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

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.

ECS

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.

CONTINUE READING TO EXPLORE THE TRENDS

Download the Full Report Now

ECStech.com/2025-Cyber-Report