RISK BRIEFING, HEALTHCARE EDITION: THE VENDOR HOLDING YOUR PATIENTS' DATA, TWO PATCH-NOW EMERGENCIES, AND PHI IN CONSUMER AI

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: Hospitals, health systems, medical-device manufacturers, and payers
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

The theme of this week's healthcare picture is concentration: patient data pooling in vendors most patients never chose. 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 risk, and one analyst estimate puts the affected client base at roughly 120 organizations [33][34]. A patient has sued Abbott Laboratories and Exact Sciences over data theft in a cancer-diagnostics unit, part of a widening pattern of plaintiffs suing the customer of the breached platform and putting the notification clock itself at issue [29]. Ernst & Young's exposure through a third-party IT support-ticket system completes the lesson: your business associates have business associates, and your revenue-cycle, telehealth, and patient-communication stacks inherit all of them [35]. Before any of that strategic work, two vulnerabilities in confirmed mass exploitation belong at the top of every hospital IT 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 with a three-day federal remediation window [1]. For SharePoint, patching alone does not finish the job, because attackers are stealing IIS machine keys that let them return afterward [2]. A advisory sealed by 27 agencies across 16 countries also documented a year-long Russian espionage campaign against Zimbra webmail, and Proofpoint reports the same actor targeting what it calls "high science", which health systems with research arms and university affiliations should read as directed at them [6][7]. Finally, OpenAI launched Health in ChatGPT, inviting patients to connect medical records to a consumer app outside covered channels; the announcement makes no HIPAA claim, and it arrived one day after a lawsuit alleging harmful ChatGPT medical advice [27][28]. Patch the two criticals first; then start the business-associate mapping and the consumer-AI policy work 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, especially in research and academic-affiliate environments	Joint advisory AA26-204A details active Russian espionage against Zimbra; the exploit triggers on viewing an email [6][7][8]
4	Launch or refresh your business-associate inventory: who holds PHI, under what BAA, with what breach-notification clock	OpenLoop shows a single backend vendor concentrating 716,000 patients' data across an analyst-estimated ~120 client organizations [33][34]
5	Issue workforce acceptable-use guidance on PHI in consumer AI tools and draft patient-facing guidance on Health in ChatGPT	Patients and staff will connect regulated-class data to a consumer app outside covered channels; the announcement makes no HIPAA claim [27][28]
6	Pre-position helpdesk and patient-relations 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 authentication controls at $18M in the 23andMe settlement [37][31]
7	Require full-tunnel VPN for traveling clinicians and executives 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]
8	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]

Priority	Action	Why Now
9	Set enterprise browser-extension policy for any machine running an AI browser agent, starting with mailboxes and workstations that touch PHI	Unpatched research shows co-installed extensions can hijack Claude for Chrome's agent actions, including reading mail and documents [24][25]
10	If you are on either side of a healthcare M&A transaction, put breach history and security obligations into diligence	The 23andMe settlement's security obligations survived bankruptcy and now bind the acquirer [31][32]

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; both platforms are widely deployed, and hospital IT estates should check for them [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; the advisory's named sectors include education, and Proofpoint separately reports "high science" targeting [6][7].
- **Vendor-breach litigation reached the diagnostics supply chain.** A proposed class action against Abbott Laboratories and Exact Sciences was filed this week over the ShinyHunters-claimed theft; no verified record counts exist [29].
- **OpenLoop analysis renewed.** Fresh commentary published July 26 frames the March-reported OpenLoop breach as the sector's clearest third-party concentration case study [34].
- **Health in ChatGPT launched.** OpenAI's consumer health-record connection went live this week for US adults, one day after a lawsuit alleging harmful ChatGPT medical advice [27][28].
- **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 with a provision extending the threat-sharing law through 2036; the Senate has no matching provision, so the September 30 sunset that underpins Health-ISAC-style sharing protections still stands [47].
- **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].

PATCH NOW: TWO KEV-LISTED EMERGENCIES IN HOSPITAL IT

- **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]. Many health systems still run on-prem SharePoint for policy libraries, committee workflows, and clinical-document collaboration, and those farms often sit behind years of deferred upgrades. Microsoft patched the flaw July 14; a public exploit landed July 20 and mass exploitation followed within hours [2]. The 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 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].
- **Check Point Security Management CVE-2026-16232 (CVSS 9.1).** An improper-authentication flaw lets an unauthenticated attacker obtain a token and authenticate with full administrative rights over the Security Management Server, which means the ability to rewrite firewall policy for everything the platform manages, including segmentation between clinical networks and the enterprise LAN [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 attacking their visitors with fake Microsoft 365 and banking login overlays, so hospital marketing sites and foundation microsites are both a target and a hazard [10]. nginx CVE-2026-42533 remains unexploited in public, but a researcher says he will publish proof-of-concept details around August 5; close out patch verification on patient-portal and API front ends before that date [9].

THE LEAD THEME: BUSINESS-ASSOCIATE CONCENTRATION

- **OpenLoop, and the vendor your patients never chose.** The OpenLoop Health breach, reported to the HHS breach portal in March at 716,000 individuals, is drawing renewed analysis this week as a case study in backend telehealth-platform concentration [33][34]. OpenLoop is white-label infrastructure: it powers telehealth services that patients experience under other brands, which means most affected individuals never chose or heard of the vendor holding their data [34]. One analyst estimate, attributed to commentary rather than HHS data, puts the affected client base at roughly 120 organizations [34]. For a hospital, health system, or payer, the planning question is direct: which of your patient-facing services

run on a backend platform like this, and would you learn of its breach from the vendor or from the HHS portal?

- **Litigation lands on the platform's customer.** An Exact Sciences patient filed a proposed class action against Abbott Laboratories over the ShinyHunters-claimed theft in its cancer-diagnostics unit, while Abbott separately investigates a second actor's claims; no verified record counts exist yet, and none should be repeated until they do [29]. Former Nissan employees filed suit over employee data exposed when attackers hit Oracle-hosted PeopleSoft HR systems, alleging a 29-day gap between breach and notice [30]. The pattern holds across sectors: plaintiffs sue the organization whose name is on the relationship, and the notification timeline is part of the claim. In HIPAA terms, that is an argument for tightening the breach-notification clocks in your BAAs well below the regulatory ceiling, so the vendor's delay does not become your litigation exposure.
- **Your professional-services firms have their own vendors.** Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform [35]. Translate that to a health-system vendor stack: the revenue-cycle firm, the patient-communication platform, and the telehealth backend each run their own ITSM, ticketing, and file-transfer tools, and PHI pasted into a support ticket inherits that fourth-party exposure. Concentration mapping should extend one tier past the entities you hold BAAs with.
- **The action set.** Rebuild the business-associate inventory against reality rather than the contract file; map which vendors concentrate data across multiple service lines; verify each BAA's breach-notification clock and audit rights; and add the HHS breach portal to your vendor-monitoring routine so a business associate's filing does not surprise you months late [33][34][35].

PHI MEETS CONSUMER AI

- **Health in ChatGPT.** OpenAI launched Health in ChatGPT this week for US adult users, connecting Apple Health data and records from participating providers, with stated commitments against training on the data and a 30-day deletion policy [27]. The announcement makes no HIPAA claim, and the launch came one day after a lawsuit alleging harmful ChatGPT medical advice; those allegations are unresolved [27] [28]. The practical consequence for covered entities is that patients will connect regulated-class data to a consumer app outside covered channels, and clinicians will field questions about it. Two deliverables follow. First, patient-communication guidance: a plain-language position your portal, front desk, and clinicians can give when patients ask whether to connect their records. Second, a workforce acceptable-use policy that addresses PHI in consumer AI tools explicitly, covering both pasting patient information into chatbots and connecting personal health accounts on work devices [27][28].
- **AI agents where the mailboxes hold PHI.** Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions, including reading mail, documents, and calendars, and that the finding remained reproducible as of late July despite a May report [24]. In a healthcare environment, the mailboxes and documents an agent can read are frequently PHI, so extension allow-listing on any machine running an AI browser agent is a HIPAA safeguard rather than an IT

preference. Separately, a disputed Claude Code behavior can expose one out-of-project file; Anthropic closed the report as consistent with its documented threat model, so treat repository trust prompts as code-execution consent [25].

- **Governance signals worth a board minute.** H.R. 9917, the AI Kill Switch Act, introduced July 23, would require large AI developers to maintain shutdown capability and report qualifying incidents within 15 days; it is one chamber's freshly introduced bill, but "could we shut it down, and who orders it?" is becoming a standard governance question that health-system AI committees should be able to answer for their own deployments [19][20]. Post-incident analysis of the Hugging Face event carries a lesson for clinical-AI pilots: model-level safeguards are not a security boundary, and effective controls live outside the model in network rules, scoped credentials, and outbound data-loss prevention [22]. Put AI incident-notification clocks into vendor contracts now, and borrow the FedRAMP 20x patch-velocity standard when buying health IT SaaS: ask vendors their remediation clock for critical internet-facing flaws, in writing [21][22][23].

ESPIONAGE AND CREDENTIAL THEFT

- **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]. Opening or previewing the phishing message is enough; no attachment or link click is required [6]. The advisory's named sectors include education, government, and technology, and Proofpoint additionally reports targeting of what it calls "nuclear installations" and "high science" [6][7]. Health systems with research arms, academic medical centers, and university affiliations should read that language as pointing at them: grant-funded research, clinical-trial data, and federated academic identity systems fit the actor's collection interests. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [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 academic affiliates or local-government partners run it, ask them the same question [8].
- **Hotel Wi-Fi as a credential trap.** ReliaQuest reports an ongoing campaign 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]. Traveling clinicians, conference-bound researchers, and executives are exactly the population exposed, and a captured session can reach mailboxes full of patient information. 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 Windows backdoor running command-and-control entirely over DNS queries routed through a public resolver [12]. The attribution rests on one vendor's

code-similarity analysis and the campaign's scale is unquantified, but the defensive lesson stands: an egress policy that inspects HTTP while letting workstations talk DNS to arbitrary external resolvers has a blind spot, and in a hospital that blind spot extends to biomedical-device VLANs. Pair this with the hotel-gateway campaign above and DNS control earns a place on this quarter's hardening list [11][12].

THE BILL COMES DUE: ENFORCEMENT, SETTLEMENTS, AND THE LONG TAIL

- **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 healthcare. First, regulators priced the missing controls: MFA, rate limiting, and login-anomaly detection are what $18 million bought in hindsight, and genetic data drew the multistate coalition that ordinary consumer data might not have [31]. Second, durability: the injunctive terms, including an enhanced security program, independent oversight, and preserved consumer deletion rights, bind TTAM, the entity that bought the company out of bankruptcy [32]. Security obligations followed the assets. Any health entity in M&A, on either side, should read that as a due-diligence instruction: breach liabilities and consent-order obligations now travel with the deal [31][32].
- **The long tail of leaked data reaches your patients and staff.** A mass sextortion campaign is impersonating the ShinyHunters group and demanding $2,000 in Bitcoin, using genuinely leaked breach data from past incidents to look credible; there is no actual device compromise behind the claims [37]. Patients and employees who appeared in any public leak, including healthcare breaches, should expect convincing scam mail that cites real personal details. Pre-position two canned responses: a helpdesk script for employees who receive the mail, and a patient-relations script for patients who call asking whether the hospital was breached again. A plain-language public statement, prepared before the calls start, keeps a commodity scam from becoming a reputational incident [37].
- **Biometrics and consent, briefly.** New class actions over AI "familiar face" doorbell features are a reminder that facial-recognition deployments draw consent-based litigation; any hospital using facial recognition for facility access should check its consent posture [38].

CONNECTED DEVICES AND THE BROADER LANDSCAPE

- **Camera and connected-device estates need their own patch program.** SonicWall's new manufacturing telemetry reports attacks shifting toward IoT entry points, with a single 2021 Hikvision camera flaw drawing 43 million exploitation hits in the first half of 2026 [54]. Those figures are one vendor's telemetry and skew toward smaller networks, but the direction translates directly to hospitals: security cameras, infusion-pump gateways, building automation, and the broader biomedical-device

estate age out of patch coverage quietly, and a five-year-old camera vulnerability still drawing tens of millions of hits shows how long that tail runs [54]. Connected devices deserve an owned inventory, their own patch-and-replace program, and network segmentation that assumes some of them are already compromised.

- **Hospital facilities and building systems.** The expanded joint advisory on Iranian-affiliated actors manipulating internet-exposed PLCs now covers Rockwell, Schneider Electric, and Siemens equipment; hospital facilities teams running building automation, chillers, or water systems on internet-reachable controllers are in scope regardless of vendor [13].
- **Production depends on IT.** Coca-Cola told regulators a ransomware attack forced it to suspend US production at its fairlife dairy subsidiary, a one-line reminder for device manufacturers and pharmacy operations that a production outage does not require OT compromise when production depends on IT systems [14][15].
- **Design data leaks through supplier hosting.** The Kudankulam nuclear-plant document leak traveled through an engineering contractor's outsourced data center, a failure mode worth one line for device makers: your crown-jewel design files sit in other people's clouds [18].
- **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, so the September 30 sunset remains live. The liability protections that underpin Health-ISAC-style indicator sharing lapse if nothing passes [47].
- **For device makers with defense contracts.** The CMMC Phase 2 suspension continues, RFI comments are due August 14, and DFARS 252.204-7012 obligations remain fully binding in the meantime [48][49][50].
- **Two one-liners for counsel.** New Jersey's A5328 bans the sale of sensitive personal data, with penalties of $50,000 per record; any organization enriching or sharing consumer health data should get an applicability read [46]. And the Fourth Circuit now permits manual border phone searches with no individualized suspicion, so traveling staff carrying devices with patient data need a travel-device policy [39][40].

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, and audit recent firewall-policy changes, with special attention to rules segmenting clinical networks [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; research arms and academic affiliates should treat themselves as targeted and ask partners running Zimbra for their status [6][7][8].
4. **Start the business-associate concentration map**: list every vendor holding PHI, flag backend platforms that patients never see, and check each BAA's breach-notification clock against what litigation now punishes [29][33][34].
5. **Ship the two consumer-AI deliverables**: patient-communication guidance on Health in ChatGPT and connected records, and a workforce acceptable-use policy on PHI in consumer AI tools [27][28].
6. **Pre-position sextortion-response scripts** for the helpdesk and patient relations, and confirm the authentication controls regulators keep pricing: MFA, rate limiting, and login-anomaly detection [37][31].
7. **Harden traveling clinicians and executives** with always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded; brief conference-bound staff on hotel Wi-Fi credential traps [11].
8. **Close the DNS egress blind spot**, including on biomedical-device VLANs: restrict DNS to sanctioned resolvers and alert on high-volume or high-entropy queries to unfamiliar domains [11][12].
9. **Govern AI browser agents on PHI-adjacent machines**: enterprise extension allow-listing, no autonomous modes, and repository trust prompts treated as code-execution consent [24][25].

Strategic Actions (This Month)

1. **Tighten BAA terms at renewal**: breach-notification clocks well inside the regulatory ceiling, audit rights, and fourth-party disclosure obligations covering the vendor's own ITSM and support tooling [33][34][35].
2. **Add the HHS breach portal to vendor monitoring** so a business associate's filing reaches you from your own process rather than from a reporter [33].
3. **Put AI incident-notification clocks into health-IT vendor contracts** and pre-approve a forensic-model plan so a provider's guardrails cannot stall your incident response [21][22].
4. **Borrow FedRAMP 20x's patch-velocity standard** in SaaS procurement: ask EHR-adjacent and telehealth vendors their remediation clock for critical internet-facing vulnerabilities, in writing [23].
5. **Fold breach history and security obligations into M&A diligence**, on both sides of any transaction; the 23andMe settlement shows those obligations binding the acquirer [31][32].
6. **Give the connected-device estate its own program**: inventory, patch-and-replace lifecycle, and segmentation for cameras, building systems, and biomedical devices [54][13].
7. **Track the threat-sharing sunset**: if CISA 2015 lapses September 30, review with counsel what your Health-ISAC and indicator-sharing participation looks like without the liability shield [47].

8. **Add a border-crossing device policy** (travel devices, minimal data, no stored credentials) for staff who cross borders with access to patient data [39][40].

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

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