INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:35 UTC

Ransomware Attack Preparation and Response Guidance

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0010
Type	Security Analysis
Severity	HIGH
Affected Products	Organizations of all sizes and sectors; no specific product or version, general enterprise IT environments
Published	Jan 16, 2026
Discovery Source	Rss

Executive Summary

Ransomware remains one of the highest-impact threat categories facing organizations across every sector, combining operational disruption, data loss, and financial extortion into a single attack chain. Threat actors have refined double-extortion tactics, pairing encryption with data theft to pressure victims even when backups exist. For boards and CISOs, the strategic signal is clear: preparation gaps, not just detection gaps, determine whether an organization survives an attack intact.

Technical Analysis

Ransomware attacks follow a consistent lifecycle documented across CISA and FBI guidance, though execution details vary by threat actor and target environment. Initial access typically arrives through phishing (T1566), exploitation of external remote services such as VPN or RDP (T1133), or abuse of valid credentials obtained through prior compromise or purchase (T1078). Once inside, adversaries conduct file and directory discovery (T1083) and collect data from local systems (T1005) before moving laterally through remote services (T1021) to maximize encryption scope. Exfiltration over command-and-control channels (T1041) precedes or accompanies encryption, enabling double-extortion leverage. The ransomware payload then inhibits system recovery by deleting shadow copies and disabling backup mechanisms (T1490) before encrypting files (T1486) and stopping critical services (T1489). The defensive gaps most consistently exploited align with CWE-306 (missing authentication on critical functions), CWE-732 and CWE-276 (incorrect permission assignments that allow lateral movement and privilege escalation), and CWE-693 (protection mechanism failures such as disabled endpoint detection or incomplete network segmentation). CISA and FBI guidance published through the StopRansomware initiative emphasizes that organizations lacking offline, tested, and immutable backups face the highest recovery risk. Network segmentation failures allow attackers to reach backup infrastructure,

eliminating recovery options entirely. The FBI explicitly advises against ransom payment, noting that payment funds further criminal operations and does not guarantee decryption. Industry implications are significant for critical infrastructure sectors, where operational technology environments introduce recovery complexity that IT-only playbooks do not address.

Action Checklist

1. Step 1: Assess backup posture, verify that backups are offline or air-gapped, encrypted, and tested for restoration within the last 30 days; confirm backup systems are isolated from domain credentials.
2. Step 2: Audit external attack surface, enumerate all internet-facing remote services (VPN, RDP, Citrix); verify MFA is enforced and apply patch management to close known vulnerabilities aligned with CISA KEV entries.
3. Step 3: Validate network segmentation, confirm that backup infrastructure, domain controllers, and operational technology networks are segmented from general user environments; test segmentation controls, not just documentation.
4. Step 4: Review and exercise the incident response plan, ensure the plan includes ransomware-specific playbooks covering isolation procedures, law enforcement notification (FBI IC3, CISA 1-888-282-0870), and legal/communications escalation paths; run a tabletop exercise if the plan has not been tested in the past year.
5. Step 5: Communicate ransomware risk to leadership, brief the board and senior leadership on recovery time objectives against current backup posture, cyber insurance coverage terms related to ransomware, and the organizational position on ransom payment aligned with FBI and CISA guidance.
6. Step 6: Monitor for precursor activity, deploy detection rules for credential abuse, shadow copy deletion, and lateral movement via remote services; review EDR and SIEM coverage against the MITRE ATT&CK techniques documented in this item.
7. Step 7: Train employees on phishing recognition, conduct phishing simulation exercises and ensure security awareness training addresses current lure themes; phishing remains a primary initial access vector per FBI reporting.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO/Board immediately if any step reveals critical gaps: offline backups not tested in >30 days, internet-facing services without MFA, no incident response plan with ransomware playbook, or EDR/SIEM monitoring absent entirely; escalate to external IR firm if detected precursor activity matches MITRE ATT&CK ransomware techniques during deployment of Step 6 monitoring.
Recovery Notes	Post-containment recovery follows NIST 800-61r3 §3.4 (Recovery): (1) Validate all systems for integrity before restore using cryptographic checksums or forensic hashing (MD5/SHA-256 of system binaries against manufacturer/vendor baselines); (2) Restore from offline backup in air-gapped environment, verify data integrity, then reconnect to network only after malware scanning and vulnerability remediation; (3) Conduct post-incident review within 72 hours to document attack chain, detection gaps, and control failures—update IR playbook and Step 6 detection rules based on findings.

