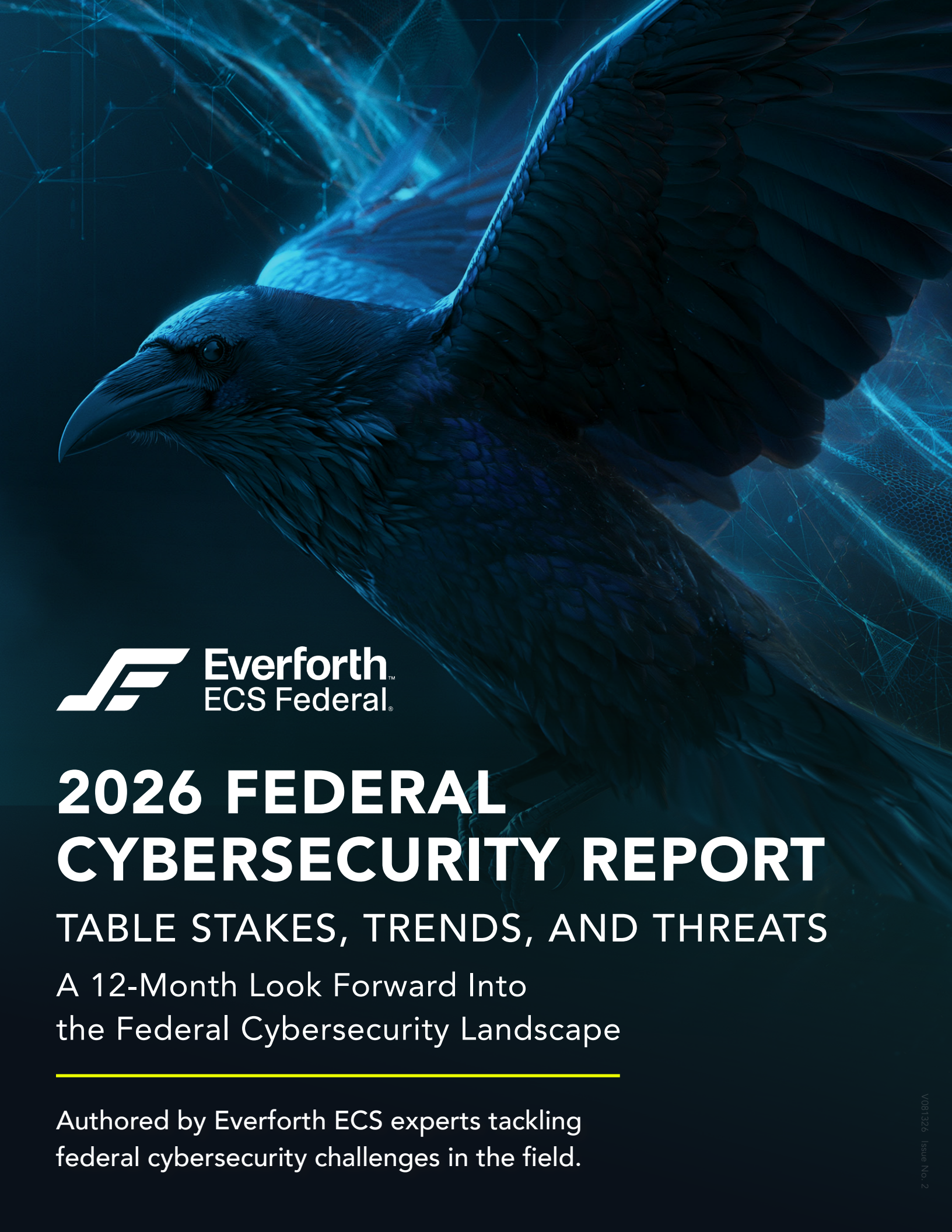

Everforth
ECS Federal

# 2026 FEDERAL CYBERSECURITY REPORT

## TABLE STAKES, TRENDS, AND THREATS

### A 12-Month Look Forward Into the Federal Cybersecurity Landscape

Authored by Everforth ECS experts tackling federal cybersecurity challenges in the field.

V081326 Issue No. 2

# Table of Contents

# Introduction

*Every year, cyber threats grow more sophisticated, more frequent, and more consequential. In the 2026 edition of our annual Cybersecurity Report,* ***Everforth ECS examines the challenges facing federal agencies and how they can stay ahead in the coming year.***

*This report contains the insights of cybersecurity leaders from the Department of War (DoW), Intelligence Community (IC), Cybersecurity and Infrastructure Security Agency (CISA), federal civilian, and commercial organizations. Drawing on operational knowledge and established frameworks, this report identifies the trends, threats, and priorities demanding focused attention in the year ahead with a single goal:* ***help decision-makers prioritize resources, reduce risk, and limit disruption****.*

## Cybersecurity in 2026: The Turning Point

2026 represents a critical turning point in cybersecurity due to several transformative forces:

