Πανεπιστήμια στην Άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ 2025:

Η εμπειρία του Πανεπιστημίου Θεσσαλίας

ΙΩΑΝΝΗΣ ΜΟΥΝΤΑΝΟΣ
Α. ΚΑΘ. ΤΗΜΜΥ, ΠΑΝ. ΘΕΣ.
jmoondan@uth.gr

‘Letter from Prison’
(19 December 1929);
also attributed to
Romain Rolland.

Pessimismo Dell'intelligenza...

ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ ΠΛΕΟΝ ΑΜΕΣΑ!!!!

BLUF (Bottom-Line Up First):

- (#4) ΚΑΤΑΣΚΟΠΕΙΑ ΣΤΗΝ ΕΡΕΥΝΑ
- (#3) ΚΙΝΗΤΙΚΟΤΗΤΑ ΦΟΙΤΗΤΩΝ ΚΑΙ ΚΑΘΗΓΗΤΩΝ
- (#2) HACKERS TESTING GROUND ΛΟΓΩ ΜΕΓΕΘΟΥΣ ΥΠΟΔΟΜΩΝ ΚΑΙ ΕΛΑΣΤΙΚΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ
- (#1) ΑΠΙΣΤΕΥΤΗ ΔΙΑΦΗΜΗΣΗ ΓΙΑ HACKERS ΑΝ ΒΛΑΨΟΥΝ ΦΟΙΤΗΤΕΣ ΛΟΓΩ ΤΕΡΑΣΤΙΑΣ ΚΟΙΝΩΝΙΚΗΣ ΚΑΤΑΚΡΑΥΓΗΣ

ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!

ΣΤΟΧΟΙ ΟΜΙΛΙΑΣ

- Ιστορική Αναδρομή
- Απενημέρωση για την Άσκηση ΠΑΝΟΠΤΗΣ`25
- Συμβολή Πανεπιστημίων στην Εθνική κυβερνοασφάλεια
  - Συνεργασία με Θεσμικούς Φορείς και Ένοπλες Δυνάμεις
- προοπτικές που ανοίγονται για την εκπαίδευση, την έρευνα
- ενίσχυση της ψηφιακής ασφάλειας των ΑΕΙ

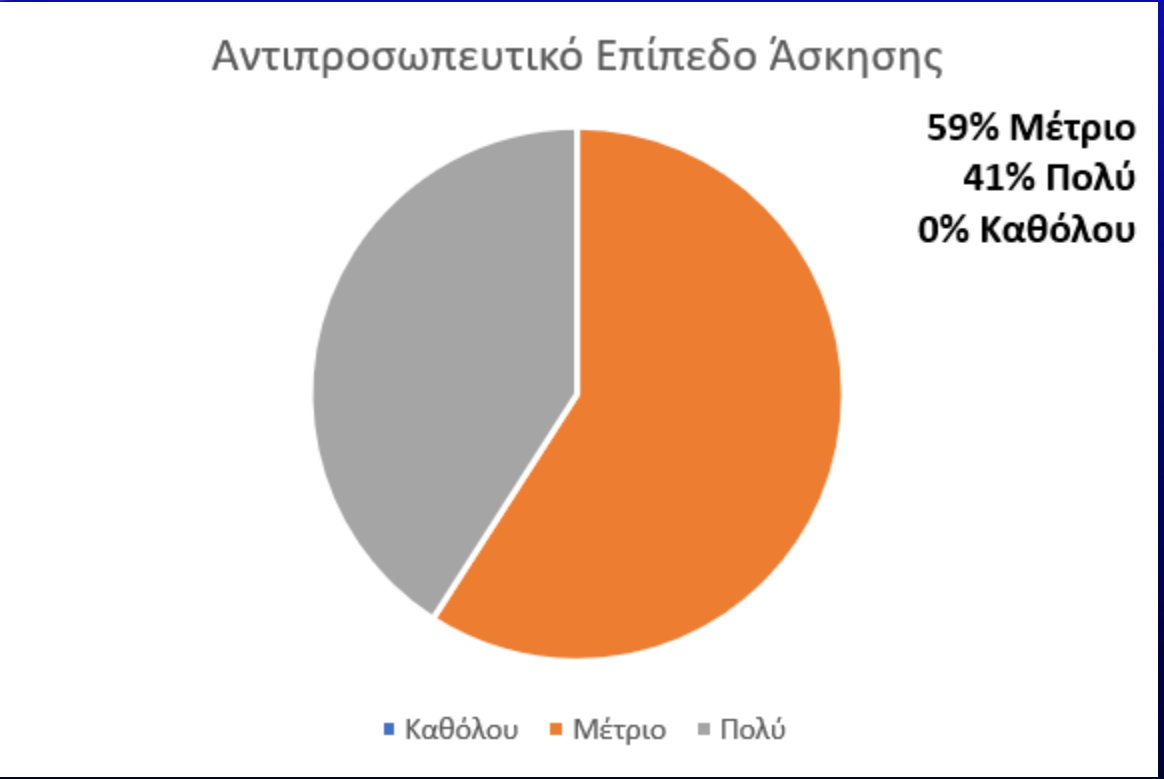
ΣΥΓΧΑΡΗΤΗΡΙΑ ΣΤΗ ΔΙ.ΚΥΒ.

Απενημέρωση ΠΑΝΟΠΤΗΣ 2025

- 471 συμμετέχοντες σε 58 ομάδες εκ των οποίων 6 ήταν πανεπιστημια
- η φετινή άσκηση διεξήχθη σε 3 διαφορετικά κομμάτια, η προσέλευση διαφέρει για το κάθε μέρος.
- 10 ομάδες αποστέλλουν αναλυτικά report
- Όλες οι ομάδες εμφάνισαν υψηλό επίπεδο γνώσεων και απόδοσης.

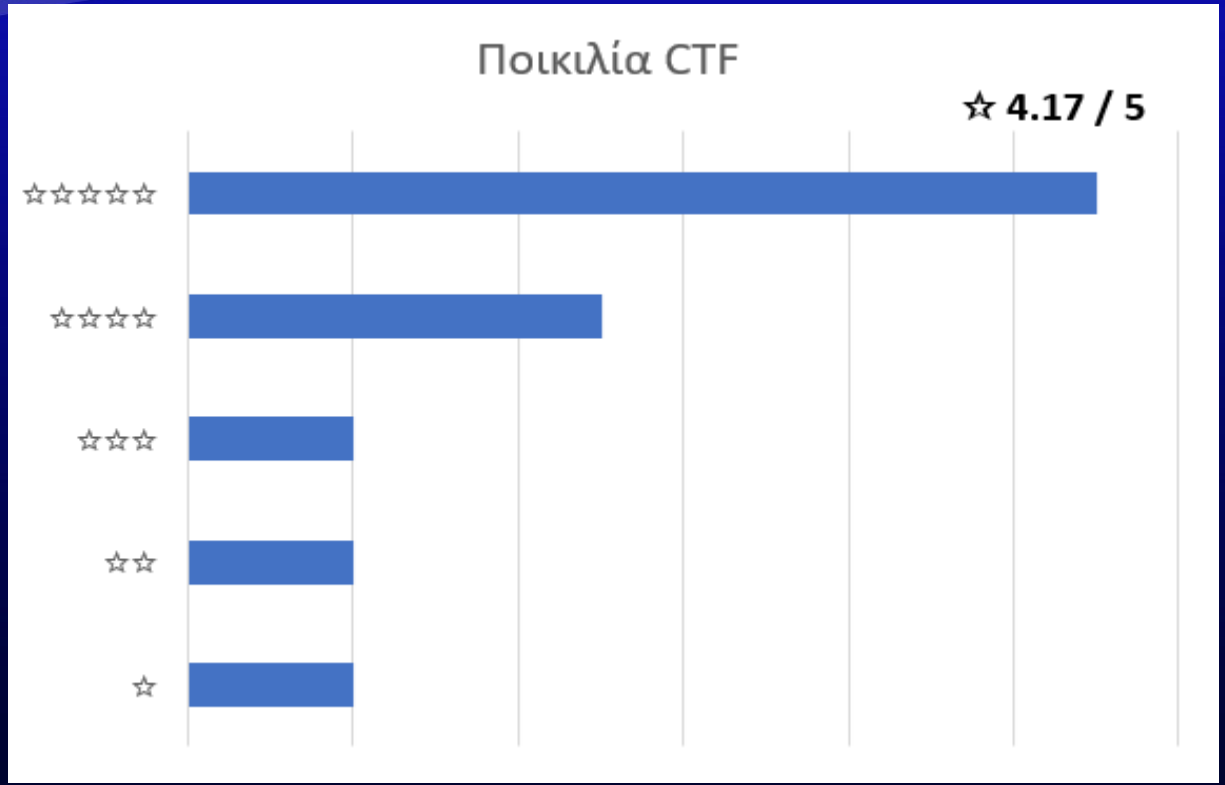
Απενημέρωση ΠΑΝΟΠΤΗΣ 2025

ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!



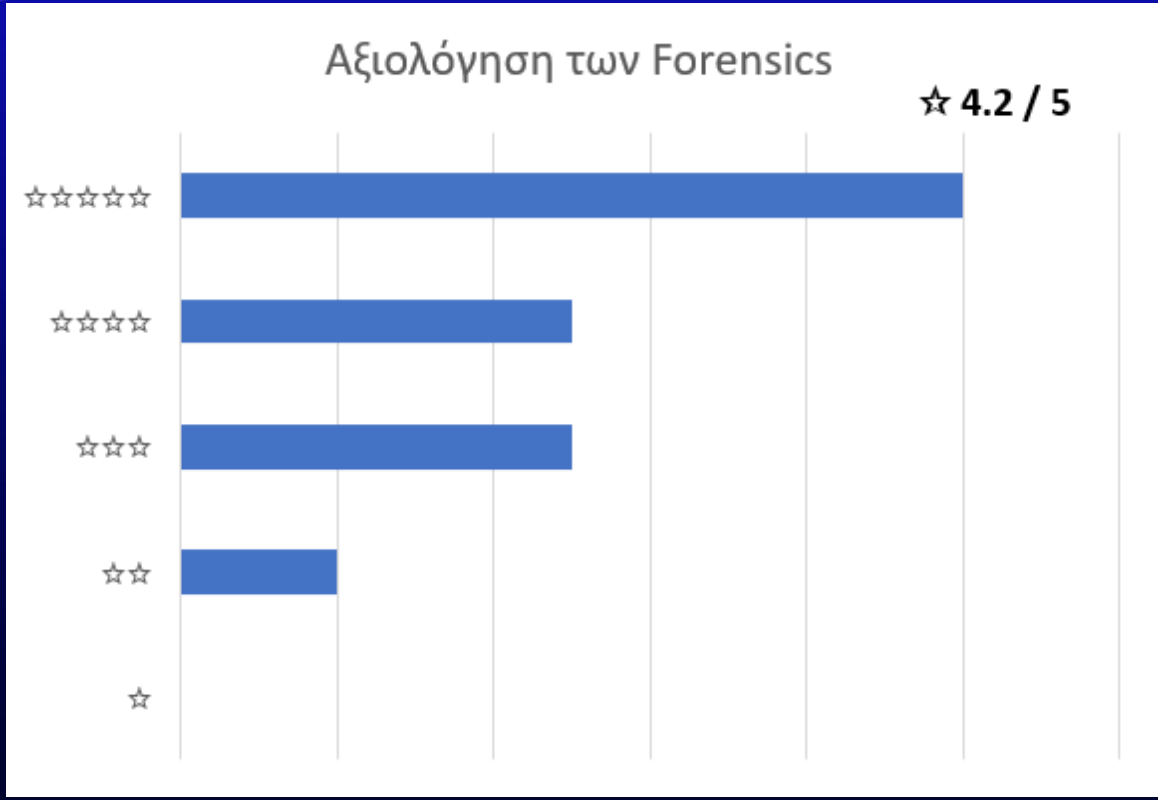
Απενημέρωση ΠΑΝΟΠΤΗΣ 2025

ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!



Απενημέρωση ΠΑΝΟΠΤΗΣ 2025

ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!



ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!

Συμβολή Πανεπιστημίων στην Εθνική κυβερνοασφάλεια

Συνεργασία με Θεσμικούς Φορείς και Ένοπλες Δυνάμεις

- ΔΙΚΥΒ = `Ερευνητικο Κέντρο` πλέον (ας μου επιτραπεί ο νεολογισμός)
- ΠΑΓΝΗ
- Εκπαιδευτικές άδειες
- SAFE

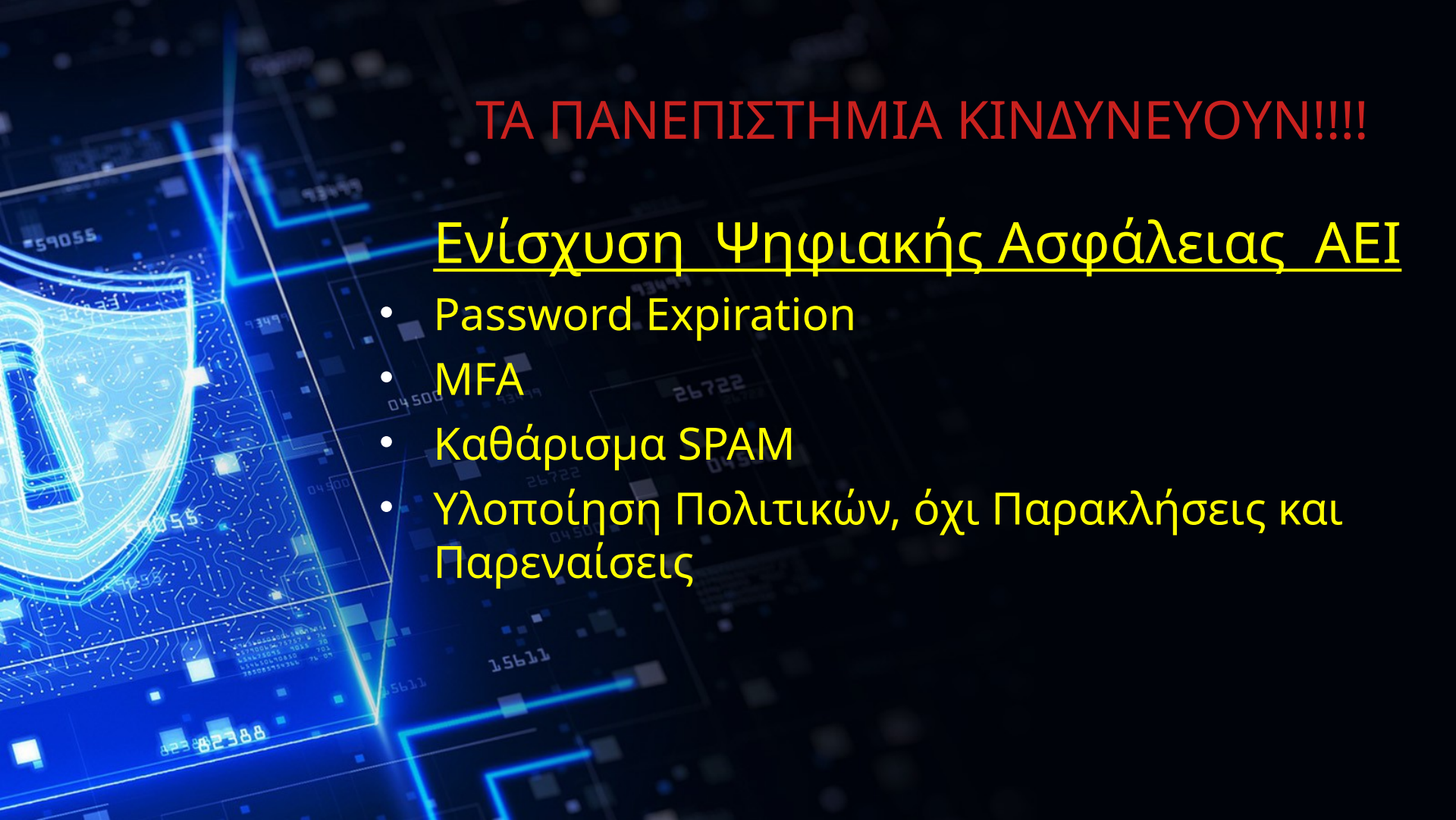
ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!

Προοπτικές Για Εκπαίδευση

- Blockchain
- Νομική Εκπαίδευση
- Social Engineering
- Cyber-hygiene

Και Έρευνα

- AI
- QUANTUM COMPUTING!!!!!!



ΤΑ ΠΑΝΕΠΙΣΤΗΜΙΑ ΚΙΝΔΥΝΕΥΟΥΝ!!!!

Ενίσχυση Ψηφιακής Ασφάλειας ΑΕΙ

- Password Expiration
- MFA
- Καθάρισμα SPAM
- Υλοποίηση Πολιτικών, όχι Παρακλήσεις και Παρεναίσεις

Letter from Prison
(19 December 1929);
also attributed to
Romain Rolland.

Pessimismo

Dell'intelligenza...

...ottimismo

della volontà


Microsoft
Microsoft Digital
Defense Report 2025
Lighting the path to a secure future
A Microsoft Threat Intelligence report

Top 10 recommendations from this report

1. Manage cyber risk at the boardroom level

Treat cybersecurity as a business risk on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization. Track and report metrics like multifactor authentication (MFA) coverage, patch latency, incident counts, and incident response time to develop a comprehensive understanding of both your organization's potential vulnerabilities and its preparedness in the event of a cybersecurity incident.

2. Prioritize protecting identities

Since identity is the top attack vector, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.

3. Invest in people, not just tools

Cybersecurity is a whole-of-organization effort. Find ways to upskill your workforce and consider making security part of performance reviews. Culture and readiness—not just technology—are primary factors in both an organization's defenses and its resilience.

4. Defend your perimeter

A third of attackers use crude tactics as the easy path into an organization's exposed footprint, often looking beyond what you deploy to the vendors and supply chain you trust, including perimeter web-facing assets (18%), external remote services (12%), and supply chains (3%). Knowing the full scope of your perimeter, auditing the accesses you grant to trusted partners, and patching any exposed attack surface forces attackers to work harder to be successful.

5. Know your weaknesses and pre-plan for breach

Combine knowledge of the organization's exposure footprint with organizational risk awareness to develop a proactive plan for responding to future breach. Tie security controls to business risks in terms the board can understand. Since a breach is a matter of when, not if, develop, test, and practice your incident response (IR) plan—including specific scenarios for ransomware attacks, which remain one of the most disruptive and costly threats to operations. How fast can you isolate a system or revoke credentials?

6. Map and monitor cloud assets

Since the cloud is now a primary target for adversaries, conduct an inventory on every cloud workload, application programming interface (API), and identity within the organization, and monitor for rogue virtual machines, misconfigurations, and unauthorized access. At the same time, work proactively to enforce app governance, conditional access policies, and continuous token monitoring.

7. Build and train for resiliency

If breaches are all but inevitable, resilience and recovery become key. Backups must be tested, isolated, and restorable, and organizations should have clean rebuild procedures for identity systems and cloud environments.

8. Participate in intelligence sharing

Cyber defense is a team, not individual, sport. By sharing and receiving real-time threat data with peers, industry groups, and government, we can make it harder for cyber adversaries to achieve their goals.

9. Prepare for regulatory changes

It's more important than ever for organizations to align with emerging laws like the European Union (EU) Cyber Resilience Act or United States (US) critical infrastructure mandates, which may require reporting cyber incidents within a certain timeframe or Secure by Design practices. These regulations reinforce the importance of timely incident reporting and stronger internal oversight of an organization's cybersecurity practices.

10. Start AI and quantum risk planning now

Stay ahead of emerging technologies. Understand both the benefits and risks of AI use within an organization and adjust your risk planning, attack surface exposure, and threat models appropriately. Prepare for a post-quantum cryptography (PQC) world by taking the time to inventory where encryption is used and create a plan to upgrade to modern standards as they evolve.

Strategic threats to the research and academia sector

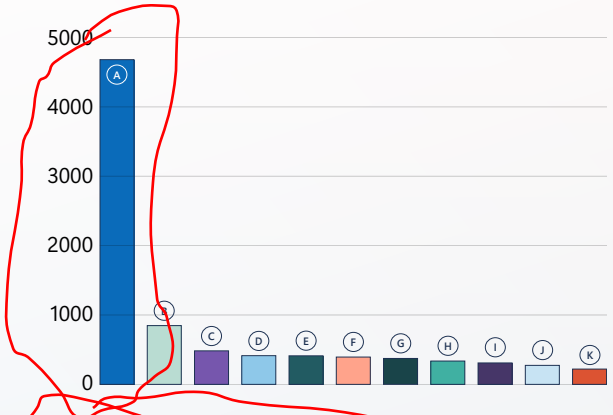
The research and academia sector continues to be a strategic incubator for adversarial cyber activity.[1] In 2025, it ranked among the top targets for threat actors due to its high-value IP, decentralized infrastructure, and expansive digital footprint. These conditions make it an ideal environment for adversaries to test and refine advanced attack techniques before deploying them against hardened targets such as government agencies and critical infrastructure.

Both nation-state actors and cybercriminal groups are leveraging the sector's open networks to pilot sophisticated identity-based attacks. Techniques such as AiTM, and AI-enhanced business email compromise (BEC) are increasingly prevalent. In the first half of 2025, identity-based attacks surged by 32%, with research and academia accounting for 39% of all identity compromise incidents observed by Microsoft. Environments across research and academia have some of the largest tenants and most complex identity systems of any sector, often making it difficult to detect and respond to advanced identity attacks.

Protecting the research and academia sector is both a community responsibility and a strategic necessity. Disrupting adversarial incubation here is critical to safeguarding downstream and upstream sectors.