Forensic Artifacts	Windows Event Log 4688 (Process Creation): command line, parent process, execution context—key for detecting ransomware process chain and lateral movement via RDP/PSexec | Windows Event Log 1024 (RDP Session): source IP, logon success/failure, duration—establishes attacker access timeline and initial compromise vector | Sysmon Event ID 19 (WmiEvent Create) + Event ID 20 (WmiEvent Executed): captures wmic shadowcopy delete and disk wipe commands with timestamp and context | MFT ($MFT) and USN Journal ($UsnJrnl): timestamps and file operations showing encryption/deletion patterns; critical for timeline reconstruction and identifying files encrypted before backup was triggered | $RECYCLE.BIN and Volume Shadow Copies: evidence of deletion/recovery attempts; compare with baseline shadow copy count from Step 1 | RDP Bitmap Cache and .rdp connection history (%APPDATA%\Microsoft\Terminal Server Client): evidence of attacker RDP usage post-compromise | Prefetch files (C:\Windows\Prefetch*.pf): execution timeline for malware loader, lateral movement tools, and credential theft utilities | Firewall and IDS logs (Windows Firewall, pfSense, IDS alerts): outbound connections to C2, data exfiltration patterns, lateral movement traffic anomalies | Email gateway logs and message tracking: phishing email metadata (sender, headers, attachment hashes, delivery time) for initial access vector confirmation

Per-Action IR Details

Step 1: Assess backup posture, verify that backups are offline or air-gapped, encrypted, and tested for restoration within the last 30 days; confirm backup systems are isolated from domain credentials.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase); §3.4.5 (Recovery planning)

Controls: NIST CP-9 (Information System Backup), NIST CP-10 (Information System Recovery and Reconstitution), CIS 3.14 (Ensure Separate Storage of Critical Data with Restricted Access)

Compensating: For air-gapped backup verification without enterprise backup software: (1) Document backup media chain-of-custody manually (date, time, administrator, destination); (2) Test restoration on isolated VM monthly using `dd` (Linux) or `Robocopy /VERIFY` (Windows) to validate integrity without touching production; (3) Verify backup encryption at rest using `openssl enc -d` or BitLocker status (`manage-bde -status`); (4) Confirm backup credentials stored in separate password vault (KeePass, Bitwarden) not in domain—audit via `net user` and domain policy review.

Evidence: Before testing: capture current backup job logs (Windows Backup Event Log ID 6008-6009, or third-party backup software logs); document backup system network isolation (screenshot arp -a, ipconfig from backup appliance); capture System Registry HKLM\Software\Microsoft\Windows NT\CurrentVersion for build baseline; photograph physical media location and access logs if tape-based.

Step 2: Audit external attack surface, enumerate all internet-facing remote services (VPN, RDP, Citrix); verify MFA is enforced and apply patch management to close known vulnerabilities aligned with CISA KEV entries.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation); NIST 800-53 AC-3 (Access Enforcement)

Controls: NIST IA-2 (Authentication; MFA), NIST IA-5 (Credential Management), NIST SI-2 (Flaw Remediation), CIS 6.1 (Establish and Maintain a Process for Secure Software Development), CIS 4.7 (Enforce MFA)

Compensating: For organizations without vulnerability scanner: (1) Use `nmap --script smb-os-discovery -p 445,3389,443` to enumerate RDP, SMB, HTTPS ports; (2) Cross-reference exposed services against CISA KEV list (JSON download from cisa.gov/known-exploited-vulnerabilities) using grep/PowerShell matching; (3) Verify MFA manually: check VPN/RDP gateway logs for successful 2FA events (Radius/LDAP auth logs); (4) Document all internet-facing services in spreadsheet with owner, patch level, and MFA status; (5) Use free Shodan queries or Censys to confirm external visibility.

Evidence: Before remediation: capture network-layer evidence—pcap of authentication traffic on RDP/VPN ports (wireshark, tcpdump `-i any -w auth.pcap port 3389 or port 443 or port 1194`); export authentication logs from VPN gateway/NPS server (Event Log 6272–successful network policy server auth); document current patch levels via `wmic

qfe list brief` (Windows) or `apt list --installed | grep -E 'openssl|openssh'` (Linux); screenshot RDP security settings via `gpedit.msc` (Policies\Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services).

Step 3: Validate network segmentation, confirm that backup infrastructure, domain controllers, and operational technology networks are segmented from general user environments; test segmentation controls, not just documentation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation); NIST 800-53 SC-7 (Boundary Protection)

Controls: NIST SC-7(3) (Access Points), NIST SC-7(8) (Wireless Access Points), CIS 1.2 (Establish and Maintain a Data Security and Handling Policy), CIS 3.1 (Configure DHCP Dynamic DNS)

Compensating: For teams without advanced firewall management: (1) Create isolation test matrix: from each segment (users, backup, DC, OT), attempt network connectivity to restricted segments using `ping`, `telnet `, and `tracert` (Windows) or `mtr` (Linux); document blocked/allowed traffic; (2) Verify firewall rules in config backup (Cisco ASA `show access-list`, pfSense XML export) against segmentation policy; (3) Deploy static ARP entries on critical infrastructure to prevent ARP spoofing; (4) Create DMZ test VMs to validate ingress/egress restrictions; (5) Use `netstat -an` and `Get-NetFirewallRule` (PowerShell) to verify local firewall rules on each segment.

Evidence: Before testing: capture network topology (visio diagram or command output—`ipconfig /all`, `route print`, `arp -a`); screenshot firewall rules for each segment boundary; log baseline network connectivity baseline (ping/tracert results from each segment to restricted zones); document VLAN configuration (`show vlan brief` on switches); capture running firewall config; backup current routing tables (`route -A inet -e -C` on Linux, `route print` on Windows).

Step 4: Review and exercise the incident response plan, ensure the plan includes ransomware-specific playbooks covering isolation procedures, law enforcement notification (FBI IC3, CISA 1-888-282-0870), and legal/communications escalation paths; run a tabletop exercise if the plan has not been tested in the past year.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation); §3.2 (Detection and Analysis); NIST 800-53 CP-2 (Contingency Planning)

Controls: NIST IR-4 (Incident Handling), NIST CP-4 (Contingency Plan Testing), CIS 17.1 (Maintain and Communicate Incident Response Plan)

Compensating: For organizations without formal IR consultants: (1) Document IR plan in shared document (wiki, SharePoint, PDF); include ransomware-specific decision trees: isolation procedures (which systems disconnect first), law enforcement contact info (FBI field office, CISA, local LEO), legal escalation (in-house counsel, insurance broker, PR firm); (2) Conduct tabletop using role-play scenario—assign IR lead, comms, technical, legal roles; simulate timeline of events (detection → analysis → containment → law enforcement call) without executing actual isolation; (3) Record decisions, timings, and communication gaps in post-exercise report; (4) Create checklist cards for desk-side IR leads with IC3 reporting steps, contact tree, and initial data preservation tasks.

Evidence: Before tabletop: photograph current IR plan document version and last review date; document IR team roster (names, roles, on-call numbers); capture baseline response times (how long to assemble IR team per communication plan); screenshot current alert/escalation thresholds in monitoring systems; document law enforcement pre-coordination status (does FBI have pre-arranged contact, has CISA been notified of organizational criticality status).

Step 5: Communicate ransomware risk to leadership, brief the board and senior leadership on recovery time objectives against current backup posture, cyber insurance coverage terms related to ransomware, and the organizational position on ransom payment aligned with FBI and CISA guidance.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation); NIST 800-53 SI-12 (Information Handling and Retention)

Controls: NIST IA-1 (System and Communications Protection Policy), NIST IR-1 (Incident Response Policy), CIS 19.1 (Establish and Maintain a Cybersecurity Governance Program)

Compensating: For organizations without dedicated risk communication staff: (1) Create one-page board brief: current RTO/RPO against backup testing data (from Step 1), cyber insurance policy terms (coverage limits, ransom payment exclusions, notification requirements), and documented organizational stance on ransom (aligned with OFAC/Treasury guidance on ransomware sanctions); (2) Quantify impact: map RTO to revenue loss per hour/day (use financial data from business continuity plan); (3) Schedule quarterly board risk briefing using CISA/FBI ransomware reporting and recent sector-specific attacks as context; (4) Obtain legal review of ransom payment policy to confirm compliance with sanctions regulations.

Evidence: Before briefing: document current backup RTO/RPO from Step 1 testing; export cyber insurance policy declarations page and exclusions; photograph previous ransomware incidents in similar organizations (news articles, CISA alerts); capture board meeting agenda template and attendance records; document any prior board-level ransomware discussions in minutes.

Step 6: Monitor for precursor activity, deploy detection rules for credential abuse, shadow copy deletion, and lateral movement via remote services; review EDR and SIEM coverage against the MITRE ATT&CK techniques documented in this item.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis); NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST AU-12 (Audit Generation), NIST SI-4 (Information System Monitoring), NIST IR-4 (Incident Handling), CIS 8.1 (Establish and Maintain an Endpoint Detection and Response Program)

Compensating: For organizations without EDR/SIEM: (1) Deploy Windows Event Log forwarding (WEF) on all machines to centralized Event Collector; monitor for credential abuse via Event IDs 4625 (failed logon), 4624 (successful logon from unusual location), 4768 (Kerberos AS request); (2) Monitor shadow copy deletion: Sysmon Event ID 19 (WmiEvent: Create) for `wmic shadowcopy delete` or Event Log 104 (Log Cleared) on System log; use `vssadmin list shadows` baseline (run hourly via scheduled task, log output); (3) Monitor lateral movement via RDP: Event ID 4688 (Process Creation) for `mstsc.exe`, Event ID 1024 (RDP Session Logon) in RDP logs; (4) Create detection rules in free tools: Sigma rules (converted to Splunk SPL or Elastic) or osquery queries for process execution and file deletion patterns; (5) Correlate across event logs using simple text-based correlation (Python scripts with Event Log parsing).

Evidence: Before deployment: capture baseline of normal credential usage patterns (export logon history from AD, create whitelist of expected RDP sources); photograph current Event Log retention settings (should be 30+ days minimum); document MITRE ATT&CK techniques for ransomware (T1486 encryption, T1561 disk wipe, T1490 inhibit system recovery); baseline shadow copy status per system (`vssadmin list shadows`); screenshot current antivirus/firewall rule set to identify gaps; export current network baseline (netstat -ano snapshot).

Step 7: Train employees on phishing recognition, conduct phishing simulation exercises and ensure security awareness training addresses current lure themes; phishing remains a primary initial access vector per FBI reporting.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation); NIST 800-53 AT-2 (Security Awareness and Training)

Controls: NIST AT-2 (Security Awareness Training), NIST AT-3 (Role-Based Security Training), CIS 14.7 (Enforce Approved Tools), CIS 17.7 (Conduct Phishing Campaign and Simulation Exercises)

Compensating: For organizations without phishing simulation platform: (1) Create internal phishing campaigns using email templates from FBI/CISA alerts (ransomware-themed, credential-harvesting scenarios); send via internal mail relay with tracking link that logs click and credential submission to shared spreadsheet; (2) Develop training content from NIST/CISA resources (free online modules); require annual training with quiz; (3) Create desk-side reference cards with red flags (urgent language, unusual sender, urgent action requests); post in breakrooms and distribute via email; (4) Track metrics: click rate by department (goal <5%), credential submission rate, and training completion percentage; report to leadership quarterly; (5) Partner with legal to establish reporting process for suspected phishing (create mailbox security@company.com, respond to reporters with thank-you and remediation steps).

Evidence: Before campaign: photograph current email gateway logs (spam filter, URL rewrite logs) to understand baseline phishing volume; document employee email address list and department mapping; capture current threat intel on active phishing campaigns (FBI IC3 reports, CISA advisories); export prior security awareness training completion rates; document any prior phishing incidents in organization (replies, credential submissions).

Detection Guidance

Focus detection on precursor behaviors rather than waiting for encryption events, which represent late-stage compromise. Key hunting priorities based on the MITRE techniques mapped to this item: (1) T1490, alert on vssadmin.exe delete shadows, wmic shadowcopy delete, or bcdedit commands disabling recovery; these are near-universal ransomware pre-encryption actions and rarely occur in legitimate workflows. (2) T1133 / T1078, monitor authentication logs for off-hours VPN and RDP logins, impossible travel events, and accounts authenticating from new geographic locations or devices; correlate with recent credential exposure via threat intelligence feeds. (3) T1021, hunt for lateral movement via SMB, WMI, and PsExec-style execution originating from workstations rather than servers; flag service account usage in interactive sessions. (4) T1486, file system telemetry showing mass file rename operations with new extensions across multiple directories in short timeframes is a late-stage encryption indicator; endpoint protection platforms should alert on this pattern. (5) T1041, review proxy and DNS logs for large outbound transfers to unfamiliar destinations, particularly in the hours preceding any encryption event, indicating exfiltration for double-extortion leverage. Log sources to prioritize: Windows Security Event Logs (Event IDs 4624, 4625, 4648, 4688), PowerShell ScriptBlock logging, EDR process telemetry, VPN authentication logs, and backup system access logs. CISA's StopRansomware advisories provide threat-actor-specific IOC sets worth cross-referencing against your environment periodically.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1005** — Data from Local System
- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery
- **T1489** — Service Stop
- **T1566** — Phishing
- **T1021** — Remote Services
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1490** — Inhibit System Recovery

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3**
- **3.3**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1005	Data from Local System	Collection
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1489	Service Stop	Impact
T1566	Phishing	Initial-Access
T1021	Remote Services	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Nysba	https://nysba.org/how-to-prepare-and-respond-to-ransomware-attacks/	T3
Ransomware - FBI	https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-fra...	T1
What is Ransomware Response and Recovery? - Palo Alto Networks	https://www.paloaltonetworks.com/cyberpedia/ransomware-response-and...	T3
How to Prepare and Respond to Ransomware Attacks	https://nysba.org/how-to-prepare-and-respond-to-ransomware-attacks/...	T3
I've Been Hit By Ransomware! - CISA	https://www.cisa.gov/stopransomware/ive-been-hit-ransomware	T1

Generated 2026-03-29 18:35 UTC by TJS Security Command Center