INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:24 UTC

Global cyberattacks ease in May 2026, but ransomware surges 48% as threats reorganize

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0186
Type	Security Analysis
Severity	HIGH
Affected Products	Business Services, Consumer Goods and Services, Industrial Manufacturing sectors globally
Published	2026-06-10
Discovery Source	Gemini

Executive Summary

Ransomware activity surged 48% year-over-year in May 2026, reaching its highest recorded growth rate, even as overall cyberattack volumes declined slightly. The pattern is consistent with post-disruption ecosystem reorganization: when law enforcement dismantles established groups like LockBit and ALPHV/BlackCat, new actors fill the vacuum faster than defenses adapt. Business services, consumer goods, and industrial manufacturing bore the heaviest targeting, and the expanding adoption of generative AI without governance controls is opening new data exposure pathways that most organizations have not yet mapped.

Technical Analysis

The May 2026 data presents a counterintuitive picture: total cyberattack volume declined marginally while ransomware specifically accelerated to a 48% year-over-year growth rate, its steepest on record. This divergence is analytically significant. It suggests the threat ecosystem is not shrinking, it is consolidating around higher-value, higher-impact operations. The pattern mirrors what researchers documented after Operation Cronos (LockBit takedown, February 2024) and the ALPHV/BlackCat exit-scam collapse (March 2024): affiliate networks do not dissolve. They fragment, rebrand, and reconstitute under new banners, often within weeks.

The MITRE ATT&CK techniques associated with this reporting period, T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), T1489 (Service Stop), T1566 (Phishing), T1078 (Valid Accounts), and T1657 (Financial Theft), describe a mature, operationally disciplined attack chain. Phishing and valid account abuse (T1566, T1078) remain the dominant initial access vectors, consistent with findings across VikingCloud's 2026 ransomware statistics reporting and IndustrialCyber's analysis of 2025 critical sector targeting trends. Once inside, operators disable recovery mechanisms (T1490), stop security services (T1489), encrypt data (T1486), and in some campaigns extract funds directly (T1657), layering extortion pressure.

Industrial manufacturing's position as a primary target is not incidental. The sector's combination of legacy OT/IT convergence, high operational disruption costs, and historically underfunded security programs makes it structurally attractive to ransomware operators who model expected ransom payment probability before deployment. Business services firms present a different value proposition: they hold data on multiple downstream clients, creating compounding extortion leverage.

The generative AI governance gap noted in the source data adds a vector that does not yet appear in most organizations' threat models. Employees using AI tools without data classification controls are inadvertently exfiltrating sensitive business data into third-party model training pipelines, not through malicious action, but through the absence of policy. This is a slow-moving exposure that ransomware groups are beginning to monitor for intelligence value ahead of campaigns.

Source quality for this story is T3 (VikingCloud industry report, IndustrialCyber analysis, Eye Security, DataGuard). Primary source verification is recommended before using specific statistics in external communications.

Action Checklist

1. Step 1: Assess sector exposure, determine if your organization operates in business services, consumer goods and services, or industrial manufacturing, as these sectors recorded the heaviest ransomware targeting in May 2026. Map OT/IT convergence points in manufacturing environments specifically.
2. Step 2: Audit initial access controls against T1566 and T1078, verify phishing-resistant MFA is enforced on all externally exposed applications (CIS 6.3), remote network access (CIS 6.4), and administrative accounts (CIS 6.5). Review dormant and shared accounts for immediate disablement (CIS 5.3).
3. Step 3: Validate backup integrity and recovery inhibition defenses. T1490 (Inhibit System Recovery) is a consistent ransomware precursor. Confirm offline or immutable backup copies exist, backup restoration procedures are tested monthly, and shadow copy deletion is alerted on. Monitor for vssadmin.exe delete shadows and wmic shadowcopy delete commands. Reference NIST CP-9 (Information System Backup) and CIS 11.5 (Protect Backup Information).
4. Step 4: Audit generative AI tool usage and data governance. Inventory which AI tools employees are using, classify what data categories are being submitted, and enforce data handling policies. This is an uncontrolled data exposure vector. Reference NIST AC-2 (Account Management) and AC-4 (Information Flow Enforcement) for policy framing, specifically for controlling what data types can be submitted to external AI services and ensuring audit logging (AU-2) of such submissions.
5. Step 5: Update threat model for post-disruption actor fragmentation. Incorporate the behavioral pattern of LockBit/ALPHV successor groups into your threat register. Hunt for T1078 (valid account abuse) and T1566 (phishing) as leading indicators. Review AU-6 (Audit Record Review, Analysis, and Reporting) cadence to ensure logs are actively reviewed, not just collected.
6. Step 6: Communicate sector-specific risk to leadership. Brief executives on ransomware's 48% YoY growth with sector-specific context. Distinguish between overall attack volume (declining) and ransomware frequency (surging) to prevent leadership from misreading the threat landscape as improving.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if any indicators of active T1078 abuse (dormant account authentication, impossible travel logins) or T1490 precursor activity (VSS deletion commands, backup service tampering) are detected, or if the organization operates in business services, consumer goods, or industrial manufacturing and has confirmed gaps in phishing-resistant MFA on externally exposed systems, as these conditions together represent active ransomware precursor exposure requiring incident declaration under NIST 800-61r3 §3.2 criteria and may trigger breach notification obligations if PII or PHI is within the ransomware blast radius.
Recovery Notes	Following any ransomware containment in these sectors, do not restore systems directly from backups without first verifying backup integrity against T1490 activity — check backup server event logs for VSS and catalog deletion events within the 30 days preceding the incident before trusting any backup set. Monitor restored systems for 30 days post-recovery with enhanced logging on Event ID 4624, 4648, and Sysmon EventID 3 (Network Connection) for outbound connections to newly registered domains, as LockBit/ALPHV successor groups are known to maintain persistent access through secondary implants that survive initial eradication. For OT/IT convergence environments in manufacturing, validate OT process integrity independently through engineering team sign-off before resuming production, as ransomware-induced configuration changes to HMIs or PLCs may not be visible in IT-centric forensic artifacts.
Forensic Artifacts	Windows Security Event Log on domain controllers: Event IDs 4624, 4625, 4648, 4768, 4769 filtered for service accounts and accounts inactive >30 days — captures T1078 valid account abuse by ransomware affiliates during the initial access and lateral movement phases | VSS and backup infrastructure event logs: Event ID 4663 (Object Access — delete) on backup server volumes and VSS storage paths, plus Event ID 7045 (New Service Installed) on backup servers — captures T1490 Inhibit System Recovery activity that ransomware operators execute before triggering encryption | Mail gateway delivery and click-through logs for the 30-60 days preceding incident discovery: filter for emails with .lnk, .iso, .vhd, .docm, .xlsm attachments and links to domains registered within 30 days — captures T1566 phishing delivery artifacts consistent with Qakbot/IcedID precursor malware used by LockBit-lineage ransomware affiliates | Sysmon EventID 1 (Process Creation) logs on all Windows endpoints filtered for parent-child process chains involving cmd.exe or powershell.exe spawned by Office applications, browser processes, or VPN client processes — captures post-phishing execution chains characteristic of ransomware precursor malware staging | Firewall and proxy egress logs filtered for outbound connections from internal hosts to newly registered domains (WHOIS age <30 days) and connections using non-standard ports over HTTP/HTTPS — captures C2 beaconing and data exfiltration activity that ransomware operators conduct prior to encryption, particularly relevant for double-extortion campaigns by LockBit/ALPHV successor groups targeting business services and manufacturing sector data

Per-Action IR Details

Step 1: Assess sector exposure — determine if your organization operates in business services, consumer goods and services, or industrial manufacturing, as these sectors recorded the heaviest ransomware targeting in May 2026. Map OT/IT convergence points in manufacturing environments specifically.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and understanding the threat environment before an incident occurs

Controls: NIST AC-4 (Information Flow Enforcement) — enforce approved authorizations for controlling information flow between IT and OT network segments at convergence points, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory all enterprise assets including OT/ICS endpoints, HMIs, and engineering workstations that represent IT/OT convergence risk, CIS 3.2 (Establish and Maintain a Data Inventory) — classify sensitive data processed in business services and manufacturing workflows to understand ransomware blast radius

Compensating: For a 2-person team: run `nmap -sn 10.x.x.0/24` against suspected OT subnet ranges to enumerate live hosts not in your asset register; cross-reference against your known IT asset list to identify undocumented convergence points. On Windows engineering workstations, run `Get-NetIPConfiguration | Select InterfaceAlias, IPAddress` and compare interface counts — dual-homed systems with both IT and OT NICs are your highest-priority convergence risks. Document findings in a flat spreadsheet with columns: hostname, IT_IP, OT_IP, function, criticality.

Evidence: Before remediating OT exposure, capture current network topology evidence: export firewall rules and NAT tables from your IT/OT boundary firewall, capture a 10-minute Wireshark pcap on the IT side of the OT DMZ filtering for Modbus (TCP/502), DNP3 (TCP/20000), or EtherNet/IP (TCP/44818) traffic originating from IT-side hosts — any such traffic indicates uncontrolled IT-to-OT flow that a ransomware actor could exploit for lateral movement into industrial systems. Preserve this pcap as baseline evidence of the pre-remediation exposure state.

Step 2: Audit initial access controls against T1566 and T1078 — verify phishing-resistant MFA is enforced on all externally exposed applications (CIS 6.3), remote network access (CIS 6.4), and administrative accounts (CIS 6.5). Review dormant and shared accounts for immediate disablement (CIS 5.3).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Hardening access controls to reduce the attack surface exploited by ransomware initial access vectors T1566 and T1078

Controls: NIST AC-2 (Account Management) — review and remediate dormant, shared, and service accounts used as T1078 valid-account footholds by LockBit/ALPHV successor groups, NIST AC-7 (Unsuccessful Logon Attempts) — enforce lockout thresholds to limit credential-stuffing and brute-force attempts against externally exposed applications and VPN endpoints, NIST AC-17 (Remote Access) — establish and enforce configuration requirements for all remote access methods including VPN, RDP gateways, and remote management platforms, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce phishing-resistant MFA on all externally exposed applications, CIS 6.4 (Require MFA for Remote Network Access) — require MFA for all remote network access including VPN and jump servers, CIS 6.5 (Require MFA for Administrative Access) — require MFA for all administrative access accounts on all enterprise assets, CIS 5.3 (Disable Dormant Accounts) — delete or disable accounts inactive for 45 days to eliminate T1078 valid-account abuse opportunities, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — prevent ransomware operators from leveraging shared admin credentials for lateral movement

Compensating: Query Active Directory for dormant accounts using PowerShell: `Search-ADAccount -AccountInactive -TimeSpan 45 -UsersOnly | Select Name, LastLogonDate, Enabled | Export-Csv dormant_accounts.csv`. For shared/service accounts: `Get-ADUser -Filter {ServicePrincipalName -ne '$null'} | Select Name, SamAccountName, Enabled`. Review VPN and RDP gateway logs for accounts authenticating without MFA by filtering on authentication method fields — in Windows Event Log, query Event ID 4624 (Logon) with LogonType 3 or 10 and cross-reference against your MFA-enrolled user list. Flag any gap as an active T1078 exposure.

Evidence: Before disabling any accounts, export the full AD account audit trail: run `Get-ADUser -Filter * -Properties LastLogonDate, PasswordLastSet, MemberOf | Export-Csv ad_snapshot_$(Get-Date -Format yyyyMMdd).csv` to capture the pre-remediation state. For T1566 phishing evidence, pull the last 30 days of mail gateway logs filtering on attachments with extensions .lnk, .iso, .vhd, .docm, and .xlsm — these are the delivery mechanisms most associated with ransomware precursor malware (Qakbot, IcedID) used by LockBit-lineage actors. Preserve before any account changes so you can reconstruct whether any dormant account was already abused.

