RISK BRIEFING — TWO PATCH-NOW EMERGENCIES, RUSSIAN WEBMAIL ESPIONAGE, AND WASHINGTON REACHES FOR AN AI KILL SWITCH

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

EXECUTIVE SUMMARY

Two vulnerabilities crossed into confirmed active exploitation this week, one of them into mass exploitation, and both belong at the top of every patch queue: a remote-code-execution flaw in on-premises Microsoft SharePoint (CVE-2026-50522) and an authentication bypass in Check Point's Security Management platform (CVE-2026-16232). CISA added both to the Known Exploited Vulnerabilities catalog on July 22 and gave federal agencies just three days to remediate, an unusually short window that signals how seriously the government is treating them [1]. For SharePoint, patching alone is not enough: researchers report attackers stealing IIS machine keys that let them return after the patch, so key rotation and compromise hunting must follow [2]. Meanwhile, a joint advisory sealed by 27 agencies across 16 countries detailed a year-long Russian espionage campaign ("Laundry Bear") that compromised Zimbra webmail at government, defense, and energy organizations through an email that executes on viewing, and Proofpoint reports the same actor reaching for targets it describes as "nuclear installations" and "high science" [6][7]. In Washington, the Hugging Face incident produced its first legislation: the bipartisan AI Kill Switch Act (H.R. 9917) would give the federal government authority to order AI model shutdowns during defined loss-of-control incidents [19][20]. The week also brought a steady drumbeat of accountability news, including an $18 million, 42-attorney-general settlement with 23andMe whose security obligations survived bankruptcy and now bind the buyer, and new class actions against Abbott Laboratories and Nissan over vendor-linked data theft [29][30][31][32]. Ransomware kept its grip on operations: Coca-Cola told regulators an attack forced it to suspend US production at its fairlife dairy subsidiary, has since confirmed data was taken, and has now restored a majority of production; the attackers' publication deadline passed Monday morning, and the stolen data has since been posted for download on the group's leak site [14][15][59][60]. Patch the two criticals first; then work the espionage-hardening and governance items below.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	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]
2	Patch Check Point Security Management (CVE-2026-16232), restrict management-plane access, and audit recent policy changes	Actively exploited zero-day grants unauthenticated full admin over the firewall management server [1][4][5]
3	Confirm Zimbra is patched for CVE-2025-66376 and current (10.1.20); hunt webmail for compromise	Joint advisory AA26-204A details active Russian espionage against Zimbra; exploit triggers on viewing an email [6][8]
4	Pull internet-exposed PLCs behind secure gateways and apply the July 22 detection guidance in AA26-097A	Iranian-affiliated actors are manipulating Rockwell, Schneider Electric, and Siemens PLCs at US water and energy victims [13]
5	Require full-tunnel VPN for traveling staff on hotel or conference Wi-Fi; disable Microsoft Entra device-code flow where not needed, 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, including an MFA-bypassing device-code lure [11]; manual phone searches at the border now require no suspicion in the Fourth Circuit [39][40]
6	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]
7	Verify WordPress (wp2shell) and nginx (CVE-2026-42533) patch completion now	A researcher-announced nginx proof-of-concept is expected ~August 5; wp2shell exploitation continues at internet scale [9][10]
8	Set enterprise browser-extension policy for any machine running an AI browser agent; treat repository trust prompts as code-execution consent	Unpatched research shows co-installed extensions can hijack Claude for Chrome's agent actions; a disputed Claude Code behavior can expose out-of-project files [24] [25]

Priority	Action	Why Now
9	Pre-position breach-communication and help-desk scripts for extortion mail citing real breach data; confirm MFA, rate limiting, and login-anomaly monitoring	Scammers are mass-mailing $2,000 sextortion demands built on genuine leaked data; regulators priced missing controls at $18M in the 23andMe settlement [37][31]
10	DIB contractors: submit CMMC reform RFI comments by 12:00 pm ET August 14; keep 800-171 controls and SPRS scores current	The reform window is open and obligations under DFARS 252.204-7012 remain fully in force [48][49][50]

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 [47].
- **CMMC reform now has hard dates.** An SBA Advocacy roundtable is set for July 30 and RFI comments are due August 14 [48][49].
- **The Iranian PLC advisory expanded.** The July 22 update to AA26-097A adds Schneider Electric and Siemens equipment to the previously Rockwell-focused guidance and ships new detection content [13].
- **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 JadePuffer agentic-ransomware research we covered last week saw no material new development.

PATCH NOW: TWO KEV-LISTED EMERGENCIES

- **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]. (Note one inconsistency worth knowing: Microsoft's advisory carries an unauthenticated attack vector while its own FAQ describes an attacker authenticated as at least a Site Owner, so treat the access precondition as unsettled and patch regardless [3].) The exploitation detail that matters most: watchTowr reports attackers stealing IIS machine keys to retain long-term access, which lets them forge valid authentication tokens and walk back in after you patch [2]. CISA's guidance for this SharePoint wave is to hunt and remediate first, then rotate machine keys, since rotating keys on a box an attacker still holds accomplishes little [1][2]. It is one of several SharePoint flaws exploited in this month's wave, with both espionage and ransomware actors using the same entry points [2].

- **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]. Treat any confirmed compromise as a potential full-network exposure event: audit recent policy changes and administrator activity, and get management interfaces off the open internet.
- **Patch-status watchlist.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites are being used to attack their visitors with fake Microsoft 365 and banking login overlays, so the exposure extends to organizations that run no WordPress at all [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.

ESPIONAGE TARGETS THE MAIL YOU READ AND THE NETWORKS YOU TRUST

- **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) [6]. The advisory describes a view-based exploit delivered by phishing email: opening or previewing the message is enough, with no attachment or link click required. Named target sectors include the defense industrial base, federal and local government, education, energy, law enforcement, media, NGOs, and technology [6]. Proofpoint, which coined the "half-click" label, additionally reports targeting of what it calls "nuclear installations" and "high science" [7]. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [8]. An alleged group member was extradited from Thailand and is facing charges in Boston federal court [8]. If you run Zimbra, patch and upgrade (10.1.20 shipped July 20 with nine additional critical fixes) and hunt for historical compromise; if your vendors or local-government partners run it, ask them the same question [8].

- **Hotel Wi-Fi as a credential trap.** 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; in some cases the attackers used a device-code sign-in flow that captures a legitimate OAuth session and bypasses MFA outright [11]. 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].
- **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 to TrickBot 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].
- **A commodity-phishing note for Ukraine-facing organizations.** CERT-UA warns that UAC-0099 is delivering its MATCHBOIL.V2 loader through a counterfeit Notepad++ plugin, reached via phishing mail and a file-sharing service [51]. Organizations with Ukrainian operations or partners should fold the indicators into their monitoring [51].

OPERATIONAL TECHNOLOGY AND PRODUCTION UNDER PRESSURE

- **The Iranian PLC campaign widened.** The July 22 update to joint advisory AA26-097A (FBI, CISA, NSA, EPA, the Department of Energy, Cyber National Mission Force, and Treasury) confirms that Iranian-affiliated actors who have been manipulating internet-exposed programmable logic controllers at US water, energy, and government-services victims since at least March are now observed on Schneider Electric and Siemens equipment in addition to Rockwell [13]. The actors exfiltrate PLC project files, alter or delete control logic, manipulate operator displays, and in at least one FBI-observed case installed a malicious project file that preserved normal downstream function while overriding safe-operating parameters [13]. The advisory attributes the activity to an unnamed Iranian-affiliated APT group. The update also ships concrete detection guidance for malicious project-file changes. If any controller in your estate is reachable from the internet, treat yourself as in scope regardless of vendor [13].
- **Ransomware halted milk production.** Coca-Cola told regulators on July 16 that a ransomware attack forced it to temporarily suspend US production at fairlife, its dairy subsidiary, after attackers reached production-related systems [14]. The Anubis ransomware group listed fairlife on its leak site July 20, claiming roughly 1 TB of stolen data and setting a publication deadline of Monday, July 27; the volume figure remains an attacker claim [15]. Two developments as of Monday morning: Coca-Cola has now confirmed that the incident involved "the taking of certain data," without specifying data types or how many people are affected, and a majority of production has resumed across the four US fairlife facilities,

with product availability largely unaffected thanks to existing inventory [59]. The publication deadline passed Monday morning, and Anubis has since posted the stolen data for download on its leak site [60]. The operational lesson is familiar and keeps being re-learned: a production outage does not require OT compromise when production depends on IT systems.

- **Energy-sector breach cluster.** 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]. Colombia's Ecopetrol disclosed unauthorized access to cloud file storage across roughly 15 subsidiaries in an SEC filing [17]. Utility customer-data estates remain a soft, monetizable target distinct from grid OT.
- **Nuclear design data lost through a supplier's data center.** In mid-July, the World Leaks extortion group published roughly 19,000 files (14.3 GB) taken from India's Reliance Group via a third-party-hosted server, purportedly including ventilation and cooling blueprints and a control-room floor layout for two under-construction units at the Kudankulam nuclear plant [18]. The plant operator says the material involves only conventional common-service facilities, and the files' authenticity has not been independently verified [18]. The failure mode deserves attention anyway: facility design data left the owner's control through an engineering contractor's outsourced hosting, and the extortionists priced the criticality of the end client rather than the breached party.

THE AI INCIDENT'S SECOND WEEK: REGULATION ARRIVES

- **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, issued through DHS with Commerce and DNI involvement during defined loss-of-control scenarios. Civil penalties scale to $20 million per day [19]. It is one chamber's freshly introduced bill, and passage is far from assured, but it is the clearest signal yet that AI incident reporting and shutdown capability are headed toward regulatory expectations. Boards should expect "could we shut it down, and who orders it?" to become a standard governance question.
- **What the sandbox escape is teaching defenders.** Post-incident analysis of the OpenAI/Hugging Face event has converged on a practical point: model-level safeguards are not a security boundary. Effective controls live outside the model, in network rules, scoped credentials, destination allow lists, DNS filtering, and outbound data-loss prevention; a test environment should hold no credentials usable against production [22]. Reporting this week also surfaced two governance wrinkles: Hugging Face says commercial frontier-model APIs refused to analyze the attack artifacts during incident response, forcing a fallback to a self-hosted Chinese open-weight model [21], and a published claim (single-outlet, so far unconfirmed) alleges OpenAI took roughly ten days to tell Hugging Face its models were responsible

[58]. Both belong in your vendor conversations: contractual incident-notification clocks for AI providers, and a pre-approved forensic-model plan so 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]. Commercial buyers can borrow the standard: ask your SaaS vendors what their critical-vulnerability clock is.
- **The AI agent attack surface keeps growing.** 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 that the finding was still reproducible in the July 7 release (v1.0.80) after a May report, with a July 26 follow-up confirming it remains unpatched [24]. Separately, Tego AI published a disputed Claude Code behavior in which a repository-committed instruction file can expose one out-of-project file; Anthropic closed the report as consistent with its documented threat model, so treat this as a boundary dispute rather than a patched-or-unpatched vulnerability, and treat "trust this folder" prompts as code-execution consent [25]. On the criminal side, Varonis documented "Dolphin X," a for-sale Windows stealer advertising an AI-based victim-ranking profiler; most capability claims come from the seller's own advertisement and executions have not been confirmed in the wild, but the direction (automated triage of thousands of infections to find the valuable ones) is credible and raises the stakes of any single infected developer endpoint [26].
- **Health data flows to a consumer chatbot.** OpenAI launched Health in ChatGPT this week for US adult users, connecting Apple Health and records from participating providers, with stated commitments against training on the data and a 30-day deletion policy [27]. The launch came one day after a lawsuit alleging harmful ChatGPT medical advice, and the announcement makes no HIPAA claim [28]. For employers and healthcare organizations, the immediate question is policy: employees and patients will connect regulated-class data to a consumer app outside covered channels, and your acceptable-use and patient-communication guidance should say something about it [27][28].

THE BILL COMES DUE: BREACH LITIGATION AND ENFORCEMENT

- **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]. The notable feature is 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. Acquirers should read that as a due-diligence instruction [31][32].
- **Vendor-breach class actions multiplied.** An Exact Sciences patient filed a proposed class action against Abbott Laboratories and Exact Sciences over the ShinyHunters-claimed theft in the cancer-diagnostics business, while Abbott separately investigates a second actor's claims; no verified record

counts exist yet [29]. Former Nissan employees filed Kerner v. Nissan North America over employee data (Social Security numbers, banking details) exposed when attackers hit Oracle PeopleSoft HR systems; the complaint attributes the theft to ShinyHunters and alleges a 29-day gap between breach and notice for a class of at least 20,648 [30]. Note the pattern in both: plaintiffs are suing the customer of the breached platform, and the notification clock is part of the claim.

