategic forms of cyber conflict characterized by intent, planning, and co-ordination.

5. Emerging shutdown risks from interconnected autonomous systems

Score: 94% – **Time to mature:** 5 years – **Most impacted domain:** Societal

Autonomous tech systems increasingly gatekeep access to life services, raising questions about algorithmic power and exclusion.

6. Expansion of sovereign control

Score: 93% – **Time to mature:** 5 years – **Most impacted domain:** Political

Governments are increasingly asserting control over data flows, content, and digital infrastructure – reshaping the structure of the global internet and redefining the rules of engagement.

7. Growing urgency of post-quantum readiness

Score: 93% – **Time to mature:** 5 years – **Most impacted domain:** Economic

The arrival of quantum computing threatens to break current encryption, exposing decades of sensitive data unless post-quantum readiness is achieved proactively.

8. Cyber literacy emerging as a core skill

Score: 91% – **Time to mature:** 5 years – **Most impacted domain:** Societal

Digital self-defense becomes essential; cybersecurity literacy must be taught like reading or math.

9. Supply chains becoming prime strategic targets

Score: 91% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic
Digital interdependencies turn supply chains into prime targets. Attacks on upstream providers ripple downstream across entire ecosystems and industries.

10. Advanced attack techniques moving into the mainstream

Score: 90% – **Time to mature:** 3-5 years – **Most impacted domain:** Economic

The tools and tactics of elite cyber actors become available to a broader range of bad actors, drastically lowering the barrier to executing complex attacks.

11. Diversification of cybercrime monetization models

Score: 89% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

Cybercrime evolves into a mature economy with diverse revenue streams, including extortion, ransomware-as-a-service, subscription-based toolkits, and exploited marketplaces.

12. Digital identity evolving into a global utility

Score: 87% – **Time to mature:** 5 years – **Most impacted domain:** Societal

Secure, verifiable digital identity is expected to become a foundational requirement for economic and social participation. This will enable innovation but also generate tensions, as governments, tech providers and civil society groups compete over questions of control, access and trust.

13. Cyber threats accelerating from slow burn to sudden impact

Score: 86% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

Threats that once emerged gradually can now explode with little warning, driven by AI acceleration, interconnected infrastructure, and geopolitical flashpoints.

14. Software-defined systems expanding the attack surface

Score: 85% – **Time to mature:** 3-5 years – **Most impacted domain:** Economic

As critical infrastructure shifts from hardware to code, vulnerabilities multiply and the attack surface expands – especially for legacy systems retrofitted with new software layers.

15. Systemic scaling of AI-driven threats

Score: 85% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

AI-driven threats are no longer isolated: they scale across systems, sectors, and functions, creating systemic vulnerabilities that are hard to contain or predict.

16. AI transforming the cyber workforce

Score: 85% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

AI tools are reshaping cybersecurity roles and skills, automating lower-level tasks while increasing the need for strategic oversight, model literacy, and governance.

17. IT, OT and CT converging into total exposure

Score: 84% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

The convergence of information technology, operational technology, and communications technology creates tightly coupled systems with cascading failure risks.

18. Shift toward proactive, collaborative cybersecurity governance

Score: 83% – **Time to mature:** 3-5 years – **Most impacted domain:** Economic

Cybersecurity governance is shifting from reactive regulation to proactive collaboration. The new triad – co-operation, education and regulation – offers a more dynamic framework for managing fast-moving threats while preserving innovation and trust.

19. Adoption of autonomous cyber defense models

Score: 81% – **Time to mature:** 1-3 years – **Most impacted domain:** Economic

Defenders must adopt AI-native operating models capable of autonomously detecting, responding to, and mitigating threats at machine speed.

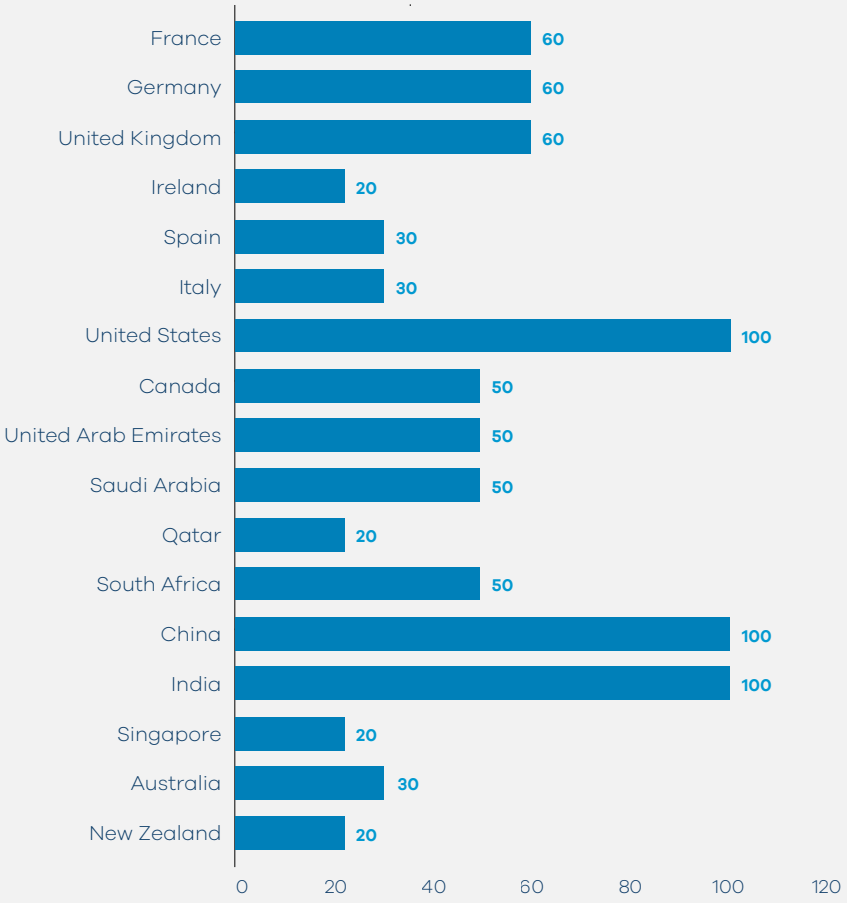
20. Growing need for trusted computing on untrusted hardware

Score: 74% – **Time to mature:** 3-5 years – **Most impacted domain:** Economic

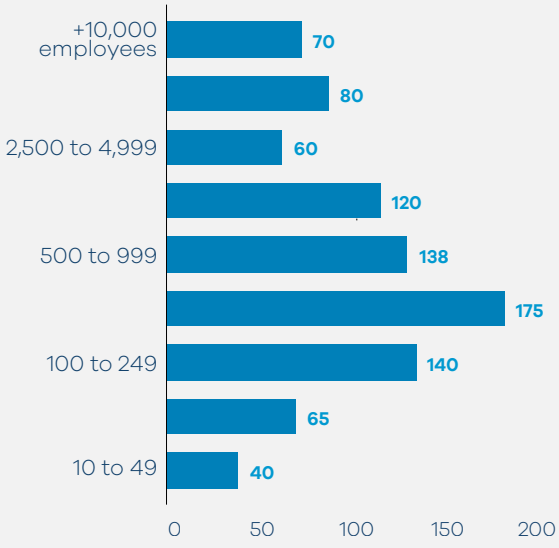
A growing gap between software trust requirements and increasingly opaque, outsourced, or backdoored hardware infrastructure raises systemic integrity concerns.

Appendix B: Survey results

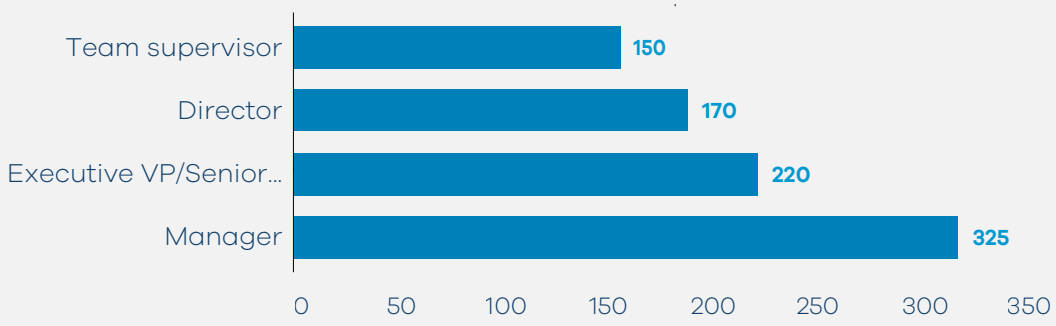
Distribution of survey respondents by country



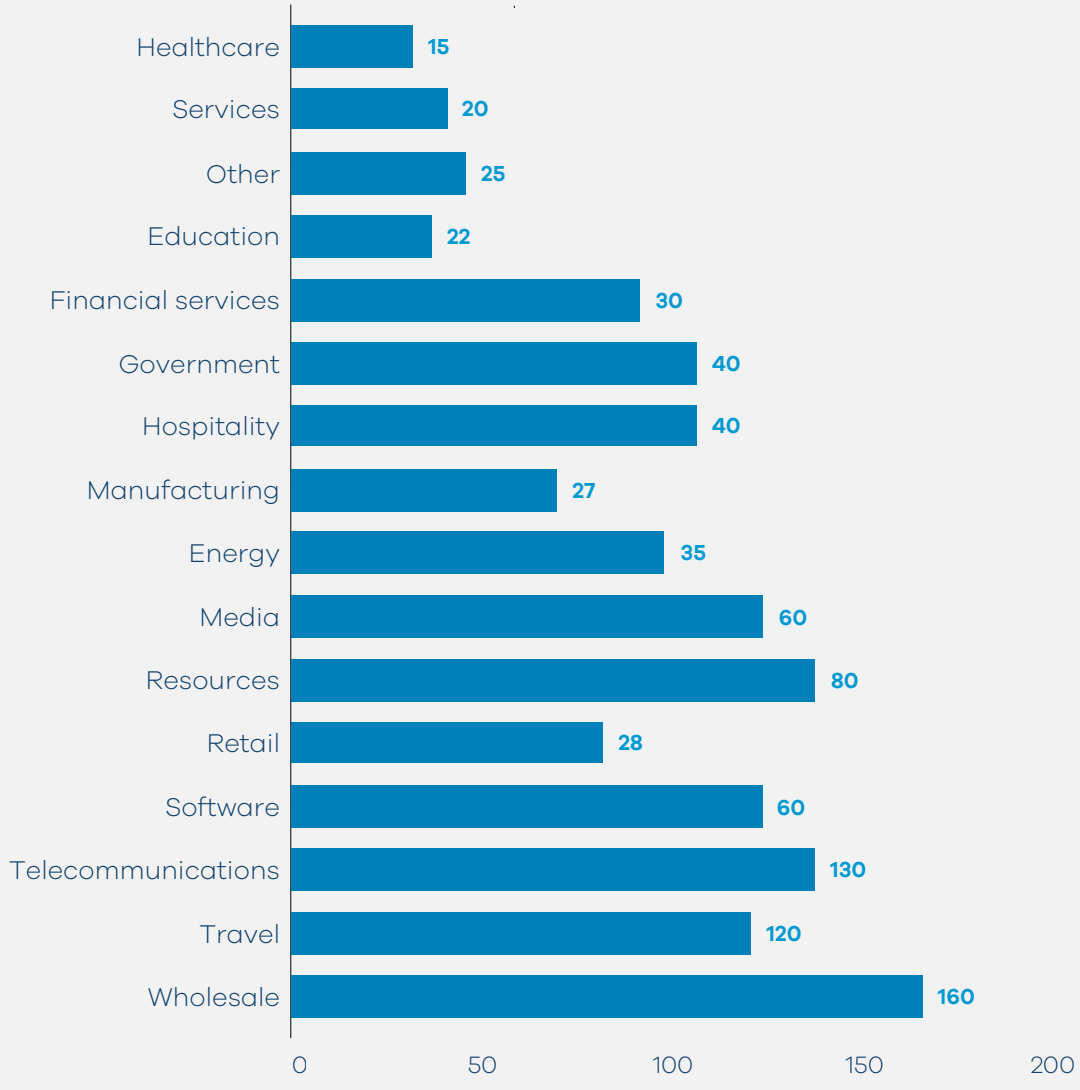
Distribution of survey respondents by organization size



Distribution of survey respondents by role



Distribution of survey respondents by industry



Appendix C: Methodology

The findings of this flagship report are grounded in a multi-layered methodology that integrates quantitative evidence, expert insights, and comparative research on emerging practices worldwide.

Global survey

- A survey of 870 cybersecurity leaders, practitioners and strategists across regions, sectors and organizational roles formed the backbone of the research.
- Respondents assessed the impact of emerging threats, key obstacles, and the effectiveness of national and organizational actions.
- Prior to launch, we conducted research on potential survey options to ensure comprehensive coverage of the relevant issues.

