2025 CYBERSECURITY REPORT

Table Stakes, Trends, and Threats

A 12-Month Look Forward

By Joanna Dempsey, Keith McCloskey, Mike Zakrzewski,
Beau Houser, Dave Howard, Greg Scheidel, and Anthony Zech.

Table of Contents

INTRODUCTION 3

Table Stakes, Trends, and Threats: A Framework for Examining Cybersecurity's Future 4

CYBER TABLE STAKES 5

1. You Are the Target 5

2. Trustworthy Data 6

3. Cybersecurity Supply Chain Risk Management 7

4. Intelligence-driven Security 8

CYBER TRENDS 9

1. From Prevention to Resilience 9

2. Empowering Cyber Professionals Through AI Augmentation 10

3. AI: Cyber Friend and Foe 11

CYBER THREATS 12

1. Lower Barriers to Offensive Cyber Operations 12

2. Faster Exploitation of Vulnerabilities 13

3. AI-powered Threats 14

4. Ransomware and the Rise of Double and Triple Extortion 15

5. State-sponsored Cyber Espionage 16

CONCLUSION 17

Introduction

The scale and scope of the cyber threats our nation faces — and the potential impact to our way of life — are only escalating and accelerating. Nation states and criminal organizations are targeting the delivery and operation of functions and services critical to our nation and fellow citizens.

High-profile nation-state adversaries are increasingly targeting our national critical functions — from water and energy infrastructure (Volt Typhoon) to telecom providers (Salt Typhoon) to broader and ever-increasing cyber threat activity across our nation (e.g., CrowdStrike observed a 150% increase in threat activity related to the People's Republic of China in 2024 compared to 2023). These threats are so critical that the first congressional Homeland Security Committee meeting of the new 119th congress was focused on the global cyber threats our nation is facing.

Over the last several years, the impacts from nation-state actors and cyber criminals have led to an estimated $10 trillion cost of **cybercrime around the globe**. And our cyber defenders are not currently able to match the speed of infiltration and exfiltration.

Speed of Breach – **"... in 25% of the cases, attackers are exfiltrating data within five hours of initial compromise."**

Time to Respond – **"Organizations on average take six days to respond to a cyber incident."**

Source: Palo Alto's Unit 42 Global Incident Response Report 2025

To combat these threats and trends, it's critical that we all spend time now focusing on improving our cyber basics, from core cyber hygiene, to automating as much as we can to reduce the load on our already limited and overworked staff and maximize their effectiveness. This will pay dividends as we work to better understand our individual and collective risks, the nature and impact of threats on our nation's most critical assets, and how and where we prioritize resources to mitigate those risks and minimize impacts.

ECS has pulled together leaders from across its defense, intelligence, CISA and Homeland Security, federal civilian, state and local, and commercial cybersecurity programs. We have collected insights and outputs from services and support, researched major industry trends, threats, and risks, as well as industry frameworks and models, to identify major themes and trends that need to be focused on in 2025 and beyond.

Table Stakes, Trends, and Threats:

A Framework for Examining Cybersecurity's Future

Cybersecurity is constantly evolving — both proactively with advances in techniques and technologies and reactively in response to changes in the threat landscape. As such, maintaining an effective cybersecurity program requires regularly assessing existing strategies and practices, including those that might be considered standard best practices; new or changing strategies, techniques, and technologies; and the status of threats and threat actors. This report performs this assessment and arms you with the insights you need to validate and strengthen your security posture.

We've framed this report around not just emerging cyber trends but also critical threats and cyber "table stakes" — the foundational elements of cybersecurity resilience. For each table stake, trend, and threat, this report delivers actionable strategies to mitigate risks and fortify defenses. Use these insights to take meaningful steps in protecting your networks, data, and people in an ever-evolving cyber landscape.

Cyber Table Stakes	Critical, baseline realities that organizations must address with foundational cybersecurity practices to protect themselves and secure their environments.
Cyber Trends	Emerging or changing aspects of cybersecurity that could have an outsized impact on your organization over the next 12 months.
Cyber Threats	Real-world environmental dangers based on changes in technology, threat behavior, actor risk appetite, or potential damage caused.

Cyber Table Stakes

1. You Are the Target

WHY IS THIS A TABLE STAKE?

Humans remain the weak link in cybersecurity and phishing the biggest entry point into the enterprise. Attackers know that employee access introduces vulnerabilities that cannot be fully mitigated through technical controls. They also know that people can often bypass technical controls and that user identity, access, and credentials can be used to pivot through an environment.

Breaches involving stolen or compromised credentials take the longest to identify and contain (292 days). Phishing and social engineering are not far behind (261 and 257 days). Employee credentials and passwords, their extended networks, and the insight they provide make targeting employees more than worth the attacker's time.

WHY WILL THIS REMAIN A TABLE STAKE OVER THE NEXT 12 MONTHS?

While cybersecurity and cyberattack technologies evolve with startling speed, the value of a person's identity and the techniques used to attack a person remain relatively static. That said, attack techniques are being enhanced as adversaries use AI to create more realistic social engineering attacks (e.g., phishing, vishing) that are harder to detect.

> Your employees are the target – their credentials, their passwords, their access, their organizational connections, the context of their work, and the roles they fill. For an adversary, your employees are invaluable.

HOW CAN THE GOVERNMENT RESPOND?

The most direct mitigation path is for the government to adopt a holistic, people-centric approach to cybersecurity.

- **Keep cybersecurity awareness training fresh and interesting to keep users engaged.** While using past threats as examples illustrates known responses and impacts, you can heighten interest by including emerging threats, such as deepfake audio attacks. Gamify training and checkpoints. Challenge users to identify and respond to simulated infiltration efforts. Keep score, make it competitive, and reward good detects.
- **Identify and focus on staff who are at high risk of attack**, both by role and by scanning social media, search engines, and the organization's external website. The nexus of those names, email addresses, and contact information represents an increased risk. Communicate that risk and provide tools for addressing it.
- **Set a "realism" target and craft simulated phishing messages consistent with it.**
- **Identify legitimate internal messages (e.g., HR alerts, closure notifications) that have characteristics of phishing messages and fix them.**
- **Employ continual feedback loops to examine failures.** Identify root causes and ways to address those failures from a technical and user perspective.

Cyber Table Stakes

2. Trustworthy Data

WHY IS THIS A TABLE STAKE?

Because data is king. And trustworthy data is not optional. 35% of breaches involve shadow data, highlighting that the sharp increase in the amount of data is making it harder to track and safeguard. And don't overlook the fact that these breaches also take longer to identify and contain. Data feeds everything in an automated, AI-enabled world. It is what the organization knows about itself, its partners, its mission, its operations, and its opponents. If any part of that data is corrupted or removed, it puts at risk all the other internal elements that rely on it to function — including automation and GenAI.

WHY WILL THIS REMAIN A TABLE STAKE OVER THE NEXT 12 MONTHS?

Because data will continue to be king and data quality is essential. Bad data, poorly sourced data, poisoned data, non-attributable data, un-alignable data, and un-normalized data all lead to the same place: bad, untrustworthy results.

As more system, personnel, and security data flood into any variety of data stores, the ongoing challenge is how to protect it and make it available to inform administrative and operational decision making, leading to effective mission accomplishment.

HOW CAN THE GOVERNMENT RESPOND?

The Evidence Act established the role of the CDO for federal agencies with responsibilities for lifecycle data management, governance, and quality to facilitate data-driven policy decisions. Since effective data security is directly dependent on proper data management, partner with the CDO to inventory and tag data. This improves insights and heightens understanding of the data sets and how they are used to better inform organizational selection, as well as the protection of high-value assets. Align zero trust based AuthN/Z access to systems and improve controlled access and auditing of data.

The criticality of clean, high-quality, accessible, and trusted data will only grow as that data is used to feed GenAI, attack surface management, and similar capabilities.

Cyber Table Stakes

3. Cybersecurity Supply Chain Risk Management

WHY IS THIS A TABLE STAKE?

