RISK BRIEFING, INDUSTRY & MANUFACTURING EDITION: PERIMETER NOISE FALLS, CONNECTED DEVICES TAKE THE HITS, AND RANSOMWARE STOPS A PRODUCTION LINE

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: Manufacturing, heavy industry, and construction
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

New sector data set the frame this week. SonicWall's 2026 Manufacturing Protect Brief reports manufacturing 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: 46.2 million IoT attack hits, more than half of monitored manufacturing networks seeing IoT exploitation attempts, the highest SCADA detection rate of any industry, and a single 2021 Hikvision camera flaw drawing 43 million hits on its own [54]. Those figures are one vendor's sensor telemetry and skew toward smaller networks, so treat the absolute numbers with care; the direction, though, matches what we see in the field. Attackers are spending less effort on the hardened perimeter and more on the connected devices plants keep adding, which means camera estates and plant-floor IoT have earned their own patch program. The week supplied the case studies to go with the data. Coca-Cola told regulators a ransomware attack forced it to temporarily suspend US production at its fairlife dairy subsidiary after attackers reached production-related IT systems, a production outage with no OT compromise required; production is now largely restored, Coca-Cola has confirmed data was taken, and the attackers posted the stolen data for download after their Monday-morning publication deadline passed [14][15][59][60]. The July 22 update to joint advisory AA26-097A confirms Iranian-affiliated actors manipulating internet-exposed PLCs are now observed on Schneider Electric and Siemens equipment in addition to Rockwell, which puts most plant floors squarely in scope [13]. Two vulnerabilities crossed into confirmed active exploitation, 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), a platform many plants still run for document control and quality records, 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 an unusually short three-day federal remediation window [1][2][4]. For manufacturers in the defense supply chain, an advisory sealed by 27 agencies across 16 countries on Russian espionage against Zimbra webmail names the defense industrial base among its targets, and the CMMC reform comment window now has hard dates [6][48][49]. Finally, two supplier incidents, the

Kudankulam design-document leak and the EY support-platform exposure, are reminders that your drawings and client data leave your control through contractors' hosting and IT vendors' SaaS [18][35]. Patch the two criticals first; then work the plant-floor and supplier 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; many plants run on-prem SharePoint for document control, 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, including plant-boundary and OT-segmentation firewalls [1][4][5]
3	Inventory internet-reachable PLCs across Rockwell, Schneider Electric, and Siemens estates; pull them behind secure gateways and run AA26-097A's new detection guidance	The July 22 update adds Schneider Electric and Siemens, the controllers on most plant floors, to an active Iranian-affiliated campaign [13]
4	Stand up a dedicated patch and firmware program for camera estates and plant IoT, starting with Hikvision CVE-2021-36260	A long-known camera flaw drew 43M hits in H1 per SonicWall telemetry; over half of monitored manufacturing networks saw IoT exploitation attempts [54]
5	Test segmentation and manual-fallback plans for production-adjacent IT (ERP, MES, scheduling, shipping)	Ransomware in production-related IT suspended fairlife's US production with no OT compromise; production is now largely restored and Coca-Cola has confirmed data was taken [14][15][59]
6	Require full-tunnel VPN for traveling staff on hotel or conference Wi-Fi, issue clean travel devices for border crossings, and disable the Entra device-code flow where unneeded	Hotel gateway DNS is being hijacked to serve fake Microsoft 365 logins, and manual phone searches at the border now require no suspicion in the Fourth Circuit [11][39][40]
7	Monitor and restrict outbound DNS on enterprise and OT networks alike	Malware is tunneling command-and-control through DNS, and hijacked gateways forge answers before they reach trusted resolvers; OT networks rarely watch DNS egress at all [11][12]

Priority	Action	Why Now
8	Confirm Zimbra is patched (CVE-2025-66376; current 10.1.20) and ask Zimbra-running suppliers the same question	Joint advisory AA26-204A documents active Russian espionage against the defense industrial base and energy sector; the exploit triggers on viewing an email [6][8]
9	Map where design documents, process data, and client records sit in contractors' and vendors' clouds	The Kudankulam leak traveled through an engineering contractor's outsourced hosting; EY client documents left through an IT-support SaaS [18][35]
10	Set enterprise browser-extension policy for AI agents on engineering workstations; treat repository trust prompts as code-execution consent	Unpatched research shows co-installed extensions can hijack AI browser-agent actions; engineering seats hold CAD, PLC project files, and BOMs [24][25]
11	Defense manufacturers: 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

- **New manufacturing telemetry.** SonicWall released its 2026 Manufacturing Protect Brief on July 22, documenting the shift from perimeter volume toward IoT and SCADA entry points across monitored manufacturing networks [54].
- **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 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 for malicious project-file changes [13].
- **The fairlife position moved.** Coca-Cola has confirmed data was taken, and a majority of production has resumed across its four US facilities; the Anubis publication deadline passed Monday morning, and the stolen data has since been posted for download [59][60].
- **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, with the defense industrial base among named target sectors [6].