Trend prioritization

- A structured scoring process assessed each trend's potential impact across societal, political, and economic domains.
- Survey data and expert assessments were weighted to balance practitioner perspectives with strategic foresight, yielding the five key trends.

Expert engagement

- The survey findings were validated by structured interviews, closed-door roundtables, and multi-stakeholder workshops with representatives from government, industry, academia, and civil society.
- Exchanges provided nuance beyond quantitative data and surfaced innovative solutions already being piloted globally.

Comparative research

- A review of actions taken by leading nations and organizations – including frameworks, regulations, and case studies – highlighted best practices and persistent gaps in cybersecurity governance and resilience.
- These insights were cross-referenced with independent research from international organizations, think tanks, and industry associations to validate findings and reinforce credibility.

Endnotes

1. CrowdStrike Holdings, Inc. (2025). Global Threat Report.
2. Fortinet, Inc. (2025). Global Threat Landscape Report.
3. Johns Hopkins University — Center for Health Security (2021). The Economic and Health Costs of COVID-19 Misinformation.
4. Say No to Disinfo and Fenimore Harper. Can A.I. Cause a Bank Run? London: Fenimore Harper, 2025.
5. European Union (2024). Resilience of Democracy and European Elections against New Challenges.
6. Canadian Centre for Cybersecurity (2025).
7. The Japan Times (2025).
8. India Ministry of Electronics & IT (2025).
9. Cyberinfoblog (2024). Real-Case Analysis #29.
10. KOVVR. The UK Cost of the Europe CrowdStrike Incident.
11. Forbes (2025). CrowdStrike Outage Latest—Fixes, Uber Voucher Backlash And More.
12. BBC (2025). Delta Airlines Hits Out at CrowdStrike, Alleging $500m Loss.
13. IDC (2025). Agentic AI to Dominate IT Budget Expansion Over Next Five Years, Exceeding 26% of Worldwide IT Spending, and $1.3 Trillion in 2029.
14. Stanford-Vienna Transatlantic Technology Law Forum (2024). The EU's Digital Services Act and Its Impact on Online Platforms (No. 85).
15. IBEF (2025). TCS Inks Pact with Development of Advanced Computing (C-DAC) to Develop India's Sovereign Cloud Ecosystem.
16. SAP (2025). SAP Expands Australian Sovereign Cloud Capabilities as Part of Ongoing Public Sector Investment.
17. Javelin Strategy & Research (2022). Identity Fraud Scams Report.
18. NBC via CNBC (2025). "How Deepfake AI Job Applicants Are Stealing Remote Work." CNBC (via NBC Chicago).
19. Europol (2025). Criminal Network Distributing Fake Dark Web Documents Busted.

Endnotes

20. Lexis Nexis (2024). Three Million 'Frankenstein' Identities Pose a Multi-Billion Pound Fraud Threat to UK Businesses, New Research Shows. Gartner (2024).

21. "Gartner Predicts 30 Percent of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to Deepfakes by 2026." February 1.

22. India TV News (2025). Aadhaar to Use Advanced AI, ML to Curb Fraudulent Changes to Birth Dates, Biometrics, More.

23. European Commission (2021). European Digital Identity Framework Proposal.

24. Forbes Technology Council (2025). How Liveness Detection Can Help Outsmart Generative AI Threats.

25. GSMA (2025). Fraud and Scams: Staying Safe in the Mobile World.

26. World Economic Forum (2025). Global Cybersecurity Outlook.

27. IBM Security (2025). Cost of a Data Breach Report 2025.

28. National Conference of State Legislatures (2025). NCSL Task Force on Artificial Intelligence, Cybersecurity and Privacy.

29. FAA (2025). New ATM Requirement: Certification Framework for AI Technology.

30. European Commission (2024). AI Act.

31. USA Department of Homeland Security (2024).

32. Business Insider (2025). "Google Cloud Outage Brings Your Favorite Sites to a Standstill." June 12.

33. EMA (2024). IT Outages: Costs and Containment.

34. European Commission (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act).

35. Infocomm Media Development Authority (IMDA) — Singapore Government (2022). AI Verify–Testing Framework for AI Governance.

36. Japan Ministry of Economy, Trade and Industry (2023). Automated Driving Vehicle Approved as Automated Operation Level 4 System for the First Time in Japan.


GLOBAL
CYBERSECURITY
FORUM
Site