Count of unique organizations with identity compromise signals, by sector

(December 2024-May 2025)



A. Research and academia	4,647
B. Services	841
C. Technology	480
D. Manufacturing	411
E. Miscellaneous	409
F. Travel	391
G. Retail	371
H. Energy	334
I. Logistics	307
J. Media	272
K. Healthcare	219

Source: Microsoft Threat Intelligence, commercial cloud

Inside the cybercrime marketplace: Brokers, mercenaries, and monetization

Cyber mercenaries can pose a serious threat to human rights, cybersecurity, and international stability as they enable governments that would otherwise lack the capability to conduct offensive cyber operations. While cyber mercenary products are often touted as enabling legitimate action against bad actors online, cyber mercenary intrusion capabilities have been widely used to target journalists, political dissidents, and other vulnerable groups. The cyber mercenary market is expanding rapidly, meeting a growing demand. According to the Atlantic Council, there are over 430 known entities operating in at least 42 countries.[2] This ecosystem includes intrusion experts, investors, intermediaries, and tech providers.

Although cyber mercenaries are frequently linked by the press to spyware, this gray market is much larger and poses even greater systemic risks—for example, the sale of zero-day vulnerabilities, which significantly destabilize the online environment and technology on which critical infrastructure relies by exposing a broad range of targets simultaneously through the breach of entire systems.

Because of the dangers associated with cyber mercenary activity, it's important for industry partners to work individually and together to combat the growing cyber mercenary market. Microsoft, for example, is committed to eradicating hack-for-hire services through its Digital Crimes Unit (DCU), which drives takedowns and enforcement actions against cyber criminals.

Microsoft is also a founding member of the Cybersecurity Tech Accord, which in 2023 laid out a set of principles on how to limit the activity of cyber mercenaries.

Governments, too, must do more to control this threat—for example, supporting the ongoing Pall Mall Process, which aims to create guardrails around the development, purchase, and use of commercially available cyber intrusion capabilities by supporting guiding principles for governments.

Learn more on page 67

*

A security researcher may earn $10,000 for responsibly disclosing a vulnerability to a bug bounty program, but may earn over $100,000 by selling the same exploit to a cyber mercenary.

Learn more

Microsoft Corporate Responsibility | Cybersecurity

Exploiting vulnerabilities: The persistent threat of unpatched systems

Vulnerability exploitation remains one of the most reliable, scalable, and silent methods of initial access for threat actors. In the last year, Microsoft Defender Experts observed a surge in exploitation campaigns targeting known flaws in widely used enterprise systems and third-party IT tools. In most cases, exploitation achieves one of three outcomes:

- initial access into protected environments,
- privilege escalation from user to admin
- arbitrary code execution to enable lateral movement or persistence

This activity demonstrates that a strategic pivot toward infrastructure-level compromise is the new baseline for initial access.

What makes this threat vector especially dangerous is its lack of dependency on user interaction. From remote code execution (RCE) in infrastructure software to logic flaws in authentication mechanisms, attackers are increasingly skipping phishing and going straight for the code. Even misconfigurations in trusted platforms become high-value entry points. Most of these attacks start with a known Common Vulnerabilities and Exposures (CVE) exploit and end in compromise.

This year, key vulnerability exploitations that our Defender Experts observed included:

- SimpleHelp RCE chain (CVE-2024-57726/27/28)
- BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability (CVE-2024-12356)
- Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2023-48788)
- Cleo Multiple Products Unrestricted File Upload Vulnerability (CVE-2024-50623)
- Apache Tomcat Path Equivalence Vulnerability (CVE-2025-24813)

Effective defense isn't just patching fast—it's expecting gaps and building layers of resilience through anomaly detection, behavior-based analytics, and hardening high-risk assets.

> “
>
> Vulnerability exploitation remains one of the most reliable, scalable, and silent methods of initial access for threat actors.

Recommendations

Patch fast, patch early
Prioritize patching for high-impact CVEs, especially in internet-facing infrastructure and remote access tools.

Isolate management interfaces.
Where possible, restrict RMM tools and administrative consoles to management networks or VPN-only access.

Employ exploit detection.
Use behavior-based analytics to flag abnormal post-exploitation behavior (for example, Local Security Authority Subsystem Service (LSASS) access, registry dumping, and outbound tunnelling).

Target demographics and exposure

Research and academic environments remain disproportionately targeted in password spray attacks, accounting for 52% of observed spray attempts. Factors contributing to this include decentralized IT management, high user turnover, and inconsistent MFA enforcement—conditions also observed in other vulnerable sectors such as rural healthcare. A May 2025 comparative analysis with the Have I Been Pwned database revealed that 85% of usernames targeted in spray attacks appeared in known credential leaks. On average, each compromised username appeared in three separate logs, highlighting the magnitude of the global credential leak problem and the importance of users regularly changing passwords.

Recommendations

To reduce the risk and impact of password spray attacks, organizations should adopt a multi-layered identity protection strategy. This includes taking the following measures:

Enforce phishing-resistant MFA for all users

Phishing-resistant MFA remains the most effective control against unauthorized access using compromised credentials. Even when attackers possess valid usernames and passwords, MFA blocks access in over 99% of cases. Organizations should monitor for accounts with valid credentials but unenrolled MFA and enforce enrollment policies to close this gap. Organizations should also implement conditional access policies and use risk-based conditional access to block or challenge sign-ins from suspicious IP addresses, geographies, or device types.

Monitor and block malicious IP addresses and ASNs

Continuously monitor authentication logs for error code 50053 and other indicators of spray activity. Block IP addresses and ASNs with repeated failed sign-in attempts or known malicious behavior.

Audit and decommission stale accounts

Regularly review and disable inactive accounts, which are often targeted in spray attacks. Ensure that deprovisioned accounts are removed from all authentication systems.

Educate users on credential hygiene

Promote the use of strong, unique passwords and discourage password reuse. Encourage users to check their credentials against breach databases such as Have I Been Pwned.[4]

Deploy AI-based detection and response

Use AI-driven tools to detect anomalous sign-in patterns and flag potential spray attacks in real time.

> On average, each compromised username appeared in three separate logs, highlighting the magnitude of the global credential leak problem.

Nation-state adversary threats

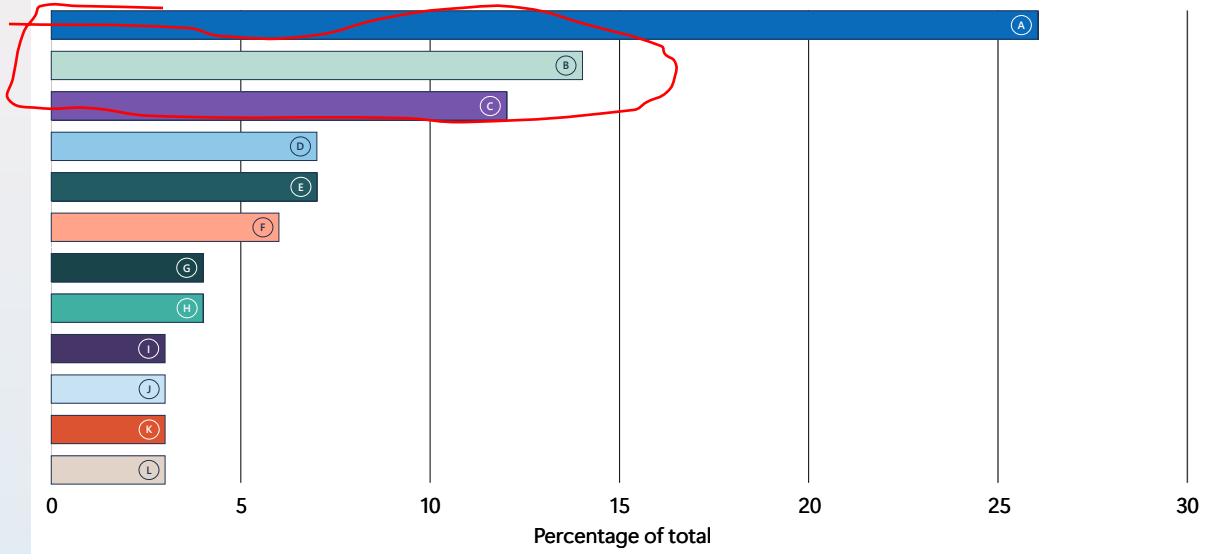
Nation-state cyber activity this year prioritized espionage against traditional intelligence targets—IT, research and academia, government, and think tanks/NGOs.

A minority of attacks, for example against the Defense Industrial Base, sought to steal proprietary information for economic advantage. An even smaller number of attacks had other goals, including sabotage and ransom.

A major threat that emerged this year was the discovery of the magnitude of North Korea's program to stealthily embed remote workers at organizations around the world. As will be discussed later, this growing threat has multiple facets, including the risk of sanctions violation, espionage, extortion, and sabotage.

In line with geopolitical hotspots and longstanding intelligence priorities, the primary geographical targets of nation-state activity this year were in Israel, the United States, and the United Arab Emirates. Predictably, Ukraine was also an extreme focus for Russian actors.

Most-targeted sectors by nation-state actors



	% of total
A. IT	26
B. Research and academia	14
C. Government	12
D. Think tanks/NGOs	7
E. Consumer retail	7
F. Manufacturing	6

	% of total
G. Transportation	4
H. Communications	4
I. Finance	3
J. Health	3
K. Defense	3
L. Energy	3

Source: Microsoft Threat Intelligence nation-state notification data

Insider risk in the age of strategic geopolitical competition

Insider threats: Emerging dimensions and mitigations

In an era of increasing geopolitical tensions and blurring of public and private sector interests, nation-state actors have increased their use of insiders to gain access to intelligence. These efforts are often long-term operations that are more difficult to detect than traditional hacks. Nation-states increasingly use non-state actors—including cyber mercenaries, criminal syndicates, and front organizations—to conduct insider threat operations that target private sector entities.[11] These proxies obscure attribution while enabling scalable, persistent campaigns.

China and Russia have both cultivated ecosystems to infiltrate corporate environments, often using academic or professional affiliations to identify and exploit vulnerable insiders.[12] The sectors most at risk—AI, quantum technologies, biotechnology, and defense—have both economic and military value. Insider espionage can cause immediate financial loss and long-term competitive harm, erasing years of innovation and market advantage through stolen research and development.

Most organizations' cybersecurity frameworks were not initially built with an insider threat in mind. Compliance standards and cybersecurity best practices traditionally assume that the attacker is an outsider trying to break in, but when the threat actor is an insider with valid access, many of those measures could be bypassed by default.

Additionally, many internal cybersecurity tools are not designed to detect trusted insiders working covertly with sophisticated external actors. For example, data loss prevention (DLP) tools that would flag large, suspicious file transfers often miss the slow, stealthy exfiltration of an espionage-minded insider. While zero trust network architecture adds protection against unauthorized devices and external connections, it requires consistent operationalization on the comprehensive zero trust principles and security strategy to prevent unauthorized use of a legitimate user account.

According to DTEX Systems and the Ponemon Institute, companies take 81 days on average to contain an identified insider incident.[13] This long dwell time gives nation-state actors a persistent foothold to expand their access, cover their tracks, and even establish back doors for future use.

Layoffs and workforce reductions across government and private industry add another dimension to the insider landscape. Such workforce adjustments can inadvertently exacerbate insider threat risks through disgruntled employees or weakened security oversight due to budget cuts and staff reductions. Malicious insiders can leak sensitive data or redirect corporate assets to corporate adversaries. Third-party suppliers with privileged access might unknowingly introduce vulnerabilities, making rigorous vetting and alignment with internal security policies essential to mitigating insider-driven exposure. Facing this threat requires an intentional strategy. For businesses, the issue of insider risk should be elevated to the boardroom and C-suite. Executives should include insider risk in regular risk assessments and incorporate insider risk programs information when business decisions may impact the workforce. Key recommendations for enterprise leaders include:

- **Identify your crown jewels.** Pinpoint the data or technologies that would be most devastating to lose (for example, trade secrets, source code, formulas, merger and acquisition plans) and implement extra safeguards around these assets such as strict need-to-know access, encryption, and monitoring of access logs in real time.
- **Implement continuous identity verification.** Move beyond one-time sign-ins and use adaptive authentication and behavioral biometrics (like typing patterns or mouse movements) to continuously verify that the person behind an account is the genuine user. If an account starts behaving oddly—for example, a finance employee begins downloading large engineering design files—require immediate re-authentication or manager approval.
- **Divide and limit access.** Architect your systems on the assumption that an insider might turn malicious. No single individual should be able to access all critical data. Use segregation of duties and data fragmentation so that even if one account is compromised, an attacker can't sweep up everything.
- **Foster a vigilant culture.** Employees are often the first to notice unusual behavior in a peer. Create a culture where reporting a concern is encouraged and rewarded.
- **Conduct exit interviews and post-employment monitoring.** Exit interviews are an effective safeguard against insider risk. They provide a final opportunity to detect warning signs, reinforce confidentiality and data protection obligations, and ensure access to sensitive information is revoked. These conversations also reduce the risk of disgruntled retaliation, highlight potential process weaknesses, and remind departing staff of their continuing obligations at a time when adversarial entities may seek to recruit them (this is more specific to those with security clearances). Documenting the exchange creates an audit trail, demonstrating that the organization has taken prudent steps to protect its assets, reputation, and people during workforce transitions.
- **Engage in holistic insider risk management.** Effective insider risk management requires a blend of technology, culture, and collaboration. Deploy behavioral analytics and DLP solutions to detect unusual data transfers or privilege escalations, particularly among highly privileged users. Intelligence sharing between government, private industry, and recruiting platforms also helps expose fake companies and protect organizations from risky potential hires.

Additionally, companies can use dedicated insider threat monitoring tools to reduce the overarching risk profile. As an example, companies utilizing Communications Compliance can be notified of potential talent recruitment outreach.[14]

AI's double-edged influence:
Defending and disrupting the digital landscape

The AI threat landscape is diverse and rapidly evolving. The distinctive nature of AI-related threats demands that organizations develop new strategies and adaptive approaches to effectively manage emerging risks.

For example, as AI adoption accelerates, so does AI's access to sensitive data. Whether through user-supplied inputs, credentialed access to existing content, or the creation of custom fine-tuned models built on proprietary data, the volume and sensitivity of data involved continue to grow—which means risks associated with the compromise of or unauthorized access to that data are also growing.

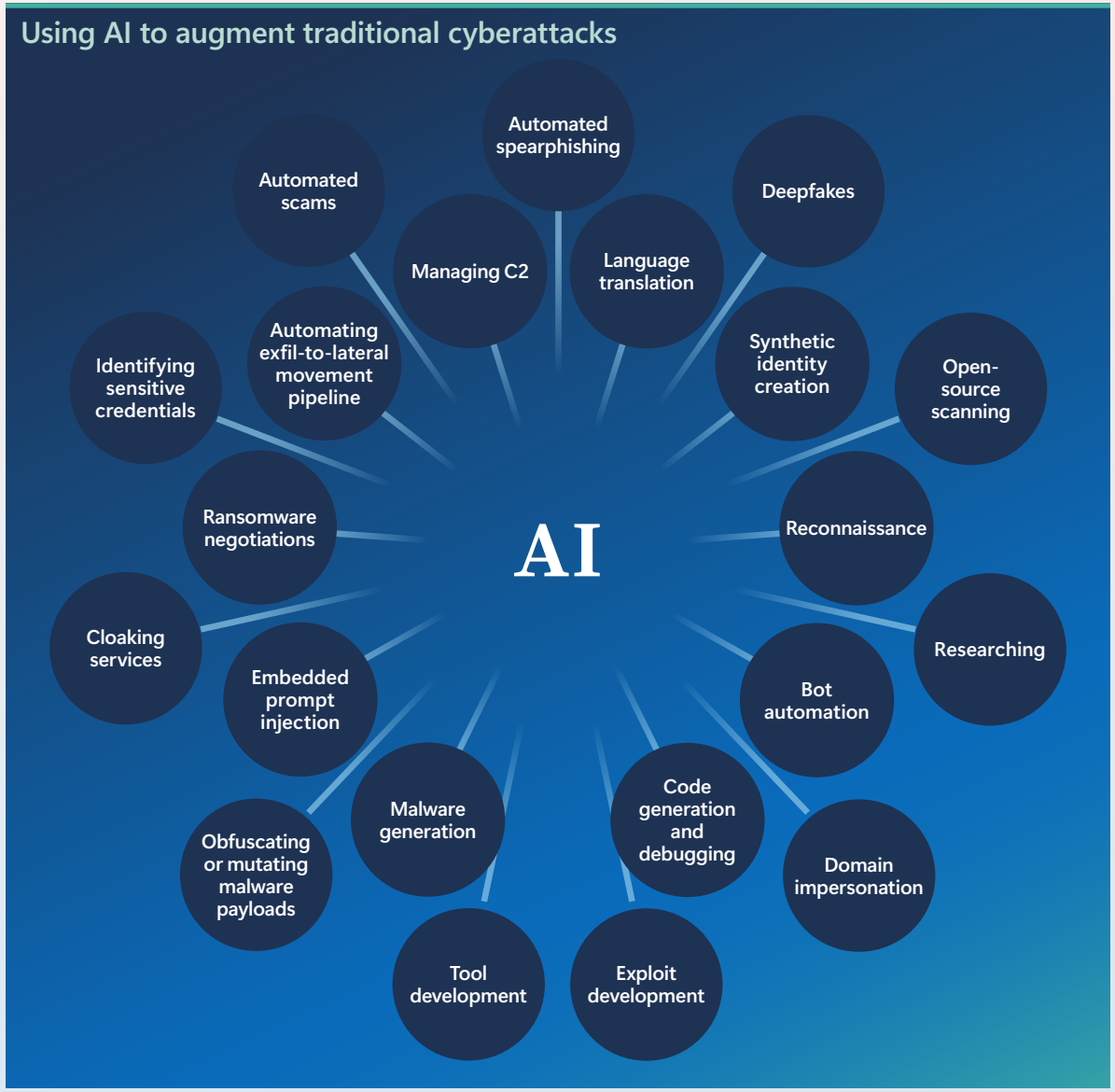
AI-associated challenges include both threats to AI and its users and threats enabled by AI. AI-associated threats can be divided into five major categories: traditional cybersecurity, malfunction, dangerous capabilities, operational issues, and emerging threats.

Traditional cybersecurity

This category encompasses both cyberattacks that are amplified using AI and direct attacks on AI systems. These threats target underlying infrastructure and exploit human vulnerabilities. Actors conducting these attacks range from less-skilled individuals to sophisticated state-sponsored groups.

Cyberattack augmentation refers to the use of AI to enhance traditional cyberattacks. The chart on the right highlights the primary areas of augmentation, most of which are based in the automation of previously time-intensive activities.

Defenders must counter AI augmentation by fostering a strong cybersecurity culture, training users to recognize manipulation tactics, and implementing authenticated communication channels. AI-driven detection systems that flag anomalies in communication patterns or identify deepfake content in real time can also serve as critical safeguards, while AI can detect vulnerabilities, automate patching, and improve threat intelligence.



Quantum technologies:
Strategic priority in a new era of competition

Quantum technologies—computing, communications, and sensing—are foundational to future economic and national security.

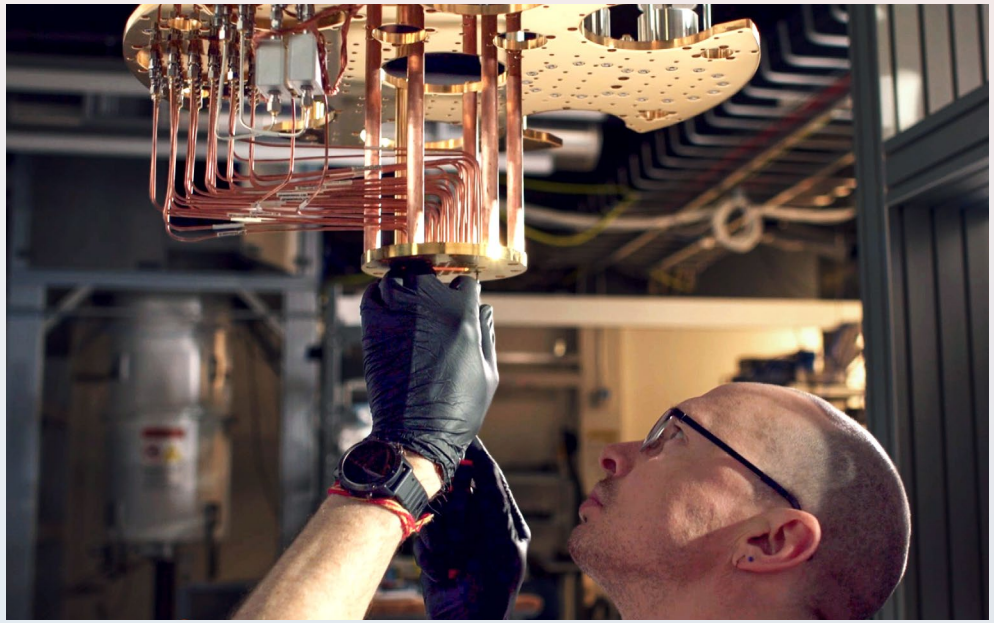
Quantum technologies' potential to accelerate scientific discovery, enable breakthroughs in secure communications, and disrupt encryption have made this technology a high-priority area. Indeed, governments have identified quantum technology as a national imperative. Allies and adversaries alike are pursuing quantum capabilities through new national research and development (R&D) programs, as well as investments to cultivate their own academic and private sector ecosystems. Certain adversaries may also leveraging additional capabilities to strengthen their position through espionage.

Commercial companies are driving a significant amount of current quantum R&D and private enterprise now sits at the epicenter of the global race to develop quantum technologies. Certain adversaries may also leverage additional capabilities to strengthen their position through espionage, including the possible targeting of Corporate R&D programs, startups, and academic spin-offs.[16] It is therefore imperative to establish robust safeguards and strategic preparedness now, before quantum technology becomes widely operational. The stakes are existential: leadership in quantum could determine not just competitive advantage but the future integrity of secure communications and the global digital economy.

The implications of the race to quantum advantage are sweeping:

- Industrial scientific leadership: Quantum technologies could drive a new wave of innovation across chemistry and material science discoveries.
- Impact to cryptography: A sufficiently powerful quantum computer could break widely used public-key algorithms, undermining the security of digital communications and data.
- Sensor superiority: Quantum sensors could detect stealth air or naval assets, eroding strategic deterrence.

Learn more on page 74



For a quantum future that is secure, prosperous, and inclusive, governments and industries must do three things:

1. Prioritize security while simultaneously embracing innovation.
2. Reshape sectors of the economy to be first movers and capitalize on the quantum future.
3. Work globally to ensure that all humanity benefits through the responsible and ethical use of transformative technology.

Key takeaways

Insights and actions for cyber defense

1. Cyber risk is business risk

As intrusion attempts become the norm, it is essential that governing boards and C-suites recognize that cyber risks are a form of business risk and treat them accordingly. Solutions to help mitigate this risk include conducting security exercises, implementing key performance indicators tied to cyber hygiene, and cross-training teams to build resilience.

Read more on p69

2. AI-powered defense is essential

As adversaries begin to move at the speed of AI, so must defenders. Microsoft uses AI to conduct threat analytics, identify detection gaps, validate detections, identify phishing campaigns, automate remediation, and shield vulnerable users.

Read more on p60

3. AI agents can help in threat mitigation and incident response

AI agents can help organizations automatically respond to threats, including by suspending suspicious accounts and initiating a password reset, containing a breach before an attacker can conduct further malicious activities. Agents can also enforce policies, monitor credentials and app permissions, and control employee accesses.

Read more on p68

4. Organizations should implement a security framework for AI use

When using AI, it's important to mitigate risks such as data leaks or data oversharing, as well as risks to the AI itself such as prompt injections and insecure extensions. This means organizations require a strong security framework that helps them: prepare for AI adoption; discover how AI is being used within the organization; protect sensitive data, AI agents, applications and models; and govern AI operations.

Read more on p63

5. Deterring cyberattacks requires political solutions

Individual defensive activities aren't enough to turn the tide of cyber threats from nation states. To protect cyber infrastructure, governments must build frameworks that signal credible and proportionate consequences for malicious behavior. This includes regularizing public attributions, signaling red lines, and imposing consequences.

Read more on p66

6. Cooperation across borders is crucial to mitigate cyber risks

Whether addressing threats like ransomware and cyber mercenaries or managing emerging technologies like AI, cooperation between the public and private sectors and academia is essential. This includes formulating policy frameworks, establishing protocols, working on shared initiatives, intelligence sharing, and engaging in dialogue.

Read more on p67

7. Resilience must be woven in by design

Given the persistence of cyber threats, it is important that systems are designed to anticipate, withstand, recover from, and adapt to disruptions. Resilience must be embedded into the very DNA of an organization's infrastructure.

Read more on p72

8. Public-private collaboration is key to disrupting cybercrime ecosystems

Successful operations like the Lumma Stealer takedown demonstrate the power of coordinated legal, technical, and operational strategies across sectors to disrupt malicious infrastructure and protect critical assets.

Read more on p64

9. Governments are moving away from voluntary compliance toward cyber requirements

Across the globe, governments are accelerating efforts to manage cyber risk through new laws and regulations. In particular, they are moving from voluntary guidelines to enforceable standards that emphasize accountability, risk management, and timely incident reporting. At the same time, to maximize their effectiveness, governments must pursue harmonized, risk-based approaches that promote interoperability and reduce duplication across borders.

Read more on p77

10. Organizations must prepare for quantum computing

Quantum computing poses a serious threat to current cryptographic systems. As a result, organizations should inventory their cryptography (keys, certificates, and protocols) and establish a roadmap to replace vulnerable algorithms with PQC standards as they become available. Microsoft has established the Quantum Safe Program to achieve "quantum readiness" by systematically integrating post-quantum cryptographic algorithms into our services.

Read more on p74

Resilience by design: Strengthening critical infrastructure for the next wave of threats

In today's hyper-connected world, new vulnerabilities are constantly emerging. As a result, cybersecurity expectations, practices, and oversight must evolve to prioritize resilience.

Cyber–physical threats can arise from a variety of sources, including natural disasters, industrial accidents, human error, technical errors, or malicious activities such as cyberattacks, terrorism, or armed conflict. These threats have the potential to disrupt the business and operations of critical infrastructures.

Given the interconnected nature of these risks, cyber–physical resilience encompasses both technical and organizational measures. Its goal is to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from incidents.[31]

Cyberattacks are inevitable. Whether due to sophisticated threat actors, human error, or system complexity, breaches will occur. The key question is therefore not if a system will be attacked, but how well it can withstand attacks and recover. This is the essence of cyber-physical resilience: the ability of systems to anticipate, withstand, recover from, and adapt to disruptions—regardless of the cause.

Leaders should shift from a purely defensive posture to one that embraces resilience as a core design principle. This means building systems that can continue to operate under duress, recover quickly, and evolve to meet future threats. For leaders, this is not just a technical issue—it's a strategic one. The resilience of our infrastructure directly impacts national security, economic stability, and public trust.

By embedding resilience into the DNA of an organization's infrastructure, we not only protect our assets but also enhance our ability to compete and thrive in a volatile world.

Cyber-physical resilience is not just a technical challenge, it's a leadership imperative.[32] CEOs and CFOs must recognize that downtime, data loss, and reputational damage from cyber incidents can have profound financial consequences. Simultaneously, government leaders must ensure that national infrastructure can withstand and recover from attacks that could otherwise disrupt societal functions at scale. Maintaining a robust defensive posture will be especially important for owners of critical infrastructure, many of whom operate with limited financial resources.

By embedding resilience into the DNA of an organization's infrastructure, we not only protect our assets but also enhance our ability to compete and thrive in a volatile world.

Key recommendations for leaders

Invest in resilience by design
Encourage the development of infrastructure that is inherently resilient. This includes modular systems, redundancy, and fail-safes that allow for graceful degradation and rapid recovery.

Foster public-private collaboration
Resilience is a shared responsibility. Governments and industries must work together to set standards, share threat intelligence, and coordinate responses to disruptions.

Support innovation and workforce development
Resilience requires cutting-edge technologies and a skilled workforce. Leaders should champion investments in research and development and education to build national capacity.

Incentivize resilience through policy and regulation
Financial and regulatory frameworks should reward organizations that prioritize resilience, much like how safety and environmental standards are incentivized today.

Measure and monitor resilience
Establish clear metrics and benchmarks to assess the resilience of critical systems. Transparency and accountability are essential for continuous improvement.

Building resilience in critical infrastructure

A strategic lifecycle, four core phases...

Anticipate

- Identify vulnerabilities and emerging threats
- Conduct risk assessments
- Model potential disruptions

Withstand

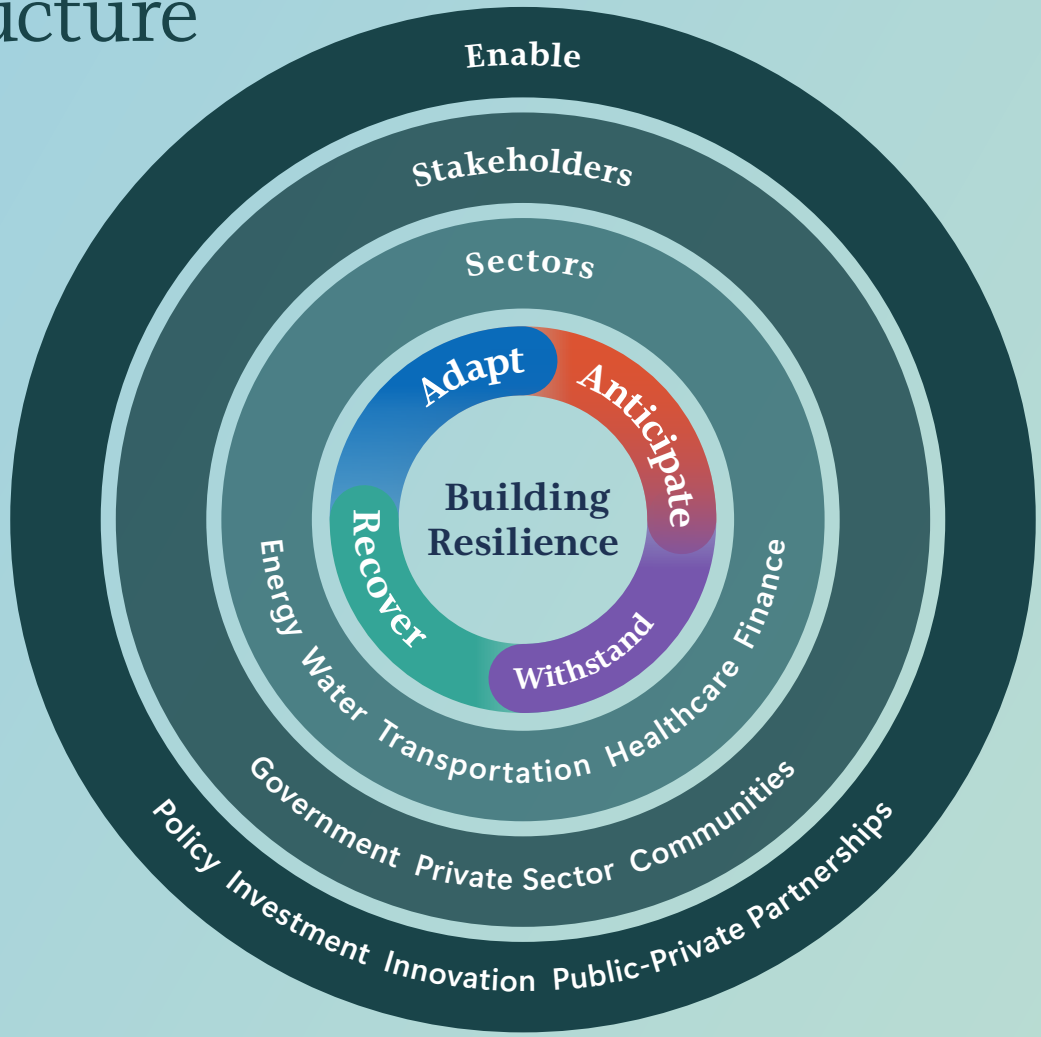
- Design systems with built-in redundancies
- Harden infrastructure against known threats
- Ensure continuity of essential functions

Recover

- Rapid response and restoration protocols
- Minimize downtime and service disruption
- Communicate transparently with stakeholders

Adapt

- Learn from incidents and near-misses
- Update systems and policies
- Invest in innovation and workforce training



Microsoft's strategic path to quantum safety

Much of modern cryptography relies on mathematical puzzles that are practically impossible for classical computers to solve—for instance, cracking the standard encryption behind a secure website or messaging app would take millions of years with today's computers.

Quantum computing is novel that can consider many possibilities at once, allowing quantum computers to process complex problems much faster than classical systems.

Quantum computing poses a serious threat to current cryptographic systems. While still an emerging technology, the expected development of a powerful cryptographically relevant quantum computer (CRQC) means that if organizations don't update our cryptography in time, we risk a scenario like the early days of the internet, when websites were on unencrypted HTTP and attackers could eavesdrop on information in transit. In the lead up to this potential data exposure, Harvest Now, Decrypt Later (HNDL) is a real concern: attackers can hoard encrypted data today so they can decrypt it in the future with quantum power.

Every organization should inventory its cryptography (keys, certificates, and protocols) and establish a roadmap to replace vulnerable algorithms with Post-Quantum Cryptography (PQC) standards as they become available. At Microsoft, there is a dedicated program to make sure our own products and services—and customers—stay safe in the quantum era. Microsoft established the Quantum Safe Program (QSP) to coordinate all its quantum security efforts across the company and achieve quantum readiness by gradually integrating PQC algorithms into Microsoft's services. As part of our efforts:

- We updated SymCrypt, Microsoft's core cryptographic library, to support new post-quantum algorithms. SymCrypt is like the engine that handles encryption under the hood in Windows, Azure, and many Microsoft products. We also enabled PQC support in Windows and Azure Linux (using SymCrypt OpenSSL).
- Microsoft Research has contributed to the design and analysis of PQC algorithms. Through blogs and publications, Microsoft shares these developments with the community, helping to lead the conversation on how to protect information in the quantum age.

Governments and industries worldwide are actively preparing for the quantum era by upgrading their cryptographic algorithms to quantum-resistant alternatives. Standards bodies like National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) have been running global competitions to select robust PQC algorithms, and international groups are working on standards to integrate these algorithms into our software so that everyone's systems can work together. In everyday terms, it's like the world has agreed to upgrade all its locks and keys and is now in the process of implementing the change.

During the last year, multiple governments have also published guidance and requirements to spur the transition, with most identifying 2035 as the deadline for completing transition. In the United States, European Union, and Australia, changes to some of the highest risk systems should be made by 2030, while in Canada and the UK, that date is 2031.

Recommendations

Governments play a critical role in enabling a quantum-safe future through strong collaboration with industry and effective policies. To accelerate readiness, we recommend governments take the following actions:

Establish quantum safety as a national cybersecurity priority. Position quantum-safe cryptography as a strategic imperative and embed it into national cybersecurity frameworks.

Align quantum-safe strategies across jurisdictions. Harmonize public policies, standards, and transition timelines. The G7 should lead by expanding its financial sector post-quantum cryptography workstream to align G7 members' broader quantum-safe strategies.

Adopt international standards. Support global standards development and avoid fragmented, region-specific approaches that hinder interoperability, innovation, and security.

Set early and progressive timelines. Drive action well before 2030. For instance, the US Committee on National Security Systems Policy 15 (CNSSP -15) mandates quantum-safe algorithms in all new products and services for national security systems by January 2027.

Lead by example with transparent transition plans. Publish and regularly update government transition roadmaps—including timelines, milestones, and budgets—to foster knowledge sharing and best practices.

Raise awareness and build workforce capacity. Educate the public and critical infrastructure sectors on quantum risks and readiness. Invest in skilling programs to equip the workforce for a quantum-safe transition.

Modernize through cloud adoption Promote cloud migration as a strategic enabler. Cloud platforms can streamline the transition by embedding quantum-safe capabilities, reducing the burden on individual organizations.

Learn more

Post-quantum resilience: building secure foundations | Microsoft On the Issues

Quantum-safe security: Progress towards next-generation cryptographyQuantum-safe security: Progress towards next-generation cryptographyQuantum-safe security: Progress towards next-generation cryptographyQuantum-safe security: Progress towards next-generation cryptography

https://quantum.microsoft.com