- **Technological Acceleration and Mass AI Adoption:** The rapid adoption and integration of AI into both offensive and defensive cyber operations have fundamentally altered the speed of and response to cyber threats.
- **Identity as a Battleground**: As organizations adopt cloud technologies, remote work, and SaaS applications, identity security has become a central cybersecurity battleground. But identity is only as good as the **cryptography** behind it, and with **quantum computing emerging as a credible threat to current encryption standards**, the foundation that identity security is built on is itself at risk.
- **Vulnerability of Interconnected Digital Ecosystems:** The deep interdependence of modern digital supply chains means that a single vulnerability (forged credentials, signed software, etc.) in a widely adopted component or trusted third-party service can trigger cascading failures that impact entire sectors.

The result of these transformative forces can be felt everywhere in the cyber landscape, from **faster breakout times to growing supply chain and ransomware risk**.

> **"Breakout time—the period between initial access and lateral movement—dropped to just 29 minutes in 2025, representing a 65% increase in speed over the prior year."**
>
> CrowdStrike 2026 Global Threat Report

2025–2026 THREAT LANDSCAPE

# Key Cybersecurity Statistics

| Average Breakout Time | Annual Cybercrime Cost | Ransomware Events | Annual Cybercrime Cost |
|---|---|---|---|
| **29 Min** | **$1.2T+** | **7,419** | **4x increase** over five years |

| FINDING | METRIC | DETAIL |
|---|---|---|
| Malware-free detections | 82% | Of all detections in 2025 were malware-free, confirming adversaries have shifted toward identity-based intrusions, living-off-the-land techniques, and exploiting trusted cloud and SaaS relationships |
| AI-enabled adversary operations | +89% YoY | AI-enabled attacks grew 89% year-over-year. Threat actors exploited generative AI tools at 90+ organizations by injecting malicious prompts to steal credentials and cryptocurrency. |

## A Framework for Examining Cybersecurity's Future

Maintaining an **effective cybersecurity program** requires regularly assessing:

- Existing strategies and practices
- New or changing strategies, techniques, and technologies
- The status of threats and threat actors

This report provides that assessment and arms you with the insights you need to validate and strengthen your security posture.

We've framed this report around not only **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 provides actionable strategies to mitigate risks and fortify defenses. Use these insights to take meaningful steps to protect your networks, data, and people in an ever-evolving cyber landscape.

# Cyber Table Stakes

## 1. You Are the Primary Target

### WHY IS THIS A TABLE STAKE?

People remain the weak link in cybersecurity and identity has become the emerging battleground of the cyber landscape.

In 2025, over **82% of detections were malware-free**[1], proving adversaries have moved to identity-based techniques (phishing, vishing) to hack in. They are logging in using stolen credentials, trusted identity flows, and approved SaaS integrations. Employee credentials and passwords, their extended networks, and the insight they provide make targeting employees more than worth an attacker's time.

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

The value of a person's identity in creating a breach remains relatively static. However, the use of AI to create more realistic social engineering attacks (phishing, vishing, deepfake impersonation, etc.) has fundamentally changed the threat. Generative AI can create hyper-realistic phishing emails that mimic a target's communication style and real-time deepfake vishing audio, making impersonation difficult to detect. An estimated **9 out of 10 organizations**[2] faced a successful identity-related breach in the last 12 months.

### HOW CAN THE GOVERNMENT RESPOND?

- **Keep training current and engaging.** Use emerging threats, gamified checkpoints, and realistic exercises to build awareness.
- **Identify high-risk staff.** Review roles and public exposure, then provide targeted support.
- **Set a realism target.** Design phishing simulations to match the level of realism you want to test.
- **Fix legitimate messages that look like phishing.** Revise internal notices that could confuse users. Digital signatures are also a good way to add trust to an email.
- **Use continuous feedback loops.** Review failures, identify root causes, and improve both technical controls and user practices.
- **Implement AI-powered email security solutions that analyze not only context, but intent and behavior.** This will help detect sophisticated AI-generated phishing attempts that traditional filters might miss.

> "We no longer defend a network perimeter; **we defend a decentralized ecosystem** of identities, devices, and data."

**Mike Zakrzewski**
Vice President, Cyber Technology

1 Crowdstrike 2026 Global Threat Report 2 Paloalto Networks 2026 Identity Security Landscape

# Cyber Table Stakes

## 2. Trustworthy Data

### WHY IS THIS A TABLE STAKE?

Because data remains king and trustworthy data is not optional. **35% of breaches involve shadow data**[3], highlighting that the sharp increase in data volume is making it harder to track and safeguard.

Data feeds everything in an automated, AI-enabled world. If any part of that data is corrupted or compromised, it puts at risk all the other elements that rely on it to function, including AI.

> "Bad data doesn't just produce bad results, it produces wrong ones, confidently. In a world increasingly run by AI, **the integrity of your data is the integrity of your organization.**"

**Scott Hoge**
Vice President,
Strategic Solutions

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

Data quality remains essential. Bad, poorly sourced, poisoned, non-attributable, unaligned, or un-normalized data all lead to the same place: bad, untrustworthy results.

As data volume and our reliance on it grow, data security and availability become even more paramount in operational decision making. Additionally, the growing trend of **data democratization** — driven by technologies like vibe coding — is reshaping how organizations operate.

While broader data access accelerates decision making and fuels innovation and agility, it comes with significant cybersecurity implications, as **wider access** to untrained technical users introduces **increased security and privacy risks.**

### HOW CAN THE GOVERNMENT RESPOND?

**The Evidence Act** established the role of the Chief Data Officer (CDO) for federal agencies, with responsibilities for lifecycle data management, governance, and quality to facilitate data-driven policy decisions. We recommend partnering with your CDO to:

- Directly **inventory and tag data** for proper data management
- Apply zero trust **data pillar principles**, including data loss prevention (DLP), data classification and tagging, and encryption at rest, in transit, and in processing
- Invest in policies and training to **improve data literacy**
- Implement policy and infrastructure to keep data accurate, compliant, and protected
- Continue **publication of guidance, policies, and standards** (M-26-14, CISA's Logging Reference Architecture, etc.) and promoting alignment to these standards

3 IBM Cost of a Data Breach Report

# Cyber Table Stakes

## 3. Cybersecurity Supply Chain Risk Management

### WHY IS THIS A TABLE STAKE?

The growing interconnectivity of modern digital operations requires organizations to actively manage supply chain risk across two critical domains:

- **Software and hardware SCRM** — Ensuring the integrity of components and code embedded in your systems
- **Third-party organizational risk** — Managing the posture of the vendors and service providers your mission depends on

Attackers can force-multiply their impact across both by inserting and disguising malware as legitimate, trusted software, as demonstrated by:

- The Change Healthcare incident (2024)
- The Axios NPM package compromise (2025)
- The Shai-Hulud npm supply chain attacks (2025/2026)

> "The most dangerous cyberattacks don't break through your defenses. **They walk in through software you already trust.**"
>
> 
>
> **Keith McCloskey**
> Vice President, National Security

These attacks typically require a well-resourced, nation-state-backed adversary, and their potential for broad, expensive impact is precisely why cybersecurity supply chain risk management (C-SCRM) remains critical.

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

Increased reliance on third-party vendors, SaaS, and cloud services means a supply chain largely outside the customer's control, visibility, or even knowledge. And statistics show the scale of exposure is significant with:

- **More than 98%** of organizations using open-source software[4]
- **98%** of applications using open-source components[5]
- **99%** of businesses using at least one SaaS-type service[6]

### HOW CAN THE GOVERNMENT RESPOND?

The government can leverage authorities established via legislation, executive orders, and FAR policies to address supply chain risk. To start:

- Adopt **secure software engineering** practices across development lifecycles
- Integrate **zero trust, C-SCRM, and SBOM** tools into **DevSecOps pipelines**
- **Strengthen CI/CD processes** through trusted repositories and integrated security testing

Key guidance resources include:

- CISA's SBOM Resources Library
- OMB's memorandum on "Adopting a Risk-based Approach to Software and Hardware Security"
- NIST's Secure Software Development Framework 800-218 v1.1

4 Open Logic 2026 State of Open Source Report 5 Black Duck Open Source Security and Risk Analysis Report 6 BetterCloud's State of SaaSOps surveys

# Cyber Table Stakes

## 4. Intelligence-driven Security

### WHY IS THIS A TABLE STAKE?

It's practically impossible for security teams to address every risk, given the large and diverse attack surfaces most organizations face. Integrating threat intelligence into a security program enables **effective risk prioritization and smarter application of resources** by:

- Identifying threats and techniques most likely to be used
- **Highlighting the highest-value assets** worth protecting
- Providing defenders with current **tactics, techniques, and procedures (TTPs)** to prioritize vulnerabilities
- Arming cyber leaders with the information needed for critical decisions and 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. Attack surfaces continue to expand as organizations increasingly adopt:

- Cloud technologies
- IoT devices
- Remote work models

This makes it increasingly unlikely that security teams can address all risks in a first-in-first-out manner.

### HOW CAN THE GOVERNMENT RESPOND?

- **Foster public-private collaboration** to enhance information-sharing around emerging threats and establish standardized frameworks for integrating threat intelligence
- **Invest in workforce development** to address the shortage of skilled cybersecurity professionals
- Fund advanced research and innovation in cybersecurity tools to ensure intelligence-driven security evolves against increasingly sophisticated threats
- Use **threat intelligence** to continuously inform zero trust policies, ensuring access controls reflect the most current picture of organizational risk

"In cybersecurity, the most dangerous word isn't 'breach.' It's 'unknown.' **Intelligence-driven security exists to eliminate the unknown before adversaries can exploit it.**"

**Mark Maglin**
Vice President,
Global Defense Cybersecurity

# Cyber Table Stakes

## 5. Continuous Risk Management

### WHY IS THIS A TABLE STAKE?

The era of periodic, checkbox-style compliance is over. The **Department of War (DoW)** is implementing **Cybersecurity Maturity Model Certification (CMMC) 2.0** through a four-phase rollout that began on November 10, 2025. CMMC formally integrates cybersecurity requirements into defense contracts, signaling a decisive shift toward ongoing risk monitoring. Rather than relying on point-in-time reviews like the traditional three-year ATO cycle, continuous risk management enables organizations to:

- Detect attacks, vulnerabilities, and compliance lapses in real time
- Shift from reactive audits to **proactive, intelligence-driven defense**
- Maintain an **accurate, living picture** of organizational risk posture

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

DoW reporting requirements will continue to evolve, placing greater accountability on contractors to **proactively demonstrate compliance**. Key pressures include:

- **CMMC 2.0 enforcement expansion,** including mandatory C3PAO Level 2 certification starting **November 2026** for new DoW contracts that include **controlled unclassified information (CUI)**
- Growing burden on contractors to prove supply chain compliance
- Increased scrutiny of third-party and subcontractor risk as supply chain attacks rise

### HOW CAN THE GOVERNMENT RESPOND?

Adopting intelligence-driven security as the foundation of continuous risk management delivers measurable benefits, including:

- **Reducing manpower and costs** by automating monitoring rather than staffing periodic review cycles
- **Identifying risks earlier** in the development lifecycle, where remediation is less expensive
- **Prioritizing and focusing** limited resources on the **risks that matter most**

> "Guidance from OMB, NIST, and CISA provides a strong foundation. Frameworks such as the RMF, Zero Trust, and CMMC offer **compliant, resilient structures for building a continuous risk management capability**."

**Joanna Dempsey**
Business Unit Leader, Federal Civilian

# Cyber Trends

## 1. From Prevention to Resilience

### WHY IS THIS A TREND?

"Design for prevention" has long been the standard, but as technology has evolved, "**presumption of compromise**" has become the new design focus. This represents a shift away from perimeter-based protection toward a resource-centric model that acknowledges adversaries will eventually gain network access.

Ultimately, embracing this new model recognizes that no preventive technology is ever perfect and **increasing cyber resilience requires** designing systems to protect your most critical resources.

> "The question is no longer whether adversaries will get in. It's whether your systems are designed to **survive it** when they do."

**Rachel Douglas**
Senior Director,
Federal Civilian Cybersecurity

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

Relying on **always-on, internet-exposed services** — combined with **security being given less priority in agile development** — has created an environment of near-continuous attack. The reality is that a determined adversary will eventually succeed. That's why it is just as important to be able to absorb, adapt, and recover from an attack as it is to prevent one from happening.

### HOW CAN THE GOVERNMENT RESPOND?

Adopting the following zero trust architecture principles will inherently improve cyber resilience:

- **Privilege controls** — Implement attribute-based access control (ABAC) and multi-factor authentication (MFA)
- **System realignment and segmentation** — Reduce connections between mission-critical and non-critical services and establish policy enforcement points close to protected resources
- **Automation** — Automate governance and compliance tracking to ensure continuous adherence to security policies

Additionally, agencies should focus on these three areas to establish proactive cyber resilience:

- **Proactive Threat Mitigation and Secure Design** — Implement **preventative Content Disarm and Reconstruction (CDR)** technologies, a **Software Bill of Materials (SBOMs)** for increased visibility, and **Post-Quantum Cryptography (PQC)** to mitigate future risk
- **Resilient Operations and Recovery** — Focus on continuous ATO (cATO), continuous monitoring, AI-accelerated detection and incident response, and tabletop exercises
- **Governance and Workforce** — This includes implementing a unified risk operations strategy, upskilling cyber talent, and reinforcing data governance

# Cyber Trends

## 2. The Agentic AI Arms Race

### WHY IS THIS A TREND?

We are in the era of agentic AI, with an estimated 43% of organizations considering its adoption in 2026. This massive investment has major cybersecurity ramifications, as AI-driven tools are increasingly being used by both defenders and adversaries, fueling an agentic AI arms race.

This isn't simply a battle of offensive versus defensive capabilities. It is a battle of speed — the attacker's speed of intrusion versus the defender's speed of response, requiring organizations to fully embrace AI-driven detection and response solutions.

> "Attackers complete full breach cycles in minutes. **Organizations average six days to respond.** The age of human-speed cybersecurity is over and the window to close that gap is narrowing fast."

**Keith McCloskey**
Vice President,
National Security

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

Threat actors are moving decisively toward AI agents that can **operate autonomously, adapt in real time, and execute attacks** at a scale no human-directed campaign can match. Tactics include:

- **Prompt Injection** — Adversaries manipulate AI to bypass guardrails and execute hidden commands (90+ organizations exploited via malicious prompts)[7]
- **Autonomous Agents** — AI systems that independently bypass MFA and scale attacks in real time (94% of executives rank AI as the #1 cybersecurity change driver)[8]
- **AI Credential Theft** — 300,000+ ChatGPT credentials found for sale on the dark web with ChatGPT mentioned 550% more in criminal forums than any other model[9]

### HOW CAN THE GOVERNMENT RESPOND?

Attackers complete full **breach cycles in minutes**. Organizations average six days to respond. Closing this gap requires moving beyond human-centric incident response entirely:

- **Adopt AI-driven detection and response** — Deploy autonomous SOC capabilities that detect, triage, and contain threats at machine speed
- **Establish AI use and governance policies** — Define clear boundaries for agentic AI use across systems, ensuring AI tools cannot be manipulated or repurposed by adversaries
- **Invest in adversarial AI testing** — Regularly red-team AI systems to identify prompt injection vulnerabilities and guardrail weaknesses before adversaries do
- **Build toward a human-on-the-loop model** — Shift from human-in-the-loop approval for every action to automated response with human oversight, enabling speed without sacrificing accountability

7 Crowdstrike 2026 Global Threat Report 8 World Economic Forum's Annual Global Cybersecurity Outlook Report 9 Crowdstrike 2026 Global Threat Report

# Cyber Trends

## 3. The Convergence of IT and OT

### WHY IS THIS A TREND?

**Information Technology (IT)** and **Operational Technology (OT)** systems have historically operated in isolation. However, over the past decade, a shift has taken place, with OT environments increasingly incorporating networking and computational technologies that have blurred the separation between the two.

Driven by the rise of **Industrial IoT (IIoT)**, the convergence of IT and OT systems offers numerous advantages, including **improved interoperability** between virtual and physical systems and advancements in **process automation and distributed operations**.

However, this convergence has had major cybersecurity implications by **expanding attack surfaces** to include interconnected IT/OT environments, without the proportionate security controls, making them a growing and worthwhile target for nation-state adversaries.

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

Several forces will only intensify IT/OT risk in the near term:

- **AI-accelerated Industrial Threats** — Generative AI continues to serve as a force multiplier, enabling rapid identification of weak points in IT/OT systems
- **Living-off-the-Land Techniques** — A practice where adversaries exploit legitimate administration tools and valid credentials rather than malware, making detection significantly more difficult (82% of all detections were malware free in 2025)
- **Operational Disruption as a Service (ODaaS)** — The rise of specialized services purpose-built to create production downtime
- **IoT and Edge Device Proliferation** — Continued expansion of connected devices broadens the attack surface further

### HOW CAN THE GOVERNMENT RESPOND?

Agencies looking to reduce IT/OT risk should focus on the following:

- **Deploy automated IoT/OT security and monitoring platforms —** Implement solutions that use passive network monitoring to safely discover, classify, and assess the risk of connected assets without disrupting operations
- **Requiring and implementing unified security models —** Enforce deeper scrutiny of supply chain vulnerabilities by implementing proper C-SCRM protocols across both IT and OT environments
- **Modernize IT and OT defenses with an emphasis on:**
  - **Identity, Credential, and Access Management (ICAM)** to control and audit who and what accesses critical systems
  - **Zero trust principles** applied to **OT networks**, not just traditional IT infrastructure

> **"The convergence of IT and OT has quietly become one of the most consequential shifts in cybersecurity, expanding the attack surface from the digital world into the physical one."**

**Greg Scheidel**
Senior Engineer, Federal Civilian Cybersecurity

# Cyber Trends

## 4. Post-Quantum Computing Moves to Action

### WHY IS THIS A TREND?

The quantum threat is no longer theoretical. It is a reality that is just around the corner. **NIST** finalized its first set of post-quantum cryptography (PQC) standards in **August 2024**, marking a significant moment in the transition away from encryption protocols that quantum computers will eventually render obsolete.

The cybersecurity community refers to the day a quantum computer becomes capable of breaking current encryption as "Q-Day", and the countdown has already begun.

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

2026 marks the year PQC moves from theoretical discussion into mandatory action plans, driven by **three converging pressures:**

- **"Harvest Now, Decrypt Later"** — Nation-state adversaries are intercepting and storing encrypted data today, planning to decrypt it once quantum capabilities mature, potentially as early as the 2030s (or before). Sensitive data collected now is already at risk.
- **Federal mandates** — NIST PQC standards and federal acquisition mandates taking effect in 2027 signal a complex, mandatory cryptographic transition for both enterprise and government sectors.
- **Transition complexity** — Migrating cryptographic infrastructure is a multi-year undertaking, meaning organizations that delay action now will be non-compliant and exposed when deadlines arrive.

### HOW CAN THE GOVERNMENT RESPOND?

- **Create a cryptographic inventory —** Identify all data, systems, and applications relying on current cryptographic protocols
- **Assess risk and prioritize —** Classify data by long-term sensitivity and determine which systems require immediate transition versus longer timelines
- **Adopt cryptographic agility —** Update infrastructure to allow cryptographic algorithms to be swapped without rebuilding entire systems
- **Implement hybrid cryptography —** Deploy a combinationof traditional and PQC algorithms during the transition period
- **Engage vendors —** Request PQC roadmaps from vendors and ensure their software and hardware updates support NIST-approved algorithms

> "**Post-quantum cryptography is no longer a future consideration**, but a present-day priority. Q-Day may still be years away, but the data being stolen now will be waiting for it."

**Mark Maglin**
Vice President,
Global Defense Cybersecurity

# Cyber Threats

## 1. Lower Barriers to Offensive Cyber Operations

### WHAT IS IT

The increasing availability of advanced hacker tools, services, and platforms has made it easier than ever for individuals with **limited technical expertise** to conduct **sophisticated cyber operations**. Key enablers include:

- **Ransomware-as-a-Service (RaaS)** — Subscription-based ransomware platforms that require no technical knowledge to deploy
- **Exploit kits and pre-built malware frameworks —** Off-the-shelf attack tools sold in underground marketplaces
- **AI and automation —** Enabling adversaries to rapidly scale operations, overwhelming defenses not designed for this volume or speed

> "When sophisticated cyberattack tools become commodities, the threat isn't just more attackers. It's an **entirely different scale of attack**."

**Beau Houser**
Senior Director,
Federal Civilian Cybersecurity

### WHY IS IT A THREAT?

Lowering the barrier to entry doesn't just increase the number of potential attackers. It fundamentally changes the threat landscape:

- **The volume, sophistication, and speed** of attacks surge as opportunistic, low-skilled actors launch ransomware operations, phishing campaigns, and data exfiltration with minimal effort
- AI allows even **unsophisticated adversaries** to operate at a scale and speed that **outpaces traditional defenses**
- Organizations and governments face a threat environment that is simultaneously **broader, faster, and harder to attribute**

### HOW CAN THE GOVERNMENT RESPOND?

- **Disrupt underground ecosystems** — Target the marketplaces and infrastructure where malicious tools and services are distributed
- **Strengthen public-private partnerships** — Share intelligence on emerging tactics, tools, detections, and countermeasures across sectors
- **Promote cybersecurity hygiene** — Encourage widespread adoption of foundational security practices to raise the bar for opportunistic attackers and enable effective detection and response
- **Invest in workforce development** — Ensure a skilled security workforce equipped to counter an expanding and diversifying threat landscape
- **Monitor AI and automation misuse** — Establish regulatory frameworks to prevent the weaponization of AI technologies for malicious purposes

# Cyber Threats

## 2. Hyper-accelerated Breakout Times

### WHAT IS IT

**Adversary speed** is reaching unprecedented levels, fundamentally **challenging traditional incident response models**. AI is accelerating that collapse, with threat actors now deploying **AI agents to automate reconnaissance, identify lateral movement paths,** and **execute attacks** with a precision and speed no human-directed campaign can match.

In 2026, any organization still relying on manual detection and response will be left behind before they even know an attack has begun.

### WHY IS IT A THREAT?

The numbers reported by CrowdStrike[10] tell the story:

- **29 minutes** — average eCrime breakout time in 2025, a 65% increase in speed over 2024
- **27 seconds** — the fastest observed breakout on record
- **4 minutes** — time to data exfiltration in one observed intrusion after initial access
- **6 days** — the average organizational response time

That gap between 29 minutes and six days is not a security problem. It is a math problem in which the math is not on the defender's side.

### HOW CAN THE GOVERNMENT RESPOND?

Closing the gap requires a fundamental shift away from manual incident response:

- **Deploy automated, AI-driven detection and response** — Machine-speed threats require machine-speed defenses. If response time is measured in minutes or hours, it's a game of catch-up that cannot be won.
- **Shift left on threat detection** — Invest in early-indicator monitoring and behavioral analytics to identify intrusions before breakout occurs.
- **Establish and regularly test response playbooks** — Tabletop exercises and continuous ATO (cATO) practices ensure response protocols are ready to execute at speed when seconds matter.

> "The advent of AI-accelerated threats has compressed response windows past the limit of human intervention capabilities, **making real-time, AI-native defense capabilities an operational necessity**.

**Charles D. Walker**
Senior Cyber Solutions Architect, National Security

10 Crowdstrike 2026 Global Threat Report

# Cyber Threats

## 3. Faster Exploitation of Vulnerabilities

### WHAT IS IT

Cyber adversaries are exploiting newly disclosed vulnerabilities faster than ever, drastically reducing the time between public disclosure and active weaponization. As supply chains grow more complex and systems rely on more connected endpoints, the attack surface increases, creating additional points of vulnerability for adversaries to exploit.

> A **42% increase** in zero-day exploitation means defenders are increasingly fighting attacks that have no patch. The vulnerability window isn't shrinking – it's disappearing."
>
> 
>
> **Mike Zakrzewski**
> Vice President,
> Cyber Technology

### WHY IS IT A THREAT?

The accelerated timeline for exploitation poses a severe risk to organizations that cannot patch systems quickly. Threat actors prioritize known vulnerabilities for low effort/high reward operations, particularly across critical infrastructure and cloud environments.

The numbers reflect this urgency:

- CrowdStrike[11] observed a **42% year-over-year increase in zero-day vulnerabilities exploited prior to public disclosure,** meaning defenders increasingly face attacks before a patch even exists
- **67% of vulnerabilities exploited by China-nexus adversaries** provided immediate system access, while **40% targeted edge devices that typically lack comprehensive monitoring**[12]
- **Growing Linux adoption has opened new attack vectors,** with adversaries exploiting vulnerabilities to exfiltrate data and establish command-and-control infrastructure

### HOW CAN THE GOVERNMENT RESPOND?

- **Adopt risk-based vulnerability management** — Prioritize patches based on asset criticality, exploitability, and environmental prevalence. Fix the biggest problems on the most important systems first.
- **Leverage automation and orchestration** — Accelerate targeted patching and reduce the manual burden on security teams.
- **Implement network segmentation** — Contain breaches and limit lateral movement when exploitation occurs.
- **Deploy deception techniques** — Honeytokens and honeypots enable early detection of exploitation attempts before widespread impact.
- **Integrate near-real-time threat intelligence** — Enhance visibility into emerging vulnerabilities and inform prioritization across an increasingly diverse vendor landscape.

11, 12 Crowdstrike 2026 Global Threat Report

# Cyber Threats

## 4. AI-powered Threats

### WHAT IS IT

Adversaries are increasingly leveraging AI to enhance the speed, precision, and scale of their attacks. AI-enabled adversary operations increased 89% year-over-year in 2025[13], with threat actors exploiting AI across every stage of the attack chain:

- **Phishing at scale** — AI crafts highly convincing, target-specific phishing emails at a speed and volume no human campaign can match
- **Autonomous malware** — AI-driven malware independently identifies vulnerabilities and adapts its behavior to evade detection, extending attack lifespan
- **Accelerated operations** — AI reduces the need for manual effort, enabling adversaries to scale campaigns while improving success rates

> **"Adversaries are weaponizing the same AI tools organizations rely on every day. The line between trusted technology and active threat has never been thinner."**

**Keith McCloskey**
Vice President,
National Security

### WHY IS IT A THREAT?

As **AI capabilities** continue to improve, adversaries will exploit them to:

- Accelerate every stage of the attack chain from **reconnaissance** to **exfiltration**
- Target critical systems with greater precision and lower cost
- **Weaponize AI tools** — **ChatGPT** was mentioned **550% more in criminal forums** than any other model[14], underscoring how widely trusted platforms are being turned against the organizations that use them
- **Proliferate deepfakes and synthetic deception** — AI-powered threats are eroding institutional trust, enabling disinformation campaigns, fraudulent impersonation, and the manipulation of audio, video, and text at scale
- Outpace security teams relying on manual detection and response workflows

### HOW CAN THE GOVERNMENT RESPOND?

- **Invest in AI-driven detection and defensive research** — Deploy machine learning tools to identify evolving attack patterns in real time and fund research to ensure security tools evolve as quickly as adversarial tactics. Project Glasswing, Anthropic's 2026 cross-industry initiative, demonstrates how frontier AI can be harnessed for defense at a scale no human team can match.
- **Foster public-private collaboration** — Share intelligence on AI-driven threats and develop countermeasures across sectors.
- **Strengthen workforce training and AI governance** — Build defender expertise in AI and threat modeling while establishing regulatory frameworks that mitigate the weaponization of AI tools.

13,14 Crowdstrike 2026 Global Threat Report

# Cyber Threats

## 5. Ransomware and Multi-layer Extortion

### WHAT IS IT

Ransomware attacks remain a persistent and escalating threat, with adversaries deploying increasingly sophisticated tactics to maximize disruption and financial gain. There are numerous developments driving this threat:

- **Multi-layer extortion** — Attackers now go beyond encrypting data, exfiltrating sensitive information and threatening public disclosure or attacks on third parties
- **Ransomware-as-a-Service (RaaS)** — Subscription-based platforms enable less skilled actors to launch devastating attacks with minimal technical expertise
- **AI integration** — Growing use of AI tools by adversaries accelerates the speed, precision, and scale of ransomware campaigns

### WHY IS IT A THREAT?

The financial and operational impacts of ransomware are staggering, particularly in sectors such as healthcare, energy, and government, where disruptions have life-or-death consequences. Ransomware by the numbers:

- **7,419** ransomware attacks recorded globally in 2025 — a **32% increase** from 2024[15]
- Attacks against critical infrastructure **rose 34%**, with manufacturing seeing a **61% surge**[16]
- Beyond monetary losses, ransomware campaigns increasingly target data integrity and institutional trust, undermining confidence in both government and commercial enterprises

> "**Ransomware's greatest damage is no longer measured in downtime or dollars.** It's measured in the erosion of trust in the institutions people depend on most."

