OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

Data Centres Under Threat

APAC OT/ICS Threat and Vulnerability Brief | H1 2026 baseline; intelligence updated 2 November 2026

Field	Detail
Classification	TLP:CLEAR – public dissemination permitted under FIRST TLP 2.0
Intended readers	Data centre operators, critical-facilities and engineering teams, cloud/colocation customers, and relevant public-sector stakeholders.

Key judgements

- Reviewed public-source H1 2026 APAC incidents do not substantiate malicious compromise of facility power or cooling controls. Absence of reporting is not proof of absence.
- Indonesia PDNS 2 experienced Brain Cipher ransomware in June 2024. This is a verified historical IT/service incident, not evidence of power or cooling controller manipulation. [17–18]
- October 2026 IDC Frontier ransomware affected a cloud/virtualisation management environment and 495 customers; a facility-OT impact was not established. [11]
- Power, cooling and management-system vulnerabilities have credible potential consequences when reachable, but published research is distinct from observed exploitation at a named data centre.
- Recovery independence, monitored vendor access and safe engineering change control remain priorities.

Five priorities for operators

- Inventory internet-reachable gateways and management interfaces; confirm current KEV status before scheduling remediation.
- Identify UPS/PDU/BMS/DCIM/BMC ownership and access paths using approved, non-disruptive discovery methods.
- Prioritise vendor-supported fixes for confirmed affected products and applicable firmware, especially reachable critical systems.
- Verify backup and recovery independence across hypervisor, cloud portal and facility configuration domains.
- Ask providers how remote vendor access, equipment restart, incident notification and shared recovery obligations are tested.

1. How to use this report

If you are…	Start with
Critical-facilities / electrical engineering	Cards A and C, then the 72-hour checklist in Section 8
BMS, EPMS or DCIM owner	Card B, Section 5 protocol watchlist
Infrastructure / platform security	Cards D and E, Section 6 priority matrix
Operations and business continuity	Section 7 incidents and Card C lessons
Customers of colocation or cloud (essential services)	Key judgements, Card H questions for your provider
Senior leadership	Key judgements and Section 8

2. Scope, method and confidence

- Scope: APAC data-centre power, cooling, engineering, BMS/EPMS/DCIM and adjacent server, identity, cloud and remote-management systems. Evidence period: H1 2026; historical and post-H1 cases are labelled.
- Method: primarily official incident statements, CISA/CERT and vendor advisories and original research through 2 November 2026. Where access conditions, deployment or exploitation are unknown, findings remain conditional.
- Exclusions: no facility-specific device exposure enumeration, exploit instructions or presumed operational network paths. Public examples do not establish deployment at any named member facility.
- Confidence: Confirmed (primary evidence); Assessed (reasoned inference); Unverified (claims not independently substantiated). Non-cyber resilience events are separately identified.

3. What is installed: data centre OT

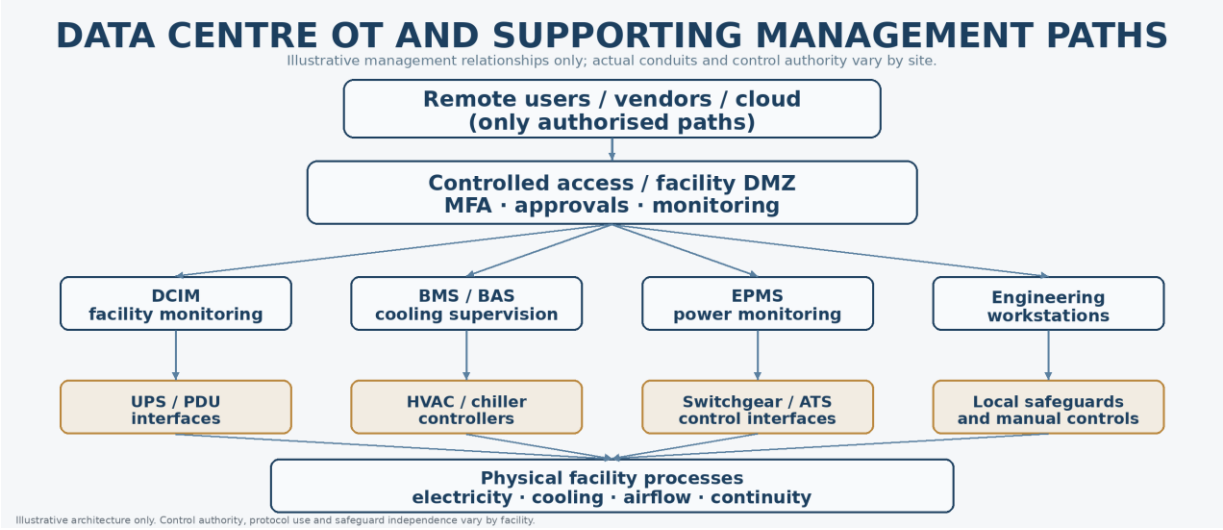

Figure 1. Illustrative data-centre IT/support-to-facility pathway. Actual access, control authority and engineering safeguards vary by site; arrows do not evidence a real intrusion route.