Step 3: Validate backup integrity and recovery inhibition defenses — T1490 (Inhibit System Recovery) is a consistent ransomware precursor. Confirm offline or immutable backup copies exist, backup restoration procedures are tested, and shadow copy deletion is alerted on. Reference NIST CP controls and CIS 11 (no mapped control in this knowledge base for CP family — verify against NIST SP 800-53 Rev. 5 directly).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Ensuring recovery capability is intact before ransomware actors execute T1490 to inhibit system recovery

Controls: NIST AU-9 (Protection Of Audit Information) — protect backup integrity logs and audit records from deletion or tampering by ransomware operators who routinely target logging infrastructure prior to encryption

Compensating: Deploy a Sysmon rule to alert on T1490 precursor activity: configure Sysmon EventID 1 (Process Creation) to log execution of `vssadmin.exe delete shadows`, `wmic.exe shadowcopy delete`, `bcdedit.exe /set recoveryenabled no`, and `wbadmin.exe delete catalog`. Export the Sigma rule `win_susp_vssadmin_delete_shadows` from the SigmaHQ repository and convert it for your log source using `sigma convert`. For offline backup validation without enterprise tooling, mount the most recent backup in an isolated VM and verify at minimum three critical system restores complete successfully; document restore time per system as your RTO baseline. Use `robocopy` with `/MIR /LOG` to verify backup completeness against a known file manifest.

Evidence: Before testing backups, first verify they have not already been compromised: check Windows Event Log on backup servers for Event ID 4663 (Object Access — file delete) targeting backup catalog paths and VSS storage volumes. Query: `Get-WinEvent -LogName Security | Where {$_.Id -eq 4663 -and $_.Message -match 'vss|backup|shadow'}`. Also check for Event ID 7045 (New Service Installed) on backup servers within the last 30 days — ransomware affiliates frequently install malicious services on backup infrastructure before triggering encryption. Capture these logs before running any restoration tests so the baseline state is preserved.

Step 4: Audit generative AI tool usage and data governance — inventory which AI tools employees are using, classify what data categories are being submitted, and enforce data handling policies. This is an uncontrolled data exposure vector. Reference NIST AC-4 (Information Flow Enforcement) for policy framing.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing data governance controls to prevent sensitive data exfiltration via generative AI tools before ransomware actors or insider threats exploit this uncontrolled channel

Controls: NIST AC-4 (Information Flow Enforcement) — enforce approved authorizations for controlling the flow of sensitive organizational data to external generative AI services, treating these as untrusted external systems, NIST AC-20 (Use Of External Systems) — establish terms and conditions governing employee use of external generative AI platforms that process organizational data, NIST AC-22 (Publicly Accessible Content) — designate who is authorized to submit organizational content to external AI services and train them on what categories of data are prohibited, CIS 3.2 (Establish and Maintain a Data Inventory) — classify data categories being submitted to AI tools; you cannot enforce what you have not inventoried, CIS 3.3 (Configure Data Access Control Lists) — apply need-to-know access controls to sensitive data repositories to limit what employees can extract and submit to external AI services

Compensating: For a 2-person team without a DLP solution: use DNS-layer blocking (Pi-hole or firewall FQDN blocking) to restrict access to non-approved AI platforms by maintaining a deny list of consumer AI endpoints (e.g., chat.openai.com, claude.ai, gemini.google.com) except for approved enterprise-licensed equivalents. Monitor proxy or firewall logs for HTTP POST requests exceeding 10KB to AI platform domains — large POSTs to these endpoints are a reliable signal of document or data submission. Run a one-time survey via a Google Form or internal ticket asking employees to self-report AI tools in use; cross-reference responses against your firewall egress logs to identify undisclosed usage.

Evidence: Pull 90 days of firewall or proxy egress logs and filter for HTTPS connections to known generative AI service domains with POST body sizes greater than 5KB — this approximates document upload activity. If your firewall supports SSL inspection, capture SNI fields for connections to *.openai.com, *.anthropic.com, *.google.com/generative*, and comparable endpoints. Document this baseline before enforcing blocks so you can demonstrate scope of prior exposure. For endpoints with browser history accessible via IR, check Chrome/Edge history at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\History` (SQLite) for AI platform visits as corroborating evidence of employee usage patterns.

