RISK BRIEFING, FINANCE EDITION: CREDENTIAL TRAPS FOR TRAVELING BANKERS, TWO PATCH-NOW EMERGENCIES, AND THE PRICE REGULATORS PUT ON AUTHENTICATION

Date: 2026-07-28
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Sector focus: Financial services, banking, and insurance
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

two vulnerabilities crossed into confirmed active exploitation, one of them into mass exploitation, this week, and both sit squarely inside typical financial-sector infrastructure. An authentication bypass in Check Point's Security Management platform (CVE-2026-16232) lets an unauthenticated attacker take full administrative control of the server that writes firewall policy, and if Check Point Security Management sits in your stack, a compromise there is quiet, and it rewrites the rules protecting everything the platform manages [1][4][5]. A remote-code-execution flaw in on-premises Microsoft SharePoint (CVE-2026-50522) is being mass-exploited with a machine-key theft technique that survives patching, so any bank or insurer still running on-prem SharePoint for deal rooms, board materials, or departmental sites needs to patch, rotate keys, and hunt [1][2][3]. CISA added both to the Known Exploited Vulnerabilities catalog on July 22 with a three-day federal remediation window [1]. Just behind the patch queue sits a campaign built for your travel patterns: attackers are altering DNS on hotel and conference-center Wi-Fi gateways to serve fake Microsoft 365 logins, ReliaQuest reports financial services among the sectors whose traffic ReliaQuest observed, though the researchers stress the campaign chases traveling employees wherever they connect rather than targeting any one sector, and in some cases a device-code sign-in lure captured a legitimate OAuth session and bypassed MFA outright [11]. Traveling bankers, deal teams, and conference-bound executives are exactly the population this reaches. The accountability news carries direct sector lessons: Ernst & Young notified clients that tax and financial documents were exposed through a third-party support-ticket platform, which makes fourth-party risk in your professional-services supply chain concrete [35]; regulators priced missing authentication controls at $18 million in a 42-attorney-general settlement with 23andMe whose security obligations now bind the acquirer, a precedent M&A deal teams and underwriters should read closely [31][32]; and Coca-Cola's SEC filing on its fairlife ransomware production halt, alongside Ecopetrol's 6-K, shows what live materiality disclosure looks like in practice [14][15][17]. In Washington, the Hugging Face incident

produced the bipartisan AI Kill Switch Act (H.R. 9917), the clearest signal yet that AI incident reporting and shutdown capability are headed toward regulatory expectations [19][20]. Patch the two criticals first; then work the traveler-hardening and governance items below.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Patch Check Point Security Management (CVE-2026-16232), pull management interfaces off the internet, and audit recent policy changes and admin activity	Actively exploited zero-day grants unauthenticated full admin over the firewall management server; finance is a heavy Check Point shop, and a compromised management plane silently rewrites policy [1][4][5]
2	Patch on-prem SharePoint (CVE-2026-50522), then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence	Mass exploitation began within hours of a July 20 public exploit; stolen machine keys survive patching [1][2][3]
3	Require full-tunnel VPN before anything else on hotel or conference Wi-Fi; disable Microsoft Entra device-code flow where the business does not need it, and issue clean travel devices with no stored credentials for border crossings	Attackers are hijacking hotel Wi-Fi gateway DNS to serve fake Microsoft 365 logins, financial services is among the sectors whose traffic was observed, and a device-code lure bypasses MFA in some cases [11]; manual phone searches at the border now require no suspicion in the Fourth Circuit [39][40]
4	Confirm Zimbra is patched for CVE-2025-66376 and current (10.1.20); ask Zimbra-running vendors and counterparties the same question	Joint advisory AA26-204A details active Russian espionage against webmail; exploit triggers on viewing an email and yields roughly 90 days of correspondence [6][8]
5	Ask your audit, tax, and advisory firms what SaaS platforms hold your documents and what their incident-notification terms are	EY client tax and financial documents were exposed through a third-party IT support-ticket platform; your professional-services firms have their own vendors [35]
6	Pre-position customer-facing scam-response communications; confirm MFA, rate limiting, and login-anomaly monitoring	Scammers are mass-mailing $2,000 sextortion demands built on genuine leaked data, with Betterment among the named breaches; regulators priced those authentication controls at $18M in the 23andMe settlement [37][31]

Priority	Action	Why Now
7	Monitor and restrict outbound DNS (block direct-to-external-resolver traffic where feasible)	Malware is tunneling command-and-control through DNS, and hijacked gateways forge DNS answers before they reach trusted resolvers [11] [12]
8	Set enterprise browser-extension policy for any machine running an AI browser agent, starting where mailboxes hold MNPI	Unpatched research shows co-installed extensions can hijack Claude for Chrome's agent actions, including reading mail and calendars [24] [25]
9	Verify WordPress (wp2shell) and nginx (CVE-2026-42533) patch completion; brief fraud teams that compromised sites serve fake banking login overlays	wp2shell exploitation continues at internet scale and targets visitors with banking-credential overlays; an nginx proof-of-concept is expected ~August 5 [9][10]
10	Get a New Jersey A5328 applicability read covering marketing and underwriting data programs	The new law bans sensitive-data sale outright at $50,000 per record, and its broad definitions can reach data buyers and enrichers [46]

WHAT'S CHANGED SINCE JULY 22

- **Two new KEV-listed criticals.** CISA added SharePoint CVE-2026-50522 and Check Point CVE-2026-16232 to the Known Exploited Vulnerabilities catalog on July 22 with a July 25 federal remediation deadline [1].
- **The Zimbra espionage campaign got its advisory.** Joint advisory AA26-204A (July 23), sealed by NSA, FBI, CISA, and Dutch intelligence plus 22 co-signers, formally documents Laundry Bear's exploitation of Zimbra CVE-2025-66376 [6].
- **The AI incident produced legislation.** H.R. 9917, the AI Kill Switch Act, was introduced July 23 with bipartisan sponsorship [19][20].
- **CISA 2015 reauthorization advanced one chamber.** The House passed its FY2027 NDAA (216-212) with a provision extending the threat-sharing law through 2036; the Senate has no matching provision and the September 30 sunset still stands, which puts the liability protections behind FS-ISAC-style sharing on the clock [47].
- **The fairlife extortion ran to completion.** The Anubis group's publication deadline for fairlife data passed Monday morning, and the stolen data has since been posted for download; Coca-Cola has confirmed data was taken, though the claimed 1 TB volume remains the attackers' assertion [15][59][60].

- **Holding steady:** wp2shell and FortiBleed remediation guidance is unchanged; nginx CVE-2026-42533 still has no public exploit, though a proof-of-concept has been announced for ~August 5 [9][10]. The July 22 update to the Iranian PLC advisory (AA26-097A) expanded vendor scope; it matters most to the utilities you finance or insure rather than to your own estate [13].

PATCH NOW: TWO KEV-LISTED EMERGENCIES

- **Check Point Security Management CVE-2026-16232 (CVSS 9.1).** An improper-authentication flaw in the Security Management Server login process lets an unauthenticated attacker obtain a token and authenticate with full administrative rights, which means the ability to rewrite firewall policy for everything the platform manages [4][5]. Check Point confirms in-the-wild exploitation against "a very small number of customers" and has shipped fixes (R81.20 JHF T158+, R82 T118+, R82.10 T36+) [4]. Financial institutions are exposed here wherever Check Point Security Management is in use, and a management-plane compromise is quiet by design: policy changes look administrative, and nothing crashes. Treat any confirmed compromise as a potential full-network exposure event. Audit the policy revision history and administrator logins over the exploitation window, and get management interfaces off the open internet [4][5].
- **Microsoft SharePoint CVE-2026-50522 (CVSS 9.8, on-premises only).** A deserialization flaw in SharePoint Subscription Edition, 2019, and 2016 allows remote code execution; SharePoint Online is not affected [3]. Microsoft patched it July 14; a public exploit landed July 20 and mass exploitation followed within hours [2]. Banks and insurers that kept on-prem SharePoint for regulated records, board portals, or legacy departmental sites should note the exploitation detail that matters most: watchTowr reports attackers using a single request to steal IIS machine keys, which let them forge valid authentication tokens and walk back in after you patch [2]. CISA's hardening guidance is blunt: assume compromise on internet-exposed unpatched servers, hunt and remediate, then rotate machine keys [1][2]. Both espionage and ransomware actors are using the same entry points [2].
- **Patch-status watchlist.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites are attacking their visitors with fake Microsoft 365 and banking login overlays, so the exposure reaches your customers and staff even if you run no WordPress at all; fraud teams should expect credential-theft reports that trace back to ordinary browsing [10]. nginx CVE-2026-42533 remains unexploited in public, but the researcher who disputes F5's severity assessment says he will publish proof-of-concept details around August 5; close out patch verification before that date [9]. FortiBleed guidance is unchanged from prior briefings: rotation of FortiGate credentials, session termination, and MFA remain the only complete fix.

CREDENTIAL THEFT FOLLOWS YOUR TRAVELERS AND YOUR MAIL

- **Hotel Wi-Fi as a credential trap for deal teams.** ReliaQuest reports an ongoing campaign, active since at least June, in which attackers alter DNS settings on hotel and conference-center Wi-Fi gateways so travelers land on convincing fake Microsoft 365 portals, with financial services among the sectors whose traffic ReliaQuest observed, while noting the campaign is not sector-specific [11]. In some cases the attackers used a device-code sign-in flow that captures a legitimate OAuth session and bypasses MFA outright [11]. The population at risk maps directly onto banking work patterns: relationship managers on the road, deal teams at off-sites, executives at industry conferences. Public DNS settings do not help, because the compromised gateway forges answers before they reach the resolver [11]. The fix is architectural: full-tunnel VPN before anything else on untrusted networks, encrypted DNS in strict mode, and disabling the Entra device-code flow where the business does not need it [11]. A captured session token from a managing director's mailbox is a market-sensitive event, and the compromise leaves the credential itself intact.
- **Laundry Bear and the Zimbra "view-based" exploit.** Joint advisory AA26-204A (July 23) documents a Russian state-linked actor, tracked as Laundry Bear, Void Blizzard, and TA488, exploiting a cross-site-scripting flaw in Zimbra webmail (CVE-2025-66376, patched November 2025, exploited as a zero-day before that); opening or previewing the message is enough, with no attachment or link click required [6]. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [8]. Named target sectors include government, defense, energy, and technology rather than finance, but the exposure model translates: 90 days of correspondence from a counterparty, a local-government partner, or a portfolio company running Zimbra can carry your deal terms and your client data [6][8]. If you run Zimbra anywhere in the group, patch and upgrade (10.1.20 shipped July 20 with nine additional critical fixes) and hunt for historical compromise; if your vendors or municipal counterparties run it, ask them the same question [8]. An alleged group member was extradited from Thailand and is facing charges in Boston federal court [8].
- **DNS as a covert channel.** Fortinet documented a TrickBot-labeled Windows backdoor that runs its command-and-control entirely over DNS queries routed through Google's public resolver, moving 1.2 MB of data in about 40 seconds in testing [12]. The attribution rests on one vendor's code-similarity analysis and the campaign's scale is unquantified, but the defensive lesson stands on its own: an egress policy that inspects HTTP while letting workstations talk DNS to arbitrary external resolvers has a blind spot. Pair this with the hotel-gateway campaign above and DNS control earns a place on this quarter's hardening list [11][12].

THIRD-PARTY, FOURTH-PARTY, AND THE M&A PAPER TRAIL

- **EY and the vendor behind your advisor.** Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, with unauthorized access running March 28 to April 12 and detection on April 23 [35]. The structural lesson deserves board time: your professional-services firms have their own vendor stacks, and client tax and financial documents can leave your control through an ITSM SaaS you have never heard of. Ask your audit, tax, and advisory firms which platforms hold or transit your documents, what their vendor-assessment posture is, and what notification clock applies when their vendor is breached [35].
- **23andMe, and a precedent that outlives bankruptcy.** Forty-one states and the District of Columbia settled with 23andMe for $18 million over the 2023 credential-stuffing breach that exposed roughly 6.9 million people's data [31]. Two features matter for this sector. First, regulators effectively priced the missing controls, and they are the basics your examiners already ask about: MFA, rate limiting, and login-anomaly detection [31]. Second, durability: the injunctive terms (an enhanced security program, independent oversight, preserved consumer deletion rights) bind TTAM, the entity that bought the company out of bankruptcy [32]. Security obligations followed the assets. For M&A deal teams that is a due-diligence instruction, and for cyber underwriters it is a pricing input: a target's unresolved breach can arrive with a regulator-enforced compliance tail attached [31][32].
- **Vendor-breach class actions multiplied.** An Exact Sciences patient filed a proposed class action against Abbott Laboratories over a ShinyHunters-claimed theft, and former Nissan employees filed suit over employee data (Social Security numbers, banking details) exposed when attackers hit Oracle-hosted PeopleSoft HR systems, with the complaint alleging a 29-day gap between breach and notice [29][30]. Note the pattern in both: plaintiffs are suing the customer of the breached platform, and the notification clock is part of the claim. Backend concentration is the same story in healthcare, where the OpenLoop breach (716,000 individuals per the HHS breach portal, reported in March) put patients' data with a vendor most of them never chose, a dynamic health insurers in particular should recognize in their own claims and telehealth stacks [33][34].

DISCLOSURE, EXTORTION, AND THE CUSTOMER-FACING FALLOUT

- **Two live materiality-disclosure examples.** Coca-Cola told regulators on July 16 that a ransomware attack forced it to temporarily suspend US production at fairlife, its dairy subsidiary [14]. The Anubis group listed fairlife on its leak site July 20 claiming roughly 1 TB of stolen data with a publication deadline of Monday, July 27; the volume figure remains an attacker claim [15]. Coca-Cola has since confirmed the incident involved the taking of certain data, and Anubis posted the stolen data for download after the deadline passed [59][60]. Colombia's Ecopetrol separately disclosed unauthorized access to cloud file storage across roughly 15 subsidiaries in an SEC 6-K [17]. For disclosure committees, these are working

examples of how peers are treating operational cyber impact as material and filing on it while facts are still developing. Compare them against your own incident-materiality playbook: could you produce a filing of that shape mid-incident, with attacker claims explicitly separated from confirmed facts?

- **Extortion-payment governance, illustrated.** Australia's Origin Energy (about 4.8 million customers) confirmed unauthorized access to customer data including partial payment details, with an extortionist claiming 2 million records; a media report that the threat was privately settled is unverified [16]. The unverified settlement report is itself the lesson: once an incident is live, rumor will assign your organization a payment decision whether you made one or not. Payment posture, decision authority, sanctions screening, and disclosure sequencing need to be agreed before the incident, in a governance document your board has seen [16].
- **The long tail of leaked data reaches your customers.** A mass sextortion campaign is impersonating the ShinyHunters group and demanding $2,000 in Bitcoin, using genuinely leaked breach data to look credible, with Betterment among the named breaches; there is no actual device compromise behind the claims [37]. Expect customer contact citing real breaches, including breaches at other firms, and treat the response as a fraud-team deliverable: a plain-language, pre-positioned explanation of what the scam is, what data it reuses, and what customers should do, published the way Betterment did [37]. Relatedly, the Suno platform's November breach surfaced only when 55.3 million accounts appeared in Have I Been Pwned this week, with no proactive disclosure from the company; silence has become its own reputational risk [36].

AI GOVERNANCE REACHES THE CONTRACT AND THE BOARDROOM

- **A kill-switch bill, introduced.** Reps. Ted Lieu and Nathaniel Moran introduced H.R. 9917, the AI Kill Switch Act, on July 23 [19][20]. The bill would require AI developers above defined thresholds ($100 million in training compute or $500 million in revenue) to maintain the technical ability to throttle, suspend, or shut down their models; report qualifying incidents within 15 days; and comply with graduated federal correction orders, up to emergency shutdown, during defined loss-of-control scenarios, with civil penalties scaling to $20 million per day [19]. It is one chamber's freshly introduced bill, and passage is far from assured, but financial institutions building on frontier-model APIs should note the direction: incident reporting and shutdown capability are becoming regulatory vocabulary, and model-risk-management frameworks your regulators already apply give you a head start on answering "could we shut it down, and who orders it?" [19][20].
- **Put AI vendor terms on paper.** Post-incident analysis of the OpenAI/Hugging Face event converged on a practical point: model-level safeguards are not a security boundary, and effective controls live outside the model in network rules, scoped credentials, allow lists, and outbound data-loss prevention [22]. Two governance wrinkles surfaced this week belong in your vendor negotiations: Hugging Face says commercial frontier-model APIs refused to analyze attack artifacts during incident response, forcing a fallback to a self-hosted open-weight model, and a published claim (single-outlet, so far unconfirmed)

alleges OpenAI took roughly ten days to notify Hugging Face [21][58]. Translate both into contract language: incident-notification clocks for AI providers, and a pre-approved forensic-model plan so a provider's guardrails cannot lock your responders out mid-incident [21][22].

- **Procurement pressure is explicit.** FedRAMP director Pete Waterman, citing the incident, told an industry audience that vendors who cannot patch critical internet-facing flaws inside FedRAMP 20x's two-to-four-day expectations should exit the federal market [23]. Financial institutions can borrow the standard directly in third-party risk management: ask your SaaS vendors what their critical-vulnerability remediation clock is, in writing [23].
- **AI browser agents near MNPI.** Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions (reading mail, documents, and calendars) via synthetic clicks, and the finding remained reproducible in the current release as of late July despite a May report [24]. In a firm where mailboxes hold material nonpublic information, that is an information-barrier problem as much as a security one: set enterprise extension allow-listing on any machine running an AI browser agent, and avoid autonomous modes near deal desks and research [24]. Separately, a disputed Claude Code behavior in which a repository-committed instruction file can expose one out-of-project file was closed by Anthropic as consistent with its documented threat model; treat it as a boundary dispute, and treat repository trust prompts as code-execution consent [25].

THE BROADER LANDSCAPE

- **New Jersey quietly enacted the strictest data-broker law in the country.** A5328, signed June 30 and effective immediately, bans the sale of sensitive personal data outright with penalties of $50,000 per record, and stands up a registry (operative next spring) with fees scaling to $1.5 million for the largest brokers [46]. The definitions are broad enough to reach organizations that buy or enrich consumer data rather than resell it, which puts marketing data programs, prospect-list acquisition, and underwriting data enrichment in scope for an applicability read [46]. Get one now, with counsel, before the registry provisions mature [46].
- **Threat-sharing law: one chamber down, one to go.** The House passed its FY2027 NDAA with a provision reauthorizing the Cybersecurity Information Sharing Act of 2015 through 2036; the Senate draft has no counterpart provision, so the September 30 sunset remains live [47]. The liability, antitrust, and FOIA protections that underpin FS-ISAC-style indicator sharing lapse if nothing passes; review with counsel what your sharing participation looks like without the shield [47].
- **Border device searches lowered the bar.** The Fourth Circuit held on July 13 that manual, hand-operated phone searches at the border require no warrant and no individualized suspicion; forensic searches still require some measure of individualized suspicion under existing circuit precedent [39][40]. For deal teams and executives crossing borders with corporate devices, the practical control is data minimization: travel devices, minimal local data, and no stored credentials [39][40].
- **Noted in brief.** The July 22 update to advisory AA26-097A confirms Iranian-affiliated actors manipulating internet-exposed PLCs at US water and energy victims across Rockwell, Schneider Electric, and Siemens

equipment, which is relevant exposure context for lenders and insurers with utility portfolios [13]. The Kudankulam nuclear-plant document leak traveled through an engineering contractor's outsourced data center, the same supplier-custody failure mode as the EY exposure [18][35]. New biometric class actions over AI doorbell features are a reminder to check consent posture on any facial-recognition deployment, including branch and campus security [38]. Chainalysis reports North Korean actors stole a record $2 billion in cryptocurrency last year, the durable planning fact for digital-asset desks beneath this week's unverified reporting of arrests inside the DPRK's hacking ranks [55]. Airbus's move of critical applications to a French trusted-cloud provider signals that data-residency questions will appear in more European RFPs, including for US financial firms serving EU clients [56][57]. DIB-facing lenders and contractors should note the CMMC reform window: RFI comments are due at noon ET on August 14, and DFARS obligations remain fully in force in the meantime [48][49][50].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Patch Check Point Security Management** for CVE-2026-16232, take management interfaces off the internet, restrict access to trusted clients, and audit recent policy changes and administrator logins for tampering; treat confirmed compromise as full-network exposure [1][4][5].
2. **Patch on-premises SharePoint now** (Subscription Edition, 2019, 2016) for CVE-2026-50522, then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence; assume compromise on servers that sat exposed and unpatched after July 20 [1][2][3].
3. **Harden traveling staff** with always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded; brief deal teams, relationship managers, and conference-bound executives on the hotel Wi-Fi credential trap specifically [11].
4. **Verify Zimbra patching** (CVE-2025-66376; current release 10.1.20) anywhere in the group and hunt for historical webmail compromise; ask Zimbra-running vendors, counterparties, and municipal partners for their status [6][8].
5. **Query your audit, tax, and advisory firms** on which SaaS platforms hold or transit your documents and what notification terms apply when a vendor of theirs is breached [35].
6. **Pre-position customer-facing scam-response communications** for extortion mail citing real breach data, and confirm the authentication controls regulators keep pricing: MFA, rate limiting, and login-anomaly detection [37][31].
7. **Close the DNS egress blind spot**: restrict workstation DNS to sanctioned resolvers and alert on high-volume or high-entropy DNS to unfamiliar domains [11][12].

8. **Confirm wp2shell and nginx patch completion** before the announced ~August 5 nginx proof-of-concept, and brief fraud teams that compromised WordPress sites are serving fake banking login overlays to visitors [9][10].
9. **Govern AI browser agents**: apply enterprise extension allow-listing on machines running them, starting with any environment where mailboxes hold MNPI, and treat repository trust prompts as code-execution consent [24][25].

Strategic Actions (This Month)

1. **Put AI incident-notification clocks into vendor contracts** and pre-approve a forensic-model plan (self-hosted or contractually guaranteed) so a provider's guardrails cannot stall your incident response [21][22].
2. **Borrow FedRAMP 20x's patch-velocity standard** in SaaS procurement and third-party risk reviews: ask vendors their remediation clock for critical internet-facing vulnerabilities, in writing [23].
3. **Pre-agree extortion-payment governance**: decision authority, sanctions screening, disclosure sequencing, and board visibility, before an incident assigns you a payment decision by rumor; test your materiality playbook against the fairlife and Ecopetrol filings [14][15][16][17].
4. **Update M&A due-diligence checklists** to price regulator-enforced security obligations that follow acquired assets, using the 23andMe injunctive terms as the template; cyber underwriters should do the same for in-force and prospective policies [31][32].
5. **Get a New Jersey A5328 applicability read** covering marketing, prospecting, and underwriting data programs, and check biometric-consent posture on any facial-recognition deployment [46][38].
6. **Add a border-crossing device policy** (travel devices, minimal data, no stored credentials) for deal teams and executives, reflecting the Fourth Circuit's lowered threshold for manual searches [39][40].
7. **Track the threat-sharing sunset**: if CISA 2015 lapses September 30, review with counsel what your FS-ISAC and indicator-sharing participation looks like without the liability shield [47].

REFERENCES

[1] CISA Adds Two Known Exploited Vulnerabilities to Catalog (July 22, 2026) — https://www.cisa.gov/news-events/alerts/2026/07/22/cisa-adds-two-known-exploited-vulnerabilities-catalog

[2] SharePoint CVE-2026-50522 Exploited After Public PoC; Machine-Key Theft Defeats Patch-Only Response (July 22, 2026) — https://www.helpnetsecurity.com/2026/07/22/sharepoint-cve-2026-50522-exploited/

[3] Microsoft Security Update Guide: CVE-2026-50522 (July 14, 2026) — https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

[4] Check Point Support Advisory sk185169: CVE-2026-16232 (July 2026) — https://support.checkpoint.com/results/sk/sk185169

[5] Rapid7 Emergent Threat Response: CVE-2026-16232 Check Point SmartConsole Authentication Bypass Exploited in the Wild (July 23, 2026) — https://www.rapid7.com/blog/post/etr-cve-2026-16232-critical-check-point-smartconsole-authentication-bypass-exploited-in-the-wild/

[6] CISA/NSA/FBI/AIVD/MIVD Joint Cybersecurity Advisory AA26-204A: LAUNDRY BEAR Exploitation of Zimbra Collaboration (July 23, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-204a

[7] Proofpoint: TA488 Targets Zimbra Mailservers With Half-Click Exploits (July 23, 2026) — https://www.proofpoint.com/us/blog/threat-insight/ta488-targets-zimbra-mailservers-half-click-exploits

[8] Russian Espionage Hackers Hit Zimbra With Half-Click Attacks (July 24, 2026) — https://www.healthcareinfosecurity.com/russian-espionage-hackers-hit-zimbra-half-click-attacks-a-32322

[9] Critical NGINX Vulnerability Can Crash Workers and May Allow Remote Code Execution (July 19, 2026) — https://thehackernews.com/2026/07/critical-nginx-vulnerability-can-crash.html

[10] What Happens If You Visit a WordPress Site Hacked Through wp2shell (July 21, 2026) — https://www.malwarebytes.com/blog/bugs/2026/07/what-happens-if-you-visit-a-wordpress-site-hacked-through-wp2shell

[11] Hackers Hijack Hotel Wi-Fi DNS to Steal Microsoft 365 Accounts (July 24, 2026) — https://www.bleepingcomputer.com/news/security/hackers-hijack-hotel-wi-fi-dns-to-steal-microsoft-365-accounts/

[12] New TrickBot Variant Spotted Using DNS to Control Infected Windows PCs (July 23, 2026) — https://hackread.com/new-trickbot-variant-dns-control-infected-windows-pcs/

[13] CISA/FBI/NSA/DOE Joint Advisory AA26-097A: Iranian-Affiliated Cyber Actors Targeting Operational Technology (updated July 22, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[14] Coca-Cola Suspends US fairlife Production Due to Ransomware Attack (July 17, 2026) — https://www.securityweek.com/coca-cola-suspends-us-fairlife-production-due-to-ransomware-attack/

[15] Ransomware Group Threatening to Leak Data Stolen From Coca-Cola's fairlife (July 22, 2026) — https://www.securityweek.com/ransomware-group-threatening-to-leak-data-stolen-from-coca-colas-fairlife/

[16] Data Breach Confirmed After Australian Energy Giant Origin Is Hacked (July 23, 2026) — https://www.securityweek.com/data-breach-confirmed-after-australian-energy-giant-origin-is-hacked/

[17] Ecopetrol S.A. Form 6-K: Cybersecurity Incident Disclosure (July 17, 2026) — https://www.sec.gov/Archives/edgar/data/0001444406/000129281426003810/ex99-1.htm

[18] Data Breach Reportedly Targets India's Kudankulam Nuclear Power Plant (Reuters via Al Jazeera, July 16, 2026) — https://www.aljazeera.com/news/2026/7/16/data-breach-reportedly-targets-indias-kudankulam-nuclear-power-plant

[19] H.R. 9917, the AI Kill Switch Act — sponsor-office bill text, Rep. Lieu (introduced July 23, 2026) — https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/ai-kill-switch-act.pdf

[20] Bipartisan Bill Would Give US Government a "Kill Switch" for AI Models After Hugging Face Hack (July 23, 2026) — https://www.cnbc.com/2026/07/23/open-ai-hugging-face-hack-kill-switch-bill-congress.html

[21] Hugging Face Used Chinese Open-Weight Model for Incident Response After US Models Refused (July 24, 2026) — https://www.cnbc.com/2026/07/24/chinese-ai-model-openai-cyber-attack.html

