Cybersecurity Executive Annual Brief: 2025

Prepared by: Benjamin Olivier
Published: 2026-01-14
Version: v1.0

Annual Intelligence Report | 2-Minute Executive Summary | Full Analysis: ~18 Pages

Coverage: January 1 – December 31, 2025 | **Regions:** Global | **Primary Sectors:** Healthcare, Technology, Government, Retail, Financial Services, Manufacturing

How to Use This Brief

CEO / Board Member

Read: Part 1 only

Time: 5 min

Purpose: Orientation, decisions, talking points

CFO / General Counsel / CRO

Read: Part 1 + Sections 6–9

Time: 12–15 min

Purpose: Regulatory, insurance, investment context

CIO / CISO / Security Leadership

Read: Full document

Time: 20–25 min

Purpose: Complete landscape, technical detail, implementation

Audit / Risk Committee

Read: Part 1 + Board Discussion Points

Time: 7 min

Purpose: Governance questions for management

Forwarding guidance: CEOs may forward the full document to their CISO or CRO with confidence that Part 2 provides the evidence and detail needed for follow-up action.

Source note: This brief is a synthesis of public advisories, incident disclosures, and reputable reporting; see Appendix C for sources.

PART 1

EXECUTIVE DASHBOARD

For CEOs, boards, and executive committees: 3–5 minutes to absorb. Designed to drive decisions.

EXECUTIVE SUMMARY: The Year Speed Became Survival

On September 21, 2025, an airline operations executive thought they were dealing with a "routine system outage." Within hours, passengers were being processed manually across multiple European airports after a cyberattack forced parts of Collins Aerospace's MUSE check-in platform offline. Flights still moved. Everything else slowed to a crawl. [1]

That incident captured the core lesson of 2025: **cyber risk is now operational risk at the speed of software and identity.** Three forces defined the year:

1. **Exploit velocity compressed the response window.** In 2025, evidence showed roughly a third of exploited vulnerabilities were weaponized *on or before* CVE publication ("day 0")—meaning "patch Tuesday" thinking is now a liability for internet-facing systems. [2,3]
2. **Identity became the control plane.** Attackers didn't need a zero-day to compromise high-value environments—they needed a trusted workflow. Vishing-driven campaigns targeted admins and support staff, persuading them to authorize malicious connected apps or modify legitimate tooling for large-scale data exfiltration and extortion. This pattern was documented across Salesforce-centric intrusions in 2025. [22,23,24,25]
3. **Third parties became primary attack surfaces.** UK retailers were hit in a coordinated campaign where attackers manipulated help desks and access brokers to reset credentials and pivot into core systems. Business impact estimates reached the hundreds of millions of pounds, with disruption rippling into supply chains and consumer trust. [6,7,8,9,10,11]

> **The uncomfortable truth:** resilience is no longer measured by whether you can "prevent" an incident. It's measured by how fast you detect, contain, and operate through one.

Critical Actions Required (if you do only six things)

1

Rotate SharePoint MachineKeys and validate patch posture

If you operate SharePoint on-prem, treat 2025's SharePoint exploitation as a "hands-on-keyboard" event: rotate MachineKeys, apply vendor fixes, and hunt for persistence. [4,5]

2

Lock down help desks and admin change paths

Implement out-of-band verification for password resets, MFA changes, and privileged access requests—especially for contractors and managed service providers. [6,7,8,9]

3

Run a 72-hour telecom degradation exercise (voice/SMS + identity continuity)

Assume carrier voice/SMS is partially unavailable *or untrusted* for 72 hours. Test what breaks when **SMS MFA**, **call-back verification**, and executive **incident command** channels degrade. Validate alternate communications and account recovery paths. This is a low-cost tabletop that tends to expose hidden single points of failure. (Salt Typhoon reinforced that telecom is both a target and a dependency.) [17,18,19,20]

4

Build a rapid exploit-response lane

Operationalize a "KEV sprint" for internet-facing systems: instrument exposure, patch fast, and measure mean-time-to-mitigate. [2,3]

5

Fund identity governance like infrastructure

Treat SaaS admin roles, connected apps, OAuth grants, and API tokens as Tier-0 assets. Instrument them, monitor them, and require proof-based access changes. [22,23,24,25]

6

Track the AI effect—but secure the basics first

AI increased phishing productivity and deepfake realism, but most compromises still started with gaps in identity controls, segmentation, and logging. [14,28,43,46]

2025 in One Slide

Exploit window compressed	≈32% of exploited vulns show exploitation on/before CVE publication ("day 0"). [2]	Your patch program needs an "emergency lane" for exposed systems.
Identity became infrastructure	Vishing + connected-app abuse enabled high-scale SaaS data theft and extortion without a software vulnerability. [22,23,24,25]	Identity governance is now a business continuity control.
Third-party blast radius expanded	Third-party involvement reached ~30% of breaches; real-world retail campaigns validated the risk. [6,7,8,9,10,11,12]	Contracts and access paths are technical risk—treat them that way.
Ransomware fragmented but persisted	Leak-site monitoring recorded 8,000+ claimed victims in 2025 amid continued ecosystem churn. [16]	Ransomware is not "over." It's diversifying and professionalizing.
Nation-state access became operationally relevant	Telecom intrusions drove government guidance and sanctions, reinforcing "pre-positioning" risk. [17,18,19,20]	Build continuity for critical dependencies (telecom, identity, cloud). Stress-test communications + MFA.