**Scott Hoge**
Vice President, Strategic Solutions

### HOW CAN THE GOVERNMENT RESPOND?

Build cyber resilience:

- Maintain **immutable, air-gapped backups** and conduct **network segmentation** to contain lateral spread
- **Deploy EDR** across all endpoints and **prioritize risk-based patching** of internet-facing and actively exploited **common vulnerabilities and exposures (CVEs)**
- Conduct ransomware **tabletop and black hat exercises** with playbooks covering **double and triple extortion** scenarios

Modernize detection and response:

- Deploy **AI-powered detection** for malware-free intrusions with cross-domain visibility across endpoint, identity, cloud, and SaaS environments
- **Automate response** at machine speed (targeting **sub-minute containment**), **map detection coverage**, and perform continuous **detection validation and gap analysis**
- Implement **honeytokens and honeypots** for early-stage threat identification

15 Comparitech Ransomware Roundup 16 KELA, Escalating Ransomware Threats to National Security

# Cyber Threats

## 6. State-sponsored Cyber Espionage

### WHAT IS IT

State-sponsored actors — particularly from **China, Russia, North Korea, and Iran** — have demonstrated the capacity to **infiltrate critical systems and exfiltrate sensitive data** at scale. These attacks use sophisticated techniques that target infrastructure vulnerabilities and exploit weak points in supply chains, with implications that extend far beyond the private sector into the realm of **national security**.

### WHY IS IT A THREAT?

Recent data from CrowdStrike[17] reflects a sharp and deliberate escalation in state-sponsored activity:

- **China-nexus intrusions increased 38%** across all sectors, with an **85% spike in logistics targeting** — systematically exploiting network edge devices such as VPN appliances, firewalls, and gateways to establish long-term access for intelligence collection
- **Cloud-conscious intrusions by state-nexus actors increased 266%**, reflecting a strategic migration of espionage operations into cloud environments where visibility is limited and detection is harder
- **DPRK-linked financial cyber operations rose 130%**, underscoring North Korea's continued use of cybercrime to fund state activities
- China's **2027 strategic timeline** adds urgency — intelligence collection efforts are widely assessed to be accelerating in support of near-term geopolitical objectives

### HOW CAN THE GOVERNMENT RESPOND?

- **Strengthen public-private partnerships —** Improve threat intelligence sharing and bolster cybersecurity standards across critical infrastructure sectors
- **Mandate regular security audits —** Coupled with advanced threat detection and response systems, audits are critical to identifying and mitigating evolving state-sponsored threats
- **Harden network edge devices —** Prioritize security of VPN appliances, firewalls, and gateways, which remain the primary entry point for state-nexus actors
- **Engage CISA and the FBI early —** Early detection and coordination with federal partners is the most effective defense against sophisticated, long-dwell espionage operations

> **"State-sponsored cyber espionage isn't opportunistic, it's systematic.** And the data shows it is accelerating across every sector, every environment, and every layer of critical infrastructure."

**Joanna Dempsey**
Business Unit Leader, Federal Civilian

17 Crowdstrike 2026 Global Threat Report

# 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 ever-evolving, requiring 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 training. 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 Everforth ECS approaches security operations; governance, risk, and compliance; or security architecture and engineering, please contact us or one of our experts:


**Joanna Dempsey**
Business Unit Leader,
Federal Civilian

**Keith McCloskey**
Vice President,
National Security

**Mike Zakrzewski**
Vice President,
Cyber Technology

**Mark Maglin**
Vice President,
Global Defense Cybersecurity

**Scott Hoge**
Vice President,
Strategic Solutions

**Rachel Douglas**
Senior Director,
Federal Civilian Cybersecurity

**Beau Houser**
Senior Director,
Federal Civilian Cybersecurity

**Greg Scheidel**
Senior Engineer,
Federal Civilian Cybersecurity

**Charles D. Walker**
Senior Cyber Solutions Architect,
National Security


## EverforthECS.com

Everforth ECS, the Federal Government Segment of Everforth, is a trusted mission operations partner helping government agencies deliver measurable outcomes through advanced technology solutions, including AI, cybersecurity, digital engineering, and enterprise modernization. By bringing together deep mission expertise, proven processes, and the right technologies, Everforth ECS helps customers accelerate decision making, strengthen resilience, and modernize the systems that power the government's most critical missions.