- **CMMC reform now has hard dates.** An SBA Advocacy roundtable is set for July 30 and RFI comments are due August 14 [48][49].
- **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 SECTOR DATA: A QUIETER PERIMETER, SOFTER DEVICES

- **What SonicWall's manufacturing brief actually says.** Sector intrusion-prevention events fell 56.2% year over year yet still totaled 474 million in the first half of 2026; IoT attacks accounted for 46.2 million hits; more than half of monitored manufacturing networks saw IoT exploitation attempts; and manufacturing showed the highest SCADA detection rate of any industry SonicWall monitors [54]. The single most instructive number is the oldest: CVE-2021-36260, a long-known Hikvision camera flaw, drew 43 million hits [54]. These are one vendor's sensor telemetry, weighted toward smaller networks, so resist treating the totals as a census of the sector [54].
- **What it means for your estate.** The perimeter noise is falling while the soft spots move to connected devices. Every camera, sensor, badge reader, and retrofit gateway added to a plant in the last decade is a networked endpoint, and most of them sit outside the IT patch cycle entirely. Camera estates and plant IoT deserve their own inventory, their own firmware program, and their own network segment; a device that cannot be patched should at minimum be unable to reach the internet or the control network. The Hikvision figure shows attackers will happily work a five-year-old flaw for as long as unpatched devices answer [54].
- **SCADA visibility cuts both ways.** The highest SCADA detection rate of any industry means attackers are probing those entry points and, in monitored environments, defenders are seeing it [54]. If your OT network has no equivalent detection layer, assume the probing is happening there too and you simply lack the sensor.

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]. This one matters disproportionately in manufacturing because on-prem SharePoint remains a workhorse for document control, engineering change management, and quality records, often on servers that predate current hardening baselines. The exploitation detail that matters most: watchTowr reports attackers using a single request to steal IIS machine keys, which let them forge valid authentication tokens and walk back in after you patch [2]. CISA's hardening guidance is blunt: assume

compromise on internet-exposed unpatched servers, hunt and remediate, then rotate machine keys [1] [2]. Both espionage and ransomware actors are using the same entry points [2].

- **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 the firewalls that separate your enterprise network from the plant floor [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, verify OT segmentation rules have not been altered, and get management interfaces off the open internet.
- **Patch-status watchlist.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites 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 disputing 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: rotation of FortiGate credentials, session termination, and MFA remain the only complete fix.

PRODUCTION UNDER PRESSURE

- **The Iranian PLC campaign now covers most plant floors.** 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 named victims are utilities, but the equipment list is the manufacturing installed base, and the tradecraft transfers directly: 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 update ships concrete detection guidance for malicious project-file changes. If any controller in your estate is reachable from the internet, including via a cellular modem or a vendor remote-access box, treat yourself as in scope regardless of vendor [13].
- **fairlife: a production halt without an OT breach.** 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]. Note the shape of that recovery when you plan your own: inventory bought the brand its shelf presence while production was down, which is a buffer many manufacturers do not have. Food and beverage manufacturing is squarely in ransomware's targeting envelope, and the operational lesson keeps being re-learned across the sector: when scheduling, batching, quality release, or shipping depends on IT systems, encrypting those systems stops the line just as surely as touching a controller would. Test the manual fallback before you need it, and know how long you can run on paper.

- **Energy-sector breach cluster, briefly.** Australia's Origin Energy (about 4.8 million customers) confirmed unauthorized access to customer data, with an extortionist claiming 2 million records, and Colombia's Ecopetrol disclosed unauthorized access to cloud file storage across roughly 15 subsidiaries [16][17]. For industrials with utility-style customer or counterparty data estates, the pattern holds: the monetizable soft target is the data estate, distinct from grid or plant OT.

YOUR DATA IN CONTRACTORS' HANDS

- **Kudankulam: design documents 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 from every owner and EPC regardless: 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. If you are the owner, your drawings sit in your contractors' systems; if you are the contractor, your clients' criticality is now your extortion exposure.
- **EY: client documents lost through an IT-support SaaS.** Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform [35]. Your professional-services firms have their own vendors, and your data flows through them. Together with Kudankulam, this week's homework is a data-custody map: where do crown-jewel documents, from process designs to financials, actually sit in other people's clouds, and what do those parties' contracts say about hosting, notification, and deletion [18][35].
- **The litigation pattern: customers of breached platforms get sued.** An Exact Sciences patient filed a proposed class action against Abbott Laboratories over a ShinyHunters-claimed theft, while Abbott separately investigates a second actor's unverified claims of access to manufacturing certificates, manuals, and specifications [29]. Former Nissan employees sued Nissan North America over employee data exposed when attackers hit Oracle-hosted PeopleSoft HR systems, alleging a 29-day gap between breach and notice [30]. In both cases plaintiffs are suing the customer of the breached platform, and the notification clock is part of the claim. The 23andMe settlement adds an M&A angle: its $18 million multistate resolution carries injunctive security obligations that survived bankruptcy and bind the acquirer, which acquirers of industrial businesses should read as a due-diligence instruction [31][32].

