MONTHLY THREAT BRIEF

August 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in August 2026

At a Glance

OT Attacks Go Transatlantic

RMM Platforms Under Attack

Healthcare Absorbs Both Extremes

Iran-Linked Hackers Force a UK Power Plant Offline for Four Days

Iran-linked hackers took a small UK power generation facility offline for four straight days in July, the first confirmed cyberattack of its kind against British energy infrastructure. Officials said the broader grid was never at risk, but staff restored operations manually.

What To Do

- Inventory and segment OT-facing generation assets
- Rehearse manual-operation
- Brief leadership on cross-border OT exposure

Ransomware Disrupts Global Operations at Boston Scientific

Boston Scientific disclosed a cyberattack on August 25 that disrupted order processing and shipping worldwide, with no group named and no confirmed data theft. It's a reminder an IT compromise alone can stall a global manufacturer's supply chain.

What To Do

- Assume IT outages can halt production
- Maintain offline backups of order-processing systems
- Pre-approve manual order and shipping workarounds
- Confirm business-continuity plans with key suppliers

Brief

Water Attacks Widen to 12 States

CISA, the FBI, and EPA confirmed Iran-linked actors have hit water utilities in 12 states, up from seven in July, exploiting exposed Rockwell PLCs. Remove engineering interfaces before the count grows.

CareCloud Breach Hits 3.75 Million Patients

CareCloud confirmed attackers accessed an AWS environment in March and stole Social Security numbers, banking details, and medical records for 3.75 million patients, disclosed only in August. Healthcare SaaS vendors remain high-value targets.

N-able N-central Flaw Fuels MSP Compromises

N-able's N-central platform suffered an authentication-bypass flaw letting attackers seize admin control and reach downstream customer endpoints, prompting two hotfixes and a CISA KEV listing.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and Business Risk

RMM Platforms Are Becoming Root Access for MSPs

N-able's N-central authentication-bypass flaw let attackers seize admin control of the remote-monitoring platform MSPs use to manage client endpoints, then tunnel through Cloudflare for persistence. When one RMM login grants access to hundreds of downstream networks, a single flaw becomes a supply-chain event.

What To Do

- Patch N-central to the latest hotfix now
- Restrict RMM console access to named admins
- Alert on new outbound tunnels from RMM hosts
- Require MFA on every RMM administrative login

A Healthcare SaaS Breach Nobody Noticed for Months

CareCloud disclosed that attackers sat inside one of its AWS environments for about a week in March, stealing Social Security numbers, banking details, and medical records on 3.75 million patients before anyone caught it. The gap between compromise and disclosure is the real story.

What To Do

- Vet third-party healthtech vendors' cloud controls
- Require breach detection SLAs in vendor contracts
- Notify patients faster than a four-month gap

Private Equity Firms Are the Newest Vishing Target

UNC6671 called Apollo employees on personal phones, posed as IT staff, and phished MFA codes to steal names and Social Security numbers. The playbook now targets finance, not just utilities.

What To Do

- Verify IT/support calls through a separate channel
- Train staff to reject phone-based MFA resets
- Restrict personal-device use for corporate MFA

FBI Dismantles a Chinese State-Hacker Network

Two UK members of Scattered Spider were sentenced to 5.5 years each for the 2024 Transport for London attack, a reminder that critical-infrastructure intrusions carry real legal consequence.

What To Do

- Patch and monitor IoT and edge devices
- Watch for hard-coded C2 domains in vendor gear

CONTINUED ON NEXT PAGE »

OPERATIONAL EXPOSURE

Infrastructure, Vulnerabilities, and Operational Risk

Edge Appliances Are Still the Fastest Way In

CISA added a Citrix NetScaler flaw to KEV after researchers turned a patched memory bug into unauthenticated code execution, and defenders found web shells on compromised gateways within days. Federal agencies had until August 29 to mitigate.

What To Do

- Patch NetScaler ADC/Gateway immediately
- Hunt for web shells on internet-facing appliances
- Disable unused AAA/SAML SSO virtual servers
- Track CISA BOD deadlines for edge devices

Nation-State OT Pressure Crosses the Atlantic

Iran-linked actors expanded U.S. water-utility attacks to 12 states and, separately, knocked a UK power generation plant offline for four days. Two continents, one pattern: internet-exposed OT gives geopolitical actors an easy physical lever.

What To Do

- Remove PLCs from internet exposure
- Coordinate OT incident response across sites
- Report cross-border incidents to CISA and NCSC

Even a Crash-Only Bug Takes Firewalls Offline

Cisco confirmed active exploitation of a flaw that reloads ASA and FTD firewalls running SSL VPN, with no workaround available. Availability, not just data theft, is now squarely in scope.

What To Do

- Apply Cisco's ASA/FTD hotfix
- Disable SSL VPN where not business-critical
- Plan for firewall failover during patch windows

A Medical Device Giant Goes Dark Mid-Quarter

Boston Scientific's cyberattack halted order processing and shipping worldwide with no restoration timeline given, days before quarter-end. When IT stalls, manufacturers feel it on the loading dock first.

What To Do

- Keep manual order-entry fallback processes current
- Test recovery time against real order backlogs

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

August 2026

Across this month's developments, several consistent themes are emerging for security and operational teams.

Trust in Third-Party Tools Is the New Blast Radius

N-able's RMM flaw, CareCloud's unnoticed cloud breach, and Apollo's vished employees share one root cause: attackers exploited trust in third-party tools, vendors, and callers rather than breaking through a defended perimeter. Vetting who and what you trust is becoming as critical as patching what you own.

Disruption, Not Just Data Theft, Is the Real Cost

Boston Scientific's shipping freeze, the UK power outage, and the widening water-utility campaign all caused disruption, not just stolen data. When attackers can halt production or generation instead of just copying files, business continuity planning matters as much as data protection.

Detection Speed Is Falling Behind Compromise Speed

CareCloud went undisclosed for months after compromise, and N-able needed two hotfixes because exploitation kept outpacing each patch. What matters now isn't whether a control exists, but how fast you detect and respond when it fails.

Geography No Longer Limits Nation-State Targeting

Iran-linked actors hit water utilities in 12 states and a UK power plant in the same stretch, while investigators dismantled Chinese-linked infrastructure used against multiple countries. Offense and defense now both operate across borders, and incident response plans should too.

This Month's Pattern: Old Playbooks, New Targets

Voice-phishing once aimed at utilities and healthcare reached a private equity firm this month, and ransomware disruption once concentrated in manufacturing hit a medical device maker. The tactics aren't new, but the sectors absorbing them keep growing, making "not our industry" a riskier assumption.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

Iran-Linked Hackers Force a UK Power Plant Offline for Four Days

The month's clearest escalation: Iran-linked actors widened U.S. water-utility attacks to 12 states, then knocked a UK power plant offline for four days, the first confirmed hit of its kind on British energy infrastructure. OT exposure is now a shared transatlantic problem.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- Australian Police Arrest Two Alleged TeamPCP Hackers Over Software Supply-Chain Attacks
- Updated Warning on Iran-Affiliated Water Utility Attacks
- FBI Seized Platforms Used by China QTFY Hackers to Target U.S. Critical Infrastructure

Threat Intelligence & Activity

- Previously Patched Citrix NetScaler Flaw Exploited in the Wild, Added to CISA KEV
- N-able Ships Hotfix as Attackers Keep Exploiting N-central Flaw
- Cyberattack Causes Global Disruption at Boston Scientific

Stay Connected

Follow us on social media for the latest updates: