RISK BRIEFING, LEGAL EDITION: THE BREACH-LITIGATION WAVE, CLIENT CONFIDENCES IN OTHER PEOPLE'S CLOUDS, AND TWO PATCH-NOW EMERGENCIES

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: Legal — law-firm managing partners, general counsel, and legal-services executives
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

The breach-litigation docket had its busiest week of the summer, and it matters to your firm twice over: once for the clients you advise, and once because law firms hold exactly the data these suits are about. Former Nissan employees filed Kerner v. Nissan North America over Social Security numbers and banking details taken from Oracle-hosted PeopleSoft HR systems; the complaint attributes the theft to ShinyHunters and pleads a 29-day gap between breach and notice for a class of at least 20,648 [30]. A Troesch plaintiff brought a proposed class action against Abbott Laboratories and Exact Sciences on the same vendor-breach pattern [29]. Three new biometric suits target Amazon Ring and Google Nest doorbell face recognition under Virginia and California law, with the conspicuous absence of an Illinois BIPA claim signaling where the plaintiffs' bar goes when the marquee statute is off the table [38]. And the $18 million, 42-attorney-general 23andMe settlement delivered a durability holding every M&A practice should file: the injunctive security obligations bind the acquirer that bought the company out of bankruptcy [31][32]. The week also produced a direct warning for professional-services firms themselves: Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, a reminder that document management, e-discovery, ITSM, and co-counsel portals all carry client confidences [35]. On the operational side, two vulnerabilities crossed into confirmed active exploitation, one of them into mass exploitation, and belong at the top of this week's queue: a remote-code-execution flaw in on-premises Microsoft SharePoint (CVE-2026-50522), the platform many firms still run for matter files, and an authentication bypass in Check Point Security Management (CVE-2026-16232); CISA added both to the Known Exploited Vulnerabilities catalog on July 22 with an unusually short three-day federal deadline [1]. For SharePoint, patching alone is insufficient, because attackers are stealing IIS machine keys that let them return after the patch [2]. Finally, the Fourth Circuit held that manual border searches of phones are routine and require no suspicion, which puts travel-device policy squarely in ethics territory for any attorney crossing borders with client data [39] [40]. Patch first; then work the litigation, vendor, and travel 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	Firms run matter files on on-prem SharePoint; mass exploitation began within hours of a July 20 public exploit, and 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	Require full-tunnel VPN for traveling attorneys on hotel or conference Wi-Fi; disable Microsoft Entra device-code flow where not needed	Attackers are hijacking hotel Wi-Fi gateway DNS to serve fake Microsoft 365 logins, including an MFA-bypassing device-code lure aimed at exactly the credentials that open your DMS [11]
4	Issue a border-crossing device policy: travel devices, minimal local client data, no stored credentials	The Fourth Circuit now treats manual phone searches at the border as routine, with no suspicion required; privilege protections do not travel with the device [39][40]
5	Map every vendor that touches client confidences (DMS, e-discovery, ITSM, co-counsel portals, court-filing services) and confirm breach-notification terms	EY's client tax documents leaked through a support-ticket SaaS; your vendors have their own vendors [35]
6	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 an AI agent's access to mail, documents, and calendars, which at a firm means privileged material [24][25]
7	Pre-position a plain-language response for clients and staff receiving extortion mail that cites real breach data	Scammers are mass-mailing $2,000 sextortion demands built on genuine leaked data; your help desk and your clients will see them [37]
8	Confirm any Zimbra webmail in your estate, or your clients' or local-government partners' estates, is patched (CVE-2025-66376; current 10.1.20)	Joint advisory AA26-204A details active Russian espionage that triggers on viewing an email; law enforcement and government are named target sectors [6][8]

Priority	Action	Why Now
9	Stand up a New Jersey A5328 client advisory and run your own applicability read	The strictest data-broker law in the country is already effective, with $50,000-per-record penalties for sensitive-data sales and a registry arriving next spring [46]
10	Verify litigation-hold and preservation workflows can respond to earlier, broader demands, and brief surveillance-adjacent clients	The ACLU's new attorney toolkit will put preservation motions in front of vendors and agencies faster and more often [41]

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 vendor-breach docket grew.** Kerner v. Nissan (filed July 1, complaint now circulating) and Troesch v. Abbott/Exact Sciences (filed July 22) both sue the customer of a breached platform, and both put the notification timeline in the pleadings [29][30].
- **The 23andMe settlement's durability terms drew analysis.** Commentary this week confirmed the operative point for deal lawyers: the injunctive security obligations bind the bankruptcy acquirer [31][32].
- **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, opening a new client-advisory lane for AI-exposed clients [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 and the September 30 sunset still stands, with the liability shield your clients' ISAC participation depends on attached [47].
- **CMMC reform now has hard dates.** An SBA Advocacy roundtable is set for July 30 and RFI comments are due August 14; obligations under DFARS 252.204-7012 remain fully in force for DIB clients [48][49][50].

THE BREACH-LITIGATION DOCKET: READ IT AS COUNSEL, AND AS A TARGET

- **Kerner v. Nissan North America: the notification clock is now a pleaded element.** Former Nissan employees filed suit in the Middle District of Tennessee over employee data, including Social Security numbers and banking details, exposed when attackers hit Oracle-hosted PeopleSoft HR systems [30]. The complaint attributes the theft to ShinyHunters and alleges a 29-day gap between the breach beginning May 27 and notice on June 25, for a class of at least 20,648 [30]. These are one-sided plaintiff allegations at the pleading stage, and should be described that way in any advisory. Two features deserve attention anyway: the plaintiffs sued the customer of the breached platform, and they built the notification timeline into the theory of harm. Every client's incident-response plan should be reviewed against the question a complaint like this asks: who owns the notice decision, and how fast does it move [30].
- **Troesch v. Abbott and Exact Sciences: the same pattern in healthcare.** An Exact Sciences patient filed a proposed class action against Abbott Laboratories over the ShinyHunters-claimed theft in its cancer-diagnostics unit; Abbott is separately investigating a second actor's claims, and no verified record counts exist yet, so resist quantifying exposure in client conversations [29].
- **Doorbell biometrics: watch where plaintiffs go without BIPA.** Three new proposed class actions target Amazon Ring and Google Nest over AI "familiar face" doorbell features, alleging faceprints of non-consenting passersby, brought under Virginia and California law with no Illinois BIPA claim; the features are already disabled in Illinois, Texas, and Portland [38]. No class has been certified. With Google's $1.4 billion Texas biometric settlement in 2025 as backdrop, the practical advisory is twofold: clients deploying facial recognition should check consent posture in every operating state, and litigators should expect biometric theories to keep migrating into general consumer-protection and computer-crime statutes [38].
- **23andMe: security obligations followed the assets through bankruptcy.** Forty-one states and the District of Columbia settled with 23andMe for $18 million over the 2023 credential-stuffing breach affecting roughly 6.9 million people [31]. The precedent-setting feature is 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]. For M&A and restructuring practices, that is a due-diligence instruction: regulatory security obligations can survive the sale, and the target's breach history prices into the deal whether or not the diligence checklist asks [31][32].
- **Your firm is on this docket's target list too.** The data in Kerner and Troesch, HR records and patient identifiers held by a large organization's vendor, looks exactly like what sits in your HR system, your DMS, and your e-discovery databases. The same plaintiffs' bar reads the same breach notices. Treat every item in this section as a mirror as well as a market.

