OBJECT FIRST

2025

Ransomware Survival Guide

for IT Operations and Security Teams

I. Executive summary

Ransomware is a when, not an if scenario. It is crucial that every IT department, including operations, security, risk management, and even backup, has a detailed understanding of what a ransomware attack looks like, how to prepare for it, and a tested recovery plan. Successful attacks often demand payments in the millions, and with ransomware targeting the backups first, it seeks to ensure that payment, not recovery, is the only way out. With many regions now enforcing regulations and directives about behavior when a cyberattack occurs, businesses can find themselves in a situation where they cannot legally pay the ransom without first consulting with their cybersecurity insurance provider and cooperating with law enforcement leaving them stuck in a state of enforced downtime and no clear path to return to business as usual.

This guide was created to help establish a baseline of expectations for what is required to ensure data resilience and what should be expected when an attack occurs. We encourage readers to compare these recommendations with their existing IT environments and ensure they are ransomware resilient and ready for a well-tested recovery.

II. Understanding ransomware

What is ransomware?

Ransomware is malicious software (malware) designed to block access to a computer system or data. It often encrypts, exfiltrates, or even destroys data until a ransom is paid. Ransomware is a major cybersecurity threat that targets individuals, businesses, and governments, frequently causing significant financial and operational damage.

Types of ransomware

Crypto ransomware

Function: Encrypts files on a victim's device, rendering them inaccessible.

Goal: Victims must pay a ransom to receive a decryption key.

Example: WannaCry, CryptoLocker.

Double extortion ransomware

Function: Encrypts data and also exfiltrates it.

Goal: Attackers threaten to leak sensitive data if the ransom isn't paid, adding pressure.

Example: Maze, REvil.

Locker ransomware

Function: Locks users out of their entire device or operating system.

Goal: Prevents access to any part of the system until a ransom is paid.

Example: Police-themed ransomware that impersonates law enforcement

Ransomware-as-a-Service (RaaS)

Function: A business model where ransomware developers lease their malware to affiliates.

Goal: Enables less technically skilled attackers to launch ransomware attacks.

Example: LockBit, DarkSide.

Ransomware Tactics, Techniques, and Procedures (TTPs)

Ransomware operators employ coordinated steps to infiltrate, spread within, and exploit target environments. These TTPs often align with the MITRE ATT&CK framework (Adversarial Tactics, Techniques, and Common Knowledge), a knowledge base of cyber adversary behavior, based on real-world observations. It categorizes the tactics and techniques attackers use across different stages of a cyberattack, helping organizations detect, respond to, and defend against threats more effectively.

The TTPs include:

1. Initial Access: Attackers typically gain entry through phishing emails containing malicious attachments or links, exploiting exposed Remote Desktop Protocol (RDP) services, or leveraging unpatched software vulnerabilities.

2. Lateral Movement: Once inside, attackers move laterally across the network using tools like PsExec or exploiting Windows Admin Shares to identify and access critical systems

3. Privilege Escalation: To maximize control, attackers escalate privileges using credential dumping tools (e.g., Mimikatz) or exploiting misconfigurations to gain administrative access.

4. Data Exfiltration: In double extortion schemes, sensitive data is exfiltrated before encryption. This data is later used to pressure victims into paying by threatening public exposure.

5. Encryption & Ransom Demand:
Finally, ransomware encrypts files across the network, and a ransom note is delivered. The note often demands payment in cryptocurrency in exchange for a decryption key and/or to prevent data leaks.

III. Preparation and prevention

Organizational readiness

Effective ransomware resilience begins with clear organizational preparedness. This includes defining **roles and responsibilities** across the enterprise. A dedicated **Incident Response Team (IRT)** should be established, comprising IT, security, and operations personnel trained to act swiftly during an incident. Also, ensure you have an offline copy of all critical contact information or connections to individuals via social networks like LinkedIn. In parallel, **decision-makers**—including legal counsel, public relations, and executive leadership—must be prepared to handle communications, regulatory obligations, and strategic decisions.

Organizations should also develop **Ransomware-Specific Playbooks** that outline step-by-step response procedures. Regular **tabletop exercises** simulate real-world attacks, helping teams identify gaps and improve coordination under pressure. Additionally, **Cyber Insurance** should be reviewed to ensure it includes coverage for ransomware-related costs, such as incident response, legal fees, and ransom payments if deemed necessary.

Checklist:

- Define roles and responsibilities
  - Incident Response Team (IRT)
  - Decision-makers (legal, PR, executive)
- Ransomware-specific playbooks and tabletop exercises
- Insurance considerations: incident response time, legal fees, ransom payments

The importance of cyber insurance

Cyber insurance plays a vital role in ransomware resilience by helping organizations manage an attack's financial and operational fallout. It can cover costs such as data recovery, legal fees, business interruption, and even ransom payments—where legally permitted. Beyond financial protection, many policies provide access to expert incident response teams, legal counsel, and forensic investigators, accelerating recovery efforts.

Additionally, insurers often require organizations to meet baseline cybersecurity standards, encouraging better overall security hygiene. While not a replacement for strong defenses, cyber insurance is a strategic complement that enhances preparedness and supports faster, more coordinated recovery.

Infrastructure hardening

A hardened infrastructure significantly reduces the likelihood and impact of ransomware attacks. Following the **Zero Trust Maturity Model** is an absolute requirement to ensure an organization's infrastructure is hardened and resilient. One key Zero Trust principle is **Network Segmentation**—dividing the network into isolated zones—which prevents attackers from moving freely across systems. For example, separating user workstations from critical servers can contain an infection to a limited area.

Another key principle of Zero Trust is enforcing **Least Privilege Access**. This is a foundational element of infrastructure hardening, ensuring that users and systems are granted only the minimum permissions necessary to perform their tasks. This reduces the attack surface and limits the potential damage if an account is compromised, helping to contain ransomware threats and prevent lateral movement across the network.

Implementing **Multi-Factor Authentication (MFA)** and deploying **Endpoint Detection and Response (EDR)** solutions is also essential. These measures limit attacker access and provide early detection of suspicious activity. Organizations must also **secure and monitor Remote Desktop Protocol (RDP)**, **Virtual Private Network (VPN), and third-party access**, as these are common entry points for ransomware actors.

Infrastructure Hardening Checklist:

- Follow Zero Trust Maturity Model guidelines
  - Network segmentation (e.g., flat vs segmented network)
  - Least privilege enforcement
- Multi-factor authentication (MFA)
- Endpoint protection and EDR solutions
- Secure and monitor RDP, VPN, and third-party access

How businesses are responding to ransomware

ESG by Tech Target recently published research on how organizations evaluate their backup and broader data protection environments in the context of the evolving ransomware threat. As ransomware attacks become more sophisticated and increasingly target backup environments, organizations are responding by adopting Zero Trust principles and modern backup techniques, like adopting immutable storage, to reduce the impact of a breach and enable the organization to recover more quickly in the case of an attack.

Read the research to learn more about how organizations are dealing with the threat of ransomware.

Patch management

Timely patching is a frontline defense against ransomware. Organizations should maintain a rigorous patch management program that includes regular updates for operating systems, applications, and firmware. Vulnerability management tools can help prioritize critical patches, while emergency patch rollout procedures ensure rapid response to zero-day threats.

Patch management checklist:

- OS, application, and firmware updates
- Vulnerability management tools
- Emergency patch rollout procedures

Email and user security

Since phishing remains a top ransomware vector, **email and user security** are critical. Implementing **anti-phishing protocols** like SPF, DKIM, and DMARC helps authenticate email sources and reduce spoofing. Advanced **email scanning tools**—including sandboxing and attachment analysis—can detect and block malicious payloads.

Equally important is **security awareness training**. Educating employees on how to recognize phishing attempts and report suspicious activity builds a human firewall that complements technical defenses.

Email and User Security Checklist:

- Anti-phishing tools (SPF/DKIM/DMARC)
- Email scanning (sandboxing, attachment scanning)
- Security awareness training

Backup strategy

A robust **backup strategy** ensures data recovery without paying a ransom. The **3-2-1 rule**—maintaining three copies of data, on two different media types, with one stored offsite or offline—provides resilience against data loss. Regular **test restores** and **backup integrity checks** validate that backups are functional and reliable.

Pairing this working strategy with **Zero Trust Data Resilience (ZTDR) principles** can help ensure that backup data remains recoverable even in a breach, where all secrets are known.

Backup Strategy Checklist:

- 3-2-1 backup rule (3 copies, 2 media types, 1 offsite/offline)
- Test restores and backup integrity validation
- Implement Zero Trust Data Resilience principles in backup infrastructure

Backup Storage with Absolute Immutability

Many vendors will claim to offer immutable backup storage, but few can deliver a backup target that ensures immutability is maintained when all secrets are known. To ensure that backup data is unimpacted by ransomware, ensure that your backup storage meets the requirements of Absolute Immutability. This core concept—and the definition of Absolute Immutability—allows Zero Access to destructive actions. Nobody—even the most privileged admin or attacker with access to backup storage—can modify or delete data.