- **Third-party and fourth-party healthcare exposure.** The OpenLoop Health breach (716,000 individuals per the HHS breach portal, reported in March) is drawing renewed analysis this week as a case study in backend telehealth-platform concentration: most affected patients never chose or heard of the vendor holding their data [33][34]. Ernst & Young separately notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, a reminder that your professional-services firms have their own vendors [35].
- **The long tail of leaked data.** A mass sextortion campaign is impersonating the ShinyHunters group and demanding $2,000 in Bitcoin, using genuinely leaked breach data (Amtrak, Hallmark, Substack, Betterment, and others) to look credible; there is no actual device compromise behind the claims [37]. If your organization has appeared in a public leak, expect your customers and employees to receive convincing scam mail that cites it, and pre-position a plain-language response the way Betterment did [37]. Relatedly, the Suno AI music 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].
- **Biometrics at the front door.** Three new proposed class actions target Amazon Ring and Google Nest over AI "familiar face" doorbell features, alleging faceprints of non-consenting passersby, under Virginia and California law (notably, no Illinois BIPA claim; the features are already disabled in Illinois, Texas, and Portland) [38]. With Google's $1.4 billion Texas biometric settlement in 2025 as backdrop, any organization deploying facial recognition on premises should check consent posture now [38].

THE BROADER LANDSCAPE

- **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 and floor opposition exists, so the September 30 sunset remains live; the liability, antitrust, and FOIA protections that underpin ISAC-style sharing lapse if nothing passes [47].
- **CMMC reform: the comment window is real.** The Phase 2 suspension continues, and the reform process now has actionable dates: an SBA Advocacy small-business roundtable July 30 and RFI comments due at noon ET on August 14 [48][49]. The legal analyses published this week agree on the operative point: DFARS 252.204-7012, NIST 800-171 self-assessments, SPRS scores, and annual affirmations remain binding, with False Claims Act exposure attached [50]. Use the pause to fix gaps, and use the RFI to be heard.
- **Aviation cyber governance, graded.** GAO's new aviation-cybersecurity report (GAO-26-107693) finds the FAA has defined cyber roles while TSA has not, and that TSA's cyber roadmap dates to 2018; both

departments agreed with all five recommendations [52]. Worth noting precisely: GAO reports there have been no reports of successful cyberattacks on avionics, so the demonstrated risk concentrates in ground systems and governance, and vendor commentary claiming otherwise is ahead of the evidence [52].

- **Manufacturing telemetry: quieter, still enormous.** SonicWall's new manufacturing brief reports sector intrusion-prevention events down 56.2% year over year yet still totaling 474 million in the first half of 2026, with attacks shifting toward IoT and SCADA entry points; more than half of monitored manufacturing networks saw IoT exploitation attempts, and a single 2021 Hikvision camera flaw drew 43 million hits [54]. The numbers are one vendor's telemetry, skewed toward smaller networks, but the direction matches what we see in the field: the perimeter noise is falling while the soft spots move to connected devices [54].
- **Congress war-gamed AI-enabled infrastructure attacks.** Members of two House committees ran a first-of-its-kind closed-door exercise simulating AI-enabled cyberattacks against US ports, rail, and airports in a 2027 Taiwan-crisis scenario [53]. Expect transportation and logistics cyber mandates to follow congressional attention; the scenario also makes a ready-made tabletop for your own exercise calendar [53].
- **Reported (and unverified) turbulence in DPRK cyber ranks.** A Daily NK report, resting on a single anonymous source and explicitly unverified, describes North Korean authorities arresting former military hackers for allegedly stealing from the regime's own banks and laundering through crypto [55]. Treat the arrest story as unconfirmed color. The durable planning fact sits in the context around it: DPRK-linked crypto theft runs at a scale Chainalysis put at roughly $2 billion last year, as cited in the same reporting, and that revenue engine is unaffected by whatever happened in Pyongyang this month [55].
- **Digital sovereignty moved from talk to contract.** Airbus selected France's Scaleway to host critical applications under a European trusted-cloud contract; its digital chief says the migration starts with 70 AWS-hosted applications against a multi-year target of about 900, with some workloads staying on AWS [56][57]. Cloud concentration and jurisdictional exposure are now board-level resilience variables in Europe, and US firms serving European customers should expect data-residency questions in more RFPs [57].

Surveillance & Privacy

- **Border phone searches: manual is now "routine" in the Fourth Circuit.** In U.S. v. Belmonte Cardozo (decided July 13), the Fourth Circuit held that manual, hand-operated searches of phones 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]. The published opinion binds Maryland, the Carolinas, Virginia, and West Virginia. For organizations whose staff cross borders with corporate devices, the practical control is data minimization: travel devices, minimal local data, and no stored credentials, because the legal threshold protecting a device at the border keeps dropping [39][40].
- **Litigation is becoming the surveillance-transparency mechanism.** The ACLU of Massachusetts released an attorney-only library of pre-drafted discovery and preservation motions designed to force disclosure of surveillance-tool use in criminal cases, including preservation demands aimed directly at

private vendors whose products auto-delete data on short cycles [41]. Any company selling surveillance-adjacent technology, and any agency customer, should expect legal-hold demands earlier and more often, and should verify their retention and preservation workflows can respond [41].

- **A phone's operating system as evidence.** Federal prosecutors are pursuing a novel theory against an Atlanta protester whose GrapheneOS phone wiped itself during a border-adjacent interrogation, treating the wipe as destruction of property subject to seizure; a suppression ruling is expected in the fall [42]. Whatever the outcome, it is a live test of whether privacy tooling itself can be framed as culpable conduct, and it belongs on the radar of anyone issuing hardened devices [42].
- **Police drones, at scale rather than at launch.** Coverage recirculated Flock Safety's autonomous "Alpha" drone this week; the product actually launched in October 2025, and the current story is scale, with Flock's technology now reportedly serving on the order of a thousand agencies while civil-liberties groups press on retention and oversight [43]. The vendor's performance figures (60 MPH, plate reads from 2,000 feet) are its own claims [43].
- **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]. Any organization that buys, sells, or enriches consumer data should get a New Jersey applicability read now, because the definitions are broad [46].
- **Connected vehicles, revisited with fresh evidence.** Vendor research published in June showed a production EV fast charger exposing root-credentialed remote access through the charging cable itself, using about $130 in hardware; the finding covers one vendor's model and requires physical access, so resist industry-wide generalization [44]. It lands against a standing baseline: Mozilla's 2023 review found all 25 car brands it examined failed its minimum privacy standards, a snapshot that is now three years old but has never been retracted or superseded [45]. Fleet operators should treat vehicles and charging infrastructure as networked endpoints with vendor-management requirements to match [44][45].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **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].
2. **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 admin logins for tampering [1][4][5].

3. **Verify Zimbra patching** (CVE-2025-66376; current release 10.1.20) and hunt for historical webmail compromise going back a year; ask Zimbra-running vendors and government partners for their status [6] [8].
4. **Act on AA26-097A's July 22 update**: inventory internet-reachable PLCs across Rockwell, Schneider Electric, and Siemens estates, pull them behind secure gateways, and run the advisory's new project-file detection guidance [13].
5. **Harden traveling staff** with always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded; brief frequent travelers on hotel Wi-Fi credential traps [11].
6. **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].
7. **Confirm wp2shell and nginx patch completion** before the announced ~August 5 nginx proof-of-concept; verify auto-updates actually applied [9][10].
8. **Govern AI browser agents**: apply enterprise extension allow-listing on machines running them, avoid autonomous modes, and instruct developers to treat repository trust prompts as code-execution consent [24][25].
9. **Pre-position 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].

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: ask vendors their remediation clock for critical internet-facing vulnerabilities, in writing [23].
3. **DIB contractors: work the CMMC reform window** — attend or follow the July 30 SBA roundtable, file RFI comments by noon ET August 14, and keep 800-171, SPRS, and affirmation posture current in the meantime [48][49][50].
4. **Review supplier data custody for design and facility documents**: the Kudankulam leak traveled through a contractor's outsourced data center, and the EY exposure through an IT-support SaaS; map where your crown-jewel documents sit in other people's clouds [18][35].
5. **Get a New Jersey A5328 applicability read** if you buy, sell, or broker consumer data, 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) 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 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