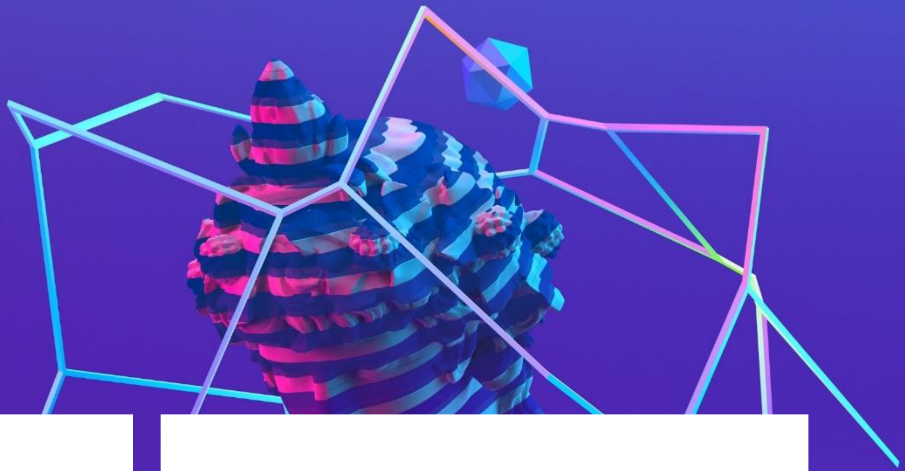
KPMG

Audit Committee Forum No.57

Embedding Trust in an AI-Driven World: Cybersecurity Insights 2025

Date: Tuesday 27 May 2025
Time: 1:00 p.m. – 2:30 p.m.

Contents



01

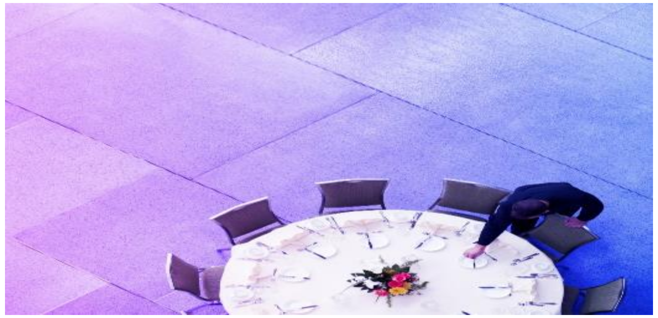
Cybersecurity Outlook

02

Reflections on a five-year journey (2020–2025)

03

Key Cybersecurity Considerations 2025



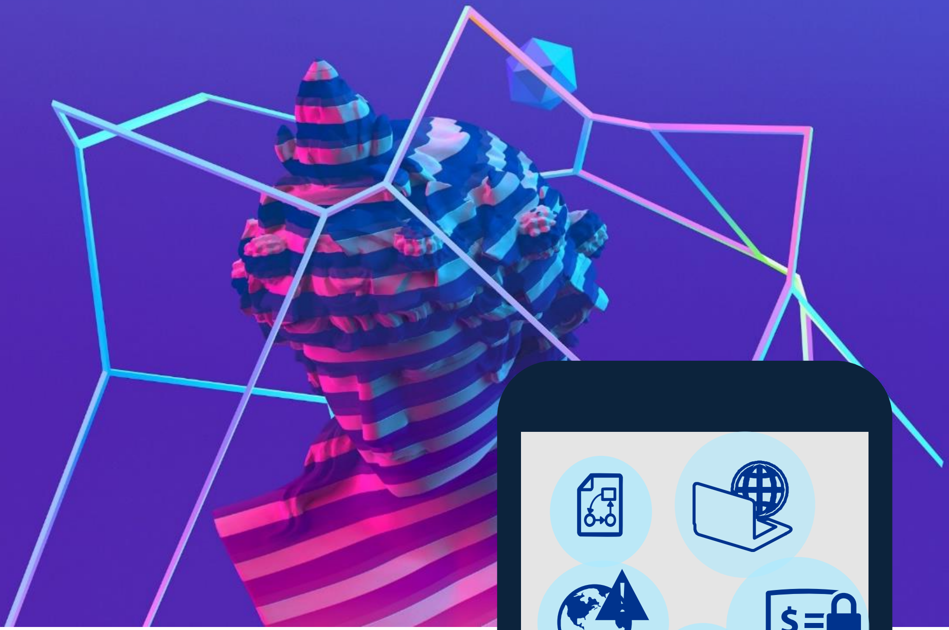
01

Cybersecurity Outlook

Mentimeter

Poll question

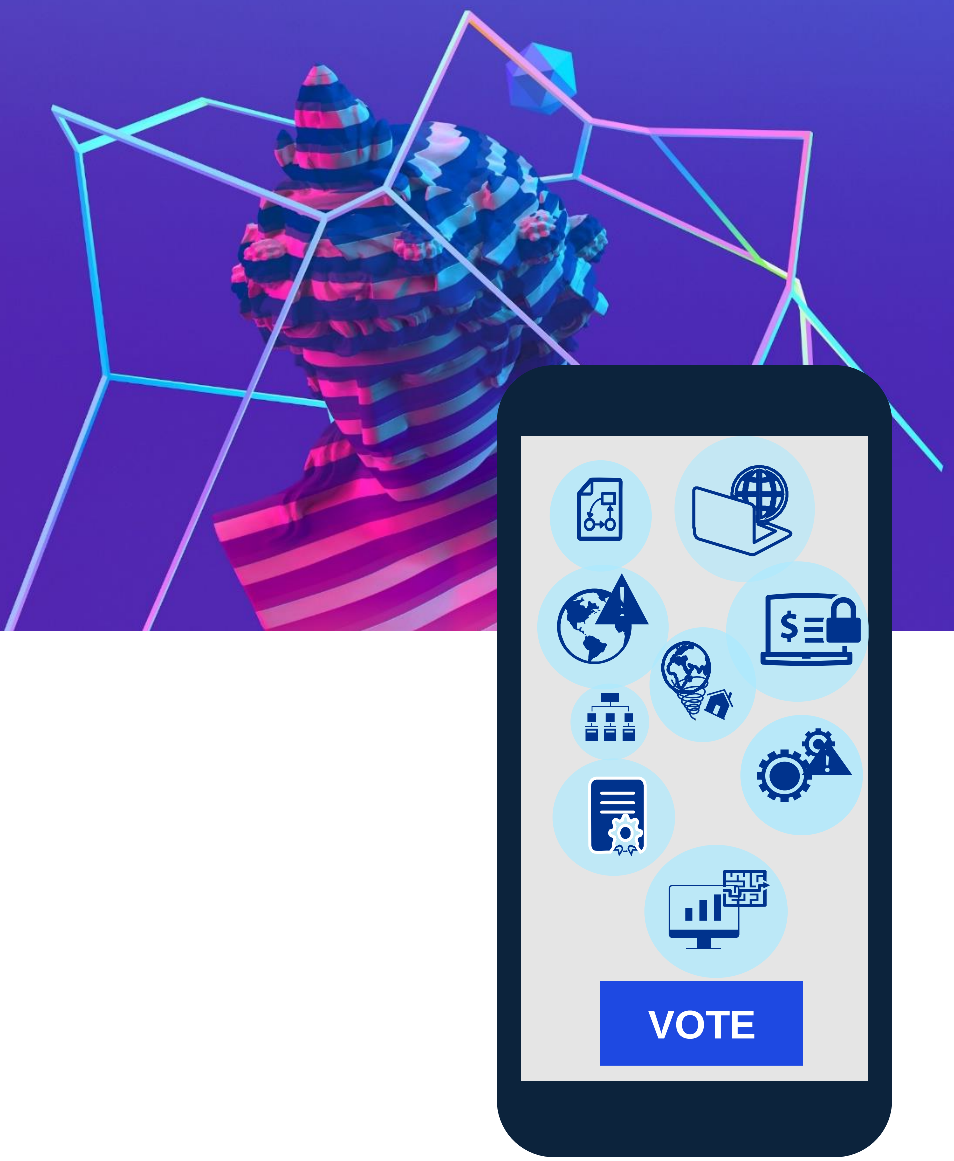
Which of the following do you believe will be the biggest cybersecurity challenge in 2025?



- Rapid adoption of emerging technologies
- Increasing sophistication of cybercrime (AI-driven threats)
- Supply chain vulnerabilities
- Expanding regulatory requirements
- Shortage of skilled cybersecurity professionals

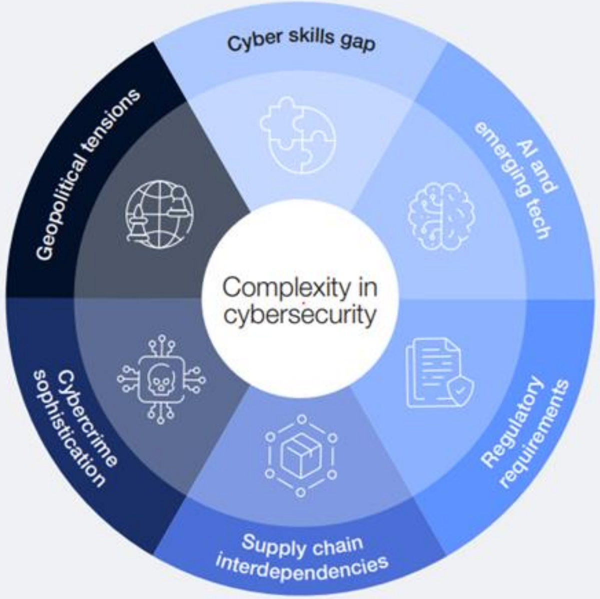
Poll Question

Do your organization well prepare for Cybersecurity?



- Very Confident
- Confident
- Neutral
- Not confident

Cybersecurity is becoming increasingly complex


Complexity in cybersecurity
Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions

Geopolitical tensions

Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication

72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies

With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements

78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech

66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

Cyber skills gap

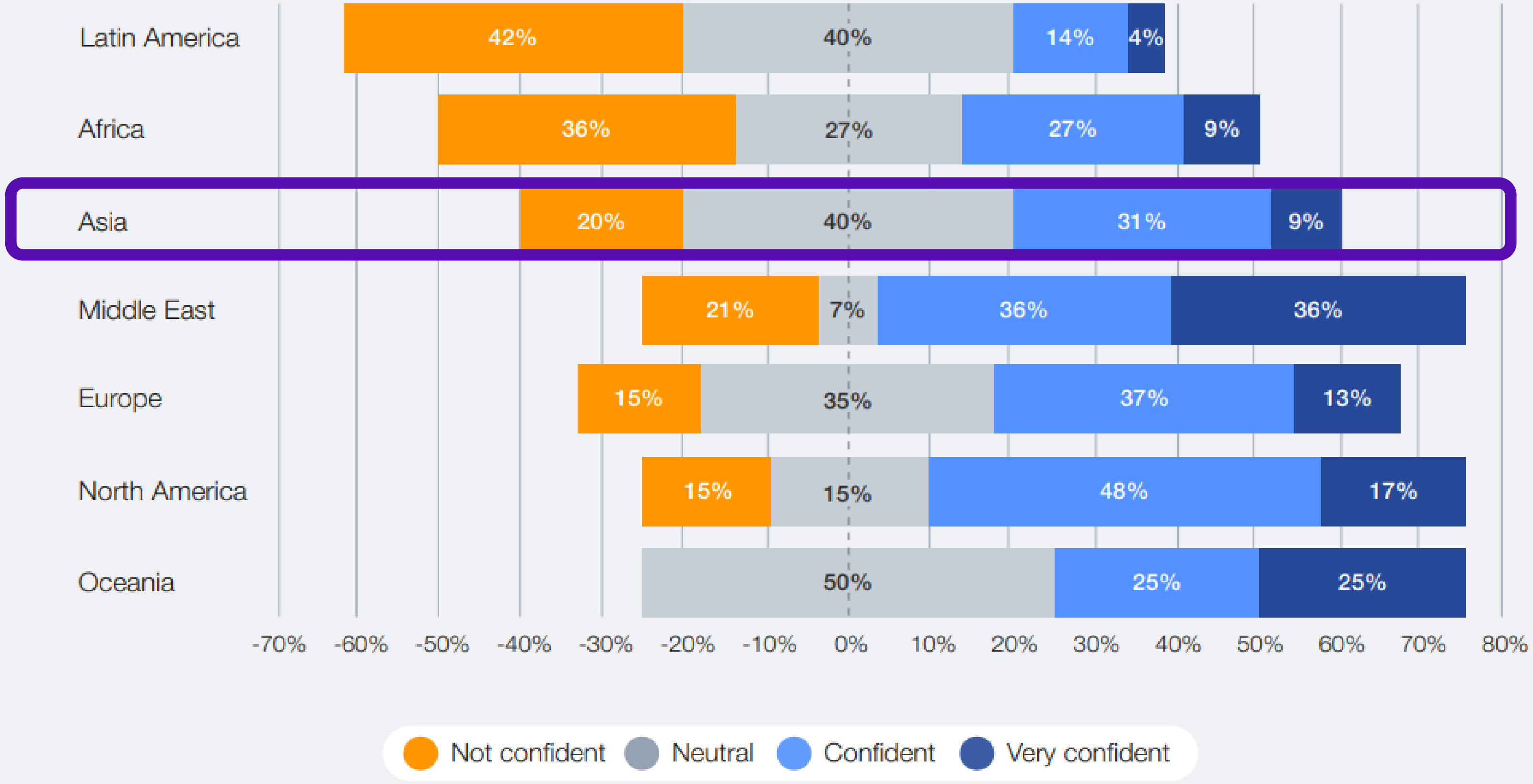
The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

KPMG

Reference: *Global Cybersecurity Outlook 2025 (World Economic Forum)*

Regional differences in cyber resilience

How confident are you that the country in which your organization is based is well prepared to respond to major cyber incidents targeting critical infrastructure?



Reference: *Global Cybersecurity Outlook 2025 (World Economic Forum)*

Cybersecurity is a top priority for CEOs

When asked to identify the top trends that could negatively impact their organization’s prosperity over the next three years, CEOs most highly ranked the cost of living, **cybercrime and cybersecurity issues, and talent**.

54% of CEOs say their organization is well-prepared for a cyberattack.

41% are unsure if they will be able to secure the talent and solutions they need to defend against AI threats.

37% of CEOs are unsure if their organization’s cybersecurity can keep pace with rapid AI advancements.

69% of CEOs are increasing their investments in cybersecurity to protect their operations and IP from AI threats.

Reference: *KPMG CEO Outlook 2024 (US and Asia Pacific)*

Top-of-mind Asia Pacific CEOs

16% SUPPLY CHAIN

14% EMERGING/ DISRUPTIVE TECHNOLOGY

12% CYBER SECURITY

02

Reflections on a five-year journey (2020–2025)

Recent cybercrime impact

Cybercrime costs

Y2024

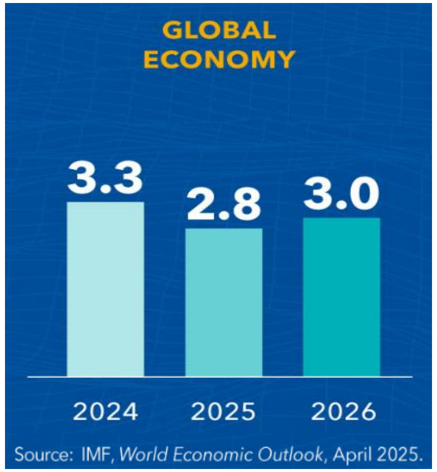
US$9.5 trillion

Y2025

US$10.5 trillion

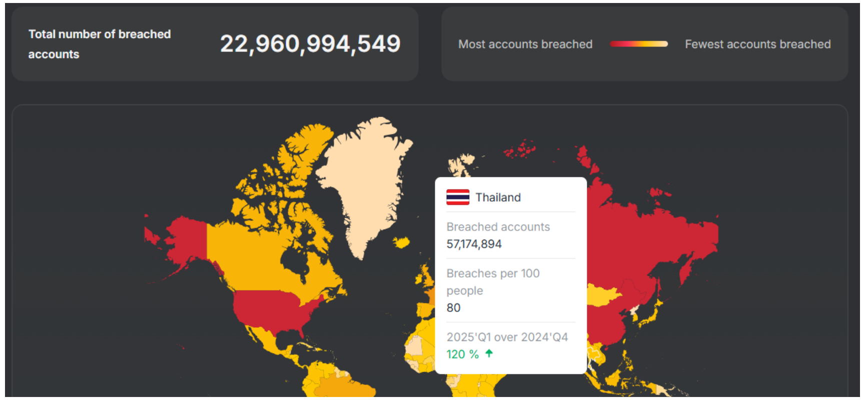
15% YoY

Source: Cybersecurity Ventures, Forbes



Source: IMF, *World Economic Outlook*, April 2025.

Number of breached accounts 22,960,994,549



Total number of breached accounts 22,960,994,549

Thailand

Breached accounts 57,174,894

Breaches per 100 people 80

2025'Q1 over 2024'Q4 120 %

Source: Surfshark Data Breach Monitoring as of 22 May 25

22.7%

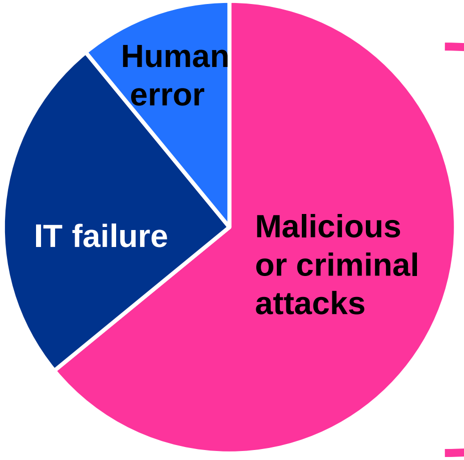
increase in the share of organizations paying fines of more than USD 50,000

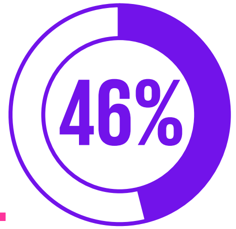
Source: IBM

US$5 million FY25

In 2024, the average cost of a data breach reached an all-time high of $4.88 million.

Root cause of the data breach





Advanced adversarial capabilities

ransomware, phishing, malware development, deepfakes

Data leaks

exposure of personally identifiable information through generative AI

Bangkok Post

NEWS THAILAND BUSINESS LIFE GURU LEARNING

Thailand tops region for ransomware attacks

Cybercriminals becoming increasingly sophisticated, warns cybersecurity firm

Thailand had the most ransomware attacks in Southeast Asia last year, according to the Russia-based cybersecurity company Kaspersky. The number of local threats, defined as threats from external devices such as USB flash drives, in Thailand ranked third in the region in 2023. “Thailand has become a major target for threat actors who are increasingly using different tactics to launch sophisticated attacks on businesses and organisations,” said Benjamas Chuthapiphat, territory manager for Thailand with Kaspersky. Personal data leaks have made headlines as both commercial and governmental service platforms have been compromised, she said. A sample of leaked data will be posted in dark-web marketplaces, with the criminals then attempting double or triple extortion for ransom.

Double extortion occurs when cybercriminals exfiltrate data before carrying out the encryption. By exfiltrating the data, the attackers can demand a ransom in exchange for not publicly releasing or selling the data or selling it. Triple extortion adds another layer of pressure on the victim, such as encrypting more of an organisation’s material and demanding money to decrypt it. Other common threats include phishing and smishing scams to download and install malware on personal and corporate devices. Phishing involves sending messages purporting to be from reputable sources in order to induce individuals to reveal personal information. Smishing scams involve contact from an unknown number, often claiming to be from a reputable business.

Thailand had the most ransomware attacks in Southeast Asia last year, according to the Russia-based cybersecurity company Kaspersky. The number of local threats, defined as threats from external devices such as USB flash drives, in Thailand ranked third in the region in 2023.

“Thailand has become a major target for threat actors who are increasingly using different tactics to launch sophisticated attacks on businesses and organisations,”.

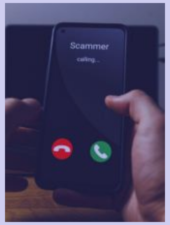
Personal data leaks have made headlines as both commercial and governmental service platforms have been compromised, she said. A sample of leaked data will be posted in dark-web marketplaces, with the criminals then attempting double or triple extortion for ransom.

Double extortion occurs when cybercriminals exfiltrate data before carrying out the encryption. By exfiltrating the data, the attackers can demand a ransom in exchange for not publicly releasing or selling the data or selling it. Triple extortion adds another layer of pressure on the victim, such as encrypting more of an organisation’s material and demanding money to decrypt it.

Other common threats include phishing and smishing scams to download and install malware on personal and corporate devices. Phishing involves sending messages purporting to be from reputable sources in order to induce individuals to reveal personal information. Smishing scams involve contact from an unknown number, often claiming to be from a reputable business. Businesses and organisations in Thailand have also been exposed to critical cyber-attacks, said Ms Benjamas.

Nation hit by surge in scams, financial fraud

Thailand one of top three in Asia Pacific



Thailand was one of the top three countries in the Asia-Pacific region to suffer a significant surge in financial fraud scams last year, according to Google's Bad Apps Report.

"**we saw a significant rise in scams and financial fraud. Notably, Singapore, Thailand and India saw a significant surge in financial fraud scams**," said Aman Dayal, head of trust & safety operations for Asia-Pacific at Google Play, during an online media roundtable on the report.

The Asia-Pacific region is a hotbed for scams as it has one of the highest smartphone penetration rates in the world at over 90%, with many of the users utilising their phone to make transactions.

กรุงเทพธุรกิจ

ข่าวทั่วไป การเมือง เศรษฐกิจ-ธุรกิจ การเงิน-การลงทุน sustainability อสังหาริมทรัพย์ ยานยนต์ เทคโนโลยี ต่างประเทศ สุขภาพ-คุณภาพชีวิต ไลฟ์สไตล์

เปิดเคสมิจฉาชีพใช้ ‘AI’ สร้างตัวตนเสมือนจริง หลอกผ่านแชตและวิดีโอคอล

❑ ในช่วงครึ่งแรกของปีนี้ คดีหลอกลวงทางไซเบอร์ในฮ่องกงเพิ่มขึ้น 31 เปอร์เซ็นต์ โดยมีการสูญเสียเงินกว่า 2.66 พันล้านดอลลาร์ฮ่องกง

❑ เป็นที่ยอมรับกันอย่างกว้างขวางว่า Generative AI ทำให้การสร้างลิงก์ฟิชชิง การเข้าถึงหรือขโมยข้อมูลทำได้ง่ายขึ้น ส่งผลให้เกิดการหลอกลวงเพิ่มขึ้นตาม

❑ พนักงานคนหนึ่งถูกชักจูงให้โอนเงิน หลังจากประชุมทางวิดีโอ จนสูญเสียเงินเกือบ 900 ล้านบาท โดยต่อมา พนักงานคนนั้นพบว่า ตัวเองเป็น “มนุษย์คนเดียวที่แท้จริง” ในการประชุม

ท่ามกลาง “**เทคโนโลยีปัญญาประดิษฐ์**” (AI) ที่ถูกนำมาใช้เป็นเครื่องมือทุ่นแรงมนุษย์และทำให้ชีวิตราบรื่นขึ้น แต่ในอีกด้านหนึ่งของเหรียญ เทคโนโลยีนี้กำลังทำให้มิจฉาชีพทางไซเบอร์ร้ายกาจยิ่งกว่าเดิม เพราะ AI ช่วยให้ปลอมแปลงตัวตนบุคคลได้อย่างแนบเนียนราวกับของจริง ผ่านการเรียนรู้พฤติกรรมเป้าหมายซ้ำแล้วซ้ำเล่า จนยากที่จะแยกแยะความจริงจากความเท็จ ความเปลี่ยนแปลงที่เห็นคือ แต่ก่อนเรากังวลถึง “ภาพ” ตัดต่อ แต่ในปัจจุบันเทคโนโลยีได้ก้าวกระโดดไปอีกขั้น เมื่อ “วิดีโอ” ที่เราเห็นก็สามารถถูกตัดต่อได้อย่างแนบเนียนเสมือนจริง การสนทนาทางวิดีโอกลายเป็นเรื่องที่ต้องระวังตัวมากขึ้น เพราะบุคคลที่ปรากฏบนหน้าจออาจไม่ใช่ตัวจริง แต่เป็นเพียงภาพลวงตาที่สร้างขึ้นจากเทคโนโลยี Deepfake ซึ่งเลียนแบบบุคคลอื่นได้คล้ายตัวจริง

The Hacker News

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Store Contact

Microsoft Warns of Surge in Cyber Attacks Targeting Internet-Exposed OT Devices

Microsoft has emphasized the need for securing internet-exposed operational technology (OT) devices following a spate of cyber attacks targeting such environments since late 2023.

"These repeated attacks against OT devices emphasize the crucial need to improve the security posture of OT devices and prevent critical systems from becoming easy targets," the Microsoft Threat Intelligence team said.

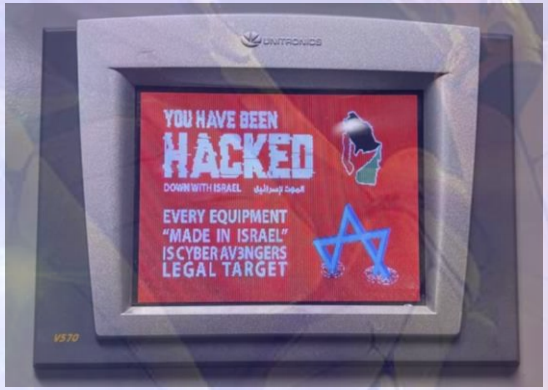
The company noted that a cyber attack on an OT system could allow malicious actors to tamper with critical parameters used in industrial processes, either programmatically via the programmable logic controller (PLC) or using the graphical controls of the human-machine interface (HMI), resulting in malfunctions and system outages.

It further said that OT systems often lack adequate security mechanisms, making them ripe for exploitation by adversaries and carry out attacks that are "relatively easy to execute," a fact compounded by the additional risks introduced by directly connecting OT devices to the internet.

This not only makes the devices discoverable by attackers through internet scanning tools, but also be weaponized to gain initial access by taking advantage of weak sign-in passwords or outdated software with known vulnerabilities.

OT systems, which control real-world critical processes, present a significant target for cyberattacks.

These systems are prevalent across various industries, from building heating, ventilation, and air conditioning (HVAC) systems, to water supply and power plants, providing control over vital parameters such as speed and temperature in industrial processes. A cyberattack on an OT system could transfer control over these critical parameters to attackers and enable malicious alteration that could result in malfunctions or even complete system outages, either programmatically via the programmable logic controller (PLC) or using the graphical controls of the human machine interface (HMI).


UNITRONICS
YOU HAVE BEEN HACKED
DOWN WITH ISRAEL
EVERY EQUIPMENT "MADE IN ISRAEL" IS CYBERAV3NGERS LEGAL TARGET
V570

The potential damage of attacks on OT systems are their often-lacking security measures

Many OT devices, notwithstanding common security guidelines, are directly connected to the internet, making them discoverable by attackers through internet scanning tools. Once discovered by attackers, poor security configurations, such as weak sign-in passwords or outdated software with known vulnerabilities, could be further exploited to obtain access to the devices.

Microsoft's analysis of multiple attacks by these actors revealed a common attack methodology: focusing on internet-exposed, poorly secured OT devices. This report will illustrate this attack methodology using the high-profile case of the November 2023 attack against Aliquippa water plant, for which CISA released an advisory in December 2023. CISA attributed the attack to the Islamic Revolutionary Guard Corps (IRGC)-affiliated actor "CyberAv3ngers", tracked by Microsoft as Storm-0784. Microsoft assesses that the same methodology has been utilized by other OT-focused threat actors in multiple other attacks as well.

The Aliquippa case: A high-profile OT attack

In late November 2023, the Aliquippa water plant was affected by a cyberattack that resulted in the outage of a pressure regulation pump on the municipal water supply line in Aliquippa, Pennsylvania. In addition to impairing functionality, the attack, which targeted a PLC-HMI system by Israeli manufacturer Unitronics, also defaced the device to display a red screen with the name and logo of the "CyberAv3ngers" actor.

NBC NEWS

POLITICS U.S. NEWS WORLD BUSINESS SHOPPING TIPLINE HEALTH SPORTS CULTURE & TRENDS • WATCH LIVE

Russian Hackers Sandworm Cause Power Outage in Ukraine Amidst Missile Strikes

A Ukrainian government official said Thursday that Russian military hackers caused a power outage in parts of Ukraine last year, a previously unpublicized cyberattack that adds to concerns about the vulnerability of critical infrastructure.

It is unclear how many people or places were without power or for how long.

The attack, which happened in October last year, is only the third known time that hackers successfully penetrated an energy system and caused a power outage. The other two incidents, in 2015 and 2016, were also in Ukraine, and the perpetrators have been widely attributed to the same unit in Russia's military intelligence agency, the GRU.

Details of the hack are complicated by the fact that much of Ukraine was under missile attacks around the same time. Russia physically damaged some of the infrastructure, making it even more difficult for responders to restore power.

Victor Zhora, head of Ukraine's cyber defense agency, told NBC News that it was an example of Russia coordinating its cyberattacks and kinetic attacks against the same target.

"They focus on the energy sector, on critical infrastructure. They strike it with cruise missiles, and they will continuously attempt to hit with cyber tools," he said. "That's the trend, that they are focusing on civilian targets.

Mandiant, a cybersecurity company owned by Google, also released a report on the incident Thursday.

Zhora and Mandiant declined to share many specifics about the attack, including the precise nature of the facility that was hacked, where it was located or how many people or places lost power because of it.

The Russian Foreign Affairs Ministry didn't respond to an emailed request for comment.

Many countries including the United States, China and Russia routinely engage in spying and espionage, but successful cyberattacks on the power grid are extremely rare. Destructive cyberattacks on critical infrastructure could be seen as an act of war.

The computer operating systems for industrial machinery are often highly specialized and can be confusing to hackers who might gain access, making it unlikely for anyone but a large, dedicated and well-resourced hacker group affiliated or working on behalf of a government to be able to pull off such an attack.

During its invasion of Ukraine, Russia has damaged far more power infrastructure with missiles rather than with cyberattacks.

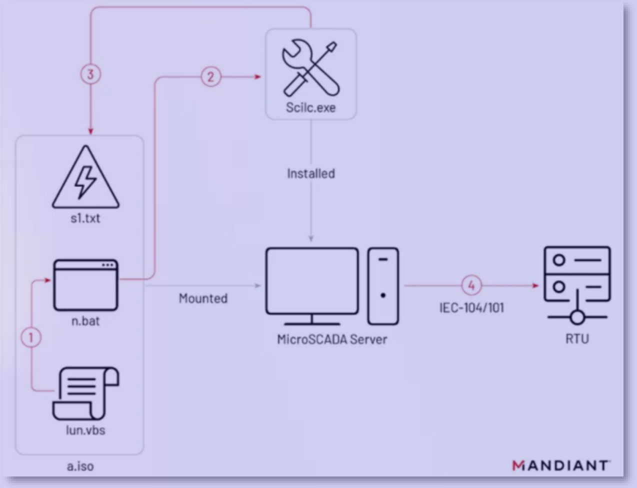
While the U.S. has never fallen victim to such a cyberattack, federal officials have warned of the possibility that its adversaries could launch one. This summer, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, said that China likely had such capabilities and could deploy them against the U.S. in times of major conflict, like if it were to invade Taiwan.

In April last year, Ukraine said it had successfully thwarted a major cyberattack that could have cut power to 2 million people.

"That case was a signal for all of us that we should work harder and improve the situation immediately because it can cause real issues for all of us," Zhora said.

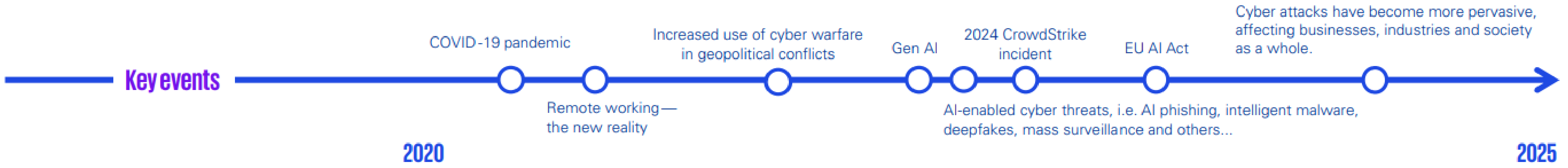
Ukraine is redoubling efforts to protect power infrastructure from hackers because it fears Russia will continue to attack as the weather turns cold, Zhora said.

"I hope that we use this year to become more prepared, to expect attacks during this autumn and winter," he said.



The attacks, which spanned several months and culminated in two disruptive events on October 10 and 12 last year, as a "novel technique" for impacting industrial control systems (ICS) and OT.

Reflections on a five-year journey (2020–2025)


Key events
COVID-19 pandemic
Remote working — the new reality
Increased use of cyber warfare in geopolitical conflicts
Gen AI
2024 CrowdStrike incident
EU AI Act
AI-enabled cyber threats, i.e. AI phishing, intelligent malware, deepfakes, mass surveillance and others...
Cyber attacks have become more pervasive, affecting businesses, industries and society as a whole.
2020
2025

Key themes

Strategy and leadership	• The CISO has become a trusted internal advisor and operational leader.	• Moving the conversation from cost and speed to strategic and effective security. • CISOs budgets increasingly tied to risk reduction for the business.	• As cyber becomes more pervasive across the organization, the pressure on the CISO to deliver increases. • The CISO role disperses but accountability increases partially due to regulatory developments.
People and talent	• Security teams are transforming into a key resource with a relevant voice at the strategy table.	• Cyber exists to support not hinder — from organizational enforcers to influencers. • Weaving cyber into the organizational fabric.	• The cyber skills gap persists — AI might offer some viable solutions, but the workforce needs new skills to adapt and adopt.
Technology and data	• New virtual infrastructure models and collaboration tooling. • Accelerated cloud transformation (due to COVID-19) but security was an afterthought. • Traditional identity authentication and management (IAM).	• Enhanced security through automation. • Rapid advancements in Gen AI create excitement around use cases in cyber. • Securing a perimeter-less and data-centric world. • Placing identity at the heart of zero trust.	• Investment in AI for cyber becomes more strategic and forward-looking. • Enterprise-wide cost-saving, efficiency, security and innovation (especially AI implementation) drive platform consolidation. • The rise of digital identities and deepfakes.
Digital trust	• Cyber and privacy regulations focus on business priorities and responsibilities — the importance of trust.	• Digital trust is a shared responsibility that starts with the business and involves multiple stakeholders, e.g. CISO, DPO, CDO, CIO, etc.	• Embedding trust as AI pierces all fabrics of business and society — focus on security, privacy, safety, ethics, etc.
Resilience	• From scenario-to impact-based — focus on critically and regulation.	• No longer just about prevention — focus on response and recovery.	• CISOs continue to build on resilience as cyber threats have evolved from tech risks to business and industry threats, with potential harm to society.

03

Key Cybersecurity Considerations 2025

Audit committees and cybersecurity: Adapting to change

Why should the organization focus on cybersecurity?

The increasing sophistication of **cyber threats**

The adoption of new technology platforms

- **AI-driven attacks:** Cybercriminals are leveraging artificial intelligence to create sophisticated attacks, including deepfakes and advanced phishing schemes.
- **Applying AI to cyber defense:** AI can sift through massive data sets in real time, derive actionable insights and be trained to take automatic defensive actions.

The ever-growing **volume of sensitive data** constantly moving across interconnected and integrated networks

Audit committees and cybersecurity: Adapting to change

The role of audit committee

Oversight of compliance with evolving AI and privacy laws and regulations.

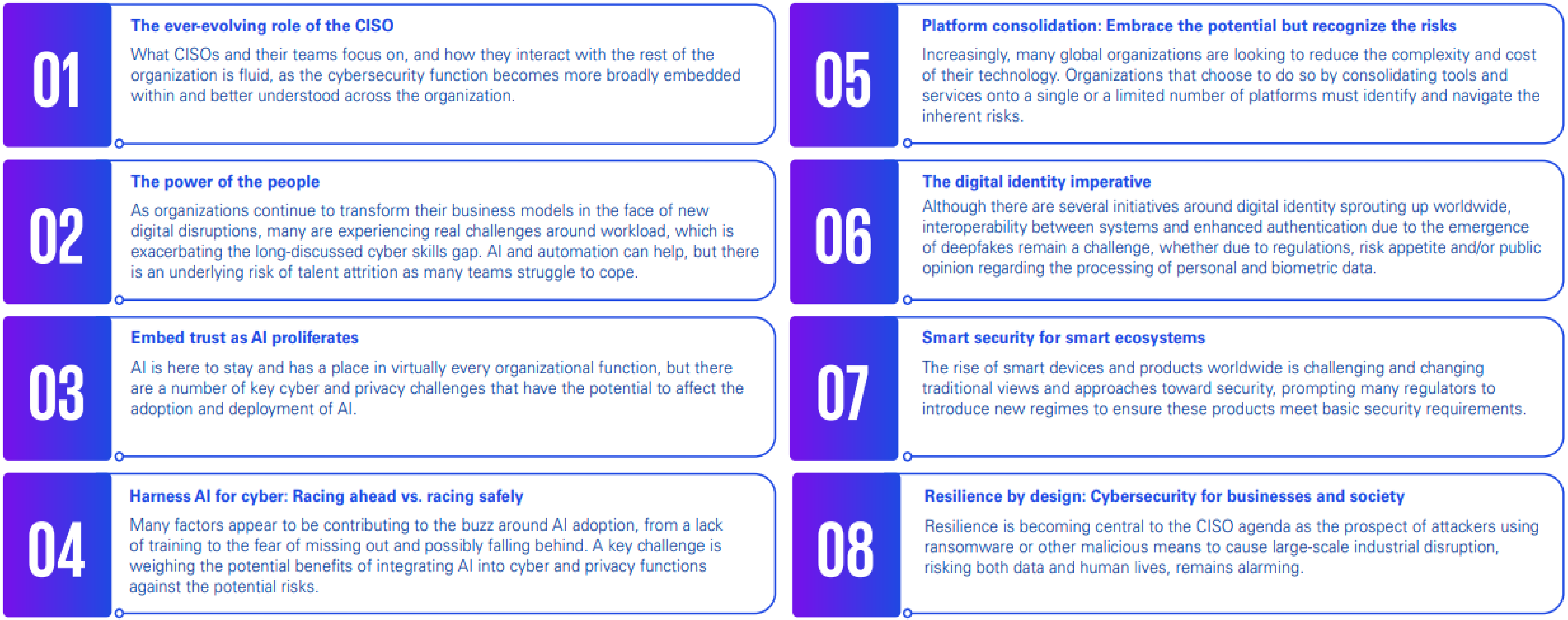
Ensure the organization are using **AI safely and securely.**

Question management on **how they're dealing with the unauthorized and ungoverned use of AI.** Ensure management has appropriately evaluated AI security.

Ensure the **cybersecurity basic practices** are firmly in place and effectively managed.

Encourage management to implement **cybersecurity exercises** between offensive and defensive cybersecurity teams.

Key Cybersecurity Considerations for 2025



01

The ever-evolving role of the CISO

What CISOs and their teams focus on, and how they interact with the rest of the organization is fluid, as the cybersecurity function becomes more broadly embedded within and better understood across the organization.

02

The power of the people

As organizations continue to transform their business models in the face of new digital disruptions, many are experiencing real challenges around workload, which is exacerbating the long-discussed cyber skills gap. AI and automation can help, but there is an underlying risk of talent attrition as many teams struggle to cope.

03

Embed trust as AI proliferates

AI is here to stay and has a place in virtually every organizational function, but there are a number of key cyber and privacy challenges that have the potential to affect the adoption and deployment of AI.

04

Harness AI for cyber: Racing ahead vs. racing safely

Many factors appear to be contributing to the buzz around AI adoption, from a lack of training to the fear of missing out and possibly falling behind. A key challenge is weighing the potential benefits of integrating AI into cyber and privacy functions against the potential risks.

05

Platform consolidation: Embrace the potential but recognize the risks

Increasingly, many global organizations are looking to reduce the complexity and cost of their technology. Organizations that choose to do so by consolidating tools and services onto a single or a limited number of platforms must identify and navigate the inherent risks.

06

The digital identity imperative

Although there are several initiatives around digital identity sprouting up worldwide, interoperability between systems and enhanced authentication due to the emergence of deepfakes remain a challenge, whether due to regulations, risk appetite and/or public opinion regarding the processing of personal and biometric data.

07

Smart security for smart ecosystems

The rise of smart devices and products worldwide is challenging and changing traditional views and approaches toward security, prompting many regulators to introduce new regimes to ensure these products meet basic security requirements.

08

Resilience by design: Cybersecurity for businesses and society

Resilience is becoming central to the CISO agenda as the prospect of attackers using ransomware or other malicious means to cause large-scale industrial disruption, risking both data and human lives, remains alarming.

Reference: https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025.html

8 ประเด็นความปลอดภัยทางไซเบอร์องค์กร: ปรับกลยุทธ์รับความเสี่ยงปี 2025

Embed trust as AI proliferates

Embed trust as AI proliferates

Establish AI governance to build trust

As AI use grows, concerns over bias, data misuse and lack of transparency are driving the need for strong governance, accountability and ethical oversight to ensure trustworthy adoption.

Strengthen data management for reliable AI

AI outcomes heavily rely on data quality, yet many organizations lack mature data governance. Agile, automated and organization-wide data practices are essential to ensure reliable, secure AI performance.

Align with evolving AI regulations

New regulations like the EU AI Act reflect global momentum toward enforcing responsible AI. Companies must monitor these changes and embed AI governance into daily operations to maintain compliance and public trust.

Manage a broad spectrum of AI risks

AI introduces technical, legal, operational and safety risks — from biased outputs and privacy violations to shadow AI and compliance challenges. Proactive monitoring and clear policies are critical to manage internal and third-party AI systems.

Suggested actions

Unite cross-functional stakeholders to update policies and align strategies for managing AI-related risks and impacts.

Understand AI-related regulatory requirements, develop and communicate clear AI usage policies, standards and procedures.

Enhance governance by establishing clear AI policies, identify risks, apply controls, and manage AI-related incidents.

Example of AI around us

Call center automation

Utilizing artificial intelligence to enhance customer service by automating interactions and managing a higher volume of inquiries across various channels.

Social media

Social media uses AI to increase personalization and efficiency while delivering relevant content to users.

Algorithmic trading

The use of algorithms and machine learning techniques to analyze vast amounts of data and identify patterns and trends in the market.

Language translation

Provide accurate translations in real-time for text, speech and images.

Generative AI

The use of generative models to produce text, images, videos or other forms of data.

Deepfake

AI is used to convincingly replace a person's likeness with another's or to make them say or do something they didn't.

Generative AI

GenAI remains a top investment priority, but data, workforce, and governance readiness along with a lack of regulations are implementation challenges.

68%

of US CEOs say GenAI is a **top investment priority** despite uncertain economic conditions.

68%

of CEOs expect to see return from their investments in GenAI in **three to five years**

21%

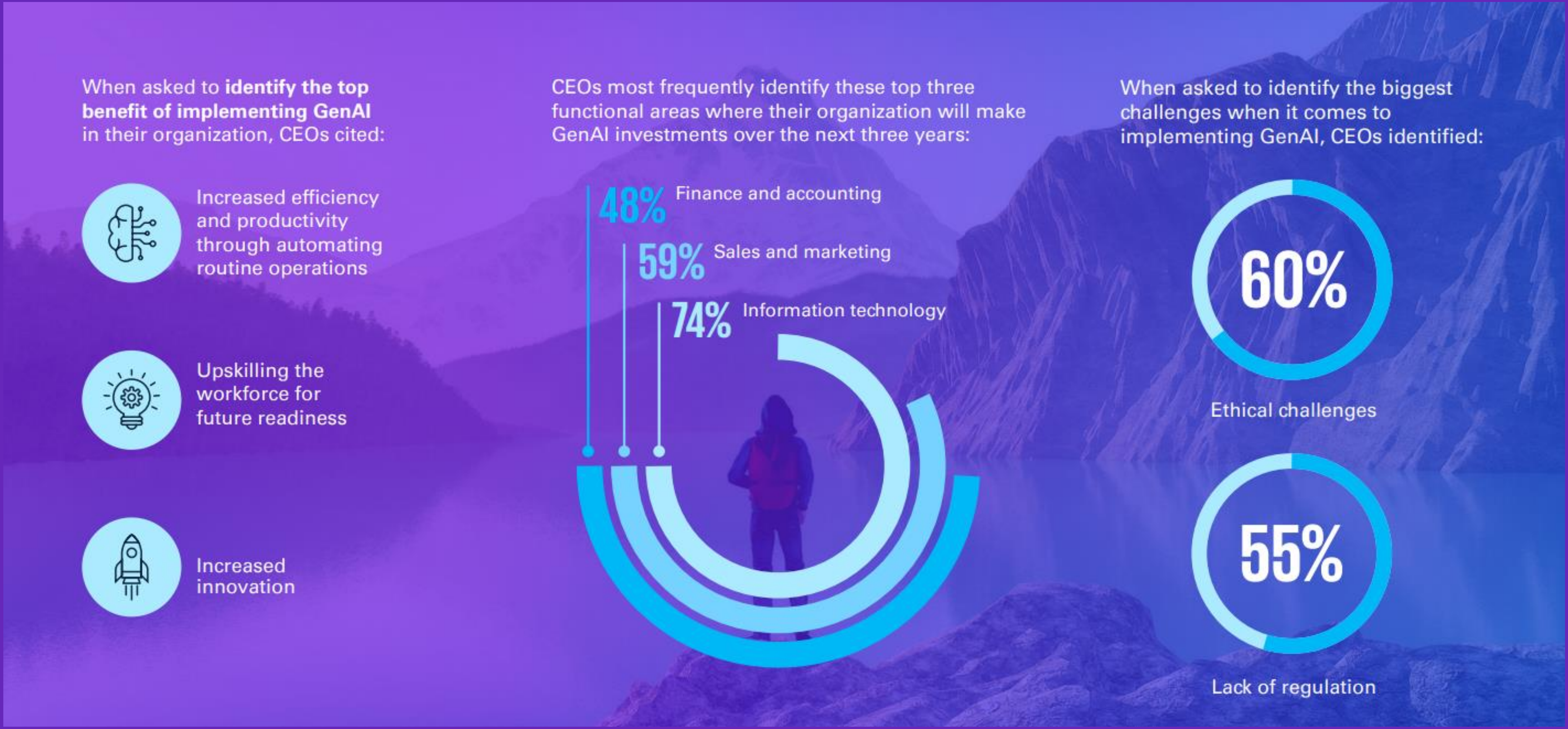
of CEOs expect to see returns in just **one to three years**

When thinking about their growth and transformation objectives, the majority of CEOs are placing capital investment in:

buying new technology 60%

developing their workforce's skills and capabilities 40%

Generative AI investment



When asked to **identify the top benefit of implementing GenAI** in their organization, CEOs cited:

- Increased efficiency and productivity through automating routine operations
- Upskilling the workforce for future readiness
- Increased innovation

CEOs most frequently identify these top three functional areas where their organization will make GenAI investments over the next three years:

When asked to identify the biggest challenges when it comes to implementing GenAI, CEOs identified:

Real-world cybersecurity in the financial services sector

Regulatory pressure and risk volume: Financial institutions face growing regulatory demands and an overwhelming volume of vulnerabilities, requiring consistent and systematic risk management.

AI/ML-Powered Solutions: KPMG developed ML-driven tools to automate vulnerability triage, assignment and prioritization, enhancing efficiency and regulatory compliance.

Built-in compliance and visibility: AI models include embedded compliance checks and maintain transparency for human oversight, aligning with regulatory expectations.

Stronger cybersecurity posture: Proactive adoption of these solutions allows faster vulnerability response, broader risk coverage, and improved resilience in a challenging cybersecurity environment.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Building Trust in AI

Fairness
Design models to reduce or eliminate bias against individuals, communities or groups

Privacy
Design AI solutions that comply with data privacy, regulations and consumer data usage

Transparency
Include responsible disclosure to provide stakeholders a clear understanding as to what is happening within the AI solution and across the AI lifecycle

Sustainability
Design AI solutions to limit negative environmental impact where possible

Explain-ability
Develop and deliver AI solutions in a way that answers the questions of how and why recommendations are made or conclusions drawn

Data integrity
Data used in AI solutions is acquired in compliance with regulations and are assessed for accuracy, completeness and quality

Accountability
Human oversight and responsibility embedded across the AI lifecycle to manage risk and comply with regulations and applicable laws

Reliability
AI systems perform at the desired level of precision and consistency

Security
Safeguard against unauthorized access, bad actors, misinformation, corruption or attacks

Safety
Safeguard AI solutions against harm to humans and/or property

Reference: kpmg-trusted-ai-approach.pdf

Rising global regulatory guidelines for AI

US

US: AI Bill of Rights (2022)

National Institute of Standards and Technology - AI Risk Management Framework (2022)

US: The American AI Initiative (2019); Algorithmic Accountability Act (2019); State and Local policies; DOD AI Strategy (2019)

(2019): The National AI R&D Strategic Plan

NYC AI Hiring Act (2023)

Latin America

Mexico: 'Towards an AI Strategy in Mexico' white paper released (2018); no dedicated strategy yet; also has IA2030 Coalition that works with the government on AI

Brazil -E-Digital Strategy, digital transformation strategy addresses AI (2018);

Brazil, Argentina, Peru, Colombia, Costa Rica follow OECD principles on AI (2019)

Africa and Middle East

Kenya: Blockchain and AI taskforce (2018)

Tunisia: AI Task Force (2018)

South Africa: Sector specific initiative launched by Government for AI (2018)

Dubai – AI Ethics Principles and Guidelines (2018)

Europe

EU: EU Artificial Intelligence Act (2021), Digital Services Act & Digital Markets Act

Finland: Released three reports 2017-19; last report focusses on ethics

Sweden: National Approach for AI (2018); launched national center for AI innovation (2019)

Denmark: Strategy for Digital Growth (2018); National AI Strategy (2019)

UK: AI Sector Deal in (2018)

Germany: National AI strategy (2018)

France: AI for humanity (2018)

Austria: Council on Robotics and AI (2017)

Spain: RDI Strategy in Artificial Intelligence (2019)

Italy: 'AI at the Service of Citizens' (2018); lab for AI created (2018)

Poland: 'Roundtable on AI strategy (2018)

Malta: Malta AI strategy Public Consultation (2019)

Estonia: Kraft Report (2019); AI taskforce (2018)

Netherlands: General Principles for the use of AI in Financial Sector (2019)

Japan

Japan: AI Technology Strategy (2017) (part of Japan's Society 5.0 initiative); AI made a part of integrated innovation strategy (2018)

Asia

Singapore: Principles to promote FEAT in the use of AIDA in Singapore's financial sector (2018)

China – Beijing AI Principles Publication (2019)

Hong Kong (SAR), China – Ethical Accountability Framework Publication (2018)

Thailand – AI Governance Guideline, ETDA (2023)

Thailand – Generative AI Governance Guidance, AIGC (2024)

Thailand – AI Guidelines for Financial Sector, SEC (2023)

Australia

Publication: AI Ethics Framework Discussion Paper (2019)

Rising global regulatory guidelines for AI

Core governance principle	Fairness	Explainability	Integrity of data	Security & resiliency	Accountability	Privacy	Risk approach
Global regulatory guidance							
National AI Initiative Act	✓	✓	✓	✓		✓	✓
AI in Government	✓		✓	✓	✓		
The National AI Research Resource Task Force				✓	✓	✓	
NIST AI Risk Framework	✓	✓	✓	✓	✓	✓	✓
FHFA AB 2020-02	✓	✓	✓	✓	✓	✓	✓
NAIC Principles on AI	✓	✓		✓	✓	✓	✓
Federal Trade Commission	✓		✓		✓		
EU Artificial Intelligence Act	✓	✓	✓	✓	✓	✓	✓
EU Digital Services Act	✓			✓	✓	✓	✓
OECD Principles	✓	✓			✓	✓	✓
Social Principles of Human Centric AI	✓	✓		✓		✓	
AIST ML Quality Management Guideline	✓	✓		✓		✓	
Brazilian AI Strategy	✓	✓				✓	
Brazilian AI Bill		✓					
AI National Policy (Chile)		✓		✓		✓	
AI National Plan (Argentina)	✓			✓		✓	
AI Governance Guideline, ETDA	✓	✓	✓	✓	✓	✓	✓
Generative AI Governance Guidance, AIGC	✓	✓			✓		✓
AI Guidelines for Financial Sector, SEC	✓	✓	✓	✓	✓	✓	✓

Harness AI for cyber: Racing ahead vs. racing safely

Harness AI for cyber: Racing ahead vs. racing safely

Balance AI with cybersecurity basics

While AI offers efficiency gains in threat detection, CISOs must ensure a solid foundation of cybersecurity practices before wide adoption to avoid introducing new vulnerabilities.

Close the AI skills gap

Rapid AI growth has outpaced cybersecurity talent. Upskilling teams in prompt engineering, model evaluation, and AI best practices is critical for effective implementation.

Prioritize high-impact use cases

Rather than chasing trends, CISOs should focus AI efforts on meaningful use cases like anomaly detection and task automation that align with business and security goals.

Prepare for AI-driven threats

Emerging risks like deepfakes and biometric spoofing require proactive measures — such as detection tools, staff training and clear governance — to protect digital assets.

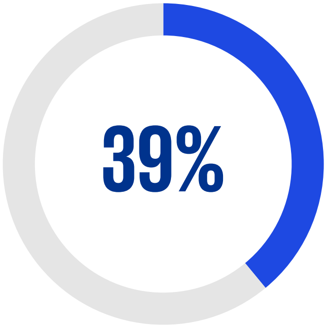
Suggested actions

Address the basics of good security such as data protection, IAM, etc. before turning to scaling AI across the enterprise.

Raise awareness among employees and customers about the risks of enterprise and adversarial AI use.

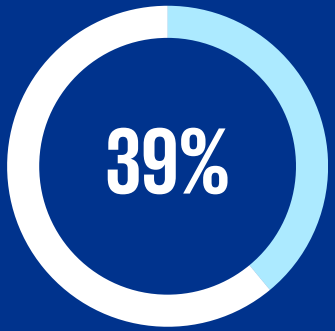
Prioritize upskilling to help them stay up-to-date with the latest AI developments.

Top Generative AI Cybersecurity Use Cases



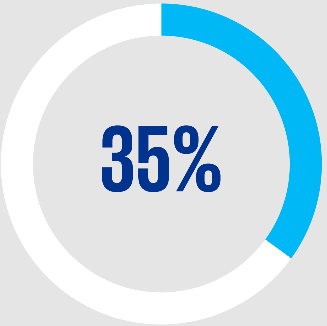
Identifying Risk

Generative AI can enhance risk-based alerting by quickly aggregating diverse datasets to provide security analysts with alerts that are context-rich. Large language models (LLMs) help to deliver this information at a speed and efficiency far beyond human capability



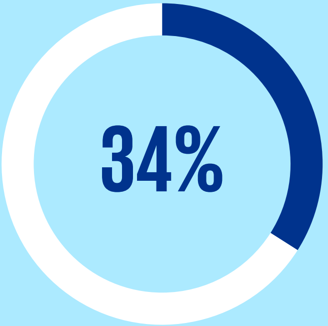
Threat Intelligence Analysis

LLMs can determine the indicators of compromise and MITRE ATT&CK techniques described in a threat intelligence report. This would save intelligence teams from a lot of drudgery and enable them to perform deeper analysis faster.



Threat Detection / Prioritization

Prioritizing and triaging alerts are tasks particularly susceptible to analyst misclassification, fatigue and human errors. Generative AI can parallel process multiple threats while improving accuracy



Summarizing Security Data

Generative AI can summarize quickly, thoroughly and accurately to help security teams save time and keep up with news and information.

The digital identity imperative

The digital identity imperative

Modernize digital identity security

CISOs must strengthen verification methods to counter deepfakes and biometric misuse while updating outdated processes with advanced authentication tools.

Build a future-proof identity framework

Implementing least privilege and user-centric design helps reduce risk, improve experience and build trust across the identity lifecycle.

Manage human and machine identities

CISOs need to monitor both user and machine accounts, including IoT and privileged services, to prevent unseen access risks.

Drive collaboration for trusted ecosystems

CISOs should engage leadership and regulators to support secure, interoperable digital identity systems across sectors.

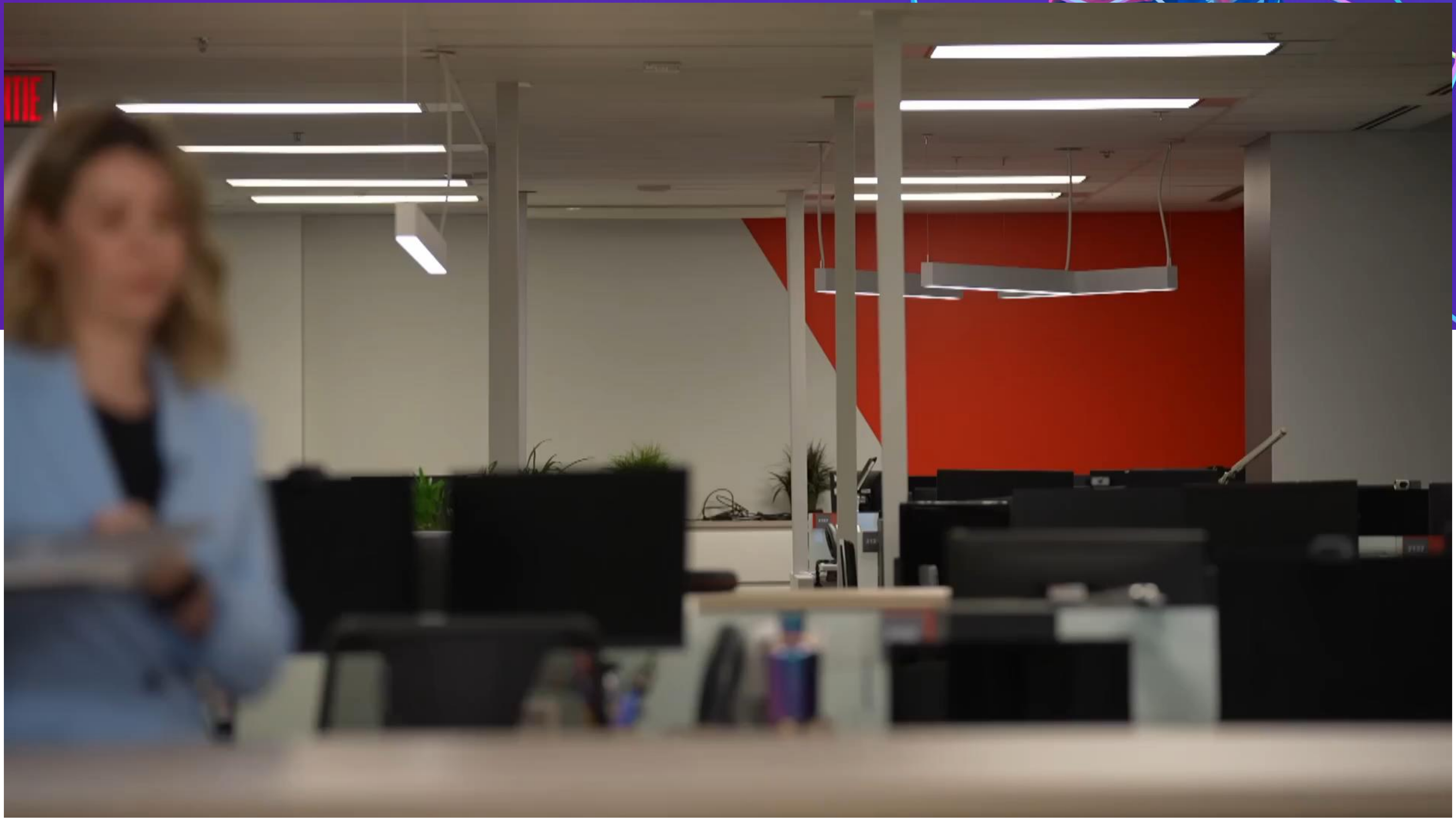
Suggested actions

Stay updated on AI and deepfake impacts on digital identities to proactively manage emerging threats.

Treat identity as the new cybersecurity perimeter, essential for protecting organizational assets and stakeholders.

Simplify identity management to enhance user experience while maintaining strong security.

The digital identity imperative



Resilience by design: Cybersecurity for businesses and society

Resilience by design: Cybersecurity for businesses and society

Embed cyber resilience across IT and OT

Resilience must be built into both IT and operational systems (OT) to quickly detect, respond to, and recover from cyber incidents — especially as ransomware threats to critical infrastructure continue to grow.

Strengthen asset and supply chain security

Effective asset management, paired with EDR/XDR tools and rigorous third-party risk oversight, is essential to reduce vulnerabilities across internal systems and external partnerships.

Adopt a holistic view of cyber-physical risks

The line between physical and digital threats is disappearing. Organizations must secure both—protecting devices, networks, and remote work environments—to prepare for real-world impacts from cyberattacks.

Government and industry collaboration

Governments play a growing role by setting regulations and enabling threat intelligence sharing. Public-private partnerships can boost national and organizational resilience.

Suggested actions

Implement proactive security measures like user behavior analysis to enhance real-time organizational resilience.

Create a resilience plan that outlines critical assets and strategies to sustain operations during a cyberattack.

Conduct cybersecurity drills to prepare leaders and strengthen organizational readiness for major attacks.

Real-world cybersecurity in energy and natural resources sector

Cyber resilience focus: CISOs in energy are prioritizing rapid recovery capabilities and risk identification to manage worst-case cyber scenarios.

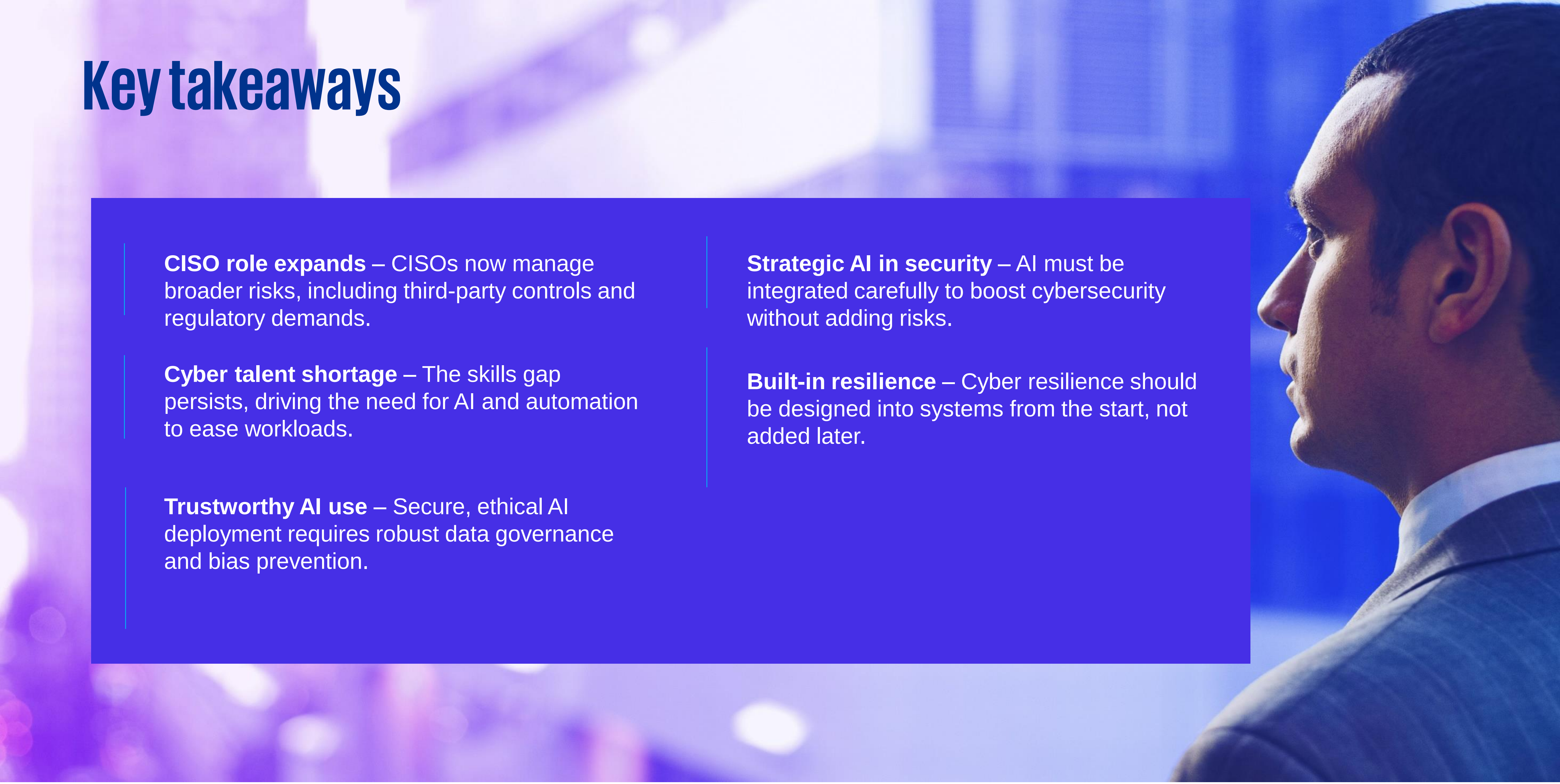
Customized playbook: KPMG developed a detailed cyber recovery playbook outlining step-by-step actions for IT restoration following total system loss.

Criticality reassessment tool: A new tool helped reclassify business-critical applications based on updated impact data, correcting legacy misclassifications.

Improved preparedness: The client enhanced its ability to reduce downtime and business disruption, strengthening its overall cyber resilience.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Key takeaways



CISO role expands – CISOs now manage broader risks, including third-party controls and regulatory demands.

Cyber talent shortage – The skills gap persists, driving the need for AI and automation to ease workloads.

Trustworthy AI use – Secure, ethical AI deployment requires robust data governance and bias prevention.

Strategic AI in security – AI must be integrated carefully to boost cybersecurity without adding risks.

Built-in resilience – Cyber resilience should be designed into systems from the start, not added later.

Top priorities for financial services cyber security professionals

Zero trust architecture: Focusing on identity-centric security and micro-segmentation strategies.

Integrating AI/ML driven tools to automate routine security operations center activities, allowing cybersecurity teams to focus on complex tasks.

Conducting continuous monitoring of third-party vendors to ensure a secure and resilient supply chain.

Developing transparent processes for assessing AI systems, including data classification and quality management, to mitigate privacy concerns and build trust.

Embedding security measures into the development lifecycle of AI technologies to avoid costly retrofitting and potential regulatory or reputational damage.

Engaging with regulatory bodies to stay ahead of compliance requirements and proactively address concerns related to AI implementation.

Top priorities for Energy and natural resources cyber security professionals

Clarifying and strengthening cybersecurity governance when it comes to roles and responsibilities, mandates, and domains.

Breaking down the siloes of IT, security (physical and cyber) and OT teams to understand the complete threat landscape, organizational environments and supply chain, as well as coordinate emergency/incident response capabilities.

Establishing a broad risk management framework for IT and OT with cybersecurity as business risk.

Implementing business continuity and disaster recovery (BCDR) strategies that account for both cybersecurity and physical risks. Testing and exercising these strategies thoroughly with realistic scenarios.

Review insurance policies in relation to third-party outages to determine whether financial impact can be reduced through coverage in business interruption insurance.

Contact us

Bunyarit Thanormcharoen
Partner,
Audit & Assurance
Tel.: +668 4075 2398
Email: bunyarit@kpmg.co.th

Saowanee Sethsathira
Partner,
Head of Tech-Cyber Advisory
Tel.: +668 2868 9638
Email: saowanee@kpmg.co.th

Jamjuree Sathapornchaiwat
Director,
Audit & Assurance
Tel.: +668 2005 7268
Email: jamjuree@kpmg.co.th

Woramon Sayalak
Director,
Tech-Cyber Advisory
Tel.: +669 4774 4496
Email: woramons@kpmg.co.th

Q&A

Please give us the feedback to improve our services.

KPMG

KPMG in Thailand
48th-50th Floor, Empire Tower
1 South Sathorn Road
Bangkok 10120
T: +66 2677 2000

KPMG in Thailand

kpmg.com/th

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public