Key Metrics and Trends

Ransomware claimed victims	8,000+ leak-site claimed victims (global). [16]	The real number is higher; "quiet" victims don't show up on leak sites.
Exploitation speed	≈32% show exploitation evidence on/before CVE publication ("day 0"). [2]	Vulnerability response must be measured in hours for exposed assets.
Third-party involvement	~30% of breaches involved third parties (≈2× prior levels). [12]	Identity and access across vendors is now a core control objective.
US average breach cost	$10.22M (US), global average $4.44M. [13,14,15]	Executives can no longer assume cyber loss is "immaterial."
Highest-cost sector	Healthcare remained the most expensive sector at ~$7.42M per breach. [15]	High disruption + regulated data + low tolerance for downtime.
Breach lifecycle	~241 days average lifecycle (time to identify and contain). [15]	Faster isn't "fast enough" when exploitation happens in days.

Definitions (board-safe):

- **Claimed victims:** Organizations posted by ransomware crews on leak sites ("name-and-shame" pages). This is *not* a verified incident count; it may include duplicates or inflated claims and excludes "quiet" victims.
- **Third-party involvement:** Breaches where a supplier/partner/service provider materially contributed to the incident chain (per DBIR's definition), not just "vendor breached first."
- **"Day 0" exploitation:** Exploitation evidence observed on or before CVE publication/issuance. It does *not* imply public exploit code existed.

Top 5 Incidents by Business Impact

01

Bybit theft (~$1.5B): state-linked crypto theft at unprecedented scale

[29,30,31,32,33]

02

Jaguar Land Rover ransomware: production halted for ~6 weeks; £1.9B estimated impact

[34,35]

03

UK retail campaign (M&S, Co-op, Harrods): help desk exploitation and sustained disruption

[6,7,8,9,10,11]

04

PowerSchool breach: mass-scale education data exposure with long-tail identity risk

[21]

05

Salt Typhoon telecom espionage: persistent access risk to critical communications infrastructure

[17,18,19,20]

Board Takeaways (what to ask your CISO this quarter)

"How would we stop a fake-but-credible executive request?"

AI voice cloning and deepfake-enabled fraud continued to mature in 2025. The controls are boring but effective: call-back procedures, payment dual control, and identity verification for high-risk requests. [27,28,43]

"Where can a vendor help desk reset our access?"

If you can't answer this quickly, attackers can. Map and harden your reset paths and contractor admin chains. [6,7,8,9]

"What breaks if carrier voice/SMS is unavailable or untrusted for 72 hours?"

If your incident response relies on SMS MFA, call-back verification, or a single provider, you have a single point of failure. [17,18,19,20]

Act now: what changed in 2025 wasn't just the threat level—it was the time you have to respond.

PART 2

STRATEGIC ANALYSIS

For CISOs, CIOs, CROs, and risk leaders: designed to move from "what happened" to "what we do next."

1. Overview: Convergence and Compression

2025 did not introduce radically new attacker goals. It changed the **tempo**:

- **Compromise-to-impact got faster.** Exploitation often occurred by the time a CVE was published for internet-exposed assets, leaving little room for traditional patch cycles. [2,3]
- **Social engineering became an access method, not a precursor.** Vishing, help desk manipulation, and connected-app abuse were not "phase one"—they were the breach. [6,7,8,9,10,22,23,24,25]
- **Business disruption became the preferred lever.** Ransomware crews, fraud actors, and state-linked groups all leaned into operational pain: outages, extortion, and dependency attacks. [1,16,17-20]

> **Strategic implication:** Security programs that are optimized for annual compliance audits will keep losing to adversaries optimized for *hourly* decision cycles. Threat reports continued to emphasize identity abuse, cloud/SaaS targeting, and supply chain compromise as dominant patterns. [45,46]

2. Critical Incidents (what happened, what mattered, what changed)

2.1 Bybit Theft (~$1.5B)

What happened:

In February 2025, Bybit disclosed the theft of roughly $1.5B in virtual assets. The FBI attributed the incident to North Korean cyber actors it tracks as ''TraderTraitor,'' with laundering activity dispersing funds across thousands of blockchain addresses. [29,30,31]

Why it mattered:

- **Scale:** It was widely characterized as the largest known crypto theft to date. [29,30,31,32]
- **Signal:** It reinforced that state-linked actors increasingly finance national objectives through financially motivated cybercrime. [29,30,32]

What changed for 2026 defenders:

- Treat crypto exposure (custody, treasury, on-chain liquidity) as a board-level risk even if you are ''not a crypto company.''
- Demand independent validation of signing workflows and privileged changes for any high-value asset transfer process (wallets, payment rails, treasury approvals).

Sources: [29,30,31,32]

2.2 Jaguar Land Rover Ransomware (UK Manufacturing)

What happened:

A cyberattack halted Jaguar Land Rover production for nearly six weeks in 2025. A UK study estimated total economic impact at ~£1.9B, with the government providing a loan guarantee to support recovery and continuity. [34,35]

Why it mattered:

- **Operational fragility:** Manufacturing downtime is a "compounding loss" (production, logistics, suppliers, contractual penalties).
- **Systemic ripple:** A disruption at a major manufacturer cascades through tier-1 and tier-2 suppliers.

What changed for 2026 defenders:

- Update OT/IT incident playbooks to explicitly prioritize "minimum viable operations" over perfect restoration.
- Contractually require ransomware readiness and incident coordination across critical suppliers.

Sources: [34,35]

2.3 UK Retail Campaign (M&S, Co-op, Harrods)

What happened:

UK retailers faced a coordinated wave of intrusions where attackers manipulated support processes to reset access and pivot into core environments. Public reporting described help desk social engineering and contractor pathways as key enabling factors. UK systemic impact estimates reached the hundreds of millions of pounds. [6,7,8,9,10,11]

Why it mattered:

- **Identity is now a supply chain.** If a vendor can reset your access, they can also reset your breach boundary.
- **Retail is a testbed for scalable disruption.** High transaction volume and tight margins mean even short outages are expensive.

What changed for 2026 defenders:

- Harden identity recovery: forced call-backs, known-device checks, and privileged reset gating.
- Audit all third-party remote access and admin roles; remove standing privilege where possible.

Sources: [6,7,8,9,10,11]

2.4 PowerSchool Breach (Education Concentration Risk)

What happened:

In 2025, investigations into the PowerSchool incident highlighted the concentration risk of education platforms: a single compromise can expose sensitive data across a large number of institutions and individuals. North Carolina's Department of Justice reported that the breach could affect more than 62 million current and former students and teachers nationwide. [21]

Why it mattered:

- **Long-tail identity harm:** Education data enables fraud, account takeover, and targeted scams for years.
- **Sector-wide exposure:** Schools inherit platform risk without having platform-level control.

What changed for 2026 defenders:

- Treat ''education SaaS'' access as critical infrastructure: enforce MFA, least privilege, and data minimization.
- Align breach response with identity protection at scale (notification, monitoring, fraud protection).

Sources: [21]

2.5 Salt Typhoon Telecom Espionage (Critical Dependency Targeting)

What happened:

US agencies issued guidance and advisories describing Chinese state-linked activity targeting telecommunications infrastructure (''Salt Typhoon''). The response included hardening guidance and sanctions, underscoring the strategic value of telecom access for intelligence collection and disruption readiness. [17,18,19,20]

Why it mattered:

- **Telecom is a dependency:** Authentication, incident response, and executive communications often rely on carrier services.
- **Pre-positioning risk is operational:** Persistent access to communications infrastructure changes crisis assumptions.

What changed for 2026 defenders:

- Assume carrier compromise or degradation is plausible during crises; build out-of-band communications for executives and incident command.
- Reduce dependence on SMS for MFA and account recovery; run a 72-hour telecom degradation exercise to validate alternatives in your crisis plan.
- Require strong monitoring for admin actions and remote access on network infrastructure.

Sources: [17,18,19,20]

2.6 Other Significant Incidents (Grouped by Risk Type)

Supply chain and developer ecosystem compromise

- **npm ecosystem ("Shai-Hulud" worm):** CISA warned of rapid, automated compromise spreading through the npm ecosystem by hijacking developer credentials and injecting malicious code into additional packages. [39]
- **North Korean developer targeting ("Contagious Interview"):** Multiple 2025 reports documented DPRK-linked activity using fake recruitment and trojanized packages to compromise developers and downstream environments. [40,41,42]

Financial infrastructure disruption

- **Brazil Pix supply-chain incident (C&M Software):** Brazil's central bank ordered provider shutdown steps after a cyberattack on a key services firm supporting financial institutions—demonstrating concentration risk in payment infrastructure. [36]

Distributor and platform concentration risk

- **Ingram Micro ransomware:** Data exfiltration affected parts of operations, highlighting concentration risk in the IT distribution supply chain. [37,38]
- **Change Healthcare (scope confirmation):** HHS/OCR maintained updated guidance on downstream impacts, reinforcing healthcare's systemic exposure to platform-level incidents. [44]

SaaS and identity abuse patterns

- **Salesforce ecosystem data theft:** 2025 advisories described vishing combined with connected-app abuse leading to large-scale data theft and extortion attempts. [22,23,24,25,26]

3. Threat Actor Evolution: Blurred Lines, Familiar Outcomes

2025 reinforced a reality executives dislike: the categories "nation-state" and "criminal" are increasingly operationally irrelevant. Motive differs, but tactics converge.

China

Telecom targeting and long-term access strategies drove defensive guidance and sanctions. [17,18,19,20]

North Korea

State-linked financial theft remained a strategic funding mechanism, exemplified by Bybit. [29,30]

Organized cybercrime

Groups continued to fragment, rebrand, and scale extortion operations without reducing total victimization. [16]

Hybrid campaigns

The same playbooks—credential theft, vishing, supply chain compromise—showed up across retail, SaaS, and developer ecosystems. [6,7,8,9,10,11,22,23,24,25,26,39]

Threat intelligence reporting in 2025 continued to emphasize identity, cloud, and supply chain as primary battlegrounds. [45,46]

4. Attack Method Evolution: The Human API Was the Vulnerability

Vishing + connected-app abuse	Documented campaigns used voice/social engineering to drive OAuth/token abuse and SaaS data theft. [22,23,24,25]	It bypasses "patching" entirely by abusing trust and workflow.
Help desk manipulation	Retail campaigns showed password reset paths and contractors as breach boundaries. [6,7,8,9,10,11]	Your identity recovery process is now an attack surface.
Deepfake / AI-enabled fraud	Prosecutors investigated AI voice scams targeting business leaders; incident reporting showed rising deepfake abuse. [27,28]	The authenticity of voice/video can no longer be assumed.
Supply chain compromise at code scale	CISA warned of rapid npm ecosystem compromise with automated propagation. [39]	Developer ecosystems can create "blast radius by default."
Exploit acceleration	Exploitation frequently occurred by the time a CVE was published for exploited vulnerabilities. [2,3]	Exposure management must be continuous and measured.

5. Sector Impact Analysis: Where Pain Was Concentrated

Healthcare

- Systemic exposure remained acute: public guidance on Change Healthcare underscored the cascading impact of a single platform outage and breach. [44]
- Healthcare continued to lead breach cost metrics in 2025. [15]

Retail & Consumer

- UK retail incidents demonstrated how customer-facing operations and thin margins magnify cyber disruption cost. [6,7,8,9,10,11]
- Third-party risk and identity reset paths were dominant factors. [12]

Manufacturing

- JLR highlighted how ransomware impacts physical throughput, suppliers, and national economic considerations. [34,35]

Technology, SaaS, and Developer Ecosystems

- SaaS compromise patterns (vishing + connected app abuse) made "identity governance" a priority control. [22,23,24,25]
- npm compromise reinforced that software supply chain is not hypothetical—it's operational. [39]

6. Regulatory Landscape: Enforcement and Operational Readiness

2025 marked a shift from "preparation" to **operational enforcement and audit reality** across several frameworks.

1

EU DORA (Digital Operational Resilience Act) – applied in 2025

DORA began applying in January 2025, driving ICT risk management expectations for financial entities and critical ICT service providers. [54,55]

Leader implication: audit evidence, testing, and third-party oversight now need to be demonstrable—not aspirational.

2

EU NIS2 – national implementation and board accountability

NIS2 establishes stronger security and incident reporting expectations and introduces meaningful maximum administrative fines (including turnover-based caps) for covered entities. [56]

Leader implication: coverage scoping, incident reporting readiness, and governance structures must be board-visible.

3

PCI DSS v4.x – future-dated requirements became real

PCI SSC reiterated that organizations should adopt the future-dated requirements of PCI DSS v4.x ahead of their March 31, 2025 effective date. [57]

Leader implication: payment environments are still a high-attacker-value target; PCI compliance remains a baseline, not a control set.

7. Market Intelligence: Consolidation Accelerated (and Identity Won)

Large 2025 transactions reinforced where buyers believe enterprise security budgets will concentrate:

$32B

Google ↔️ Wiz

Google Cloud signed an agreement to acquire Wiz; the deal was cleared by the US DOJ later in 2025. [47,48,49]

$25B

Palo Alto Networks ↔️ CyberArk

A landmark identity/privileged access consolidation move—reflecting the market shift toward identity as a platform layer. [50,51,52]

$7.75B

ServiceNow ↔️ Armis

Another signal that cyber is being absorbed into broader enterprise operations and risk platforms. [53]

Strategic interpretation: the control plane narrative (identity, cloud posture, and operational resilience) is now the center of gravity—not perimeter tooling.

8. Eight Decisions for 2026

This is not a list of 30 controls. It's **eight decisions** that materially change risk.

Decision 1: Build an Emergency Patch Lane

Pre-authorize an "incident patch" process for actively exploited vulnerabilities. Define who can accept service risk to close exposure quickly. Use compensating controls when patching is delayed.

Decision 2: Treat Identity Verification as Infrastructure

Make helpdesk resets and privileged access high-assurance workflows. Push phishing-resistant MFA where feasible. Monitor for token theft, impossible travel, and suspicious OAuth grants.

Decision 3: Reclassify SaaS/CRM as Critical Infrastructure

Tighten third-party SaaS governance (logging, access reviews, app allow-listing). Assume: "If it can be socially engineered, it will be."

Decision 4: Run Supplier Concentration Like Systemic Risk

Identify single points of operational failure. Require continuity plans, not just questionnaires, for critical vendors.

8. Eight Decisions for 2026 (continued)

Decision 5: Optimize for Operational Continuity

Invest in recoverability: immutable backups, restore drills, manual workarounds. Plan for "partial outage" scenarios.

Decision 6: Make Breach Readiness a Standing Governance Function

Define disclosure thresholds, decision rights, and external communications playbooks. Run at least one board-level exercise that assumes data theft + disruption.

Decision 7: Reduce Data Blast Radius

Minimize retention; segment sensitive datasets; encrypt aggressively. Assume exfiltration is plausible even without "ransomware encryption."

Decision 8: Close the AI Oversight Gap

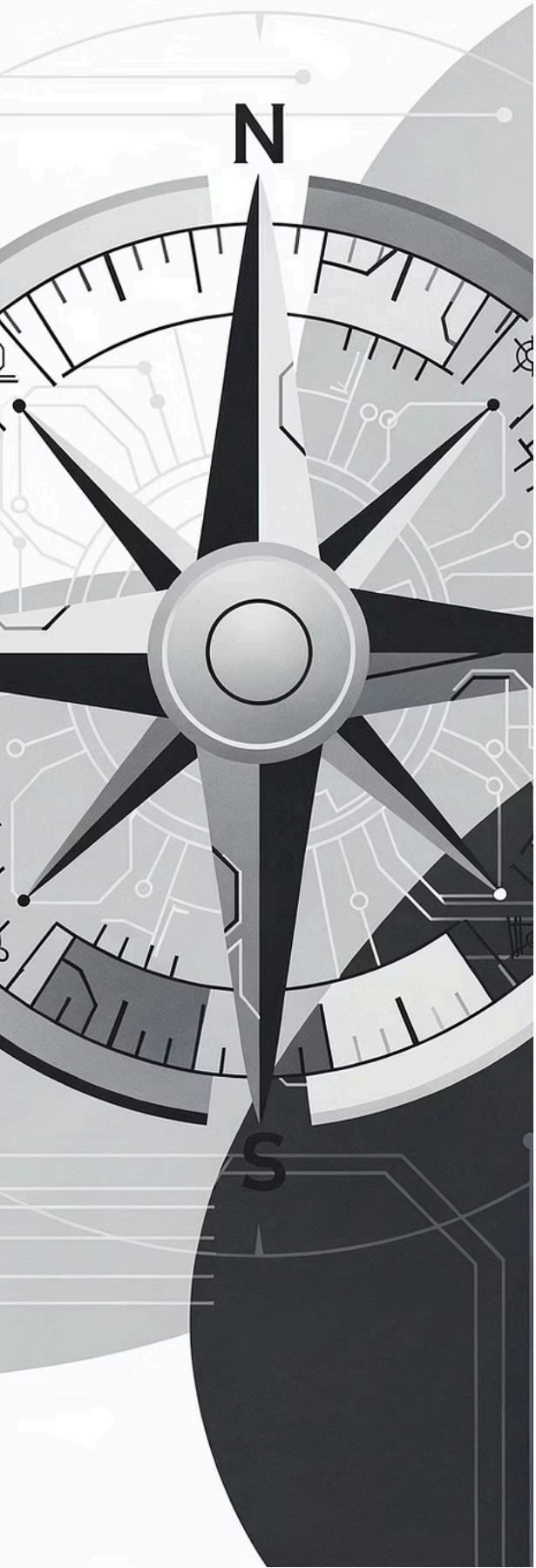
Inventory AI usage, enforce access controls, log interactions. Treat "shadow AI" like shadow IT—with clearer risk ownership.

9. Investment Priorities

Exploit Response Program	Asset inventory + owner accountability + weekend coverage	NOW	4-8 weeks for first wins
Identity Artifact Governance	Token inventory + rotation automation + monitoring	NOW	6-12 weeks
Third-Party Containment	Vendor access mapping + isolation playbooks	Q1	8-12 weeks
Behavioral Analytics	Counters AI-adaptive malware	Q1-Q2	6-12 months
ERP/Collaboration Hardening	Segmentation + admin path controls + telemetry	Q2	3-6 months
PQC Discovery & Planning	Cryptographic asset inventory	H2	Ongoing

10. Board Discussion Points

1. What are our top 10 internet-facing enterprise services, and can we mitigate them inside 72 hours?
2. If an attacker steals an admin token or API key today, how quickly would we know—and can we contain it?
3. Which vendors represent single points of operational failure, and what's our tested workaround?
4. Do we have an explicit stance on extortion and decision rights under time pressure?
5. How do we verify identity for high-value transactions when video and voice are no longer trustworthy?



Key Conclusions

2025 proved that modern enterprises operate in contested digital environments where the boundaries between nation-state espionage, criminal enterprise, and supply chain compromise have dissolved.

The common failure mode wasn't missing controls—it was **controls that couldn't execute fast enough.**

Organizations that built emergency response capability—not just security programs—absorbed less damage. Those that treated identity as infrastructure, not IT plumbing, reduced blast radius. Those that planned for vendor compromise, not just vendor assessment, maintained operational continuity.

The uncomfortable truth from 2025: You can't prevent every breach, but you can determine whether a compromise becomes an incident, and whether an incident becomes a catastrophe.

That determination is now a leadership function, not a technical one.

APPENDICES

For technical leaders and audit trails.

A. Technical Indicators & 2026 Vigilance List

Priority exploitation items referenced in this brief (start here):

- **Microsoft SharePoint on-prem (CVE-2025-53770 and related chaining):** rotate MachineKeys, validate patch posture, and hunt for persistence. [4,5]
- **Automated software supply chain propagation (npm ecosystem):** validate developer credential hygiene, enforce signed commits where feasible, and monitor package integrity. [39]
- **Telecom infrastructure targeting ("Salt Typhoon" pattern):** validate out-of-band communications and MFA fallbacks, harden network infrastructure access, and improve logging/monitoring. [17,18]
- **Use CISA KEV as your baseline "hot list."** If it's on KEV and exposed, treat it as urgent. [3]

MITRE ATT&CK techniques frequently observed in 2025 narratives (non-exhaustive):

- T1078 Valid Accounts (incl. cloud/SaaS admin roles)
- T1566 Phishing / Vishing (voice-based social engineering)
- T1552 Unsecured Credentials / Token theft
- T1195 Supply Chain Compromise
- T1486 Data Encrypted for Impact / extortion variants

B. Methodology & Notes

This brief is a synthesis of:

- Public government advisories (CISA, NSA, Treasury), incident disclosures, and regulator guidance. [3,4,6,17-20,54-57]
- Vendor and industry reporting (IBM Cost of a Data Breach, Verizon DBIR, threat intel roundups). [12-16,45,46]
- Reputable journalism for timeline corroboration (primarily Reuters; supplemented where helpful). [1,8-10,22,26,27,30,34-38,48-53]

Scope note: Events are selected for executive relevance (operational disruption, concentration risk, systemic dependency, or demonstrated shift in attacker playbooks). Not every major 2025 incident is included. Some incidents may have initial compromise activity outside the calendar-year window but had material investigation, disclosure, or business impact during 2025; those are included.

AI assistance: AI tools were used to assist drafting and editing. All factual claims are supported by cited sources. Final curation and accountability: Benjamin Olivier.

Disclaimer: This document is for informational purposes only and does not constitute legal, regulatory, or investment advice.

Corrections: If you spot an error or have an update, please see Appendix D (About / Contact / License / Corrections).

C. Sources (References 1-20)

- **[1]** Reuters. "European airports race to fix check-in glitch after hacking disruption." (2025-09-21) **https://www.reuters.com/business/aerospace-defense/european-airports-race-fix-check-in-glitch-after-hacking-disruption-2025-09-21/**
- **[2]** VulnCheck. "1H 2025 Vulnerability Exploitation Trends." (2025) **https://www.vulncheck.com/blog/state-of-exploitation-1h-2025**
- **[3]** CISA. "Known Exploited Vulnerabilities (KEV) Catalog." (2025) **https://www.cisa.gov/known-exploited-vulnerabilities-catalog**
- **[4]** CISA. "CISA Releases Alert on Microsoft SharePoint Vulnerabilities." (2025-08-01) **https://www.cisa.gov/news-events/alerts/2025/07/20/update-microsoft-releases-guidance-exploitation-sharepoint-vulnerabilities**
- **[5]** Palo Alto Networks Unit 42. "Microsoft SharePoint Vulnerabilities (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770)." (2025) **https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/**
- **[6]** CISA. "CISA and Partners Release Updated Advisory on Scattered Spider Group." (2025-07-29) **https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group**
- **[7]** FBI IC3. "Cybersecurity Advisory: Scattered Spider." (2025-07-29) **https://www.ic3.gov/CSA/2025/250729.pdf**
- **[8]** Reuters. "British retailer Marks & Spencer, Co-op cyberattackers duped help desks." (2025-05-06) **https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/**
- **[9]** Reuters. "UK retailer Marks & Spencer says hackers broke in through third-party contractor." (2025-05-21) **https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/**
- **[10]** Reuters. "UK retailer Harrods latest target of cyber attack." (2025-05-01) **https://www.reuters.com/business/retail-consumer/harrods-is-latest-british-retailer-be-hit-by-cyber-attack-2025-05-01/**
- **[11]** Cyber Monitoring Centre. "Statement regarding recent ransomware incidents in the UK retail sector." (2025-06-09) **https://cybermonitoringcentre.com/2025/06/20/cyber-monitoring-centre-statement-on-ransomware-incidents-in-the-retail-sector-june-2025/**
- **[12]** Verizon. "2025 Data Breach Investigations Report (DBIR)." (2025) **https://www.verizon.com/business/resources/reports/dbir/**
- **[13]** IBM. "Cost of a Data Breach Report 2025." (2025) **https://www.ibm.com/reports/data-breach**
- **[14]** IBM Newsroom. "IBM report: 13% of organizations reported breaches of AI models or applications; Cost of a Data Breach 2025 findings." (2025-07-30) **https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls**
- **[15]** IBM (PDF copy). "Cost of a Data Breach Report 2025 (PDF)." (2025-08-22) **https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf**
- **[16]** Emsisoft. "The State of Ransomware in the U.S.: Report and Statistics 2025." (2025) **https://www.emsisoft.com/en/blog/54577/the-state-of-ransomware-in-the-u-s-report-and-statistics-2025/**
- **[17]** CISA. "Cybersecurity Advisory AA25-239A (Salt Typhoon)." (2025) **https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a**
- **[18]** CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems" (2025) **https://www.cisa.gov/news-events/news/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise**
- **[19]** U.S. Department of the Treasury. "Treasury Sanctions Chinese Company Involved in Salt Typhoon Intrusions (Press Release JY2792)." (2025) **https://home.treasury.gov/news/press-releases/jy2792**
- **[20]** SecurityWeek. "Salt Typhoon Targeting Old Cisco Vulnerabilities in Fresh Telecom Hacks." (2025) **https://www.securityweek.com/salt-typhoon-targeting-old-cisco-vulnerabilities-in-fresh-telecom-hacks/**

C. Sources (References 21-42)

- **[21]** North Carolina Department of Justice. "Attorney General Jeff Jackson is Investigating PowerSchool Over Data Breach" (2025-02-06) **https://ncdoj.gov/attorney-general-jeff-jackson-is-investigating-powerschool-over-data-breach/**
- **[22]** Reuters. "Hackers abuse modified Salesforce app to steal data, extort companies, Google says" (2025-06-04) **https://www.reuters.com/sustainability/boards-policy-regulation/hackers-abuse-modified-salesforce-app-steal-data-extort-companies-google-says-2025-06-04/**
- **[23]** Google Cloud. "The Cost of a Call: From Voice Phishing to Data Extortion" (2025-06-04) **https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion**
- **[24]** FBI IC3. "Cybersecurity Advisory: UNC6040 / Salesforce-focused extortion activity (CSA 250912)." (2025-09-12) **https://www.ic3.gov/CSA/2025/250912.pdf**
- **[25]** Salesforce. "Protect Your Salesforce Environment from Social Engineering Threats" (2025-03-12) **https://www.salesforce.com/blog/protect-against-social-engineering/**
- **[26]** Reuters. "Almost 1 billion Salesforce records stolen, hacker group claims" (2025-10-03) **https://www.reuters.com/sustainability/boards-policy-regulation/almost-1-billion-salesforce-records-stolen-hacker-group-claims-2025-10-03/**
- **[27]** Reuters. "Italian police freeze cash from AI-voice scam that targeted business leaders" (2025-02-12) **https://www.reuters.com/technology/artificial-intelligence/italian-police-freeze-cash-ai-voice-scam-that-targeted-business-leaders-2025-02-12/**
- **[28]** Resemble AI. "Q1 2025 Deepfake Incident Report: Mapping Deepfake Incidents" (2025) **https://www.resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf**
- **[29]** FBI IC3. "PSA: DPRK Responsible for $1.5 Billion Theft from Bybit." (2025-02-26) **https://www.ic3.gov/PSA/2025/PSA250226**
- **[30]** Reuters. "FBI says North Korea was responsible for $1.5 billion ByBit hack" (2025-02-27) **https://www.reuters.com/technology/cybersecurity/fbi-says-north-korea-was-responsible-15-billion-bybit-hack-2025-02-27/**
- **[31]** AP News. "FBI accuses North Korean-backed hackers of stealing $1.5 billion in crypto from Dubai-based firm" (2025-02-27) **https://apnews.com/article/bybit-exchange-crypto-hack-north-korea-7c8335c1397261554138090c2c38f457**
- **[32]** Wilson Center. "The Bybit Heist: What Happened & What Now?" (2025-03-31) **https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now**
- **[33]** Nansen. "Bybit Hack 2025 (analysis)." (2025-02-26) **https://research.nansen.ai/articles/by-bit-hack-what-happened-and-where-are-the-funds-going-on-chain**
- **[34]** Reuters. "Cyber attack halted Jaguar Land Rover production, cost £1.9 bln, study finds." (2025-10-22) **https://www.reuters.com/sustainability/boards-policy-regulation/jaguar-land-rover-hack-cost-uk-economy-25-billion-report-says-2025-10-22/**
- **[35]** Cyber Monitoring Centre. "CMC announces record financial impact of cyber attack on Jaguar Land Rover." (2025-10-22) **https://cybermonitoringcentre.com/2025/10/22/cmc-announces-record-financial-impact-of-cyber-attack-on-jaguar-land-rover/**
- **[36]** Reuters. "Brazil central bank orders shut down payments firm after cyberattack." (2025-07-02) **https://www.reuters.com/world/americas/brazils-cm-software-hit-by-cyberattack-central-bank-says-2025-07-02/**
- **[37]** Reuters. "Ingram Micro says identified ransomware on certain of its internal systems" (2025-07-06) **https://www.reuters.com/business/ingram-micro-says-identified-ransomware-certain-its-internal-systems-2025-07-06/**
- **[38]** Ingram Micro. "Cybersecurity Incident" (2025-07-07) **https://www.ingrammicro.com/en-us/2025cybersecurityincident**
- **[39]** CISA. "Widespread Supply Chain Compromise Impacting npm Ecosystem." (2025-09-23) **https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem**
- **[40]** Socket.dev. "Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages" (2025) **https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages**
- **[41]** BleepingComputer. "North Korean XORIndex malware hidden in 67 malicious npm packages" (2025) **https://www.bleepingcomputer.com/news/security/north-korean-xorindex-malware-hidden-in-67-malicious-npm-packages/**
- **[42]** The Hacker News. "North Korean Hackers Flood npm Registry with XORIndex Malware in Ongoing Attack Campaign" (2025) **https://thehackernews.com/2025/07/north-korean-hackers-flood-npm-registry.html**

C. Sources (References 43-57)

- **[43]** World Economic Forum. "Why detecting dangerous AI is key to keeping trust alive in the deepfake era" (2025-07) **https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/**
- **[44]** HHS (HIPAA / OCR). "Change Healthcare cyberattack: FAQs on medical information sharing and data breach notifications." (2025) **https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html**
- **[45]** Mandiant. "M-Trends." (2025) **https://www.mandiant.com/m-trends**
- **[46]** CrowdStrike. "2025 Global Threat Report." (2025) **https://www.crowdstrike.com/global-threat-report/**
- **[47]** Google. "Google Cloud signs agreement to acquire Wiz." (2025-03-18) **https://cloud.google.com/blog/products/identity-security/google-announces-agreement-acquire-wiz**
- **[48]** Reuters. "Google owner Alphabet to buy cybersecurity firm Wiz for $32 billion." (2025-03-18) **https://www.reuters.com/technology/cybersecurity/google-agrees-buy-cybersecurity-startup-wiz-32-bln-ft-reports-2025-03-18/**
- **[49]** Reuters. "Google owner Alphabet's $32 bln deal for Wiz cleared by US DOJ." (2025-11-05) **https://www.reuters.com/business/googles-32-billion-deal-wiz-clears-doj-antitrust-review-wiz-ceo-tells-wsj-2025-11-05/**
- **[50]** Palo Alto Networks (Investor Relations). "Palo Alto Networks announces agreement to acquire CyberArk." (2025-07-30) **https://www.paloaltonetworks.ca/palo-alto-networks-in-agreement-to-acquire-cyberark**
- **[51]** Reuters. "Palo Alto Networks to buy CyberArk in $25 billion deal." (2025-07-30) **https://www.reuters.com/world/middle-east/palo-altos-25-billion-deal-cyberark-targets-rising-ai-driven-threats-2025-07-30/**
- **[52]** CNBC. "Palo Alto Networks to acquire CyberArk for $25 billion." (2025-07-30) **https://www.cnbc.com/2025/07/30/palo-alto-networks-cyberark-deal.html**
- **[53]** Reuters. "ServiceNow to buy Armis for $7.75 billion as AI-fueled cyber risks surge" (2025-12-23) **https://www.reuters.com/legal/litigation/servicenow-buy-cybersecurity-startup-armis-775-billion-2025-12-23/**
- **[54]** EUR-Lex. "Regulation (EU) 2022/2554 (Digital Operational Resilience Act - DORA)." (2022 (applies from 2025-01-17)) **https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng**
- **[55]** European Banking Authority. "EBA amends its guidelines on ICT and security risk management measures in the context of DORA application." (2025-02-11) **https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application**
- **[56]** EUR-Lex. "Directive (EU) 2022/2555 (NIS2 Directive)." (2022) **https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng**
- **[57]** PCI Security Standards Council. "Now is the time for organizations to adopt the future-dated requirements of PCI DSS v4.x." (n.d. (future-dated requirements effective 2025-03-31)) **https://blog.pcisecuritystandards.org/now-is-the-time-for-organizations-to-adopt-the-future-dated-requirements-of-pci-dss-v4-x**

D. About / Contact / License / Corrections

About the author:

Benjamin Olivier is a technology and cybersecurity executive. He publishes practical, source-backed briefings on cyber risk, operational resilience, and the security decisions that matter at executive and board level.

How to cite this brief:

Olivier, Benjamin. *Cybersecurity Executive Annual Brief: 2025.* Concipio, v1.0, published 2026-01-XX.

Contact:

- Website: **https://concipio.cc**
- LinkedIn: **https://www.linkedin.com/in/bolivier**
- Email: **benjamin@concipio.cc**

Corrections / updates:

If you spot an error or have an update, send a note (with a supporting source link) to the contact address above. Updates will be reflected in a new version number.

License:

Third-party materials:

This brief includes summaries of third-party sources; all trademarks and source content remain the property of their respective owners.

Version History

v1.0	2026-01-14	Initial publication.

End of Document