Device class	Function	Common protocols / interfaces	If disrupted or manipulated (conditional)
UPS and network management cards	Ride-through and conditioning of critical power	SNMP, HTTP/HTTPS, Modbus TCP, vendor serial	Protected load switched off or transferred unexpectedly
PDUs / rack PDUs	Outlet-level power distribution and metering	SNMP, HTTP, SSH, vendor cloud	Individual racks or outlets de-energised
Switchgear, ATS/STS, EPMS	Utility/generator transfer, power monitoring	Modbus TCP, IEC 61850, DNP3, BACnet	Failed or unsafe transfer; loss of power visibility
Generators	Backup power	Controller Modbus, vendor remote monitoring	Backup unavailable when utility fails
Chillers, CRAH/CRAC, CDUs	Heat rejection and air or liquid cooling	BACnet/IP, Modbus TCP, vendor controllers	Thermal shutdown of IT within minutes to hours
BMS / DCIM	Supervision, alarms, capacity and change	BACnet, Modbus, SNMP, Fox, SOAP/REST	Loss of visibility; false or suppressed alarms; pivot point
BMC / IPMI / Redfish; hypervisors	Server and virtualisation management	IPMI 2.0, Redfish (HTTPS), vSphere APIs	Mass server control, firmware tampering, ransomware at hypervisor level
Fire detection and suppression; access; CCTV	Life safety and physical security	Vendor panels, ONVIF/RTSP, web consoles	Unsafe discharge or missed alarm; access integrity lost

4. Device-by-device: exploitable vulnerabilities and actions

Cards A–H are public-source summaries. Verify exact affected product, configuration, access prerequisites and the current OEM fix before taking action. Published vulnerabilities are not evidence of exploitation against a specific facility.

A. UPS, PDU and power-chain management

What is inside	UPS network management cards, rack PDUs, power-management software and DCIM agents that can issue shutdown or outlet-off commands.
Exploitable vulnerabilities	Vertiv Liebert IS-UNITY-DP and RDU101: CVE-2025-46412 and CVE-2025-41426; Claroty demonstrated a potential unauthorised UPS output-off effect in its research setup. No verified real-world data-centre OT attack is established by this disclosure. [1] Trellix disclosed four CyberPower PowerPanel Enterprise and five Dataprobe iBoot PDU issues in 2023, including management-interface exposure with potential power consequences. [2]
Access needed	Requires reachability of a vulnerable management interface; some issue combinations require authentication or chaining. Internet exposure is not universal.
Check now	Inventory model, firmware and interfaces; check whether vendor web/SNMP write paths are externally accessible or improperly shared.
Fix	Follow current OEM-fixed firmware guidance for each product/branch. Use staged maintenance windows; isolate management interfaces, disable unnecessary SNMP write access and validate fail-safe behaviour.
Detect	Investigate unusual UPS output/off commands, power-management configuration changes, new administrators and off-zone logins; verify equipment state with engineering staff.

B. BMS, EPMS and DCIM

What is inside	BMS servers and controllers, EPMS, DCIM servers that aggregate alarms from power and cooling.
Exploitable vulnerabilities	Johnson Controls Metasys CVE-2025-26385 affects specified products/configurations involving SQL Express; the published attack vector is network, subject to reachability and deployment conditions. [3] Nozomi reported 13 Tridium Niagara issues with a potentially serious chain under defined configurations. [4] Schneider Data Center Expert: CVE-2026-8045 and September CVE-2026-19233/-8044 require distinct advisory checks; the latter affect 9.1.2 and earlier. [5][20] PHP2Shell CVE-2026-109618/-109619: Delta Controls identified specified enteliWEB/V4 IP-controller products as affected. Exposure is product/configuration dependent, not evidence of live-facility exploitation. [28][29]
Access needed	Metasys: network reachability plus affected SQL Express conditions. Niagara: specific configuration and protocol reachability. DCE: individual advisory prerequisites, including authentication for some issues.
Check now	Map exact versions and architecture; identify trusted supervisory-to-controller paths and validate least-privilege administrative access.
Fix	Follow product-specific OEM instructions; Schneider identifies DCE 9.2 for its September advisory. Do not treat 9.1.2 as fully remediated. For affected Delta products, apply OEM-provided application/firmware fixes, not a generic PHP update. [20][29]
Detect	Review unexpected BMS/EPMS accounts, configuration changes, alarm suppressions, SQL access outside approved sources and suspicious DCE login/activity patterns.

C. Cooling, power transfer and batteries (lessons from non-malicious failures)

What happened	Microsoft Australia East (August 2023): utility power event and chillers not restarting automatically. [6] Equinix Singapore (October 2023): chilled-water disruption affected banking services. [7] South Korea NIRS Daejeon (September 2025): UPS battery fire interrupted government systems; separate non-cyber resilience event. [8]
Why this matters for cyber	These are documented engineering/physical failure modes, NOT malicious OT compromises. They illustrate dependencies and consequences to test in contingency planning.
Check now	Ask facilities teams for evidence of controlled chiller restart testing, protected power-transfer procedures, battery handling controls and staffing for manual recovery.
Fix	Test only under an approved method statement with adequate redundancy. Verify manual recovery and independent alerts; do not introduce live power interruptions for routine cyber validation.
Detect	Set-point or sequence changes not linked to work orders; chiller trips without matching electrical events; battery temperature or state-of-charge anomalies.

D. Server management plane (BMC / IPMI / Redfish)

What is inside	Baseboard management controllers (BMC), IPMI and Redfish provide out-of-band server management and can influence availability independently of guest operating systems.
Exploitable vulnerabilities	AMI MegaRAC SPx CVE-2024-54085: critical Redfish authentication bypass; listed by CISA KEV in June 2025. Actual affected OEM images and firmware must be verified. [9][15] EDK II PXE CVE-2026-97631: conditional pre-boot network-boot risk in affected firmware, not a blanket vulnerability in all running servers. [22]
Access needed	BMC: reachability of affected service; PXE: affected firmware and network-boot exposure during provisioning/recovery.
Check now	Confirm no BMC is internet-reachable; identify servers using AMI MegaRAC firmware (via OEM advisories); confirm the out-of-band network is separate from production and guest networks.
Fix	Use OEM firmware images; isolate BMC networks and disable unnecessary services. Audit PXE boot settings and provisioning traffic before planning safe firmware changes.
Detect	Redfish or IPMI sessions from unexpected sources; new BMC accounts; firmware updates outside change windows.

E. Virtualisation layer

What is inside	Hypervisors and management servers hosting tenant and internal workloads, including BMS and DCIM virtual machines.
Exploitable vulnerabilities	Broadcom VMSA-2025-0004 covers CVE-2025-22224/-22225/-22226, with particular guest/host privilege prerequisites; KEV inclusion concerns those vulnerabilities, not every ESXi incident. [10][15] VMware ESX CVE-2026-41709 concerns insufficient logging of some actions by a malicious administrator, not unauthenticated hypervisor access; later added to KEV. [24] IDC Frontier confirmed a distinct October 2026 ransomware incident involving an exploited cloud-portal authentication component and compromised virtualisation management. [11]

Access needed	VM-escape issues require particular guest privileges; logging issue requires an already privileged administrator; IDC Frontier entry was via its cloud portal. These are different paths.
Check now	Confirm ESXi hosts are on fixed builds per VMSA-2025-0004; confirm vCenter and ESXi management interfaces are not reachable from tenant or corporate networks.
Fix	Patch per applicable Broadcom bulletins, keep independent management audit logs, enforce MFA and separate backup administration; restore-test critical workloads and BMS/DCIM configurations.
Detect	New ESXi shell or SSH enablement; bulk snapshot deletion; mass VM power-off; logons to vCenter outside change windows.

F. Physical security and life safety

Exploitable vulnerabilities	CISA advisories cover selected Johnson Controls C-CURE 9000/victor and Simplex Incident Manager vulnerabilities. Applicable devices and software serve physical security and life safety; no direct power/cooling compromise is established. [13][14] Legacy CCTV vulnerabilities may be KEV-listed, but relevance must be determined from actual exposure and connection to operational services. [12]
Access needed	Varies by affected product and CVE; network and local-access prerequisites must not be conflated.
Check now	Confirm cameras and access-control servers are not internet-reachable and sit in their own zone; confirm fire-suppression panels have no remote write path.
Fix	Use the latest vendor-supported updates; separate physical-security networks from facility control and confirm independent safe operation of protection systems.

G. Remote-access edge

Remote-access and service-edge risks	KEV-listed vulnerabilities in internet-facing VPN/ADC/firewall infrastructure warrant urgent assessment when the exact affected product and exposure are present. Treat each CVE separately; not all recent NetScaler or gateway issues have the same exploit status. [15][16] CVE-2026-111497 affects some Brotli decoder integrations and was added to KEV; it is a software-dependency exposure, not a generic HTTP/2 protocol compromise. [23]
Check now	Check current KEV and OEM advisories against asset inventory; include OEM/contractor gateways, identity brokers and critical cloud-facing services.
Fix	Reduce external management exposure; apply approved updates, independent logging, MFA and on-demand vendor session controls.

H. If you depend on a data centre: questions for your provider

Ask	Are UPS/PDU/BMS/DCIM/BMC access paths segregated and documented? Who owns vendor remote links? What was the last controlled chiller restart and recovery test? Are immutable backups outside the affected site, region and administrative domain? What is the customer notification timeline and provider–tenant restoration responsibility?
Why	Indonesia PDNS 2 (Brain Cipher, 2024) and IDC Frontier (2026) show cloud-service continuity and recovery dependence; historical engineering failures show different, non-cyber operational risks. [17][11]

5. Protocol watchlist

Protocol	Used for	Native authentication	Secure option	What operators should do
SNMP v1/v2c	UPS, PDU, sensor monitoring and some control	Community string only, cleartext	SNMPv3 (authPriv)	Move to SNMPv3; disable write communities; restrict sources
Modbus TCP	Switchgear, gensets, chillers, meters	No	Modbus/TCP Security (TLS)	Allow TCP/502 only from named masters
BACnet/IP	BMS, cooling	No	BACnet Secure Connect	Zone BMS; plan BACnet/SC for new works
IEC 61850 / DNP3	Substation and power monitoring	No (legacy)	IEC 62351; DNP3 Secure Authentication	Restrict to EPMS hosts; monitor writes
IPMI 2.0	Server BMC management	IPMI 2.0 has legacy cryptographic and authentication weaknesses; risk depends on implementation.	Disable unneeded IPMI-over-LAN; prefer supported managed access.	Never expose; disable IPMI-over-LAN where not needed
Redfish	Server BMC management	Authentication over HTTPS can be bypassed by affected firmware (CVE-specific).	OEM-patched Redfish, HTTPS, role separation.	Patch; isolate out-of-band network
Vendor web / SOAP consoles	UPS cards, DCIM, PDUs	Password; flaws above	HTTPS and MFA where supported; controlled access gateway.	Patch; restrict to management VLAN

6. Prioritisation

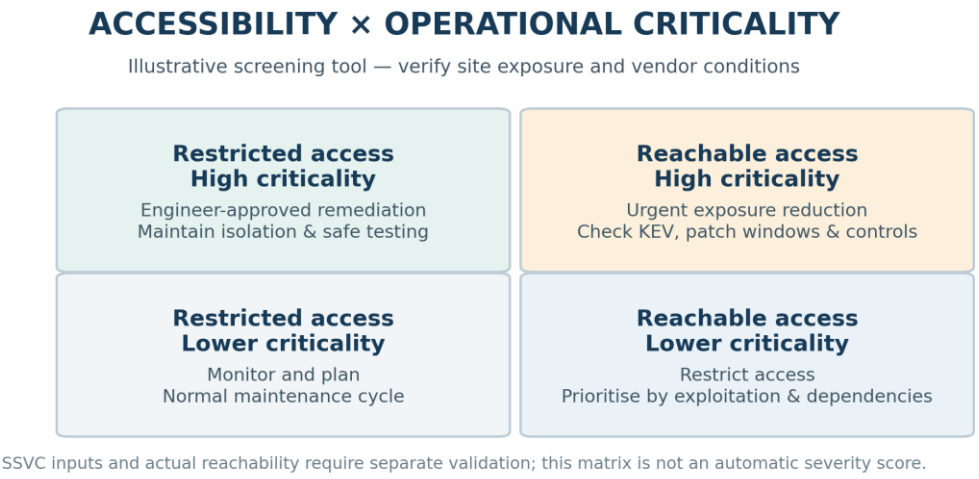

Figure 2. Illustrative accessibility-versus-criticality screen. Site reachability, actual mission dependencies and KEV evidence must be validated separately; not a computed SSVC score.

The table below gives conditional screening actions, not universal CISA SSVC decisions. Operators must verify product presence, reachability, operational criticality and approved remediation constraints.

Item	Exploit evidence	Access needed	Impact if compromised	Local relevance	Indicative action
Exposed gateway on KEV	Confirmed in KEV	Network access	Service/admin impact	If used by site	Act if exposed
AMI MegaRAC CVE-2024-54085	Confirmed in KEV	BMC reachability	Server control	If affected OEM	Act if reachable
ESXi CVE-2025-22224/-25/-26	Confirmed in KEV	Guest privileges / chain	Host compromise	If affected version	Act as applicable
Brotli CVE-2026-111497	Confirmed in KEV	Affected decoder path	Application/service	If decoder reachable	Act if exposed
Vertiv Liebert cards	No public exploitation confirmed	Mgmt network	Potential power action	If deployed	Attend / isolate
CyberPower / Dataprobe	Research disclosure	Mgmt network	Potential outlet-off	If unpatched	Attend / isolate
JCI Metasys CVE-2025-26385	Research/advisory	Conditional network	BMS supervision	If affected SQL	Attend
Tridium Niagara	Research disclosure	Configuration-dependent	Integration server	If relevant config	Attend
Schneider DCE September CVEs	Research/advisory	CVE-specific	DCIM service/data	If version ≤9.1.2	Patch to 9.2
Johnson Controls Simplex	Research/advisory	Local access	Supporting security	If deployed	Track / isolate

7. Observed incidents in APAC

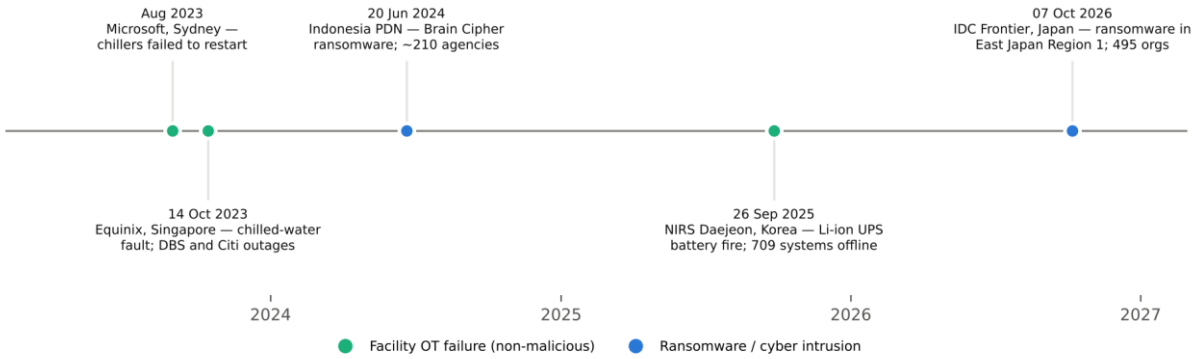

Figure 3. Selected APAC cyber incidents and non-cyber facility disruptions, 2023–2026. Brain Cipher identifies ransomware used at Indonesia PDNS 2, not a verified operator identity. Cases are illustrative, not a regional incident count.

Date	Event	What was reported	Confidence	Source
Aug 2023	Microsoft, Sydney (Australia)	Utility voltage sag during a storm took chillers offline; they did not restart automatically; Microsoft later cited insufficient on-site staff for recovery.	Confirmed	[6]
14 Oct 2023	Equinix, Singapore	Chilled-water system fault raised temperatures; DBS and Citibank services offline; MAS took supervisory action.	Confirmed	[7]
20 Jun 2024	Indonesia PDNS 2, Surabaya	Brain Cipher ransomware, identified by Indonesia's BSSN; the malware was described as derived from LockBit 3.0. Public-service disruption affected immigration and government systems. Evidence does not establish facility power/cooling controller compromise. [17][18]	Confirmed ransomware; no OT evidence	[17][18]
26 Sep 2025	NIRS, Daejeon (Korea)	Lithium-ion UPS battery fire during relocation; 709 government systems offline at peak; G-Drive (858 TB) believed lost with no backup; arrests made.	Confirmed	[8]
7 Oct 2026	IDC Frontier, Japan	Provider-confirmed IDCF Cloud ransomware following exploitation of a cloud-portal authentication component and compromise of virtualisation management; 495 customers affected. No confirmed facility OT compromise. Attacker-only wipe figures omitted. [11]	Confirmed IT/cloud incident; facility OT unconfirmed	[11]
21 Oct 2026	GMO Onamae.com Desktop Cloud, Japan	Provider confirmed unauthorised access, customer data exposure and extortion. Its 28 Oct investigation did not confirm ransomware execution; do not count as a verified ransomware deployment or facility OT attack. [25]	Confirmed intrusion; ransomware not confirmed	[25]

Date	Event	What was reported	Confidence	Source
May 2026	NSCC ASPIRE 2A, Singapore	Official service bulletin describes a security-related service event; no verified malicious facility-OT manipulation. [27]	Reported service/cyber event; OT unconfirmed	[27]
May–Jun 2026	NTTPC WebARENA SuiteX, Japan	Provider reported suspicious traffic and service management interruption; facility OT compromise not established. [26]	Reported service/cyber event; OT unconfirmed	[26]

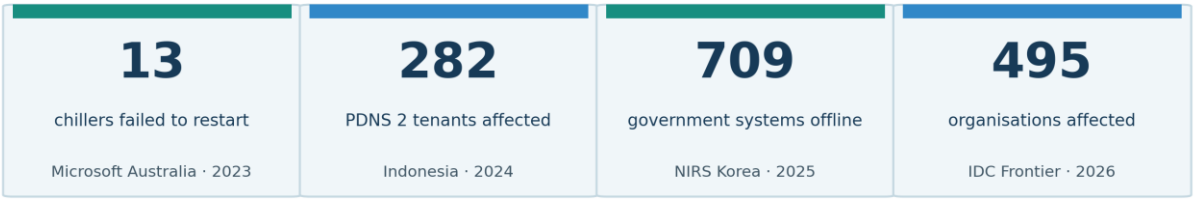

Figure 4. Individual, non-comparable reported impact indicators from four separate events. Units, causes and reporting dates differ; do not aggregate.

Threat actors and context

Public reporting reviewed through 2 November 2026 does not establish malicious access to APAC data-centre facility power or cooling controls. Brain Cipher is a verified ransomware family linked to PDNS 2, but a malware family name alone is not attribution to a particular operating group. Other cases principally concern IT, cloud and virtualisation management.

Actor or activity (as named by source)	Documented activity	Relevance
Brain Cipher ransomware (family)	Indonesia PDNS 2, 20 June 2024; BSSN identified the malware as a LockBit 3.0 derivative. [17][18]	Confirmed service ransomware; no demonstrated facility OT compromise; actor identity unproven.
Unnamed ransomware operator	IDC Frontier cloud/virtualisation compromise, October 2026; no verified named ransomware group. [11]	Provider-confirmed ransomware, but attacker-only claims about volume of wiping are not accepted as evidence.
Unattributed ESXi chain	Published intrusion research shows potential edge-to-hypervisor abuse; language artefacts alone do not establish state sponsorship. [10]	Technically relevant pathway; avoid actor or APAC data-centre facility-OT attribution.
Other provider intrusions	GMO Onamae.com Desktop Cloud (October 2026): confirmed unauthorised access/extortion; no verified ransomware execution in the cited update. [25]	Identity, service and customer recovery relevance; facility control compromise not established.

Regional context

Singapore's Digital Infrastructure Bill passed its third reading on 7 October 2026, with staged commencement expected in 2027. Operators should check their own regulatory status, licensing requirements and applicable cyber-resilience codes; the defensive guidance here is not a legal-compliance determination. [19]

8. Action plan

Timeframes assume normal change control and that power and cooling work happens in planned windows. Each action names who acts (data centre provider, tenant, or both), what it depends on, and an interim measure to apply if the action cannot be completed in time.

Operational constraints this plan accounts for

- Split ownership: power and cooling are often run by facilities contractors or a landlord, the BMS by an integrator, servers by platform teams.
- Uptime commitments: work on power and cooling controls usually needs a method statement, approval and a maintenance window.
- Vendor dependency: firmware is often available only through OEM service contracts, sometimes with an engineer on site.
- Limited visibility: facility devices are rarely in the IT asset register, and vendor connections (cellular modems, cloud connectors) do not show in external scans.
- Legacy equipment: some devices cannot be patched or moved to SNMPv3; isolation and replacement planning are the realistic answer.
- Shared responsibility in colocation: most facility actions sit with the provider; tenants act on their own servers and data, and ask the provider the rest.

When	Action	Who	Depends on	Interim if late	Done when
72 hours	Identify internet-facing VPN, ADC and firewall devices on the Card G KEV list; patch where an approved window exists	Both – IT Security	Change approval; HA failover window	Restrict admin interfaces to named source addresses; increase log review	Every device patched, or restricted with a patch date booked
72 hours	Use approved passive inventory and safe external exposure validation for owned or authorised address space; do not indiscriminately scan live OT controllers.	Both – IT Security	Engineering owner approval; known asset scope	Close any exposure found at the firewall	Exposure register validated with facilities/IT
72 hours	Check ESXi hosts against VMSA-2025-0004; restrict the out-of-band (BMC) network to named jump hosts	Both – Platform Eng.	Network change for out-of-band access	Firewall ACL in front of the out-of-band network	ESXi status listed; out-of-band reachable only from jump hosts
30 days	Census of vendor remote connections: written request to each UPS, chiller, generator and BMS vendor for every path, including cellular modems and cloud connectors	Provider – Facilities (Procurement)	Vendor responses	Disable unidentified paths once operational impact is confirmed	Register of every vendor path with an owner
30 days	Map servers using AMI MegaRAC firmware through OEM advisories; plan firmware updates	Both – Platform Eng.	OEM firmware availability	Out-of-band isolation (72-hour action)	Affected models listed with update dates

When	Action	Who	Depends on	Interim if late	Done when
30 days	Restrict access to UPS cards, PDUs, BMS and DCIM with ACLs; disable SNMP write and default communities	Provider – Facilities (Network)	Confirm DCIM polling still works	–	ACLs in place; SNMP write disabled
30 days	Plan and book fixes for Vertiv cards, Metasys, Niagara and DCE: method statements, vendor attendance, windows	Provider – Facilities; BMS owner or landlord	Vendor, landlord, maintenance window	ACLs above; monitor configuration changes	Each fix booked with date and owner
30 days	Restore one critical workload and the BMS/DCIM configuration from an off-site copy; agree who backs up what	Both – Platform Eng. (Ops)	Backup tooling; customer contracts	–	Restore recorded; provider/tenant responsibility agreed in writing
30 days	Send the Card H questions to the data centre provider	Tenant – Risk / Vendor Mgmt	Contract terms	–	Written answers received
90 days	Apply the booked fixes; record end-of-support devices that cannot be patched	Provider – Facilities (Vendors)	Concurrent-maintainability rules; vendor attendance	ACLs and change monitoring stay in place	Fixed versions installed, or replacement plan recorded
90 days	Review chiller and CRAH restart logic in controller configuration; observe it during the next scheduled generator transfer test. Live sag tests only in a planned window with full redundancy	Provider – Facilities Eng.	Scheduled test; redundancy available	Documented manual restart; confirm night-shift staffing	Restart behaviour confirmed and recorded
90 days	Review lithium-ion battery handling: source isolation, state of charge, detection and suppression	Provider – Facilities (HSE)	Contractor briefing	–	Procedure updated and briefed
90 days	Exercise hypervisor ransomware plus a cooling alarm; measure time to safe thermal state and to customer notification	Both – Crisis Mgmt	Team availability	–	Times recorded; improvement plan owned

When	Action	Who	Depends on	Interim if late	Done when
90–180 days	Isolate UPS/PDU/BMS/BMC management paths in appropriate security zones. Adopt SNMPv3 authPriv where supported; apply protocol-specific controls for BACnet, Modbus and Redfish.	Provider – Network (Facilities)	Network redesign; DCIM reconfiguration; legacy kit	ACLs from the 30-day action	Documented zone controls; supported protocols hardened
90–180 days	Extend immutable, off-site backups to all critical workloads, outside the virtualisation admin domain	Both – Platform Eng.	Budget; storage capacity	Restore-tested copy of the most critical workload	Coverage agreed and tested

9. Intelligence gaps and how to contribute

- Which UPS card, PDU and BMS firmware versions are deployed across APAC facilities? Anonymous counts would let OT-ISAC issue targeted alerts.
- How was IDC Frontier entered, and did facility OT or BMS share any management path with the affected region?
- Have members seen scanning or login attempts against UPS cards, BMCs or BMS from the internet?
- How long does chiller restart take in practice after a sag at your sites?

Share through info@otisac.org. Handled under FIRST TLP 2.0 at the label you set; used only in aggregate or with explicit permission.

Taking this forward together

The gaps above cannot be closed by any single operator. OT-ISAC proposes four joint efforts. OT-ISAC convenes, analyses and facilitates; members contribute what they see in their own facilities. Each effort produces something participants can use directly in their own operations.

Joint effort	What OT-ISAC brings	What we ask of members	What participants gain
Member alert (TLP:AMBER), within 7 days: power-chain management flaws and exploited BMC/ESXi vulnerabilities	Verified triage of the Card A–E vulnerabilities, fixed versions, detection signals and SSVC priorities for data centre estates	Tell us whether affected products are in your estate, and share any scanning or login attempts seen against UPS cards, BMCs or BMS	A prioritised action list checked against what peers are actually seeing
PREDICT tabletop: hypervisor ransomware combined with a cooling alarm	Scenario design, facilitation and decision scoring on the PREDICT platform, with anonymised peer comparison	One colocation or enterprise operator to co-design; facilities, platform and crisis teams to take part	Measured time to a safe thermal state and to customer notification, with an owned improvement plan
ORION benchmark: chiller and CRAH restart after a power sag	Anonymised collection and analysis into a regional benchmark	Results from your own restart tests, shared at the TLP level you choose	A peer benchmark to set targets and justify investment
Provider–customer assurance question set	Drafting and convening, building on Card H	Data centre providers and essential-service customers to review and agree common questions	One shared question set that reduces duplicate assurance requests for providers and gives customers consistent answers

How to take part

- Reply to any of the four efforts through **info@otisac.org**, naming the effort and a point of contact.
- PREDICT tabletop; TLP:AMBER alert is shared with members.
- Contributions are handled under FIRST TLP 2.0 at the label you set, and used only in aggregate or with your explicit permission.

