MONTHLY THREAT BRIEF

July 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in July 2026

At a Glance

Water & OT Under Attack

Identity & SaaS Credential Sprawl

Edge Devices Fueling Ransomware

Attackers Lock Water Utilities Out of Their Own PLCs

Starting July 26, attackers exploited internet-exposed Rockwell PLCs to lock operators out of water systems across seven states, hitting roughly 36 Minnesota utilities in one weekend. Some plants lost pressure or flooded before staff forced manual control and restored service.

What To Do

- Remove PLCs from direct internet exposure
- Segment OT networks behind a DMZ
- Change default and reused PLC credentials
- Rehearse manual-operation failover procedures

Ransomware Halts Production at Coca-Cola's Fairlife Plants

Coca-Cola disclosed that ransomware group Anubis breached its Fairlife dairy unit, halting U.S. production at four plants. Anubis claimed a terabyte of stolen data and threatened to leak it after Coca-Cola refused to pay; most lines resumed within days.

What To Do

- Assume ransomware can halt physical production
- Keep offline backups of MES/SCADA configs
- Pre-approve manual-mode production runbooks
- Confirm supplier and co-pack continuity plans

Brief

Iranian PLC Campaign Expands to Siemens, Schneider

CISA's updated advisory on Iranian PLC targeting now names Siemens and Schneider platforms alongside Rockwell. At one victim, actors disabled safety shutdown logic undetected - audit ladder logic for unauthorized changes.

Cisco Firewall Manager Backdoored by Static Credentials

Cisco confirmed active exploitation of a Firewall Manager flaw rooted in embedded static credentials, letting attackers log in as a hidden account. CISA added it to KEV and recommends patching now.

Stale Salesforce Token Breaches Nearly 200 Companies

An extortion crew used a forgotten four-year-old Salesforce token issued to Klue to reach customer data at almost 200 companies, including LastPass and Snyk. Dormant SaaS tokens can outlive the vendors that issued them.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and Business Risk

Forgotten SaaS Tokens Are a Silent Backdoor

A four-year-old Salesforce API token issued to a single vendor, Klue, gave an extortion crew access to nearly 200 companies' customer data, no breach of Salesforce itself required. As integrations pile up, the riskiest credentials are often the ones nobody remembers granting.

What To Do

- Inventory all third-party API tokens and OAuth grants
- Revoke tokens tied to inactive vendors immediately
- Set expirations on every long-lived integration credential

Management Consoles Are Now the Target

Cisco's Firewall Management Center flaw let attackers log in through embedded static credentials nobody could rotate. Centralized consoles that manage firewall or PLC fleets are high-value single points of failure, and static or hardcoded credentials remain a recurring, avoidable root cause.

What To Do

- Audit vendor products for hardcoded credentials
- Restrict management-console access to jump hosts
- Monitor for unexpected admin logins and config changes

Help Desks Remain the Easiest Way In

Voice-call impersonation of IT staff drove a reported 277% jump in remote-support tool abuse this year, often escalating straight to ransomware. It works because it targets trust, not technology.

What To Do

- Restrict who can install remote-access tools
- Verify support requests through a second channel
- Train staff to recognize callback and vishing lures

Prosecutions Are Catching Up to Attackers

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

- Report incidents promptly to build prosecutable cases
- Track threat-actor takedowns relevant to your sector

CONTINUED ON NEXT PAGE »

OPERATIONAL EXPOSURE

Infrastructure, Vulnerabilities, and Operational Risk

VPN Appliances Keep Handing Out Root Access

SonicWall, Check Point, and Fortinet all disclosed exploited VPN and SD-WAN flaws this month, with INC and Qilin ransomware weaponizing them within weeks. Remote-access gear remains the fastest path from internet exposure to domain compromise.

What To Do

- Disable unused remote-access features and portals
- Require MFA on every remote-access login
- Patch VPN and SD-WAN appliances on an accelerated cycle

OT Is a Live Physical-Risk Battlefield

The seven-state water utility attacks and an expanded Iranian PLC campaign show nation-state actors now targeting operational outcomes, not just data. Pressure loss and forced manual operation are the new blast radius for OT intrusions.

What To Do

- Baseline PLC logic and alert on unauthorized changes
- Tie OT incident response to physical safety impact
- Remove engineering workstations from internet exposure

Patch Backlogs Are Becoming Breaches

CISA added four more actively exploited SharePoint flaws to KEV this month, on top of the spring's ToolShell chain. Unpatched enterprise software keeps functioning as a bridge into OT-adjacent corporate networks.

What To Do

- Track CISA KEV additions weekly
- Prioritize patching by exploitation, not CVSS alone
- Verify remediation with follow-up scanning

Manufacturing Absorbs the Most Ransomware

Manufacturing again ranked as ransomware's top target this year, and Fairlife's four-plant shutdown shows why: IT compromises routinely stop physical production lines, not just back-office systems.

What To Do

- Map which IT outages can halt production
- Segment MES/SCADA from general business networks

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

July 2026

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

Water & Energy Systems Are Now Live Targets

The seven-state water utility intrusions and an expanded Iranian campaign against Siemens and Schneider PLCs show attackers pursuing physical disruption, not just data theft. Pressure loss, forced manual operation, and disabled safety logic are now realistic outcomes, not theoretical ones, for under-segmented OT environments.

Remote-Access Appliances Are the Common Denominator

SonicWall, Check Point, Cisco, and Fortinet all disclosed actively exploited flaws in edge and remote-access gear this month, feeding directly into ransomware campaigns. Whatever vendor you run, the pattern holds: internet-facing appliances need faster patching and tighter access controls than anything behind them.

Forgotten Credentials Are as Dangerous as New Exploits

A four-year-old Salesforce token and hardcoded credentials in Cisco's firewall manager both bypassed defenses without a single novel exploit. Credential lifecycle management, not just patching, decides whether stale access becomes an attacker's easiest way in.

Manufacturing Sits Squarely in the Blast Radius

Coca-Cola's Fairlife plants went dark for days after a ransomware hit, reaffirming manufacturing as the sector attackers target most this year. When IT and production networks aren't segmented, a business-systems breach quickly becomes a factory-floor shutdown.

Regulation and Consequences Are Both Catching Up

CISA expects to finalize CIRCIA's incident-reporting rule by September, and a new Senate bill would force updated cybersecurity plans across all 16 infrastructure sectors. Meanwhile, real prison sentences for Scattered Spider members show that critical-infrastructure attacks now carry lasting personal consequences.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

Attackers Locked Water Operators Out of Their Own PLCs in Seven States

The month's defining event: attackers exploited internet-exposed Rockwell PLCs to seize control of water utilities across seven states, forcing plants into manual operation and, in some cases, causing pressure loss. It's a stark reminder that removing OT from the internet isn't optional.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- CISA Advisory AA26-097A Update: Iranian PLC Campaign Expands to Siemens, Schneider
- FBI/EPA/CISA Alert on Water Sector PLC Attacks
- CISA Expects to Finalize CIRCIA Reporting Rule by September

Threat Intelligence & Activity

- SonicWall SMA1000 Zero-Days Exploited by INC Ransomware
- Stale Salesforce Token Breaches Nearly 200 Companies
- Ransomware Halts Production at Coca-Cola's Fairlife Plants

Stay Connected

Follow us on social media for the latest updates: