1. Consider Adoption of its March 13 and 2025 Fall National Meeting Minutes

Attachment A

Michael Peterson (VA)

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Draft: 03/18/26

Cybersecurity (H) Working Group
Virtual Meeting
March 13, 2026

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 13, 2026. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Alex Romero and Molly Nollette (AK); Mark Fowler and Richard Fiore (AL); Lori Dreaver Munn (AZ); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Kallie Ruggiero Somme (LA); Dmitriy Valekha (MD); Danielle Torres (MI); Gregory Maus (MN); Kim Dobbs (MO); Martin Swanson (NE); Joshua Hilliard (NH); Roger Hayashi (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Sebastian Conforto (PA); Jamie Adams (WI). Also participating was: Matthew Gendron (RI).

1. Discussed Proposed Edits to the Cybersecurity Event Notification Portal Project Intake Form

Peterson presented a brief summary of the proposed changes made in response to the most recent public exposure period. He noted the inclusion of the first draft of the standard form through which licensees will report cybersecurity event notifications in the portal. Peterson reiterated there is no intention to charge licensees to use the portal. Additional language was added to clarify the System and Organization Controls (SOC) 3 report as requested by industry stakeholders. He reminded the Working Group that SOC exams are performed by licensed Certified Public Accountant (CPA) firms operating under the American Institute of Certified Public Accountants (AICPA) attestation standards

Peterson suggested the next steps for the portal project would be to get the document adopted and, then begin the design and development of the portal through consultation and discussion with stakeholders. The first step in ensuring the portal operates correctly is for regulators to draft the standard form based on Section 6B of the Insurance Data Security Model Law (#668). Peterson said once the NAIC has completed enough development, testing will begin with regulators to ensure it is working correctly. He described that the governance and security procedures could be tested through tabletop exercises using synthetic data to simulate various event types and illustrate the different controls and functions that ensure data is protected. He said that the next steps would require substantial engagement with stakeholders, the industry and regulators, to ensure the portal is developed to deliver the expected functionality, usability, and reduction in complexity

2. Adopted the Centralized Cybersecurity Event Notification Portal Project Document

Dobbs provided a summary of the change management process and explained that many of the comments focused on details such as user access, which is typically provided in different technical requirements documents associated with later parts of the process. She explained that the industry would be invited to provide feedback and participate in collaborative discussions and testing.

Schulz highlighted that, although there is limited direct overlap between the groups, the drafting group for the *Market Conduct Exam Handbook* has begun developing a national response framework for cybersecurity events affecting multiple jurisdictions and entities. He noted that this work assumes the existence of shared reporting and coordination functionality similar to what is being discussed for the portal and encouraged the Working Group to remain mindful of other related workstreams that may touch on or benefit from these capabilities.

Holly Weatherford (Wholesale and Specialty Insurance Association—WSIA) thanked the Working Group for the revised project proposal and expressed appreciation for the collaborative engagement. She stated that the WSIA supports the concept of a licensee-directed cybersecurity event notification portal and recognizes that the revisions reflect movement toward that model. She raised concerns, however, that certain proposal language regarding regulator access could be interpreted to allow broader regulatory discretion. Specifically references to departments being "legally entitled" to access notifications could raise concerns about data governance and legal boundaries. She requested additional clarity and transparency on the intent, scope, and limits of regulator access, and on how access would be structured to align with state law while preserving the licensee-directed framework. She also acknowledged revisions emphasizing reduced compliance costs, noted the removal of references to portal fees and revenue concepts, and asked for ongoing transparency on costs and any future revenue considerations.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) stated that NAMIC submitted comments and redlines consistent with themes raised throughout the project and thanked leadership for ongoing engagement and discussion. She requested that the meeting minutes reflect that the discussion of the depth and sensitivity of information to be collected will occur later, potentially as part of future technical document discussions. She explained that this request is driven by concerns about concentration risk and concluded her remarks.

Peterson thanked Ms. Stephani and acknowledged her interests and stated there will be multiple future opportunities to discuss those topics. He emphasized that there is no intention to move forward unilaterally or predetermine outcomes, and that questions regarding both the substance and implementation will be addressed as they arise.

LaCosta Wix (AHIP) thanked the Working Group for the opportunity to comment on the recent iteration of the centralized portal intake request form and expressed appreciation for the goal of reducing administrative friction for plans experiencing reportable cybersecurity events. She acknowledged the work completed to date and noted that her organization submitted written comments with more detailed questions and requests for clarification, some of which may be addressed in the revised draft. She emphasized the importance of ensuring robust security and confidentiality protections for the portal given the sensitivity of the information it will house and concluded by thanking the Working Group for the opportunity to comment.

Peterson thanked AHIP and stated that the Working Group appeared aligned and prepared to begin work on the project, with the understanding that outstanding questions and concerns raised in comments would continue to be addressed as the work progresses. He noted his intent to keep those issues in view and work toward resolving the most important items as the project moves forward.

Peterson made a motion, seconded by Dobbs, to adopt the revised centralized cybersecurity event notification portal project document (Attachment XX) as exposed.

The motion passed unanimously.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-Cybersecurity/2026 0313Interim-Meeting/Minutes-CyberWG031326.docx

Draft: 12/17/25

Cybersecurity (H) Working Group
Hollywood, Florida
December 10, 2025

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Hollywood, FL, Dec. 10, 2025. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Julia Jette (AK); Mark Fowler and Richard Fiore (AL); Chris Erwin (AR); Lori Dreaver Munn (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Kathleen Nakasone (HI); Daniel Mathis (IA); Ryan Gillespie (IL); Eric Turek and Shane Mead (KS); Dominique Jones (LA); Danielle Torres (MI); Kim Dobbs (MO); Gregory Maus (MN); Jacqueline Obusek (NC); Joshua Hilliard and Christian Citarella (NH); Roger Hayashi (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono (PA); Todd Lovshin (WA); Rebecca Rebholz and Christina Keeley (WI); and Lela D. Ladd (WY).

1. Adopted its Sep. 25 Minutes

The Working Group met Sept. 25 and took the following action: 1) adopted its Summer National Meeting minutes; and 2) adopted the IDSM Compliance Guide and Chief Financial Regulator Forum response.

Mathis made a motion, seconded by Torres, to adopt the Working Group's Sept. 25 (Attachment Three-A) and Summer National Meeting minutes (*see NAIC Proceedings – Summer 2025, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Discussed the Cybersecurity Event Notification Portal and Heard Comments from Interested Parties

Peterson provided an overview on the Working Group's progress toward achieving convergence in implementation and operation of the *Insurance Data Security Model Law* (#668). Two major work products completed so far are the Cybersecurity Event Response Plan and the IDSM Compliance Enforcement Guide. These tools are designed to align states responses and enforcement practices under Model #668, reducing regulatory complexity and marginal costs for industry. He explained that the portal is intended to streamline cybersecurity event notifications, reducing administrative burden and marginal costs for insurers operating in multiple states. Petersons described how Section 4 and Section 5 of Model #668 impose low marginal costs, but Section 6 and Section 7 create significant challenges, which the portal aims to address.

Peterson explained that following the Working Group's motion for the NAIC to explore the development of the portal at the 2024 Fall National Meeting, the project management office has implemented a new process in order to ensure as much buy in and support as possible. He described the portal being planned as a modest, push system, where a licensee experiencing a cybersecurity event would select the states for which they want to send their notifications. The system would only allow state insurance regulators from states selected to view any information submitted in the form.

Ladd and Peterson discussed the limitation of the portal to only those states that have adopted Model #668, the idea being the data security law affects insurance specifically. Opening the portal to other agencies would be a long and challenging process.

Torres suggested the portal could be helpful for companies and state insurance regulators. She emphasized that it must be a secure option that allows for correspondence between the states and the insurers, to ensure that all necessary information is available.

Kirsten Wolfford (American Counsel of Life Insurers—ACLI) encouraged further adoption of Model #668 and uniformity across the insurance jurisdictions. She also stressed the importance of confidentiality and security of the portal.

Kristin Abbott (American Property Casualty Insurance Association—APCIA) supported the centralized portal concept and requested opportunities for feedback on prototypes and operational details as the project develops.

John Meetz (Wholesale and Specialty Insurance Association—WSIA) whose submitted comments were joined by the Council of Insurance Agents and Brokers (CIAB) agreed with the previous comments and raised questions about reconciling varying state notification requirements. Meetz and Peterson discussed regulatory access to the portal as role-based access granted only to the states included in the notification selections made by the licensee's submitting.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) expressed support for improving efficiency in cybersecurity event reporting, noting that inconsistent requirements across states and agencies create significant burdens and divert resources from incident response. However, NAMIC raised concerns about the level of sensitive information that would be centralized in the proposed portal, particularly if detailed data were required. Stephani requested that the Working Group clarify and document expectations regarding data granularity in the project proposal to help address these concerns. NAMIC reiterated its appreciation for the opportunity to provide input and referenced its extensive written comments submitted for consideration.

Peterson and Miguel Romero (NAIC) presented and discussed options for the Working Group to consider as the appropriate next steps for the project's advancement. The Working Group's members suggested the document be updated to provide additional details to address the concerns raised.

Munn suggested making corrections and revisions to the portal documentation first, to allow an opportunity for other concerns to be raised by members and interested parties of the Working Group.

Schulz shared that North Dakota implemented a SharePoint-based notification system about three years ago, which took only a few hours to build and functions similarly to the proposed portal. This system improved security and access control compared to the previously used shared email method, which was relatively unsecure. Schulz emphasized that most states still rely on email for notifications and stated that moving to the proposed portal would be significantly more secure. He recommended building the portal now and allowing state insurance regulators to use it and provide feedback.

Mathis and Peterson emphasized that security and confidentiality were top priorities for both state insurance regulators and industry stakeholders. Suggestions included adding more detail in project documentation about security measures to reassure participants and committing them to demonstrate compliance with recognized standards (e.g., SOC 3) on an ongoing basis, rather than simply stating intent. Regulators also noted that data governance and access control, ensuring that only regulators with legal authority can view notifications, must be clearly implemented and verifiable. The Working Group agreed that these assurances can best be demonstrated once the portal is built, but the intent to include robust review and security validation should be documented.

Stephani reiterated concerns about the portal project intake form specifying all aspects of Section 6B of Model #668, particularly Subsection 10 and Subsection 11, which could require highly detailed and sensitive information. NAMIC requested that the Working Group clarify its intent and document that submissions should remain high-level to avoid centralizing excessive sensitive data. Peterson responded that, in practice, Section 6B questions typically require brief, basic reporting rather than detailed disclosures, and additional information can be requested directly if needed. The Working Group discussed whether to revise the intake form to reflect this clarification before adoption or proceed with the current version and address concerns during implementation.

Dobbs clarified that the current document under discussion serves as a high-level project proposal to determine whether the portal should be pursued, rather than a technical specification. She noted that detailed elements, such as specific questions, user access levels, and other operational details, would typically be addressed later in a technical proposal after the decision to proceed with the project.

Romero noted that revisions to clarify intent could be made without significantly delaying the project but emphasized that the decision ultimately comes down to whether the Working Group wants to adopt the document as-is or request revisions before proceeding. The Working Group acknowledged that the complexity of revisions could vary and would become clear once proposed edits are reviewed

The Working Group decided to revise the form based on input received.

3. Heard a Presentation on the 2025 Cybersecurity Insurance Report

Chou provided highlights from the 2025 Cyber Insurance Report, noting that the cyber supplement was revised in 2024 to integrate primary, excess, and surplus lines reporting. He shared that the global cyber insurance market reached approximately $15 billion in 2024, with the U.S. representing the majority of business and growth emerging in Asia and other regions. Chou observed underwriting cycle trends, including a decline in ransomware incidents in recent years and the emergence of new attack types such as “Scattered Spider.” He emphasized that AI-driven threats underscore the continued importance of cyber insurance and encouraged members to review the report prepared by the NAIC for further discussion.

Henry presented key findings from the 2025 Cyber Insurance Report, noting that after slowed growth in 2023, the U.S. cyber insurance market declined for the first time in 2024 by approximately 7.11% (or 2.3% excluding alien surplus lines). He highlighted that 65% of policies were written as primary, while excess and endorsement policies represented a smaller share of premium volume. Henry suggested exploring alternative metrics, such as direct written premium compared to loss ratios, in future reports to provide more meaningful insights. He invited state insurance regulators to collaborate on the 2026 report to make it more actionable and useful, encouraging feedback on additional data points to include.

Romero emphasized the importance of ensuring that the annual cyber insurance report is useful and actionable for state insurance regulators and industry stakeholders. He encouraged feedback on whether the current data presentation meets market intelligence needs and invited suggestions for improving how information is compiled and displayed. Romero stressed that input from the community is essential to make the report more valuable for state insurance regulatory oversight and market analysis, and urged members to review the content and share ideas for enhancements

Having no further discussion, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2025_Fall/WG-Cybersecurity/Fall-Minutes/Minutes-CyberWG-121025-Draft.docx

2. Hear a Presentation from CyberCube on Cyber Threats and Trends

Attachment B

William Altman (CyberCube)

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

CyberCube

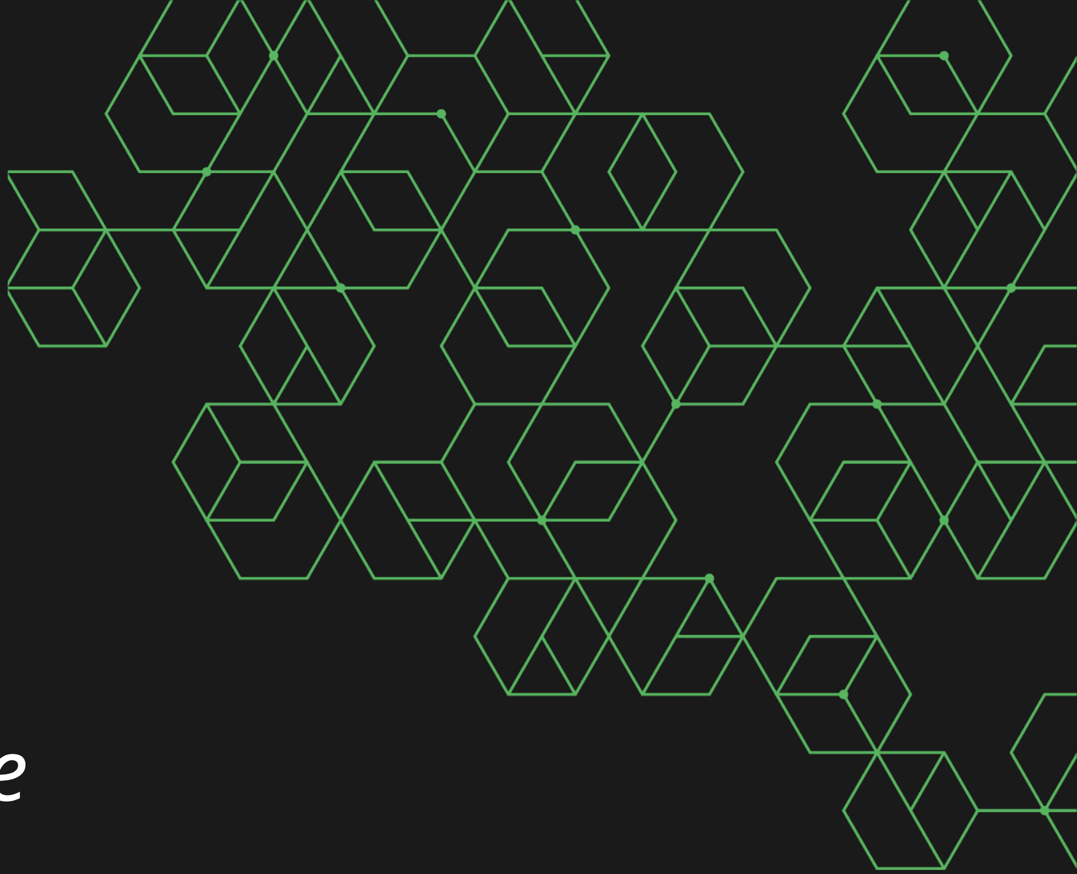
NAIC Cyber Risk Briefing

Prepared March 2026

A look at cyber criminal and AI-driven cyber risk trends

William Altman (CyberCube)

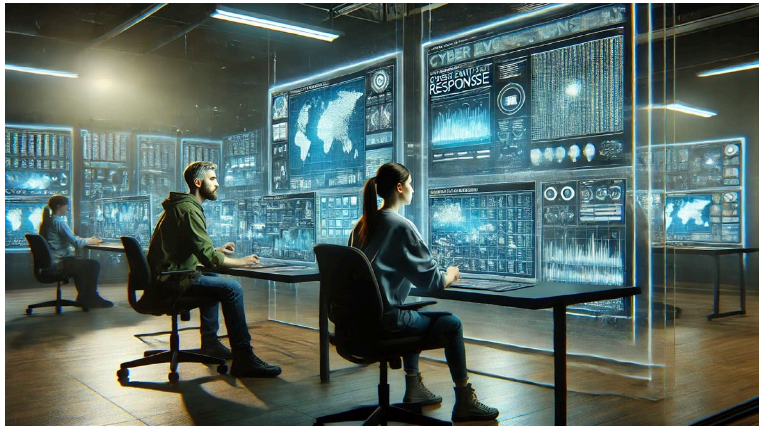
CyberCube



We deliver the world’s leading analytics to quantify cyber risk. Our financial cyber analytics improve the resilience of organizations and society.

CyberCube Concierge Threat Intelligence Service

Concierge makes our experts an extension of your team.



Cyber Threat Intelligence

1. **Full semi-annual threat briefings**
2. **Security Advisory Reports (SARs)**

Event Response Support

3. ***Full Security Incident Report (SIR)***

Cyber Expertise Support

4. **Cyber Hotline to our experts for ad-hoc questions**
5. **Quarterly threat intel. check-in**

We find ourselves navigating a world of complex cyber criminal threats

Ransomware has solidified as a global phenomenon, with most attacks still in the US

Ransomware is a global cyber threat, with incidents now spanning virtually every region and sector. The United States continues to experience the highest number of ransomware indicators of compromise (IOCs), reflecting both its economic prominence and the density of digitally dependent enterprises.

Notable Cyber Attacks In The Top Ten Countries Ranked By Volume of Annual Ransomware IOC Sightings: Mid-2024 to Mid-2025

*A ransomware IOC sighting refers to observable artifacts or data points that signal potential ransomware-related malicious activity within a network.

Key:
Country IOC Rank
Country
Industry
Notable Attack Description

1
United States
Manufacturing / IT
Ingram Micro ransomware July 2025, global IT distributor hit by ransomware causing multi-day outage

2
United Kingdom
Healthcare
NHS / Synnovis ransomware June 2024, UK media confirmed the first patient death linked to a UK cyberattack

3
Canada
Energy / Utilities
Nova Scotia Power ransomware May 2025, led to the theft of personal data belonging to 280,000 customers

4
France
Public
France’s national employment agency suffered a large data breach losing employment records on 340,000 people

5
Germany
Public
Stadtwerke Schwerte / Südwestfalen-IT ransomware March 2025, attack cascaded to utilities prompting city service interruptions

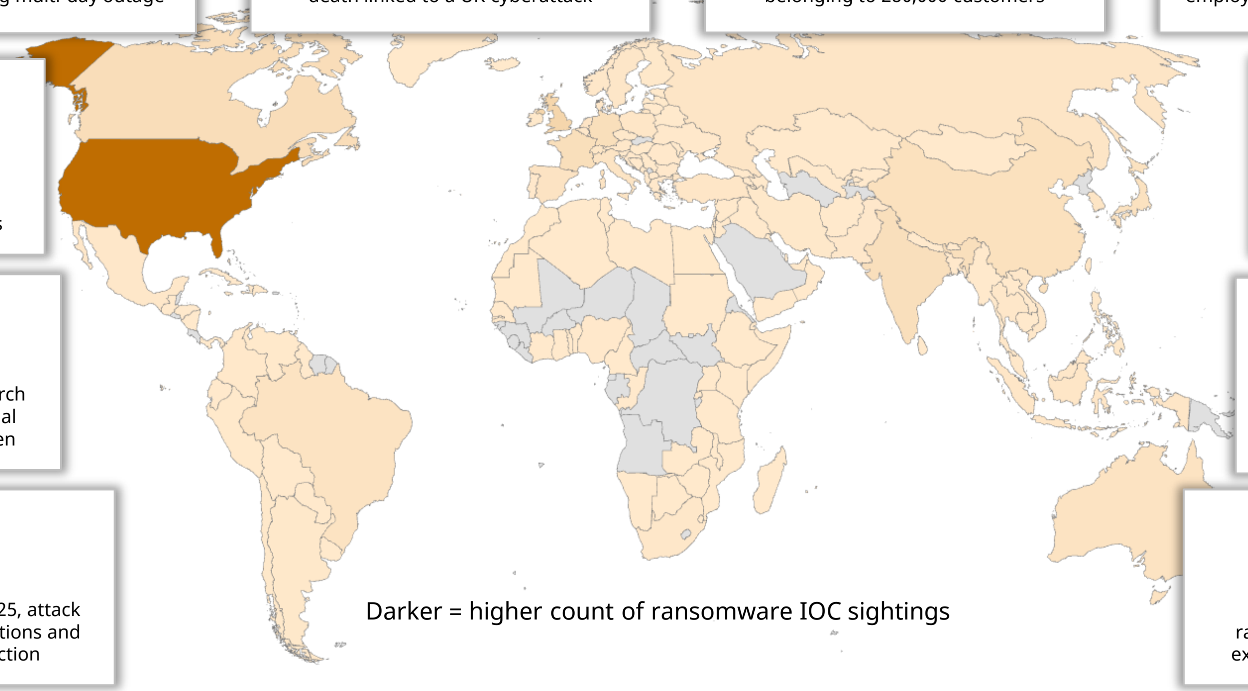
6
India
Healthcare
Sant Parmanand Hospital and NKS Super Special attack led to operational outage in care delivery and exposed patient/admin data

7
China
Banking
Bank of China (Singapore branch) ransomware April 2025, customer data exposed via vendor (Toppan Next Tech)

8
Japan
Manufacturing
Asahi ransomware September 2025, attack halted orders and shipping operations and forced a shut down to production

9
Brazil
Education / Public
National Fund for Education (FNDE) March 2025 ransomware disrupted educational funding with 12GB of information stolen

10
Australia
Aviation
Quantas data breach July 2025, extortion campaign tied to a third-party platform, threatening millions of customer records



Darker = higher count of ransomware IOC sightings

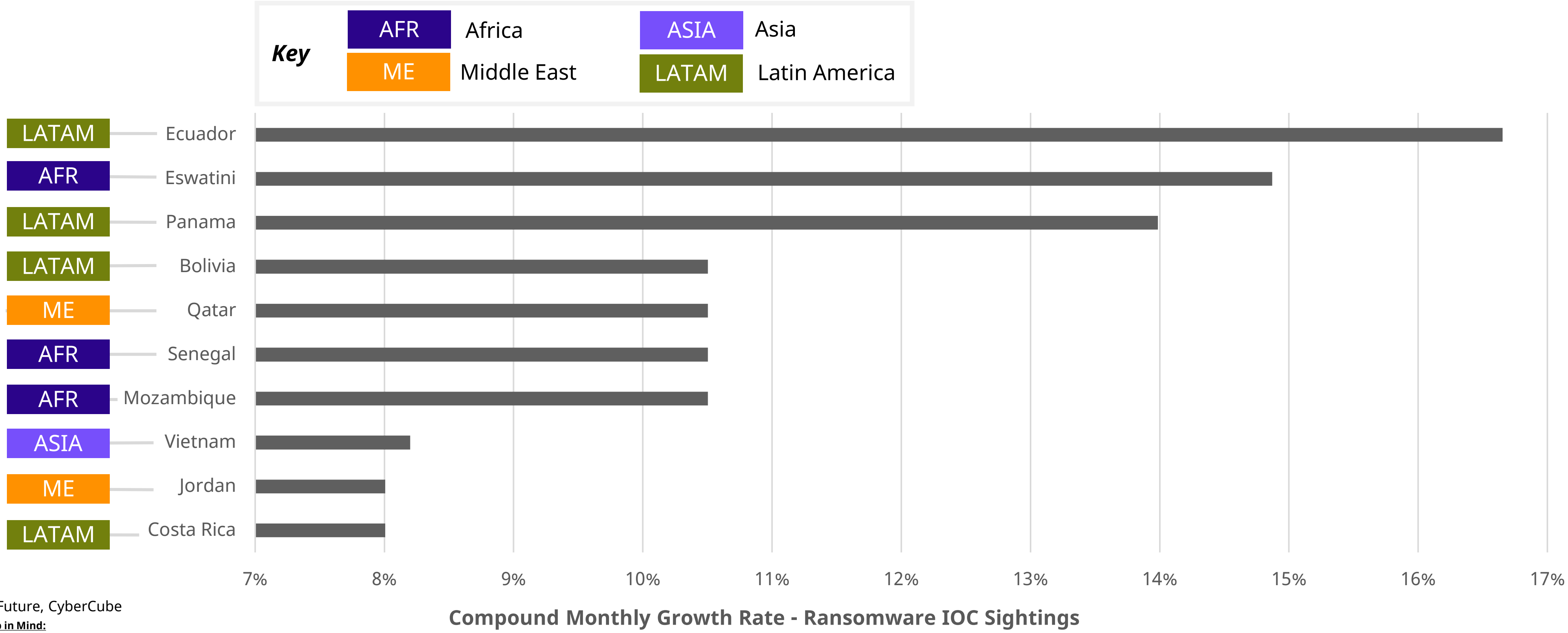
Source(s): Recorded Future, CyberCube

Ransomware is expanding beyond traditional hotspots into emerging economies

This chart highlights where ransomware is spreading fastest, based on compound monthly growth rates of ransomware indicators of compromise (IOCs) from mid-2024 to mid-2025. Concentrated in emerging economies across Latin America, Africa, the Middle East, and Asia, these trends underscore ransomware's shift beyond traditional hotspots and toward regions undergoing rapid digitalization, uneven defense, and growing strategic importance.

Ranking of Top 10 Countries With The Most Growth In Ransomware IOC Sightings: Mid-2024 to Mid-2025

*A ransomware IOC sighting refers to observable artifacts or data points that signal potential ransomware-related malicious activity within a network.



Source(s): Recorded Future, CyberCube

Potential Limitations to Keep in Mind:

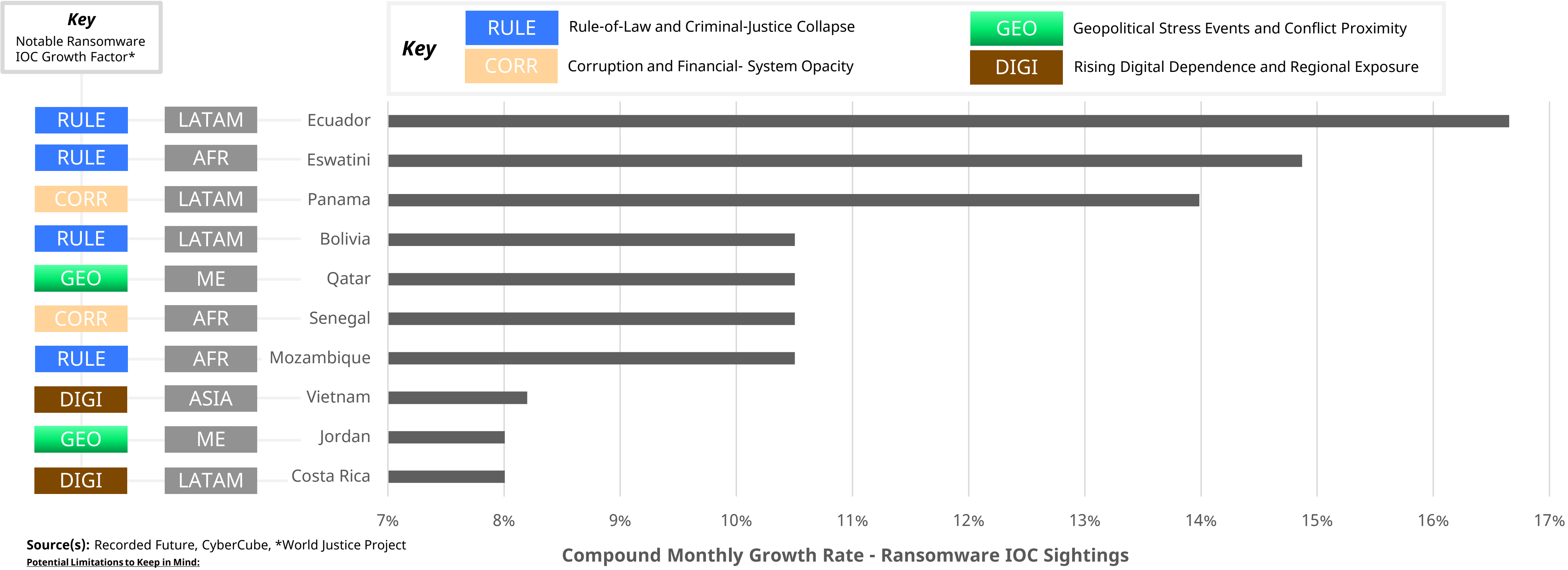
•**Data bias:** IOC reporting density varies sharply by country. Nations with better telemetry may show flatter growth.
•**Attribution lag:** Some IOC increases may reflect detection/reporting improvements rather than true attack surges.
•**Temporal sensitivity:** A one-year CMGR window can exaggerate volatility from a few discrete campaigns.
•**No normalization for internet user base:** Growth may seem faster in small economies.

Ransomware proliferation is influenced by structural and geopolitical factors

In addition to showing where ransomware is spreading fastest (See Slide 11), this chart highlights four macro forces associated with the acceleration and regional concentration of ransomware activity. Growth in ransomware is fueled by a combination of weak rule-of-law and governance structures, corruption and financial-system opacity, geopolitical stress and conflict dynamics, and rising digital and economic interdependence that broadens systemic exposure.

Ranking of Top 10 Countries With The Most Growth In Ransomware IOC Sightings: Mid-2024 to Mid-2025

*A ransomware IOC sighting refers to observable artifacts or data points that signal potential ransomware-related malicious activity within a network.



Source(s): Recorded Future, CyberCube, *World Justice Project

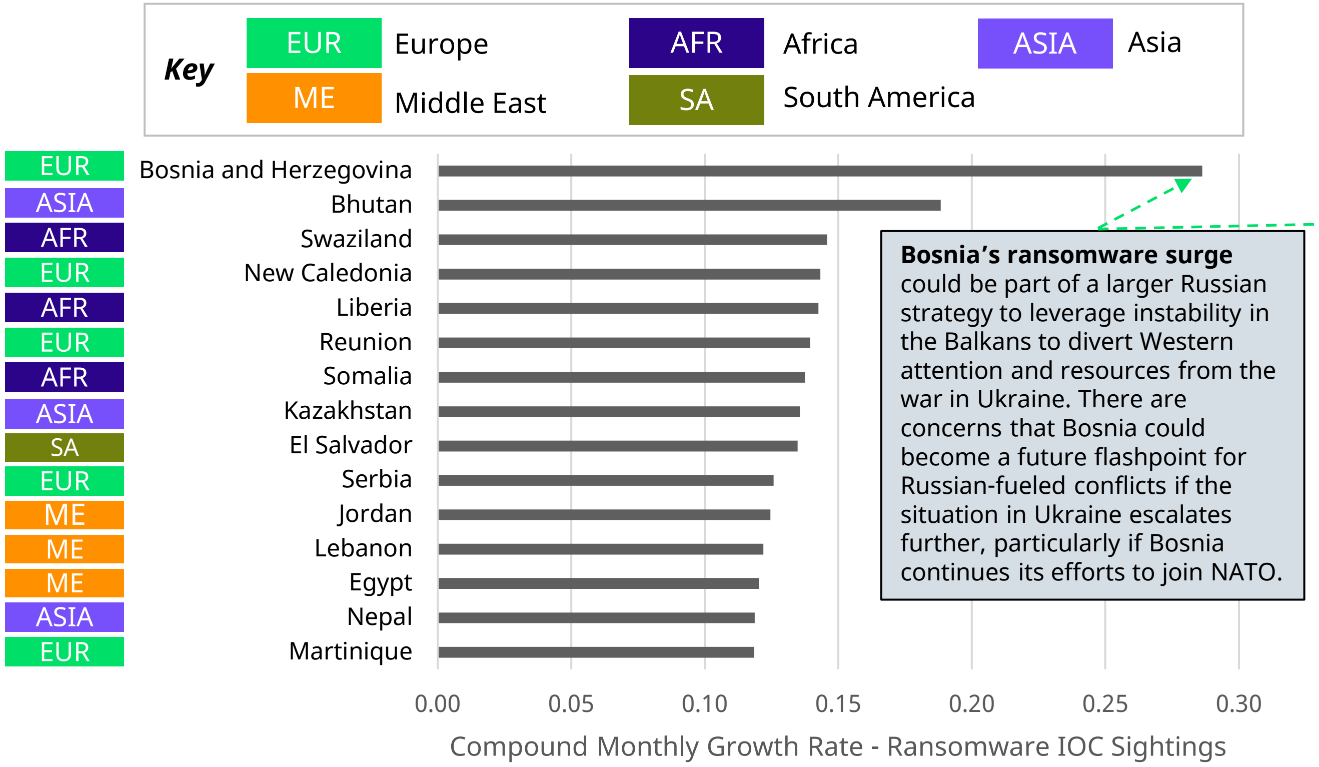
Potential Limitations to Keep in Mind:

- **Data bias:** IOC reporting density varies sharply by country. Nations with better telemetry may show flatter growth.
- **Attribution lag:** Some IOC increases may reflect detection/reporting improvements rather than true attack surges.
- **Temporal sensitivity:** A one-year CMGR window can exaggerate volatility from a few discrete campaigns.
- **No normalization for internet user base:** Growth may seem faster in small economies.

CyberCube Finds: Ransomware Grows In-and-Around Conflict Zones

Recorded Future and CyberCube data reveal that, (while ransomware still predominantly impacts the US), there are specific countries witnessing a rise in the threat (Chart 1), as measured by compound monthly growth rate (CMGR) of ransomware indicator of compromise (IOC) sightings in 2024.

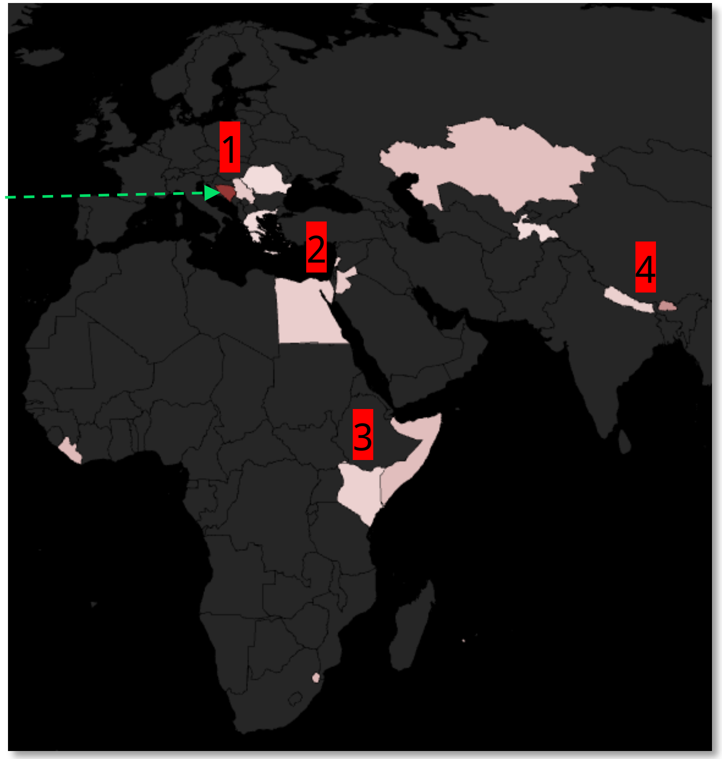
(Chart 1) Ranking of Top 15 Countries With The Most Growth In Ransomware IOC Sightings: 1/1/2024 – 8/30/2024



Bosnia's ransomware surge could be part of a larger Russian strategy to leverage instability in the Balkans to divert Western attention and resources from the war in Ukraine. There are concerns that Bosnia could become a future flashpoint for Russian-fueled conflicts if the situation in Ukraine escalates further, particularly if Bosnia continues its efforts to join NATO.

Source(s): Recorded Future IOC data combined with CyberCube Global EIL database firmographic data

(Chart 2) Select Territorial-Conflict Zones Among the Top 25 Countries With the Most Growth in Ransomware IOC Sightings: 1/1/2024 – 8/30/2024



1 – Countries operating supply routes for Ukraine, ex. Romania

2 – Countries surrounding Israel vs. Hamas

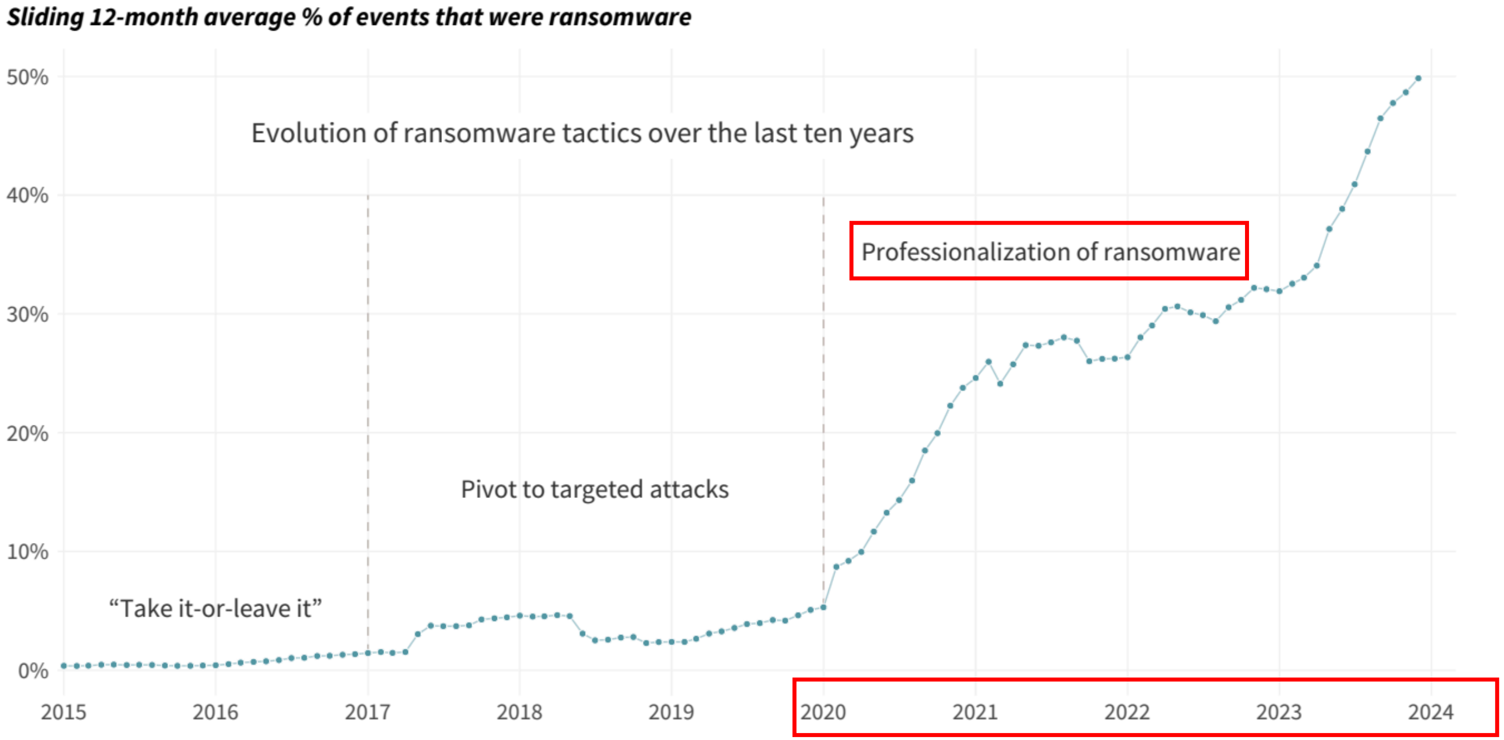
3 – Kenya vs. Somalia conflict over oil reserves

4 – Territorial disputes with India / China, ex. Doklam Plateau

In Tandem with Ransomware Growth Around Conflicts, We See a Greater Militarization and Professionalization of the Threat In The Last Four Years

Data from Cyentia Institute shows a steady rise in the proportion of security incidents classified as ransomware over the past decade.

Monthly Percentage of All Security Incidents Categorized as Ransomware, Global: 2015 – 2024



Source(s): https://www.cyentia.com/wp-content/uploads/2024/08/IRIS_Ransomware.pdf

Attacks on Critical Industry Sectors Around The World

Threat actors target critical industry sectors globally: Energy & Utilities, Public, Oil & Gas, Transportation & Logistics, Telecommunications, Manufacturing.

Select Cyber Attacks on Critical Industry Sectors By Country: 2024 Through September

United Kingdom
Energy & Utilities
Southern Water breached and customer data stolen.

Netherlands
Transportation & Logistics
Port of Rotterdam attack causes port to shutdown.

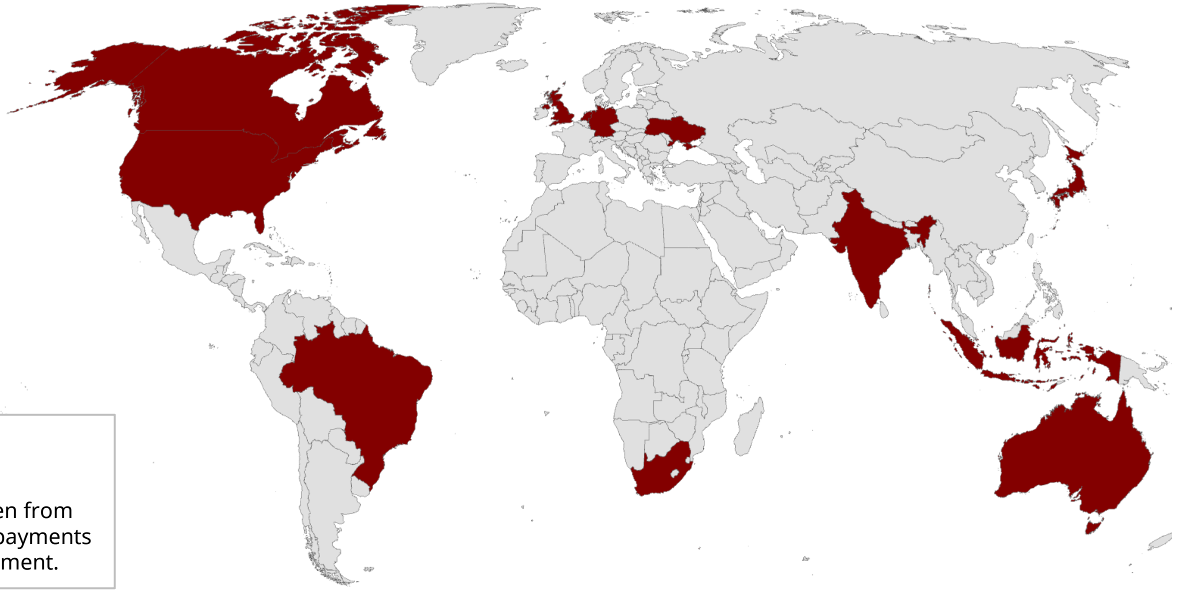
Germany
Transportation & Logistics
National air traffic control confirms hit by a cyberattack.

Ukraine
Oil & Gas
Naftogaz, Ukraine's largest O&G company's datacenter downed.

Canada
Public Sector
Ransomware attack on the city of Hamilton affected every facet of government functions.

United States
Transportation & Logistics
Ransomware attack disrupted Seattle-Tacoma International Airport operations for weeks.

Brazil
Public Sector
Data and money stolen from Siafi; the tool used for payments made by the government.



Japan
Manufacturing
Hoya, one of the world's largest manufacturers of optical gear forced to halt production.

India
Energy & Utilities
Polycab, one of India's leading electrical solutions providers impacted by ransomware.

Indonesia
Public Sector
Ransomware attack on a key national datacenter paralyses government services.

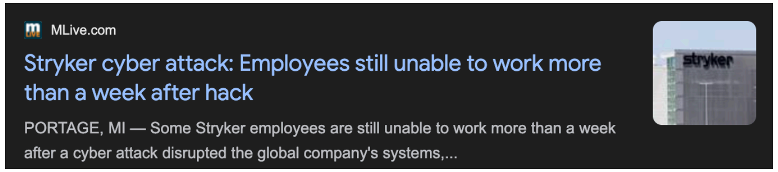
South Africa
Public Sector
Worker's Pension fund operations disrupted.

Singapore
Telecommunications
Absolute Telecom Pte Ltd network servers breached.

Australia
Energy & Utilities
Customers of utility Sumo, impacted by data exposure.

Source(s): See Appendix

Spotlight: Cyber Attack on American Healthcare Company; Stryker



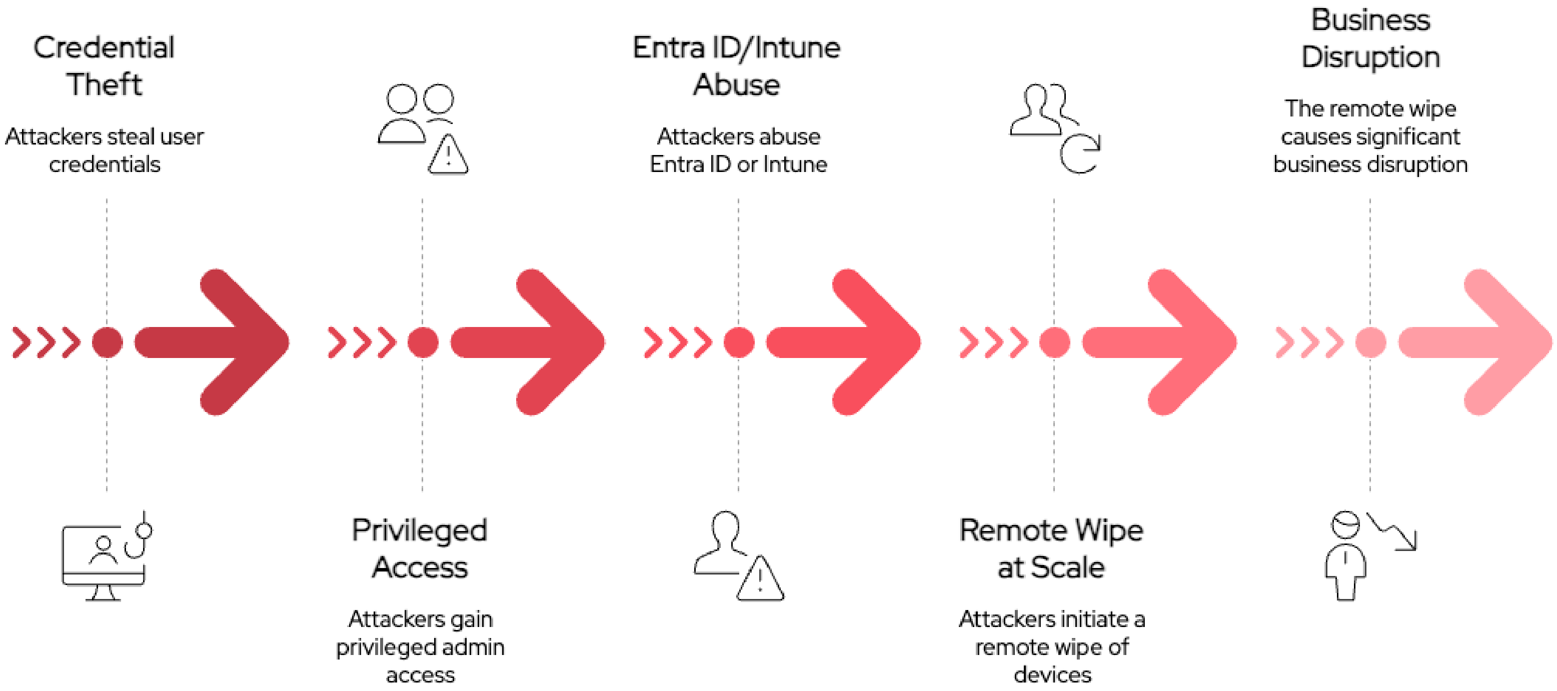
MLive.com

Stryker cyber attack: Employees still unable to work more than a week after hack

PORTAGE, MI — Some Stryker employees are still unable to work more than a week after a cyber attack disrupted the global company's systems,...

An Iran-linked hacking group launched a massive cyberattack on Michigan based Stryker Corporation, wiping more than 200,000 devices worldwide.

High-Level Kill Chain: Cyber Attack on Stryker, 2026



Credential Theft

Attackers steal user credentials

Privileged Access

Attackers gain privileged admin access

Entra ID/Intune Abuse

Attackers abuse Entra ID or Intune

Remote Wipe at Scale

Attackers initiate a remote wipe of devices

Business Disruption

The remote wipe causes significant business disruption

Source(s): https://socradar.io/blog/stryker-cyberattack-what-you-need-to-know/

Cyber Attacks on Small Businesses Occur Around the World Across Industries

(Small = $10M - $250M annual revenue)

Threat actors target small business sectors globally including Financials, Banking, Education, Transportation, IT, Healthcare, Public, and Non-Profit.

Select Cyber Attacks on Small Businesses by Country: 2024 Through February 2025

United States
Financials
Accident Fund's online systems were shutdown.

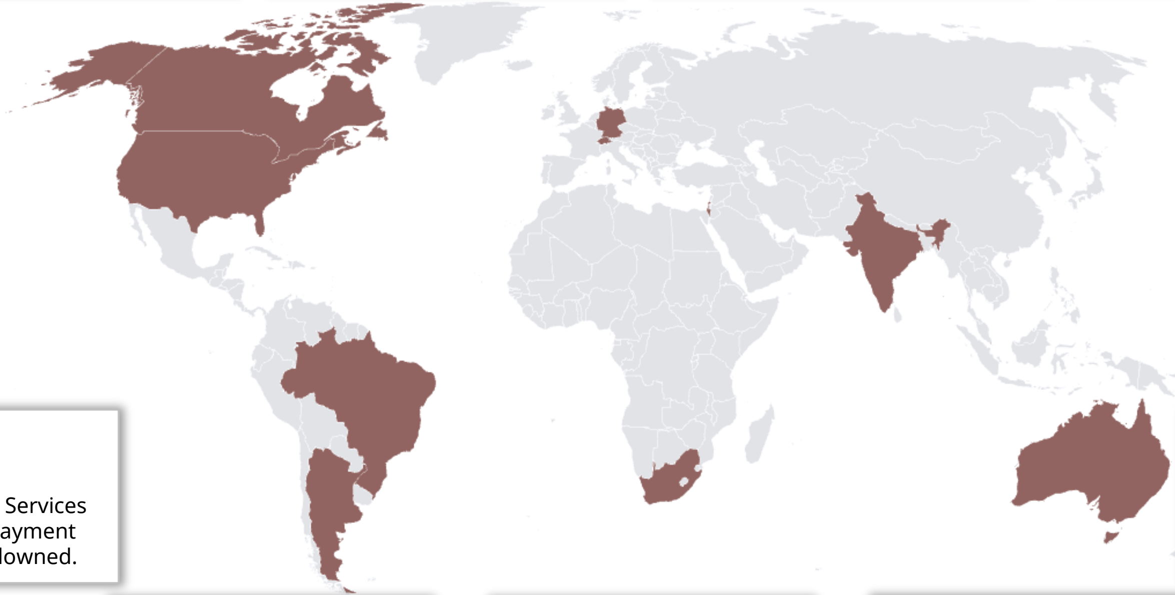
Canada
Education
Hamilton-Wentworth District School Board taken offline.

Germany
Transportation & Logistics
DDoS downed websites of three regional railway companies.

Switzerland
Information Technology (IT)
Xplain, an IT provider to the government was breached.

United States
Healthcare
Memorial Hospital and Manor notified 120,000 individuals that their personal data was stolen.

Singapore
Financials
The cryptocurrency platform Phemex was forced to pause operations and lost $69M.



United States
Non-Profit
Angel Horses Inc., a Billings-based non-profit dedicated to aiding the elderly loses $70K.

India
Banking
300 small banks were forced to go offline due to a ransomware attack on C-Edge Technologies.

Israel
Financials
Shva (Automatic Bank Services Ltd.), attacked and payment processing systems downed.

Australia
Education
The Australian Association of Independent Schools in New South Wales targeted in attacks.

Argentina
Public Sector
Municipality attacked and results in losing 19M pesos.

Brazil
Public Sector
Ransomware on a small city government in Brazil.

South Africa
Public Sector
Weather Service attack hits aviation/marine services.

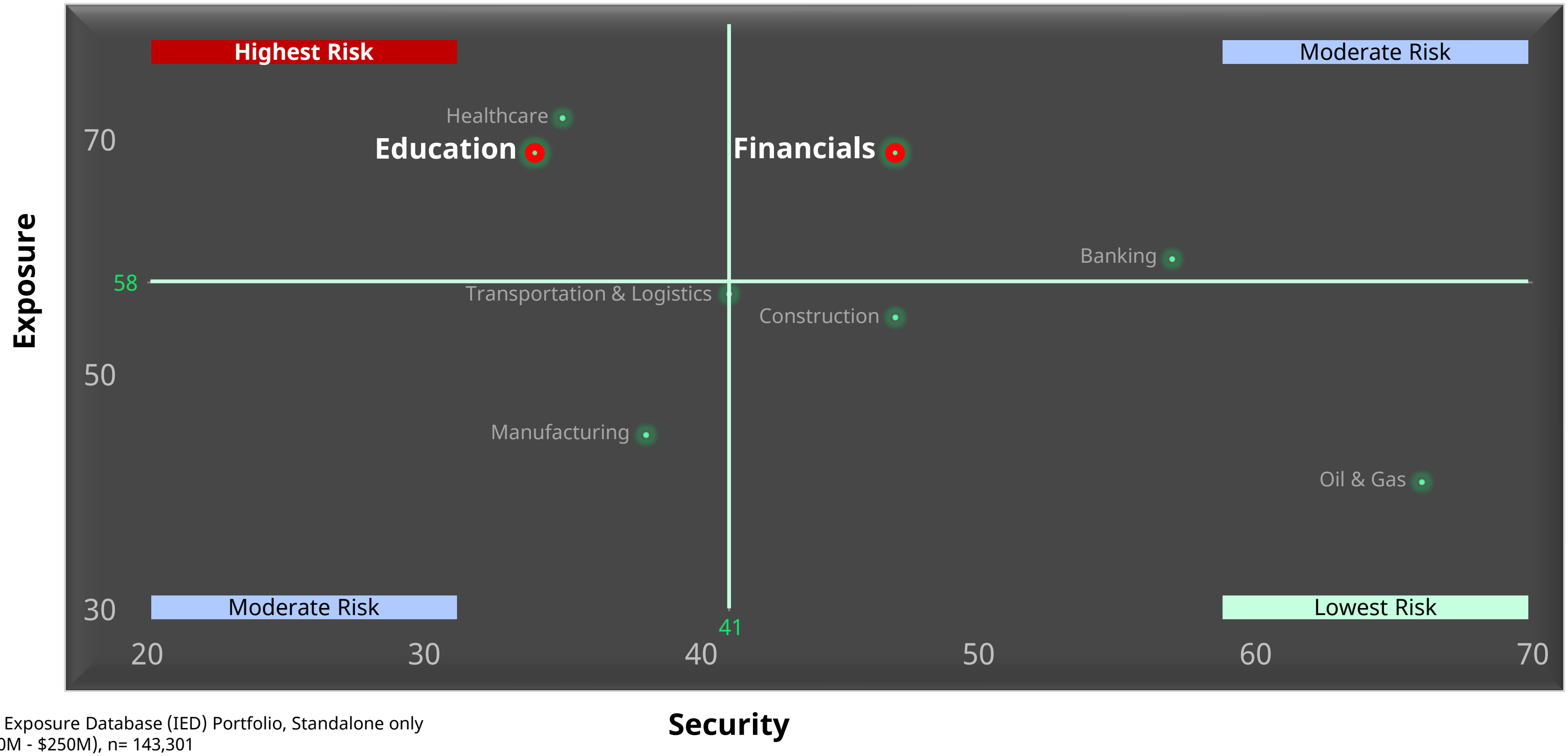
Source(s): See Appendix

Financials Represent an Opportunity Zone for Cyber Brokers and (Re)Insurers, Whereas Education Is Among the Highest-Risk Sectors Requiring Greater Scrutiny

The combination of Exposure and Security provides a clear view of industry-level cyber risk differentiation, identifying both opportunities and sectors requiring greater scrutiny.

Median Security and Exposure Score Matrix: Select Small Business Sectors, January 2025

- 🔴 Select Industry Sector
- 🟢 Other Industry Sector
- ┼ Median of Security/ Exposure in sample, see data notes below



Definitions

- Exposure Score: inherent cyber risk. Higher = higher risk, all else equal
- Security Score: ability to secure digital assets. Higher = less risk, all else equal

Source(s): CyberCube Global Insurance Exposure Database (IED) Portfolio, Standalone only
Small companies (annual revenue of $10M - $250M), n= 143,301
CyberCube Account Manager v5.5 Security & Exposure Scores, January 2025

Threat Actors Are Using AI In 2026

Threat Actors Are Using AI

AI coding introduces software vulnerabilities that get exploited at machine speed

The rapid adoption of AI-assisted coding is accelerating software development but also introducing new security risks at unprecedented speed.

2025
GenAI Code Security Report
ASSESSING THE SECURITY OF USING LLMS FOR CODING
Build an app that...
VERACODE

55% of tasks result in secure code. In other words, in 45% of tasks the model introduces a known security flaw into code.

Average eCrime breakout time dropped to 48 minutes, with the fastest breakout observed at just 51 seconds.

Source(s): Veracode, https://www.veracode.com/wp-content/uploads/2025_GenAI_Code_Security_Report_Final.pdf

CrowdStrike, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

We are now in the “self-driving” era of AI-enabled cyber attacks

By 2026, cyber threats are expected to reach a stage where AI systems can independently execute key phases of cyberattacks, operating with minimal or even no human involvement, much like autonomous vehicles function without continuous driver input. Defenders could need adaptive, AI-driven defenses.

AI-Driven Threat Progression Timeline: 2020 – 2035+

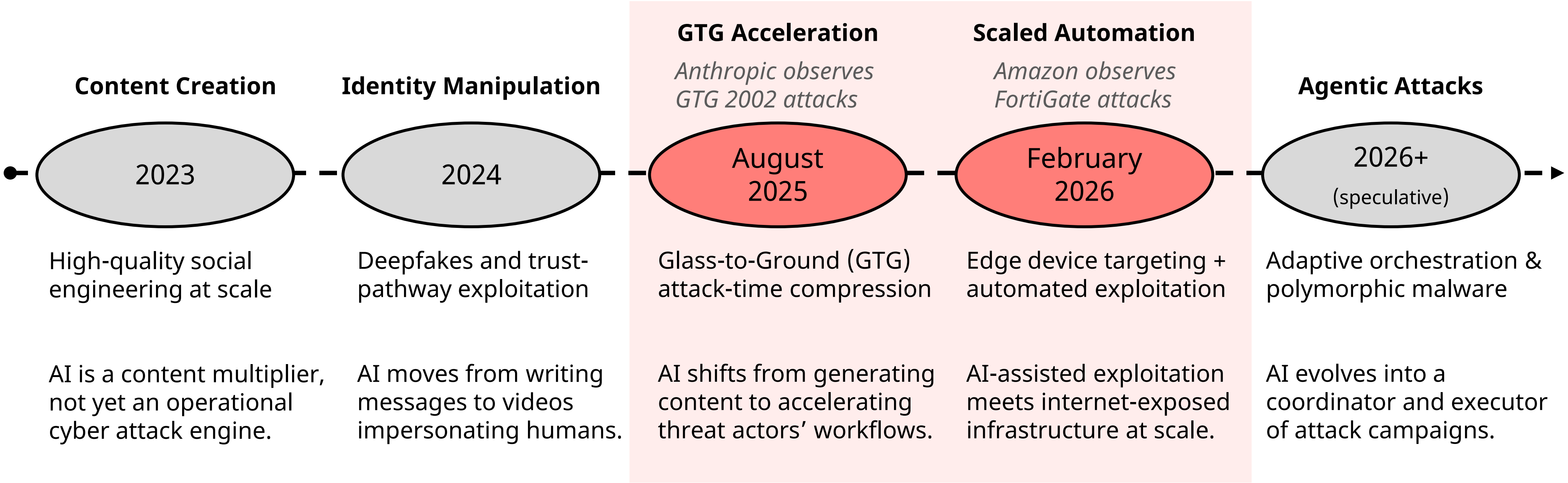
Recent Past | Present Day | Near Future* | Near-Distant Future*

	2020 – 2022 **Generative AI Use Cases**	**2023 – 2025** **AI-Augmented Attacks**	**2026 – 2030** **“Self-Driving” Attacks**	**2030 – 2035+** **Fully Agentic AI Threats**
Evolution of Human-to-AI Ratio in Attacks:	*Human threat actors using AI as a productivity tool*	*Hybrid “human + AI” attacker teams (LLM copilots for red teams)*	*Semi-autonomous AI-run intrusion-as-a-service (AIaaS) marketplaces*	*AIs coordinating across darknet forums and botnets with minimal oversight*
AI Defensive Coevolution:	*Static defenses, signature-based AI misuse detection*	*AI-assisted SOC operations, generative deception systems*	*Adaptive AI-driven defense (self-healing networks, AI SOC copilots)*	*Autonomous “blue agents” negotiating or counteracting hostile AIs in real time*

**Illustrative timeline*

Between August 2025 – February 2026, two attack campaigns signal the evolution of AI-enabled attacks toward faster exploitation of common cyber defense gaps

Evolutionary View of AI-Enabled Ransomware Attacks



Content Creation

2023

High-quality social engineering at scale

AI is a content multiplier, not yet an operational cyber attack engine.

Identity Manipulation

2024

Deepfakes and trust-pathway exploitation

AI moves from writing messages to videos impersonating humans.

GTG Acceleration

Anthropic observes GTG 2002 attacks

August 2025

Glass-to-Ground (GTG) attack-time compression

AI shifts from generating content to accelerating threat actors' workflows.

Scaled Automation

Amazon observes FortiGate attacks

February 2026

Edge device targeting + automated exploitation

AI-assisted exploitation meets internet-exposed infrastructure at scale.

Agentic Attacks

2026+ (speculative)

Adaptive orchestration & polymorphic malware

AI evolves into a coordinator and executor of attack campaigns.

Source(s): Anthropic Threat Intelligence, https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf?,
Amazon Threat Intelligence, https://aws.amazon.com/blogs/security/ai-augmented-threat-actor-accesses-fortigate-devices-at-scale/?utm

What did we learn from GTG 2002 & FortiGate attacks?

(1) AI Is a Force Multiplier, Not a New Attack Type

Faster targeting, better coordination, increased automation

(2) Identity Security Is Key

GTG 2002 relied on identity-layer exploitation

Once identity is compromised, attackers can move, scale, and operate using trusted access, making identity security a primary control over how far and how fast an AI attack spreads.

(3) Timely Patching Is Key

FortiGate relied on vulnerable device exploitation

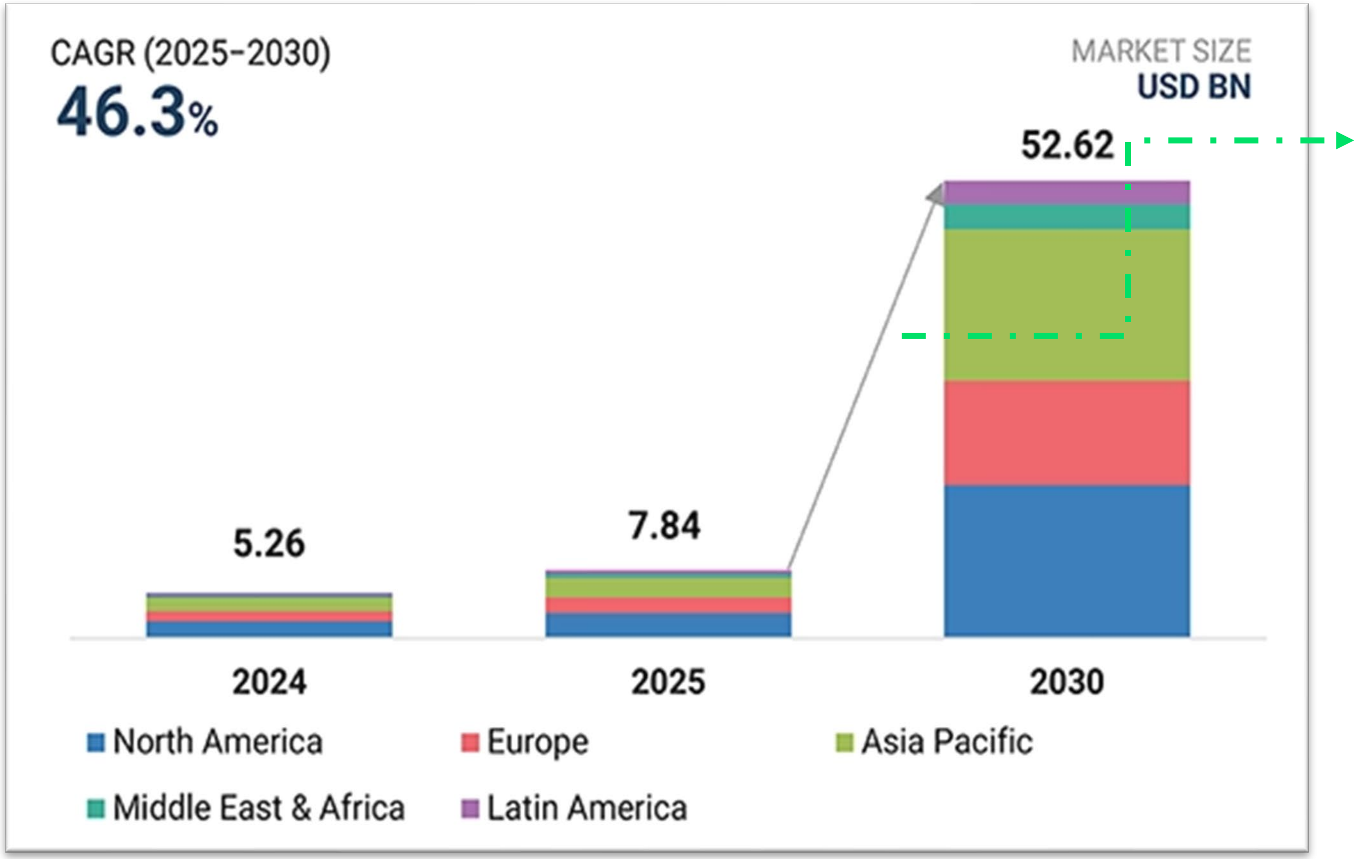
The FortiGate campaign shows that widely deployed, unpatched vulnerabilities in internet-facing systems can enable rapid, large-scale initial access, making patch latency a driver of correlated AI-driven risk.

Emerging AI Driven Risks To Watch In 2026

The market for AI agents is expected to explode over the next five years

The market for AI agents is expected to expand as more organizations deploy AI that autonomously executes tasks across systems, applications, and data.

AI Agent Global Market Size and Share By Country: 2024 – 2030



Source(s): Markets and Markets

How Does Agent Growth Impact Cyber (Re)insurance?

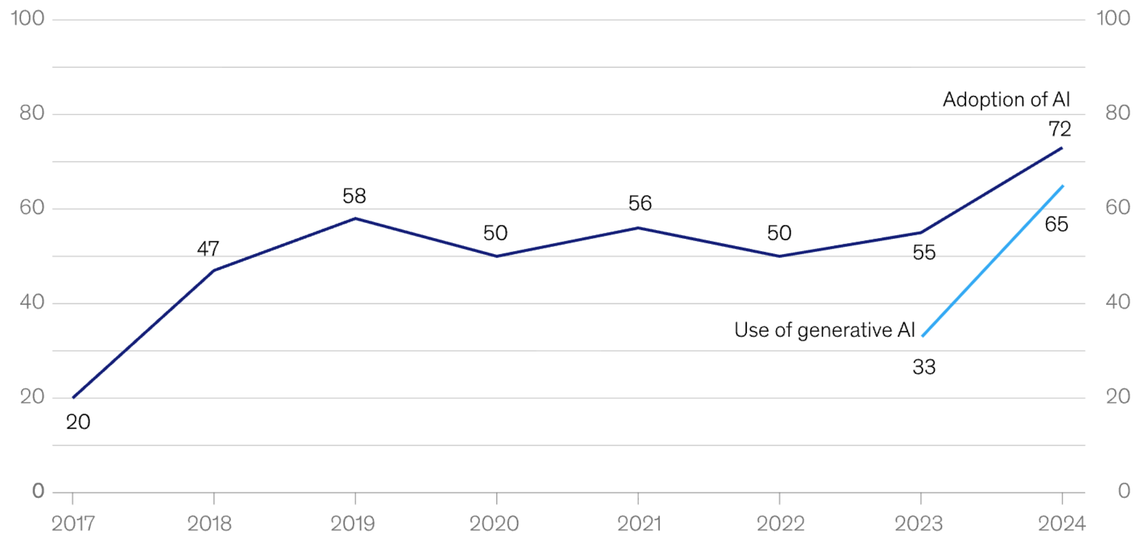
- Secure deployment of AI agents is the next big enterprise risk for cyber (re)insurers to address
- AI agents can introduce a new privileged execution layer inside critical enterprise systems.
- This creates new cyber risk pathways that can lead to data theft, or operational disruption.

As businesses grow dependent on AI, the potential impact of disruptions may rise

In 2025, foundational model developer Open AI’s ChatGPT saw major disruptions, including a 34-hour global outage in June, widespread performance issues in July, and shorter paid-user and minor August outages; rare events that nonetheless showed how a single AI failure can ripple across users and industries.

AI adoption worldwide has increased dramatically in the past year, after years of little meaningful change.

Organizations that have adopted AI in at least 1 business function,[1] % of respondents

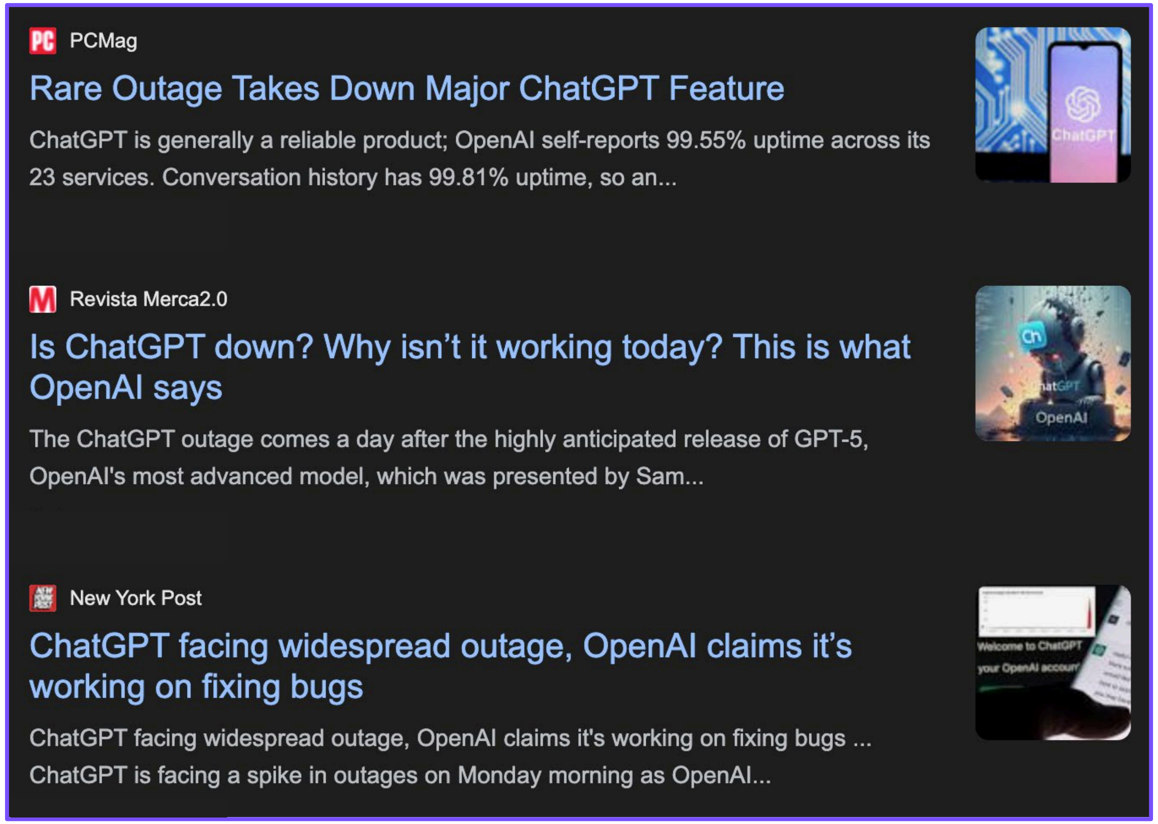


[1] In 2017, the definition for AI adoption was using AI in a core part of the organization’s business or at scale. In 2018 and 2019, the definition was embedding at least 1 AI capability in business processes or products. Since 2020, the definition has been that the organization has adopted AI in at least 1 function.

Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

Chat GPT Outage News Clippings – June 2025



PCMag

Rare Outage Takes Down Major ChatGPT Feature

ChatGPT is generally a reliable product; OpenAI self-reports 99.55% uptime across its 23 services. Conversation history has 99.81% uptime, so an...

Revista Merca2.0

Is ChatGPT down? Why isn’t it working today? This is what OpenAI says

The ChatGPT outage comes a day after the highly anticipated release of GPT-5, OpenAI's most advanced model, which was presented by Sam...

New York Post

ChatGPT facing widespread outage, OpenAI claims it’s working on fixing bugs

ChatGPT facing widespread outage, OpenAI claims it's working on fixing bugs ... ChatGPT is facing a spike in outages on Monday morning as OpenAI...

CyberCube

Thank You

Questions? Email us at info@cybcube.com

FOLLOW US cybcubecom CyberCube CyberCube

This document is for general information purpose only and is not and shall not under any circumstance be construed as legal or professional advice. It is not intended to address all or any specific area of the topic in this document. Unless otherwise expressly set out to the contrary, the views and opinions expressed in this document are those of CyberCube's and are correct as at the date of publication. While all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of the content of this document, no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. CyberCube and its affiliates shall not be liable for any action or decisions made on the basis of the content of this document and accordingly, you are advised to seek professional and legal advice before you do so. This document and the information contained herein are CyberCube's proprietary and confidential information and may not be reproduced or redistributed without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any license or right to use CyberCube's intellectual property. All CyberCube's rights are reserved.

3. Hear a Presentation from the Center for Internet Security (CIS) on its Artificial Intelligence (AI) Controls Companion Guidelines

Attachment C

Curtis W. Dukes (CIS)

AI Controls Companion Guides

Curtis W Dukes
EVP & GM Security Best Practices

March 25, 2025

About Me

- **Curt Dukes**
- **EVP & GM Security Best Practices**
- **Senior Executive NSA**
- Infosec, IA, CyberSecurity
- **Computer Scientist**
- **USAF – *Aim High, Fly-Fight-Win***
- **Runner, cyclist, old**

About the Center for Internet Security (CIS)

Consensus Best Practices + Operational Expertise = Sustainable Cybersecurity

Independent and Trusted

Proven and Effective

Collaborative

Operational Expertise

Sustainable

Expanding CIS Controls for AI & Agentic Systems

- Organizations are rapidly adopting AI-powered and agentic systems capable of autonomous actions, tool usage, and API-driven interactions.
- To address these emerging risks, new cybersecurity guidance is being developed to extend the CIS Critical Security Controls® into AI environments.

Goal

- Provide practical, vendor-agnostic security guidance that helps organizations apply CIS Controls as the foundation for reasonable security in AI environments.

Key Areas of Focus

- **Securing proprietary data used for/by Large Language Models (LLMs)**
- **Securing the AI agent system lifecycle, including deployment, operation, and governance.**
- **Addressing risks introduced by use of Model Context Protocol (MCP)**
- **Managing security challenges such as:**
  - Credential exposure and misuse
  - Uncontrolled local execution of AI tools
  - Unapproved third-party connections
  - Unmonitored data flows between models, agents, and enterprise systems
  - Strengthening protection of non-human identities (NHIs) such as API keys, service accounts, and Oauth tokens used by AI agents

From Chatbots to Layered AI Systems

- Enterprise adoption of artificial intelligence has moved beyond simple chat interfaces.
- Modern deployments are typically layered:
  - Large Language Models (LLMs),
  - Agent frameworks that orchestrate tools and actions, and
  - Standardized integration layers such as the Model Context Protocol (MCP).
- Treating “enterprise AI” as a single monolithic capability can blur important differences and create gaps in risk management—so a layered view is essential for building defensible, auditable systems.

LLM Layer: High Value Data Processing

- LLMs ingest prompts, retrieve contextual data, and produce outputs that may influence decisions or automation.
- Sensitive data and business logic concentrate here.
- This layer is a focal point for data protection, access control, and monitoring of inputs/outputs.

Agent Layer: From Predictions to Actions

- Agents turn model outputs into execution by accessing tools, APIs, credentials, and sometimes memory.

- This step changes the risk profile: the “blast radius” expands from response quality to real operational impact (e.g., data changes, credential use, production actions).

MCP Layer: Standardized Tool Discovery & Governance

- MCP and similar standards formalize how models discover, invoke, and interact with tools.

- This interface layer can strengthen governance through consistency—or weaken it if capability rollout, permissions, and change control are implemented unevenly across teams.

Accountability and Precise Control Placement

- Separating AI/LLM security, AI agent controls, and MCP governance avoids blurred accountability and enables precise control placement.

- Improves mapping to established frameworks (e.g., CIS Controls), supports threat modeling and targeted audits,

- Reduces ambiguity for vendors, developers, and operators as AI scales.

Wrap Up

- Security Controls Based on Existing Security Frameworks
- A Small Number of additional Security Considerations
- Companion Guide(s) Releasing o/a 8 April 2026
- Webinar End of April
- Opportunity for CIS and SANS future training collaboration

Thank You