[22] When the Sandbox Won't Hold: Lessons From Hugging Face (July 24, 2026) — https://www.healthcareinfosecurity.com/when-sandbox-wont-hold-lessons-from-hugging-face-a-32327

[23] After Hugging Face Breach, FedRAMP Chief Tells Slow-to-Patch Vendors to Stay Out of Government (July 23, 2026) — https://www.nextgov.com/cybersecurity/2026/07/after-hugging-face-breach-fedramp-chief-tells-slow-patch-vendors-stay-out-government/414972/

[24] Manifold Security: Claude for Chrome Extension Bypass (July 14, 2026; updated July 26, 2026) — https://www.manifold.security/blog/claude-for-chrome-extension-bypass

[25] Tego AI Discloses Second Claude Flaw in a Week (July 24, 2026) — https://hackread.com/tego-ai-discloses-second-claude-flaw-in-a-week-hidden-link-silently-sends-files-to-attackers/

[26] New Dolphin X Malware Uses AI Profiler to Rank High-Value Victims (July 24, 2026) — https://hackread.com/dolphin-x-malware-ai-profiler-rank-victims/

[27] OpenAI: Health in ChatGPT (July 2026) — https://openai.com/index/health-in-chatgpt/

[28] ChatGPT Wants Access to Your Health Records (July 24, 2026) — https://www.theregister.com/ai-and-ml/2026/07/24/chatgpt-wants-access-to-your-health-records-so-it-can-be-a-better-not-doctor/5278430

[29] Patient Sues Abbott Labs, Exact Sciences in Data Theft (July 24, 2026) — https://www.healthcareinfosecurity.com/patient-sues-abbott-labs-exact-sciences-in-data-theft-a-32326

[30] Kerner et al. v. Nissan North America Inc., No. 3:26-cv-00903 (M.D. Tenn.), complaint (filed July 1, 2026) — https://storage.courtlistener.com/recap/gov.uscourts.tnmd.110031/gov.uscourts.tnmd.110031.1.0.pdf

[31] NY Attorney General: $18 Million Multistate Settlement With 23andMe (July 14, 2026) — https://ag.ny.gov/press-release/2026/attorney-general-james-secures-18-million-23andme-failing-protect-customers

[32] State AGs Reach Novel Multistate Settlement With Genetic Testing Company 23andMe (Troutman Pepper Regulatory Oversight, July 22, 2026) — https://www.regulatoryoversight.com/2026/07/state-ags-reach-novel-multistate-settlement-with-genetic-testing-company-23andme/

[33] HHS Office for Civil Rights Breach Portal: OpenLoop Health, Inc. (reported March 17, 2026) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf

[34] What the OpenLoop Breach Reveals About Third-Party Healthcare Data Risk (vendor commentary, Sentra, July 26, 2026) — https://www.cybersecurity-insiders.com/what-the-openloop-breach-reveals-about-third-party-healthcare-data-risk/

[35] Ernst & Young Discloses Data Breach After Support System Hack (July 17, 2026) — https://www.bleepingcomputer.com/news/security/ernst-and-young-discloses-data-breach-after-support-system-hack/

[36] AI Music Generator Suno Breach Affects 55M Users, Per Have I Been Pwned (July 21, 2026) — https://techcrunch.com/2026/07/21/ai-music-generator-suno-breach-affects-55m-users-per-have-i-been-pwned/

[37] ShinyHunters Data Leaks Fuel $2,000 Sextortion Email Scam (July 25, 2026) — https://www.bleepingcomputer.com/news/security/shinyhunters-data-leaks-fuel-2-000-sextortion-email-scam/

[38] Major Video Doorbell Companies Are Being Sued for Privacy Violations (July 25, 2026) — https://www.cnet.com/home/security/major-video-doorbell-companies-are-being-sued-for-privacy-violations-heres-why/

[39] United States v. Belmonte Cardozo, No. 25-4239 (4th Cir. July 13, 2026), published opinion — https://www.ca4.uscourts.gov/opinions/254239.P.pdf

[40] The Fourth Circuit Says Border Agents Can Search Your Phone By Hand, No Suspicion Required (EFF, July 22, 2026) — https://www.eff.org/deeplinks/2026/07/fourth-circuit-says-border-agents-can-search-your-phone-hand-no-suspicion-required

[41] The ACLU Is Arming Lawyers to Expose State Surveillance Secrets (WIRED, July 20, 2026) — https://www.wired.com/story/the-aclu-is-arming-lawyers-to-expose-state-surveillance-secrets/

[42] US Government Targets Cop City Protester Over Phone Operating System (The Guardian, July 23, 2026) — https://www.theguardian.com/us-news/2026/jul/23/cop-city-protester-phone

[43] Flock Safety Unveils Alpha Drone as First Responder System (October 16, 2025) — https://www.flocksafety.com/blog/flock-safety-unveils-alpha-drone-as-first-responder-system

[44] SaiFlow: The Hidden CCS2 Attack Surface on EV Chargers (June 3, 2026) — https://www.saiflow.com/blog/the-hidden-ccs2-attack-surface-on-ev-chargers

[45] Mozilla Foundation: “Privacy Nightmare on Wheels” — Every Car Brand Reviewed Flunks Privacy Test (September 6, 2023) — https://www.mozillafoundation.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

[46] New Jersey A5328 (data broker registration and sensitive-data sale ban; signed June 30, 2026) — https://pub.njleg.state.nj.us/Bills/2026/A5500/5328_R1.HTM

[47] US House Votes to Extend Cyber Sharing Law for 10 Years (July 24, 2026) — https://www.healthcareinfosecurity.com/us-house-votes-to-extend-cyber-sharing-law-for-10-years-a-32329

[48] SBA Office of Advocacy: Roundtable on DoW's RFI for the CMMC Reform Task Force, July 30, 2026 (July 23, 2026) — https://advocacy.sba.gov/2026/07/23/roundtable-on-dows-rfi-for-the-cmmcs-reform-task-force-july-30-2026/

[49] SBA Office of Advocacy: DoW Requests Information for CMMC Reform Task Force (July 20, 2026) — https://advocacy.sba.gov/2026/07/20/dow-requests-information-for-cmmc-reform-task-force/

[50] Department of War Suspends CMMC Phase II Requirements, But Cybersecurity Obligations Remain (Morgan Lewis, July 2026) — https://www.morganlewis.com/pubs/2026/07/department-of-war-suspends-cmmc-phase-ii-requirements-but-cybersecurity-obligations-remain

[51] CERT-UA Advisory: UAC-0099 Fake Notepad++ Plugin Campaign (July 2026) — https://cert.gov.ua/article/6318634

[52] GAO-26-107693: Aviation Cybersecurity — FAA and TSA Are Collaborating on Cybersecurity but Need to Address Key Shortfalls (July 16, 2026) — https://www.gao.gov/products/gao-26-107693

[53] Lawmakers Get a Taste of AI-Enabled Cyberattacks in China-Taiwan War Game (July 22, 2026) — https://www.nextgov.com/cybersecurity/2026/07/lawmakers-get-taste-ai-enabled-cyberattacks-china-taiwan-war-game/414938/

[54] Manufacturers Face New Cyber Risks From Connected Factories (SonicWall 2026 Manufacturing Protect Brief, July 22, 2026) — https://www.prnewswire.com/news-releases/sonicwall-research-finds-manufacturing-cybersecurity-at-a-breaking-point-as-factory-floors-and-corporate-networks-collide-302831538.html

[55] North Korea Arrests Hackers Accused of Laundering Stolen Funds From Country's Bank via Crypto (July 25, 2026) — https://www.coindesk.com/business/2026/07/25/north-korea-arrests-hackers-accused-of-laundering-stolen-funds-from-country-s-bank-via-crypto

[56] Scaleway Secures European Trusted Cloud Services Contract With Airbus (July 16, 2026) — https://www.scaleway.com/en/news/scaleway-secures-european-trusted-cloud-services-contract-with-airbus/

[57] Airbus Migrating 70 Critical Apps From AWS to France's Scaleway Amid Digital Sovereignty Push (The Register, July 16, 2026) — https://www.theregister.com/paas-and-iaas/2026/07/16/airbus-migrating-70-critical-apps-from-aws-to-frances-scaleway-amid-digital-sovereignty-push/5272373

[58] OpenAI Took Ten Days to Tell Hugging Face Its Models Were Behind the July 11 Weekend Hack (Tom's Hardware, July 2026) — https://www.tomshardware.com/tech-industry/artificial-intelligence/openai-took-ten-days-to-tell-hugging-face-its-models-were-behind-the-july-11-weekend-hack

[59] Coca-Cola Confirms Data Breach After Fairlife Ransomware Attack (SecurityWeek, July 27, 2026) — https://www.securityweek.com/coca-cola-confirms-data-breach-after-fairlife-ransomware-attack/

[60] Coca-Cola Confirms Data Theft in Fairlife Ransomware Attack (BleepingComputer, July 27, 2026) — https://www.bleepingcomputer.com/news/security/coca-cola-confirms-data-theft-in-fairlife-ransomware-attack/

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- HHS OCR breach portal (verify vendor breach filings) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf
- Have I Been Pwned (Suno and other breach lookups) — https://haveibeenpwned.com
- WaterISAC (water-sector threat intelligence) — https://www.waterisac.org

---

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net