10. Sources

[1] Claroty Team82 – Vertiv Liebert UPS research (2026) – https://claroty.com/team82/research/attacking-ups-network-cards-to-take-down-data-centers
[2] Trellix ARC – The Threat Lurking in Data Centers (CyberPower and Dataprobe, 2023) – https://www.trellix.com/blogs/research/the-threat-lurking-in-data-centers/
[3] CISA ICSA-26-027-04 – Johnson Controls Metasys – https://www.cisa.gov/news-events/ics-advisories/icsa-26-027-04
[4] Nozomi Networks – Tridium Niagara vulnerability research (2025) – https://www.nozominetworks.com/blog/critical-vulnerabilities-found-in-tridium-niagara-framework
[5] Schneider Electric – SEVD-2026-160-01, Data Center Expert – https://www.se.com/us/en/download/document/SEVD-2026-160-01/
[6] Microsoft Azure – Australia East 30 August 2023 PIR – https://azure.status.microsoft/en-us/status/history/?trackingId=VVTQ-J98
[7] The Business Times – Equinix Singapore chilling-water outage and operator explanation (2023) – https://www.businesstimes.com.sg/companies-markets/telcos-media-tech/contractor-error-caused-server-outage-behind-dbs-citi-banking
[8] Republic of Korea – Ministry of Interior and Safety NIRS recovery context (2025) – https://www.korea.kr/news/policyNewsView.do?newsId=148952245
[9] AMI – MegaRAC SPx CVE-2024-54085 advisory identifier AMI-SA-2025003 – https://www.cve.org/CVERecord?id=CVE-2024-54085
[10] Broadcom – VMware Security Advisory VMSA-2025-0004 – https://support.broadcom.com/group/ecx/productsecurityadvisories
[11] IDC Frontier – investigation and response statement, 27 October 2026 – https://www.idcf.jp/news/topics/20261027001/
[12] CISA – Known Exploited Vulnerabilities catalogue – https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[13] CISA ICSA-26-204-01 – Johnson Controls C-CURE 9000 and victor – https://www.cisa.gov/news-events/ics-advisories/icsa-26-204-01
[14] CISA ICSA-26-232-01 – Johnson Controls Simplex Incident Manager – https://www.cisa.gov/news-events/ics-advisories/icsa-26-232-01
[15] CISA – Known Exploited Vulnerabilities catalogue (live status) – https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[16] Johnson Controls – product security advisories and exposure conditions – https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories
[17] Indonesia Komdigi/BSSN – Brain Cipher identified at PDNS 2 (24 June 2024) – https://www.komdigi.go.id/berita/berita-pemerintahan/detail/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware
[18] Indonesia Komdigi/BSSN – PDNS 2 response and segregation (26 June 2024) – https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-np-tentang-percepat-pemulihan-kominfo-bssn-dan-telkom-operasikan-server-baru-pengganti
[19] Singapore MDDI – Digital Infrastructure Bill second-reading closing speech, 7 October 2026 – https://www.mddi.gov.sg/newsroom/closing-speech-by-sms-tan-kiat-how-for-the-second-reading-of-the-digital-infrastructure-bill/
[20] Schneider Electric – SEVD-2026-251-01: DCE versions 9.1.2 and earlier – https://www.se.com/my/en/download/document/SEVD-2026-251-01/
[21] CISA – Stakeholder-Specific Vulnerability Categorization (SSVC) – https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc
[22] Hetzner – CVE-2026-97631 EDK II PXE provider advisory – https://status.hetzner.com/incident/54493dac-b3a2-44f0-8d8b-6de8b25d8f17
[23] Red Hat – Brotli decoder CVE-2026-111497 bulletin – https://access.redhat.com/security/vulnerabilities/RHSB-2026-015
[24] Broadcom – VMware VMSA-2026-0006 including CVE-2026-41709 – https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
[25] GMO Internet – Onamae.com Desktop Cloud incident fourteenth report (28 October 2026) – https://internet.gmo/en/news/article/260
[26] NTTPC – WebARENA SuiteX incident update 23 June 2026 – https://www.nttpc.co.jp/press/info/2026/06/202606231102.html
[27] Singapore NSCC – ASPIRE 2A official service bulletin – https://help.nscc.sg/aspire2a/bulletin/
[28] CSA Singapore – PHP2Shell PHP security vulnerabilities AL-2026-151 – https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-151/
[29] Delta Controls – SecB0015 official security bulletin on affected products – https://deltacontrols.com/wp-content/uploads/SecB0015_Security_Bulletin.pdf

About this report

Prepared by OT-ISAC, a community of operational technology asset owners, operators and practitioners across Asia-Pacific who share threat intelligence in a trusted setting. TLP:CLEAR: may be shared freely. Guidance only; not a compliance assessment or legal advice. Confirm vulnerability details against primary advisories before acting.