As demonstrated by the SolarWinds Orion hack in 2020, the Log4J vulnerability in late 2021, and the MOVEit compromise in 2023, attackers can force multiply their attacks by inserting and disguising malware as legitimate, trusted software. This can include the insertion of malware into shared libraries and software dependencies or the leveraging of exploitable vulnerabilities in those libraries and dependencies.

It takes a well-resourced adversary to successfully execute supply chain attacks, typically backed by a nation-state actor. The potential for broad and expensive impact is a reminder as to why cybersecurity supply chain risk management (C-SCRM) is and will continue to be so important.

WHY WILL THIS REMAIN A TABLE STAKE OVER THE NEXT 12 MONTHS?

According to **Open Logic's 2024 report**, more than 95% of organizations use open-source software, including those that produce COTS products. The **2024 GitHub Octoverse report** revealed that 97% of apps use open-source software. And according to Gartner, 99% of businesses use at least one SaaS-type service. Reliance on SaaS software translates to reliance on cloud services, which inherently means a supply chain outside of the customer's control, visibility, or even knowledge. This issue will be magnified by any increase in the use of cloud computing, which is projected to grow by 17.9% CAGR from 2022-2027.

With the pervasive use of open-source software and components across industry and government, these numbers will serve as a forcing function for due diligence given the increased potential cyber supply chain risk they reflect.

HOW CAN THE GOVERNMENT RESPOND?

The government can leverage various authorities established via legislation, executive orders, and Federal Acquisition Regulation (FAR) policies and procedures. It can adopt secure software engineering practices, integrate zero trust and C-SCRM/Software Bill of Materials (SBOM) tools into DevSecOps. It can also improve its use of tools and processes in continuous integration and continuous delivery pipelines (inventory, supply chain/trusted reops, integrated security testing).

There is guidance on these topics and more from senior organizations such as OMB, NIST, and CISA. Examples include:

- CISA's **SBOM Resources Library**
- OMB's **memorandum on "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices"**

> Growing dependence on externally developed and controlled software, hardware, and data without adequate protections becomes an increasingly critical concern for the nation.

Cyber Table Stakes

4. Intelligence-driven Security

WHY IS THIS A TABLE STAKE?

It's practically impossible for security teams to address every risk to their organization's systems and data, especially given the large and diverse attack surface, vulnerabilities, and threats that most organizations face. Integrating intelligence data into a security program enables effective risk prioritization and effective application of the organization's resources.

Threat-intelligence data enables proactive identification of threats, techniques, and attacks that are most likely to be used against the organization and are therefore a higher priority to address. Intelligence on the organization's own business processes, data, and systems enables identification of assets that are of highest value to the organization, and therefore a priority to protect while at the same time being the highest values target of potential cyber actors. Knowing the details of current and emerging attacks and associated tactics, techniques, and procedures (TTPs) gives defenders a better chance and helps to prioritize vulnerability management.

Through intelligence-driven security, cyber leaders are armed with the information they need to make critical decisions, and security teams are able to leverage actionable information for faster, more focused defensive strategies.

WHY WILL THIS REMAIN A TABLE STAKE OVER THE NEXT 12 MONTHS?

The complexity and frequency of cyberattacks continues to escalate, driven by sophisticated threat actors and the rapid digital transformation of industries. Also, organizations' attack surfaces will continue to expand both in scope and scale as organizations increasingly adopt cloud technologies, IoT devices, and remote work models.

These factors will make it even less likely that security teams will be able to address all risks in a first-in-first-out fashion.

The complexity and frequency of cyberattacks will continue to escalate, driven by sophisticated threat actors and the rapid digital transformation of industries.

HOW CAN THE GOVERNMENT RESPOND?

The government can foster collaboration between the public and private sectors to enhance information-sharing around emerging threats and vulnerabilities, and to establish standardized frameworks for the integration of threat intelligence. This standardization would help reduce inconsistencies and ensure that actionable insights are operationalized effectively. The government can also invest in workforce development programs to address the shortage of skilled cybersecurity professionals, enabling more effective implementation of intelligence-driven strategies.

Finally, by funding advanced research and innovation in cybersecurity tools and technologies, the government can help ensure that intelligence-driven security evolves to counteract increasingly sophisticated cyber threats.