Step 5: Update threat model for post-disruption actor fragmentation — incorporate the behavioral pattern of LockBit/ALPHV successor groups into your threat register. Hunt for T1078 (valid account abuse) and T1566 (phishing) as leading indicators. Review AU-6 (Audit Record Review, Analysis, and Reporting) cadence to ensure logs are actively reviewed, not just collected.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Integrating current CTI on LockBit/ALPHV successor group TTPs into detection and log review workflows; aligns with DE.AE-07 (CTI integrated into adverse event analysis)

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting) — review and analyze system audit records at a defined frequency for indications of T1078 valid account abuse and T1566 phishing precursors associated with post-LockBit/ALPHV ransomware groups, NIST AU-2 (Event Logging) — identify and ensure logging is enabled for event types relevant to ransomware precursor detection: authentication events, process creation, network connections, and VSS/backup interactions, NIST AU-12 (Audit Record Generation) — ensure audit record generation is active on all systems relevant to ransomware kill chain: VPN gateways, domain controllers, file servers, and backup infrastructure, CIS 8.2 (Collect Audit Logs) — ensure logging is enabled across enterprise assets to support detection of T1078 and T1566 activity patterns used by LockBit/ALPHV successor groups

Compensating: Deploy Sysmon with the SwiftOnSecurity configuration baseline (github.com/SwiftOnSecurity/sysmon-config) as your primary process and network telemetry source. For T1078 hunting without SIEM: run this PowerShell query daily against Security Event Logs on domain controllers — `Get-WinEvent -LogName Security | Where {$_.Id -eq 4624 -and $_.Message -match 'LogonType: 3'} | Group-Object {($_.Message -split 'Account Name:')[1].Split(' ')[0].Trim()} | Sort Count -Descending | Select -First 20` — and flag any service or dormant account in the top 20 authenticators. For T1566 phishing hunting: query mail gateway logs for users who clicked links in emails where the sending domain was registered within the last 30 days (newly registered domains are a consistent indicator in ransomware phishing campaigns).

Evidence: For T1078 hunting, collect: Windows Security Event Log Event ID 4624 (successful logon), 4625 (failed logon), 4648 (logon with explicit credentials), and 4768/4769 (Kerberos TGT/service ticket requests) from domain controllers for the prior 30 days — focus on accounts that were inactive for >30 days before showing authentication activity, as this is a strong indicator of compromised credential reuse by ransomware affiliates. For T1566, collect mail gateway delivery logs, URL click-through logs, and any sandbox detonation reports for the same period. Preserve all logs to immutable storage before initiating threat hunting so the investigation baseline is not contaminated.

Step 6: Communicate sector-specific risk to leadership — brief executives on ransomware's 48% YoY growth with sector-specific context. Distinguish between overall attack volume (declining) and ransomware frequency (surging) to prevent leadership from misreading the threat landscape as improving.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Incorporating threat landscape intelligence into organizational awareness and improving preparedness posture; aligns with GV/ID functions for governance-level risk communication

Controls: NIST AC-1 (Policy And Procedures) — ensure leadership communication results in updated access control policy directives that reflect the current ransomware threat landscape affecting your sector, NIST AU-6 (Audit Record Review, Analysis, And Reporting) — brief leadership on current log review frequency and gaps as part of the ransomware risk communication; executives must understand whether detection capabilities match the threat cadence, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — frame the leadership brief around the organization's documented vulnerability management process and whether its cadence is adequate given 48% YoY ransomware growth, CIS 7.2 (Establish and Maintain a Remediation Process) — present leadership with the current risk-based remediation strategy and any gaps in remediation velocity relative to the threat tempo described in the May 2026 threat data

Compensating: For a 2-person team without a dedicated threat intelligence platform: build a one-page executive brief using publicly available data from CISA Known Exploited Vulnerabilities catalog (cisa.gov/known-exploited-vulnerabilities-catalog), ENISA threat landscape reports, and sector-specific ISAC advisories (e.g., MS-ISAC for state/local, FS-ISAC for financial). Structure the brief around three numbers leadership can act on: (1) 48% YoY ransomware growth rate for May 2026, (2) your organization's sector ranking in targeting frequency, and (3) your current mean time to patch critical vulnerabilities — this frames the gap between threat tempo and your response velocity in terms executives can authorize budget against.

Evidence: Before the leadership brief, compile a pre-brief evidence package documenting your current security posture against the specific gaps this threat exposes: export your current MFA enrollment rate for externally exposed applications, count of dormant accounts pending disablement, and last verified backup restoration test date. This package serves dual purpose — it provides executives with actionable metrics and creates a dated baseline record

(NIST 800-61r3 §4 post-incident documentation standard) that demonstrates due diligence in the event of a subsequent ransomware incident requiring regulatory notification.

Detection Guidance

Prioritize detection engineering around the T1078/T1566 initial access chain and the T1490/T1489 pre-encryption preparation sequence. These are the behavioral signatures that differentiate ransomware intrusions from general commodity malware.

Log sources to verify are active and reviewed (AU-2, AU-6, CIS 8.2):

Authentication logs: Hunt for off-hours logins, logins from new geographies, and successful authentications preceded by multiple failures (AC-7 threshold alerting). Valid account abuse (T1078) frequently presents as normal authentication activity; context and velocity matter more than individual events. Monitor Windows Event ID 4625 (failed login) and 4624 (successful login) for anomalies.

Endpoint telemetry: Alert on deletion of volume shadow copies (vssadmin.exe delete shadows, wmic shadowcopy delete) and disabling of Windows Backup (T1490). Monitor for rapid sequential service stop commands targeting AV, EDR, or backup agents (T1489) using Event ID 4689 (Process Termination). These actions have near-zero legitimate operational use in most environments.

Service control logs: Monitor Windows Event ID 7034 (Service Stopped Unexpectedly) and Event ID 4688 (Process Creation) for commands invoking net stop, sc stop, or taskkill against security services. Rapid sequences of these commands are high-fidelity ransomware precursors.

Email gateway logs: Monitor for phishing indicators consistent with T1566 - newly registered sender domains, mismatched reply-to headers, HTML smuggling attachment patterns. Correlate suspicious emails with subsequent authentication anomalies (T1078).

Data loss prevention / AI tool egress: Audit outbound traffic to known generative AI endpoints (OpenAI, Anthropic, Google AI, etc.). Flag uploads of files containing PII, financial data, or IP classifications. Build detection rules manually against your DLP platform to catch submissions to public AI services.

Privilege escalation indicators: Lateral movement following initial access often exploits misconfigured local admin rights. Conduct regular audits of local admin group membership (CIS 5.4, NIST AC-2) and user account permissions (CIS 5.3, NIST AC-6) to surface overprivileged accounts before attackers do.

For organizations in industrial manufacturing: Monitor for anomalous IT-to-OT traffic flows and any attempts to enumerate or access historian servers, HMIs, or engineering workstations from IT network segments. Alert on unexpected connections to port 102 (S7comm) or port 20000 (Siemens S7Plus) from non-engineering workstations.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to VikingCloud 2026 Ransomware Statistics Report for published indicators`	VikingCloud's report references campaign-specific indicators associated with active ransomware groups; actual hash, domain, and IP values are not available in the provided source text	LOW

Framework Mappings

MITRE-ATTACK

- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft
- **T1489** — Service Stop
- **T1566** — Phishing
- **T1078** — Valid Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1490	Inhibit System Recovery	Impact

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact
T1489	Service Stop	Impact
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Half of 2025 ransomware attacks hit critical sectors as manufacturing ...	https://industrialcyber.co/reports/half-of-2025-ransomware-attacks-...	T3
Top 5 Cyber Threats Manufacturers Face in 2025 - Eye Security	https://www.eye.security/blog/top-cyber-threats-manufacturers-face-...	T3
46 Ransomware Statistics and Trends Report 2026 - VikingCloud	https://www.vikingcloud.com/blog/ransomware-statistics	T3
Security Breach: The Industrial Sector's New Battlefield - YouTube	https://www.youtube.com/watch?v=7IULgk_fOf8	T3
How to face top 10 cyber threats to manufacturing industry	https://www.dataguard.com/blog/top-10-cyber-threats-to-manufacturin...	T3

Generated 2026-06-10 07:24 UTC by TJS Security Command Center