ESPIONAGE AND THE DEFENSE SUPPLY CHAIN

- **Laundry Bear puts DIB suppliers on notice.** Joint advisory AA26-204A (July 23) documents a Russian state-linked actor exploiting a cross-site-scripting flaw in Zimbra webmail (CVE-2025-66376) through a view-based exploit: opening or previewing the message is enough, with no attachment or link click required [6]. Named target sectors include the defense industrial base, government, and energy, and Proofpoint additionally reports targeting of what it calls "nuclear installations" and "high science" [6][7]. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [8]. Any manufacturer holding defense contracts or supplying primes sits inside this targeting envelope. If you run Zimbra, patch and upgrade (10.1.20 shipped July 20) and hunt for historical compromise; if your suppliers or local-government partners run it, ask them the same question [8].
- **Hotel Wi-Fi as a credential trap.** Attackers are altering DNS settings on hotel and conference-center Wi-Fi gateways so travelers land on convincing fake Microsoft 365 portals, in some cases using a device-code sign-in flow that captures a legitimate OAuth session and bypasses MFA outright [11]. Plant managers, sales engineers, and executives on trade-show circuits travel constantly. 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]. For staff crossing borders with corporate devices, pair this with a travel-device policy of minimal local data and no stored credentials, since a recent Fourth Circuit ruling lets border agents search phones by hand with no suspicion required [39][40].
- **DNS as a covert channel, including on OT networks.** Fortinet documented a Windows backdoor running its command-and-control entirely over DNS queries routed through a public resolver, moving 1.2 MB in about 40 seconds in testing [12]. The attribution rests on one vendor's code-similarity analysis and the campaign's scale is unquantified, but the defensive lesson stands: an egress policy that inspects HTTP while letting hosts talk DNS to arbitrary external resolvers has a blind spot [12]. OT networks deserve particular attention here, because DNS egress from control segments is rarely monitored and almost never needed; restrict it to sanctioned internal resolvers and alert on the exceptions [11][12].
- **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]. Defense manufacturers, especially small and mid-size machine shops and fabricators for whom assessment cost is existential, should use the RFI to be heard. Every legal analysis published this week agrees 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].
- **Threat-sharing law: one chamber down.** The House passed its FY2027 NDAA with a provision reauthorizing the Cybersecurity Information Sharing Act of 2015 through 2036; the Senate has no matching provision and the September 30 sunset remains live [47]. If it lapses, the liability protections

underpinning ISAC-style sharing lapse with it, which affects manufacturers participating in sector ISACs and DIB threat-sharing programs [47].

AI GOVERNANCE REACHES THE ENGINEERING WORKSTATION

- **A kill-switch bill, introduced.** Reps. Ted Lieu and Nathaniel Moran introduced H.R. 9917, the AI Kill Switch Act, on July 23; it would require large AI developers to maintain shutdown capability, report qualifying incidents within 15 days, and comply with graduated federal correction orders during defined loss-of-control scenarios [19][20]. It is one chamber's freshly introduced bill, but boards adopting AI in production planning, quality, and design should expect "could we shut it down, and who orders it?" to become a standard governance question [19][20].
- **Lessons from the sandbox escape.** Post-incident analysis of the OpenAI/Hugging Face event has converged on a practical point: model-level safeguards are not a security boundary, and effective controls live outside the model in network rules, scoped credentials, destination allow lists, DNS filtering, and outbound data-loss prevention [22]. Put AI incident-notification clocks into vendor contracts, and note the FedRAMP director's procurement standard, publicly telling vendors who cannot patch critical internet-facing flaws within two to four days to exit the federal market; commercial buyers can borrow the question for their SaaS and industrial-software vendors [21][22][23].
- **AI agents on engineering seats.** Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions via synthetic clicks, a finding still reproducible in the current release as of late July [24]. Separately, a disputed Claude Code behavior can expose one out-of-project file via a repository-committed instruction file; Anthropic closed the report as consistent with its documented threat model, so treat "trust this folder" prompts as code-execution consent [25]. Engineering workstations concentrate CAD models, PLC project files, and bills of materials, exactly the data an agent hijack would reach; apply enterprise extension allow-listing on any machine running an AI browser agent and avoid autonomous modes [24][25]. On the criminal side, the "Dolphin X" stealer advertises an AI-based victim-ranking profiler; most capability claims are the seller's own, but the direction, automated triage of infections to find the valuable endpoints, raises the stakes of any single infected engineering seat [26].

THE BROADER LANDSCAPE

- **Digital sovereignty moved from talk to contract, at a manufacturer.** 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 for European industry, and US manufacturers serving European customers should expect data-residency questions in more RFPs [57].

- **Congress war-gamed AI-enabled infrastructure attacks.** Members of two House committees ran a closed-door exercise simulating AI-enabled cyberattacks against US ports, rail, and airports in a 2027 Taiwan-crisis scenario [53]. Manufacturers live downstream of exactly those logistics nodes; the scenario makes a ready-made tabletop for your own supply-chain continuity exercise, and transportation cyber mandates tend to follow congressional attention [53].
- **Aviation cyber governance, graded.** GAO's aviation-cybersecurity report finds FAA has defined cyber roles while TSA has not, and notes precisely that there have been no reports of successful cyberattacks on avionics; aerospace suppliers should expect the governance gaps, and the recommendations both agencies accepted, to flow down into program requirements [52].
- **Scam mail built on real breach data.** A mass sextortion campaign demands $2,000 in Bitcoin using genuinely leaked breach data to look credible, with no actual device compromise behind the claims; if your organization has appeared in a public leak, pre-position a plain-language response for employees who receive it [37].
- **Quick notes.** New Jersey's A5328 bans the sale of sensitive personal data outright with penalties of $50,000 per record; any industrial with a consumer-data sideline should get an applicability read [46]. New class actions over AI "familiar face" doorbell features are a consent-posture warning for any facility deploying facial recognition at the gate [38].

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 instances holding document control and quality records [1][2][3].
2. **Patch Check Point Security Management** for CVE-2026-16232, take management interfaces off the internet, audit recent policy changes and admin logins, and verify OT-segmentation rules are intact [1][4][5].
3. **Act on AA26-097A's July 22 update**: inventory internet-reachable PLCs across Rockwell, Schneider Electric, and Siemens estates, including cellular modems and vendor remote-access paths, pull them behind secure gateways, and run the advisory's new project-file detection guidance [13].
4. **Start the connected-device inventory**: enumerate cameras, sensors, and plant IoT; patch or firmware-update what you can, starting with Hikvision CVE-2021-36260; segment and internet-isolate what you cannot [54].

5. **Pressure-test production-adjacent IT**: confirm ERP, MES, scheduling, and shipping systems are segmented from backups and from OT, and rehearse the manual fallback the fairlife outage illustrates [14][15].
6. **Close the DNS egress blind spot** on enterprise and OT networks: restrict hosts to sanctioned resolvers and alert on high-volume or high-entropy DNS to unfamiliar domains [11][12].
7. **Verify Zimbra patching** (CVE-2025-66376; current release 10.1.20) and hunt for historical webmail compromise; ask Zimbra-running suppliers and partners for their status, especially if you hold defense work [6][8].
8. **Harden traveling staff** with always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded; brief the trade-show circuit on hotel Wi-Fi credential traps [11].
9. **Govern AI agents on engineering seats**: enterprise extension allow-listing, no autonomous modes, and treat repository trust prompts as code-execution consent [24][25].

Strategic Actions (This Month)

1. **Build the supplier data-custody map**: identify where design documents, process data, and client records sit in EPC contractors', engineering firms', and IT vendors' clouds, and check those contracts for hosting, notification, and deletion terms [18][35].
2. **Defense manufacturers: work the CMMC reform window**, following the July 30 SBA roundtable and filing RFI comments by noon ET August 14, while keeping 800-171, SPRS, and affirmation posture current [48][49][50].
3. **Put AI incident-notification clocks into vendor contracts** and borrow the FedRAMP 20x patch-velocity question for SaaS and industrial-software procurement: what is your remediation clock for critical internet-facing vulnerabilities, in writing [21][22][23].
4. **Give the camera and IoT estate a standing program**, with an owner, a firmware cadence, and a network segment, rather than a one-time cleanup; the sector telemetry says this is where the attacks moved [54].
5. **Confirm wp2shell and nginx patch completion** before the announced ~August 5 nginx proof-of-concept; verify auto-updates actually applied [9][10].
6. **Add a border-crossing device policy** (travel devices, minimal data, no stored credentials) for staff visiting overseas plants and suppliers [39][40].
7. **Track the threat-sharing sunset**: if CISA 2015 lapses September 30, review with counsel what your ISAC and DIB indicator-sharing participation looks like without the liability shield [47].
8. **Run the Taiwan-scenario tabletop** for your logistics dependencies: ports, rail, and air cargo disruption against your inventory and shipping posture [53].

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