Ransomware Response Checklist

Step-by-Step Procedures for Detection, Containment, and Recovery

A risk management resource from **First Underwriters Insurance Brokers**

■ **CRITICAL: Ransomware attacks can encrypt your entire network in minutes. The first 60 minutes after detection are the most critical. Print this checklist now and keep physical copies accessible—your digital systems may be unavailable during an active attack.**

Incident Information

Complete this section immediately upon discovering a potential ransomware incident. Accurate timestamps and details are essential for forensic investigation and insurance claims.

Date/Time Discovered: _____

Discovered By: _____

Systems Affected: _____

Ransom Note Found: _____

Ransom Amount (if known): _____

Cryptocurrency Wallet ID: _____

Variant Name (if known): _____

File Extension (encrypted): _____

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

1. Immediate Response — First 15 Minutes

■ TIME-CRITICAL: These actions must happen immediately upon detection. Every minute of delay allows ransomware to spread to additional systems and backups.

Isolation and Containment

- ☐ **Disconnect affected systems from the network** immediately—unplug Ethernet cables and disable Wi-Fi (do NOT power off machines)
- ☐ Disable Wi-Fi access points and VPN connections serving affected network segments
- ☐ **Isolate network segments** by disabling switch ports, VLAN connections, or firewall rules to contain lateral spread
- ☐ Disconnect shared drives, NAS devices, and mapped network storage from all systems
- ☐ Disable remote access services (RDP, VPN, TeamViewer, AnyDesk) across the entire organization
- ☐ Block known malicious IPs and domains at the firewall if indicators of compromise (IOCs) are available
- ☐ **Do NOT shut down or restart affected machines**—volatile memory may contain decryption keys and forensic evidence
- ☐ Isolate backup systems and verify they are not connected to the compromised network

Initial Notifications

- ☐ Alert **IT leadership and the incident response team** (use phone or out-of-band communication—email may be compromised)
- ☐ Notify **executive management** (CEO, CFO, COO) of the incident severity and initial scope
- ☐ Contact your **cyber insurance carrier** immediately—most policies require notification within 24–72 hours
- ☐ Engage your **incident response retainer firm** (if pre-arranged) or request one through your insurer
- ☐ Alert your **legal counsel** to establish attorney-client privilege over incident communications

Insurer Contact Tip: Your cyber insurance policy likely includes access to a 24/7 breach response hotline, pre-approved forensics firms, legal counsel, and negotiation specialists. Contact your insurer BEFORE engaging third-party vendors—unauthorized expenses may not be covered.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

2. Assessment and Scoping — First 1–4 Hours

Once containment measures are in place, assess the full scope of the attack. This information drives every subsequent decision, from recovery strategy to regulatory notifications.

Determine the Blast Radius

- ☐ Identify **all affected systems**: servers, workstations, laptops, mobile devices, cloud instances, and IoT devices
- ☐ Determine which **data and file types** have been encrypted (databases, documents, financial records, customer data)
- ☐ Assess whether **Active Directory or domain controllers** have been compromised (critical for recovery scope)
- ☐ Check if **email systems** (Exchange, Microsoft 365, Google Workspace) are affected or were used as the attack vector
- ☐ Determine whether the attacker has **exfiltrated data**—check for unusual outbound traffic, data staging, or ransom note references to stolen data
- ☐ Inventory which **business-critical applications and services** are offline and estimate operational impact
- ☐ Verify the status of **all backup systems**: on-site, off-site, cloud-based, and air-gapped

Preserve Forensic Evidence

- ☐ Capture **memory images** from affected systems before any changes occur (use tools like FTK Imager or similar)
- ☐ Take **full disk images** of representative affected systems for forensic analysis
- ☐ Preserve all **log files**: firewall, endpoint detection, Active Directory, email gateway, VPN, and authentication logs
- ☐ Screenshot **ransom notes** and any attacker communications—save originals where possible
- ☐ Document the **timeline** of events: when was the first sign of compromise, when was encryption first noticed
- ☐ Preserve all **email headers and attachments** that may have been the initial infection vector
- ☐ Maintain a **written chain-of-custody log** for all evidence collected

> **Evidence Preservation:** Forensic evidence is essential for insurance claims, law enforcement investigation, and understanding how the breach occurred. Failure to preserve evidence may jeopardize your insurance claim or limit law enforcement's ability to help.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

3. Communication and Notification — First 24 Hours

Controlled, accurate communication is critical during a ransomware event. Coordinate all messaging through legal counsel to protect privilege and ensure regulatory compliance.

External Notifications

- ☐ File a report with the **FBI's Internet Crime Complaint Center (IC3)** at ic3.gov and contact your local FBI field office
- ☐ Report the incident to **CISA** (Cybersecurity and Infrastructure Security Agency) at report@cisa.gov or (888) 282-0870
- ☐ Notify your **cyber insurance carrier's claims department** with incident details, scope assessment, and initial timeline
- ☐ Engage **external legal counsel** experienced in data breach and cyber incident response
- ☐ Assess **regulatory notification obligations**: state breach notification laws, HIPAA, PCI-DSS, SEC, GDPR, or industry-specific requirements
- ☐ If personal data was exposed, prepare **individual notification letters** as required by applicable law (consult legal counsel on timing)
- ☐ Notify **business partners, vendors, and clients** whose data or systems may be affected

Internal Communications

- ☐ Establish a **secure out-of-band communication channel** for the incident response team (e.g., personal cell phones, Signal, separate email accounts)
- ☐ Brief all employees on the situation using **approved messaging only**—instruct them not to discuss the incident publicly or on social media
- ☐ Provide employees with **clear instructions**: which systems to avoid, how to report suspicious activity, and where to direct inquiries
- ☐ Designate a single **spokesperson** for any media inquiries—all other staff should decline comment
- ☐ Schedule regular **status briefings** (every 4–8 hours initially) for executive leadership and the incident response team
- ☐ Document all **decisions and actions taken** with timestamps in an incident log

✕ WARNING: Do not publicly disclose the ransomware attack, the ransom amount, or your decision-making process without guidance from legal counsel. Premature disclosure can complicate negotiations, trigger regulatory scrutiny, and affect insurance coverage.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

4. Evaluating the Ransom Decision

The decision to pay or not pay a ransom is complex and should involve executive leadership, legal counsel, your cyber insurer, and law enforcement. Consider these factors carefully.

- ☐ Assess whether **viable backups exist** that can restore operations without paying the ransom
- ☐ Determine the **total cost of downtime** vs. the ransom demand (include lost revenue, overtime labor, customer impact, and reputational damage)
- ☐ Verify whether the attacker has **exfiltrated data**—payment may not prevent them from publishing or selling stolen information
- ☐ Consult legal counsel on **OFAC sanctions compliance**—paying ransoms to sanctioned entities or countries is illegal under U.S. law
- ☐ Check if the ransomware variant has **known decryption tools available** (see nomoreransom.org for free decryptors)
- ☐ Assess the **attacker's credibility**—have they provided proof of decryption capability on sample files?
- ☐ Confirm your **cyber insurance policy covers ransom payments** and understand any sub-limits, deductibles, or pre-approval requirements
- ☐ If payment is considered, engage a **professional ransomware negotiator** (often provided through your cyber insurer)
- ☐ Document the **business justification** for the decision, regardless of outcome, for regulatory and insurance purposes

> **FBI Guidance:** The FBI does not recommend paying ransoms, as payment does not guarantee data recovery, may fund criminal organizations, and encourages future attacks. However, the FBI acknowledges that each organization must evaluate its own risk. Regardless of the payment decision, always report the attack to law enforcement.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

5. Recovery and Restoration

Recovery is a methodical process. Rushing to restore systems without eliminating the threat can result in re-infection. Follow these steps in order to ensure a clean, complete recovery.

Step	Action	Done
1	**Confirm the threat is eliminated**—forensic analysis must verify the attacker's access has been fully removed before any restoration begins	☐
2	**Reset ALL credentials**: Active Directory passwords, service accounts, local admin accounts, API keys, and certificates (assume all are compromised)	☐
3	**Rebuild domain controllers** from clean media if they were compromised—do not restore from potentially tainted backups	☐
4	**Validate backup integrity**—scan backup media for malware before restoring; test restoration on isolated systems first	☐
5	**Restore business-critical systems first**—prioritize based on your business continuity plan (e.g., email, ERP, financial systems, customer-facing services)	☐
6	**Rebuild affected workstations** from clean images—do not attempt to "clean" ransomware from infected machines	☐
7	**Restore data from verified clean backups**—restore incrementally and verify data integrity at each stage	☐
8	**Re-enable network connectivity** in phases—monitor closely for signs of re-infection or persistent threats	☐
9	**Conduct vulnerability scanning** on all restored systems before returning them to production	☐
10	**Verify all systems and data**—confirm applications function correctly, data is intact, and no unauthorized changes remain	☐

Recovery Validation: Before declaring recovery complete, verify that all critical business functions are operational, all data has been restored and validated, all credentials have been rotated, and enhanced monitoring is in place to detect any signs of persistent access.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

6. Post-Incident Security Hardening

After recovery, implement immediate security improvements to prevent re-infection and reduce the risk of future ransomware attacks.

- ☐ Patch all **known vulnerabilities** identified during the forensic investigation, including the initial attack vector
- ☐ Implement or strengthen **multi-factor authentication (MFA)** on all remote access, email, VPN, and privileged accounts
- ☐ Disable **Remote Desktop Protocol (RDP)** on all internet-facing systems or restrict it behind VPN with MFA
- ☐ Deploy or upgrade **Endpoint Detection and Response (EDR)** tools across all endpoints and servers
- ☐ Implement **network segmentation** to limit lateral movement—separate critical systems from general user networks
- ☐ Review and tighten **Active Directory permissions**—remove unnecessary admin rights and enforce least-privilege access
- ☐ Implement **application whitelisting** or allowlisting on critical servers to prevent unauthorized software execution
- ☐ Enable **PowerShell logging and script block logging** for improved detection of living-off-the-land attacks
- ☐ Verify **backup procedures**: confirm 3-2-1 rule compliance (3 copies, 2 media types, 1 off-site/air-gapped) and test restoration regularly
- ☐ Update **email security**: implement DMARC enforcement, advanced threat protection, and attachment sandboxing

7. Post-Incident Review and Documentation

A thorough post-incident review improves your resilience against future attacks and fulfills insurance and regulatory documentation requirements.

- ☐ Conduct a **formal post-incident review** (lessons learned) with all stakeholders within 30 days of recovery
- ☐ Prepare a comprehensive **incident report** documenting the timeline, root cause, scope, business impact, and response actions taken
- ☐ Calculate **total incident costs**: forensic investigation, legal fees, notification expenses, ransom payment (if any), business interruption losses, overtime labor, hardware/software replacement, and regulatory fines
- ☐ File all documentation required for your **cyber insurance claim**—work closely with your broker and adjuster to maximize coverage
- ☐ Update your **incident response plan** based on lessons learned—address gaps in detection, containment, communication, and recovery
- ☐ Revise your **business continuity and disaster recovery plans** to reflect new procedures
- ☐ Schedule **employee security awareness training** focused on the attack vector used in this incident
- ☐ Conduct a **tabletop exercise** within 90 days to validate updated response procedures
- ☐ Review and update **cyber insurance coverage** with your broker—ensure limits, sub-limits, and coverage terms address lessons learned

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.

8. Essential Contacts — Complete Before an Incident

Preparation is key. Complete this section NOW and keep printed copies in multiple locations. During an active ransomware attack, you may not have access to digital records.

Contact	Name / Organization	Phone / Reference
Cyber Insurance Carrier	_____	Policy #: _____
Insurance Broker	_____	24/7 Claims Phone: _____
Incident Response Firm	_____	Retainer #: _____
Legal Counsel (Cyber)	_____	Direct Phone: _____
FBI Field Office	_____	Phone: _____
IT Leadership / CISO	_____	Cell Phone: _____
CEO / Executive Sponsor	_____	Cell Phone: _____
CFO / Finance Lead	_____	Cell Phone: _____
Managed IT Provider	_____	Emergency Line: _____
Backup Vendor / Contact	_____	Support Phone: _____

Protect Your Business with Cyber Insurance

Ransomware attacks cost businesses an average of $4.5 million per incident when accounting for downtime, recovery costs, and reputational damage. A comprehensive cyber insurance policy from First Underwriters provides financial protection including ransom payment coverage, business interruption, forensic investigation costs, legal and regulatory expenses, notification costs, and access to expert incident response teams.

Contact First Underwriters Insurance Brokers
Phone: (425) 242-5357
Web: www.firstunderwriters.com
Email: info@firstunderwriters.com

This checklist is provided as a risk management resource by First Underwriters Insurance Brokers and is intended as a companion to our article *Ransomware Defense: Prevention, Detection, and Recovery*. It does not constitute legal or financial advice. Consult with your legal counsel, IT security professionals, and cyber insurance broker to establish ransomware response procedures appropriate for your organization.

This checklist is provided as a risk management resource. It does not constitute legal or financial advice.