Cyber Trends

1. From Prevention to Resilience

WHY IS THIS A TREND?

"Design for prevention" has been the standard for decades, and many legacy systems are architected without resiliency or zero trust principles as primary drivers. As technology has evolved, "presumption of compromise" has become the new design focus and an important part of security architecture. It describes a movement away from a sole perimeter-based protection model towards a resource-centric model.

Acknowledging that technology is inherently flawed pushes architects and cyber leaders to assume that adversaries will find their way into the network and design to protect critical resources regardless of that compromise. The concept of resilience does not replace security, but it does need to become an attribute of the overall security profile agencies and organizations adopt. This issue is relevant for both new and legacy systems and environments.

WHY WILL THIS TREND CONTINUE OR ACCELERATE OVER THE NEXT 12 MONTHS?

Reliance on always-on and widely-exposed services connected to the internet and the web, combined with lack of attention to solid security design (driven in many cases by the desire to develop in an agile process but without security baked into the processes) has created an environment of nearly continuous attack across industry and government, at all levels. One reality of this continuous barrage is that an attacker will eventually establish a foothold, and the need to mitigate the damage of that inevitable successful attack points directly to the need to increase both operational and security resiliency.

HOW CAN THE GOVERNMENT RESPOND?

The adoption of zero trust architecture principles inherently improves resilience. Here are some related tactics for government technology leaders to consider:

- **Privilege controls** — Adopt the principle of attribute-based access control (ABAC) to answer the questions: "Is it the right person?" (MFA); "Are they connecting from a device we expect?" (device pillar); and "Are they connecting from a physical location we expect?" (session).
- **System realignment** — Reduce connections between mission-critical and non-mission-critical services and establish protections close to the resources you want to protect (policy enforcement point).
- **System segmentation** — Define and separate system elements based on criticality and trustworthiness.
- **Automation** — Automate governance and compliance tracking to ensure adherence to security policies and standards.

PLAN FOR THE INEVITABLE.

Your systems will be impacted, hacked, and compromised. How will you ensure the mission can go forward?

Cyber Trends

2. Empowering Cyber Professionals Through AI Augmentation

WHY IS THIS A TREND?

As cyber threats grow in sophistication and volume, AI-driven tools are increasingly being used to enhance cyber capabilities. These tools act as force multipliers, enabling analysts, threat hunters, and incident responders to process vast amounts of data, identify patterns, and make faster, more accurate decisions.

AI augments existing expertise by automating repetitive tasks, improving situational awareness, and uncovering needle-in-the-haystack insights that would otherwise be missed. This trend reflects the growing need for speed and scalability in SecOps.

WHY WILL THIS TREND CONTINUE OR ACCELERATE OVER THE NEXT 12 MONTHS?

Organizations face pressure to reduce response times and improve detection speed and accuracy in the face of near continuous attack. AI-powered tools — such as anomaly detection, automated threat triage, and predictive analytics — are becoming essential for cybersecurity teams to stay ahead of evolving threats. Advances in GenAI will further enhance tasks such as real-time reporting, contextual analysis, and incident response playbook optimization, making augmentation an operational necessity.

HOW CAN THE GOVERNMENT RESPOND?

The government can lead by fostering the innovation and adoption of AI-driven solutions across the public and private sectors. Investments in AI research tailored to cybersecurity challenges will enable the development of more sophisticated and adaptable tools. Also, facilitating AI integration into security operations can help agencies detect, analyze, and respond to threats more effectively.

By promoting AI training and education, the government can ensure cyber professionals are equipped to leverage these tools effectively. In many cases, software vendors are adding AI functionality into their security software products.

Finally, encouraging collaboration between AI developers, cybersecurity professionals, and policymakers will ensure AI augmentation delivers measurable improvements to national cyber resilience.

With AI rapidly becoming a critical mission-enablement tool, equipping professionals with AI education and tools increases acceptance and magnifies efficiencies.

Cyber Trends

3. AI: Cyber Friend and Foe

WHY IS THIS A TREND?

As cyber threats grow in sophistication and volume, AI-driven tools are increasingly being used to enhance cyber capabilities — for good and bad. As referenced above, there is a need to use AI to be more effective and productive, but that comes with an emphatic caveat: it is absolutely necessary to ensure that you use AI securely.

WHY WILL THIS TREND CONTINUE OR ACCELERATE OVER THE NEXT 12 MONTHS?

The government is adopting AI and AI-powered tools across the board to gain efficiency, strengthen capabilities, and secure systems and operational environments. As with any other leap in technology, the implementation of AI is not without its challenges. However, by adequately training your defenders in use and purposefully implementing and maintaining AI tools in accordance with your security plans, those potential risks can be minimized.

HOW CAN THE GOVERNMENT RESPOND?

The government can lead by fostering innovation in the use and acquisition of AI while strengthening a core set of risk management and cybersecurity practices: Take active steps to protect the integrity of the large language model (LLM) relative to supply chain, prompt injection, insecure output handling, and insecure plugin design.

- Carefully vet data sources and suppliers.
- Monitor for bias intentionally injected by bad actors, especially into training data.
- Implement continuous monitoring and timely patch management to address vulnerabilities.
- Implement strong access controls, like role-based access controls (RBAC) and the principle of least privilege.
- Regularly audit and monitor access logs.
- Automate governance and compliance tracking to ensure adherence to security policies and standards.
- Investigate and implement GenAI security and governance platforms to protect the LLM.

Don't let speed of adoption outpace purposeful and secure acquisition, implementation, and maintenance of your AI tools.

Cyber Threats

1. Lower Barriers to Offensive Cyber Operation

WHAT IS IT?

The increasing availability of advanced hacker tools, services, and platforms has made it easier for individuals and groups with limited technical expertise to conduct cyber operations.

The rise of ransomware-as-a-service (RaaS), exploit kits, and pre-built malware frameworks has significantly reduced the skill and resources needed to launch sophisticated attacks. These tools, often sold in underground marketplaces, enable even low-skilled actors to execute disruptive and impactful cyber campaigns.

WHY IS IT A THREAT?

This trend has led to a surge in the volume and frequency of cyber threats, as more opportunistic attackers take advantage of readily available tools. With minimal effort, less experienced adversaries are carrying out ransomware operations, phishing campaigns, and data exfiltration.

The accessibility of these tools lowers the barriers to entry, increasing the number of potential attackers and amplifying risks for organizations and governments. When combined with automation and AI-driven capabilities, adversaries can rapidly scale their operations, overwhelming defenses that are not designed for this volume and speed.

HOW CAN THE GOVERNMENT RESPOND?

The government can address this growing threat by focusing on disrupting the underground ecosystems where malicious tools and services are distributed, while strengthening public-private partnerships to share intelligence on emerging tactics, tools, detections, and countermeasures.

Encouraging widespread adoption of strong cybersecurity hygiene will help mitigate less sophisticated attacks, enable effective detection and response, and raise the bar for attackers. Investments in workforce development can ensure a skilled security workforce that's equipped to counter these threats.

Additionally, monitoring and regulating the use of automation and AI technologies will be critical to prevent their misuse for malicious purposes.

LOWER BARRIERS + MORE PLAYERS IN THE GAME = MORE RISK

Cyber Threats

2. Faster Exploitation of Vulnerabilities

WHAT IS IT?

Cyber adversaries are exploiting newly disclosed vulnerabilities at a rapid pace, drastically reducing the time between public disclosure and active weaponization. This accelerated exploitation timeline means attackers swiftly turn known vulnerabilities into workable exploits, applying them across a wide range of environments.

Key events like **Log4j (Log4Shell)** illustrate how quickly adversaries can pivot to weaponize vulnerabilities on a global scale. As agencies and organizations expand the number of systems and connected endpoints, the attack surface grows larger and more intricate, providing a much larger target for attackers. And as those same actors expand their focus to a broader array of vendors, it puts the onus on defenders to cover their entire attack surface instead of relying on flying under the attacker's radar.

WHY IS IT A THREAT?

The accelerating timeline for exploitation poses a severe risk to organizations that cannot patch systems quickly.

Threat actors are increasingly prioritizing known vulnerabilities due to their low effort and high reward. This trend magnifies the risk for widely deployed systems, particularly those in critical infrastructure and cloud environments.

Furthermore, the diversification in attacker targets means that organizations relying on niche or less-common third-party providers are equally at risk. For example, as Linux adoption grows in enterprise environments, adversaries are exploiting both kernel-level and framework vulnerabilities to disrupt systems, exfiltrate data, or establish command-and-control infrastructure.

HOW CAN THE GOVERNMENT RESPOND?

To counter the rapid exploitation of vulnerabilities, organizations should adopt a risk-based approach to vulnerability management rather than attempting to patch everything equally. Focusing on the vulnerabilities that pose the greatest risk — based on prevalence in the environment, asset criticality, and exploitability — ensures resources go where they have the most impact. In other words, fix the biggest problems on the most important systems first.

Automation and orchestration tools accelerate this targeted patching process. Network segmentation remains essential for containing breaches, while robust detection, including deception techniques such as **honeytokens and honeypots**, enable response to exploitation attempts before widespread impact.

Risk-based vulnerability management, supported by intelligence-driven operations and automation, helps ensure the most effective use of an organization's limited resources.

Cyber Threats

3. AI-powered Threats

WHAT IS IT?

Adversaries are increasingly leveraging AI to enhance the speed, precision, and scale of their attacks.

WHY IS IT A THREAT?

The integration of AI into cyberattack methods dramatically increases the efficiency and effectiveness of malicious campaigns. AI tools reduce the need for manual effort, making it easier for attackers to scale operations while improving success rates.

For example, AI can craft convincing phishing emails tailored to specific targets at a scale and speed that humans cannot match. Advanced AI-driven malware can autonomously identify vulnerabilities and adjust its behavior to avoid detection, extending the lifespan of attacks.

As AI capabilities continue to improve, adversaries will exploit them to accelerate operations, target critical systems, and amplify damage, placing immense strain on organizations' cybersecurity defenses.

HOW CAN THE GOVERNMENT RESPOND?

To counter the rising threat of AI-powered attacks, the government must invest in advanced detection technologies that incorporate AI and machine learning to identify evolving attack patterns in real time.

Collaboration between the public and private sectors is critical to share intelligence on AI-driven threats and develop countermeasures. Promoting research into AI-based defensive solutions will help ensure security tools evolve as quickly as adversarial tactics.

Additionally, strengthening workforce training programs focused on AI and threat modeling can prepare defenders to combat emerging attack techniques. By regulating the misuse of AI tools and fostering responsible innovation, the government can mitigate risks while harnessing AI's potential to strengthen national cyber resilience.

AI is rapidly lowering the barriers to entry while simultaneously improving the success rates and scalability of attacks.

Cyber Threats

4. Ransomware and the Rise of Double and Triple Extortion

WHAT IS IT?

Ransomware attacks remain a persistent and escalating threat, with adversaries deploying increasingly sophisticated tactics to maximize disruption and financial gain.

Recent trends indicate a shift toward double and triple extortion techniques, where attackers go beyond encrypting data by exfiltrating sensitive information and threatening public disclosure or attacks on third parties. Also, RaaS platforms have lowered the barrier to entry, enabling less skilled actors to launch damaging campaigns.

These developments, coupled with the growing integration of AI in ransomware tools, suggest that the threat landscape will continue to evolve in complexity and scale.

WHY IS IT A THREAT?

The financial and operational impacts of ransomware are staggering, with attacks targeting critical sectors such as healthcare, energy, and government, where disruptions have life-or-death consequences.

Beyond monetary losses, ransomware campaigns increasingly target data integrity and trust, undermining confidence in public services and private enterprises alike. The use of AI and automation by attackers could further accelerate the speed and efficacy of ransomware campaigns, making traditional defenses less effective.

In 2025, we are likely to see ransomware attacks become more targeted, leveraging custom techniques to exploit sector-specific vulnerabilities and circumvent conventional protections.

HOW CAN THE GOVERNMENT RESPOND?

To address the growing ransomware threat, the government must take a proactive stance by enforcing stricter regulations on cybersecurity standards for critical infrastructure and by facilitating faster incident reporting to improve national response efforts.

Investments in advanced detection and response capabilities, including the use of AI and machine learning, will be crucial to counter the speed and sophistication of modern ransomware attacks. Strengthening international collaboration is essential to disrupt ransomware ecosystems, including targeting operators, dismantling RaaS platforms, and addressing cryptocurrency misuse for ransom payments.

Finally, fostering resilience through regular scenario-based exercises, widespread adoption of zero trust architecture, and robust public awareness campaigns will be key to mitigating the evolving ransomware landscape.

Beyond monetary losses, ransomware campaigns increasingly target data integrity and trust, undermining confidence in public services and private enterprises alike.

Cyber Threats

5. State-sponsored Cyber Espionage

WHAT IS IT?

A series of cyber espionage campaigns attributed to state-sponsored actors, particularly from China, have demonstrated the capacity to infiltrate critical U.S. systems and exfiltrate sensitive data.

These attacks employ sophisticated techniques, targeting vulnerabilities in infrastructure and exploiting weak points in supply chains, with implications far beyond the private sector. The campaigns underscore the broader trend of adversarial nations leveraging cyber operations to gain intelligence, disrupt services, erode public trust in critical infrastructure, or make geopolitical statements related to specific conflicts (e.g., Ukraine) or organizations (e.g., NATO).

WHY IS IT A THREAT?

The implications of these state-sponsored campaigns are profound, as they threaten the security of sensitive data, disrupt critical operations, and pose a direct risk to national security. The presence of foreign actors in IT and operational technology positions throughout our critical infrastructure only magnifies the potential threat.

Exfiltrated data could provide adversaries with strategic insights into U.S. governmental and industrial operations, supply chains, and emerging technologies. The interruption of critical infrastructure pieces could cause harm to the security and economy of this country.

This trend highlights the growing reliance on cyber capabilities as a tool of geopolitical competition, emphasizing the need for vigilance. The risk is particularly acute given the increasing interconnectedness of critical systems and the expanding attack surface.

HOW CAN THE GOVERNMENT RESPOND?

The government must prioritize a coordinated response to counter cyber espionage by state-sponsored actors. This includes enhancing public-private partnerships to improve threat intelligence sharing and bolstering cybersecurity standards across critical infrastructure sectors.

Regular, mandatory security audits, coupled with the deployment of advanced threat detection and response systems, are critical to identifying and mitigating evolving threats. Additionally, investments in workforce training and public awareness campaigns can help safeguard against phishing and social engineering tactics, which often serve as entry points for these sophisticated operations. Even with these measures, this level and type of attack is extremely sophisticated and has proven to be nearly unstoppable by an agency on its own. The key is early detection and working with CISA and the FBI.

There are nation-state actors in IT and operational technology positions within the critical infrastructure waiting to exploit their positions.

Conclusion

An Ever-evolving Threat Environment Requiring Constant Attention

There is no magic cybersecurity bullet — nothing that can provide an all-in-one answer. Every mission and every system is unique, and the threat environment is an ever-evolving space that requires constant attention.

Most cyber risk is mitigated through consistent application of the basics: multifactor authentication, encryption (at rest and in transit), endpoint detection and response, logging, and workforce. The table stakes, trends, and threats we've described in this document are a snapshot of that changing external environment.

If you have questions about the information in this report or if you want to learn how ECS approaches security operations; governance, risk, and compliance; or security architecture and engineering, please **contact us through our website**. We also invite you to connect with us on LinkedIn.

Joanna Dempsey
Vice President, CISA Portfolio

Keith McCloskey
Vice President and Chief Technology Officer

Mike Zakrzewski
Vice President, Cyber Technology

Beau Houser
Senior Director of Cybersecurity

Dave Howard
Senior Director, Cyber Operations

Greg Scheidel
Chief Cybersecurity Officer

Anthony Zech
Senior Director, Data & AI