PATCH NOW: TWO KEV-LISTED EMERGENCIES

- **Microsoft SharePoint CVE-2026-50522 (CVSS 9.8, on-premises only).** Many firms still run on-premises SharePoint for matter files and workspaces, which puts this at the top of the firm's own queue. 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]. 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]. A SharePoint farm full of privileged client documents is a worst-case place to discover forged-token persistence months from now.
- **Check Point Security Management CVE-2026-16232 (CVSS 9.1).** An improper-authentication flaw lets an unauthenticated attacker obtain a token with full administrative rights over the firewall management server, which means the ability to rewrite 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]. Audit recent policy changes and administrator activity, and get management interfaces off the open internet.
- **Watchlist.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites serve fake Microsoft 365 login overlays to their visitors, so firm websites and the sites your staff browse are both in scope [10]. nginx CVE-2026-42533 remains unexploited in public, but a researcher has announced proof-of-concept details for around August 5; close out patch verification first [9].

CLIENT CONFIDENCES IN OTHER PEOPLE'S CLOUDS

- **EY's exposure is the professional-services warning shot.** Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, with the exposure window running March 28 to April 12 and detection on April 23 [35]. A Big Four firm's client confidences left through a helpdesk SaaS the clients never chose. Every law firm runs an equivalent stack: document management, e-discovery platforms, ITSM and support tooling, co-counsel and deal-room portals, court-filing and docketing services. Map which of them can see client data, what their breach-notification commitments say, and who at the firm gets the call [35].
- **Concentration risk compounds it.** The OpenLoop Health breach (716,000 individuals per the HHS breach portal) is drawing renewed analysis as a case study in backend-vendor concentration: most affected patients never chose or heard of the vendor holding their data [33][34]. The legal-sector analogue is the handful of e-discovery and DMS platforms that hold a meaningful share of the profession's privileged material. Your engagement letters and outside-counsel guidelines increasingly ask about this; your own vendor file should answer it before a client asks [33][34][35].

- **Supplier custody failures travel upstream.** In mid-July an extortion group published files taken from India's Reliance Group through a contractor's outsourced hosting, purportedly including facility design documents for a nuclear plant; the extortionists priced the criticality of the end client rather than the breached party [18]. For firms advising on critical-infrastructure and industrial matters, that is the pattern to brief: crown-jewel documents inherit the security of the weakest custodian in the chain [18].

PRIVILEGE ON THE MOVE: BORDERS, HOTELS, AND DEVICES

- **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 attorneys, this lands differently than for most travelers: a device carrying client communications, matter documents, and firm-portal credentials can be reviewed by hand at the border with no threshold showing at all. Travel-device policy is now an ethics-adjacent control, and the answer is data minimization: dedicated travel devices, minimal local client data, and no stored credentials, so there is nothing privileged for a manual search to reach [39][40].
- **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]. Attorneys on trial travel, closings, and conferences are a target-rich population, and a captured Microsoft 365 session opens mail, DMS integrations, and shared matter workspaces at once. 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 firm does not need it [11]. Pair that with DNS egress control at the office, since malware is also tunneling command-and-control through DNS [12].
- **Privacy tooling as alleged culpable conduct.** Federal prosecutors are pursuing a novel theory against a 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, firms issuing hardened devices should watch this docket, because it tests whether device-security features can themselves be framed as obstruction-adjacent conduct [42].

DISCOVERY, PRESERVATION, AND THE SURVEILLANCE FILE

- **The ACLU just published a discovery playbook, and preservation demands will arrive earlier.** 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, covering facial recognition, license-plate readers, gunshot detection, cell-site simulators, brokered location data, and AI-generated police reports, with preservation demands aimed directly at private vendors whose products auto-delete data on short cycles [41]. For criminal-defense and civil-rights practices, this is ready-made work product. For any client selling surveillance-adjacent technology, and any agency client using it, it is a compliance test: legal holds will land earlier, more broadly, and increasingly on the vendor rather than only the agency. Verify that retention and preservation workflows, including short-cycle auto-deletion defaults, can actually respond to a preservation demand before one arrives [41].

- **Espionage context worth one paragraph in the client file.** A joint advisory sealed by 27 agencies across 16 countries (AA26-204A) documents a Russian state-linked actor exploiting Zimbra webmail through an email that executes on viewing; named target sectors include government, law enforcement, defense, energy, education, media, NGOs, and technology [6]. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens, and an alleged group member is facing charges in Boston federal court [8]. Few large firms run Zimbra, but local-government clients, courts, and smaller co-counsel may; ask the question, and note the prosecution as a live example of cyber charges moving through US courts [6][8].

AI INSIDE THE FIRM, AND AI AS A PRACTICE AREA

- **An AI browser agent at a law firm reads privileged material by design.** Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions, including reading mail, documents, and calendars, via synthetic clicks, and that the finding remained reproducible in the current release as of late July despite a May report [24]. At a firm, the mailbox an agent reads is privileged correspondence. The control is enterprise extension allow-listing on any machine running an AI browser agent, and avoiding autonomous modes. Separately, a disputed Claude Code behavior can expose one out-of-project file via a repository-committed instruction file; the vendor closed the report as consistent with its documented threat model, so treat it as a boundary dispute and treat "trust this folder" prompts as code-execution consent [25].
- **Health in ChatGPT previews your data-handling problem.** OpenAI launched Health in ChatGPT this week for US adults, connecting Apple Health and records from participating providers, with stated commitments against training on the data and a 30-day deletion policy; the announcement makes no HIPAA claim, and it arrived one day after a lawsuit alleging harmful ChatGPT medical advice [27][28]. The pattern generalizes to legal practice directly: staff and clients will paste regulated and privileged material into consumer AI tools outside sanctioned channels unless acceptable-use policy, and the client-facing guidance you give on communications channels, says something specific about it [27][28].
- **The AI Kill Switch Act opens an advisory lane.** H.R. 9917, introduced July 23 with bipartisan sponsorship, would require AI developers above defined thresholds ($100 million in training compute or $500 million in revenue) to maintain shutdown capability, report qualifying incidents within 15 days, and

comply with graduated federal correction orders, with civil penalties scaling to $20 million per day [19][20]. It is one chamber's freshly introduced bill and passage is far from assured, but AI-exposed clients will ask what it means, and boards will start asking "could we shut it down, and who orders it?" as a governance question [19][20].

- **Contract terms from the incident's second week.** Post-incident analysis of the OpenAI/Hugging Face event converged on controls living outside the model, and surfaced a vendor-relations lesson worth drafting into agreements: a published claim, single-outlet and so far unconfirmed, alleges the responsible provider took roughly ten days to notify the affected platform [21][22][58]. Incident-notification clocks for AI providers belong in your clients' vendor contracts and in your firm's own [21][22]. FedRAMP's director, citing the incident, set a two-to-four-day patch expectation for critical internet-facing flaws; commercial buyers can borrow the standard in procurement [23].

CLIENT-ADVISORY RADAR

- **New Jersey A5328: effective now, registry next spring.** Signed June 30 and effective immediately, A5328 bans the sale of sensitive personal data outright with penalties of $50,000 per record, and stands up a data-broker registry (operative next spring) with fees scaling to $1.5 million for the largest brokers [46]. The definitions are broad, so the advisory audience extends well past companies that call themselves brokers: any client that buys, sells, or enriches consumer data needs an applicability read, and firms whose marketing operations touch consumer data should run one on themselves [46].
- **Sextortion's long tail will hit inboxes you answer for.** A mass sextortion campaign impersonating ShinyHunters demands $2,000 in Bitcoin and uses genuinely leaked breach data from Amtrak, Hallmark, Substack, Betterment, and others to look credible; there is no actual device compromise behind the claims [37]. Clients whose names appear in public leaks will field panicked calls, and so will your own staff. Pre-position a canned, plain-language response for the help desk and for client advisories: the leaked data is real, the compromise claim is not, do not pay, report and delete [37].
- **Disclosure practice, illustrated.** Coca-Cola's July 16 SEC filing disclosing a ransomware-driven production suspension at its fairlife subsidiary, made before the attackers surfaced publicly and while their 1 TB claim remains unconfirmed, is a clean teaching example for disclosure-counsel work on materiality timing and on labeling attacker claims as claims [14][15].
- **OT advisories are client-advisory material.** The expanded joint advisory on Iranian-affiliated actors manipulating internet-exposed PLCs at US water and energy victims (AA26-097A, updated July 22) is directly relevant to clients in water, energy, and manufacturing, and to the breach-duty questions that follow an incident on unpatched, internet-exposed equipment [13].
- **The threat-sharing sunset is a live counseling question.** If CISA 2015 lapses September 30, the liability, antitrust, and FOIA protections underpinning ISAC-style sharing lapse with it; clients participating in sharing programs will need advice on what participation looks like without the shield [47].
- **CMMC reform: the comment window is real.** The Phase 2 suspension continues, with an SBA Advocacy roundtable July 30 and RFI comments due at noon ET on August 14; every legal analysis published this

week agrees that DFARS 252.204-7012, NIST 800-171 self-assessments, SPRS scores, and annual affirmations remain binding, with False Claims Act exposure attached [48][49][50]. DIB clients should use the pause to fix gaps and the RFI to be heard [48][49][50].

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, and prioritize farms holding matter files [1][2][3].
2. **Patch Check Point Security Management** for CVE-2026-16232, take management interfaces off the internet, and audit recent policy changes and admin logins for tampering [1][4][5].
3. **Harden traveling attorneys** 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 before the next conference cycle [11].
4. **Issue or update the border-crossing device policy**: travel devices, minimal local client data, no stored credentials, reflecting the Fourth Circuit's holding that manual searches need no suspicion [39][40].
5. **Map the client-confidence vendor stack** (DMS, e-discovery, ITSM, co-counsel portals, filing services), confirm each vendor's breach-notification commitments in writing, and identify which hold privileged material [35].
6. **Govern AI browser agents**: enterprise extension allow-listing on any machine running one, no autonomous modes, and treat repository trust prompts as code-execution consent [24][25].
7. **Pre-position scam-response language** for extortion mail citing real breach data, for both the firm's help desk and client advisories [37].
8. **Ask the Zimbra question** of your own estate, local-government clients, courts, and co-counsel (CVE-2025-66376; current release 10.1.20), and hunt for historical webmail compromise where it applies [6][8].
9. **Confirm wp2shell and nginx patch completion** on firm web properties before the announced ~August 5 nginx proof-of-concept [9][10].

Strategic Actions (This Month)

1. **Refresh incident-response plans against the pleadings**: Kerner makes the notification clock part of the claim, so confirm who owns the notice decision, on what timeline, for the firm and for clients you advise [30][29].

2. **Brief M&A and restructuring teams on 23andMe durability**: injunctive security obligations followed the assets through bankruptcy, and diligence checklists should price breach history and open regulatory obligations accordingly [31][32].
3. **Verify preservation workflows**, including vendor auto-deletion cycles, can respond to earlier and broader legal holds, and brief surveillance-adjacent clients on the ACLU toolkit's implications [41].
4. **Stand up the New Jersey A5328 advisory** for clients that buy, sell, or enrich consumer data, and check biometric-consent posture on any client or firm facial-recognition deployment [46][38].
5. **Put AI incident-notification clocks into vendor contracts**, the firm's and clients', and borrow FedRAMP 20x's patch-velocity standard in SaaS procurement [21][22][23].
6. **Work the CMMC reform window for DIB clients**: the July 30 SBA roundtable and the August 14 RFI deadline are the levers, and existing DFARS obligations continue to bind in the meantime [48][49][50].
7. **Track the threat-sharing sunset**: prepare counsel guidance on ISAC and indicator-sharing participation if CISA 2015 lapses September 30 [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

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