Practical implementation of Absolute Immutability requires adherence to three core principles:

1. S3 Object Storage:
A fully documented, open standard with native immutability that enables independent penetration testing.

2. Zero Time to Immutability:
Backup data must be immutable the moment it is written.

3. Purpose-Built S3 Target Storage Appliance:
A dedicated target storage appliance segments storage from backup software, and removes the risks associated with DIY backup storage during operations—particularly during setup, updates and maintenance.

IV. Detection and early warning

Early detection is critical to minimizing the impact of ransomware attacks. A proactive approach that combines behavioral monitoring, threat intelligence, and centralized visibility enables organizations to identify and respond to threats before significant damage occurs.

Indicators of Compromise (IOCs)

Recognizing early warning signs of ransomware activity can help security teams act swiftly.

Common IOCs include:

- **Abnormal file access patterns**, such as mass file renaming or encryption.
- **Sudden spikes in CPU or disk usage**, often signaling encryption processes.
- **Outbound connections to known malicious domains or IP addresses**,
- indicating command-and-control (C2) communication.
- **Disabling of antivirus or logging tools**, a tactic used to evade detection.

These anomalies should trigger immediate investigation and containment procedures.

Monitoring & logging

Comprehensive visibility across the IT environment is essential. Organizations should implement:

- **Centralized logging** through a **Security Information and Event Management (SIEM)** system to aggregate and analyze logs in real time.
- **Endpoint and server activity monitoring** to detect suspicious behavior at the device level.
- **Alerts from antivirus, Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR), firewalls, and Intrusion Detection Systems (IDS)** to provide layered detection across the network.

This integrated monitoring approach enables faster detection and coordinated response.

Threat intelligence

Leveraging threat intelligence enhances an organization's ability to anticipate and defend against ransomware campaigns. Best practices include:

- **Integrating external threat intelligence feeds** to stay informed about emerging threats and known ransomware indicators.
- **Maintaining updated blacklists** of malicious IPs, domains, and file hashes
- **Mapping threats to the MITRE ATT&CK framework** helps contextualize attacker behavior and improve detection strategies.

Organizations can build a more adaptive and informed defense posture by combining internal telemetry with external intelligence.

V. Incident Response (IR)

A well-orchestrated incident response (IR) plan is essential for minimizing the damage and recovery time following a ransomware attack. Timely and coordinated actions can prevent further spread, preserve critical evidence, and support legal and regulatory compliance.

Immediate actions (first 0-2 hours)

The first moments of a ransomware incident are critical. Organizations should:

1. **Identify and isolate affected systems** to prevent the ransomware from spreading laterally.
2. **Disconnect compromised devices from the network**, either physically or by disabling switch ports.
3. **Preserve forensic evidence**, including RAM snapshots, disk images, and relevant logs, to support investigation and potential legal action.
4. **Activate the incident response plan** and notify key stakeholders, including IT, legal, executive leadership, and communications teams.

Communication protocol

Transparent and secure communication is vital during a ransomware event:

- Use **secure internal communication channels**—avoid email or chat platforms on potentially compromised networks.
- Prepare an **external communication plan** to inform customers, partners, and regulators as needed
- Engage **legal counsel, public relations, and law enforcement** (e.g., FBI, CISA) early to ensure compliance and manage reputational risk.

Do's and don'ts during an attack

To avoid compromising the investigation or worsening the situation:

- ✓ **Do** preserve all evidence and document actions taken.
- ✗ **Do not** delete files, logs, or other potential evidence.
- ✗ **Do not** power off systems unless advised by IR professionals.
- ✗ **Do not** engage with attackers directly without guidance from legal and incident response experts.

Engage incident response services

If not already in-house, organizations should:

- **Contact a pre-vetted incident response firm** to assist with containment, investigation, and recovery.
- **Notify the cyber insurance provider** immediately, as many policies require prompt reporting to activate coverage and access approved vendors.

VI. Containment and eradication

Once a ransomware attack is detected, swift containment and thorough eradication are essential to prevent further damage and ensure a clean recovery. This phase focuses on isolating the threat, understanding how it entered and spread, and removing it completely from the environment.

Containment strategies

The first step is to **contain the threat** to prevent it from spreading across the network:

Network quarantine: Immediately isolate infected systems from the network to halt lateral movement.

Disable compromised accounts: Lock or reset credentials for any accounts suspected of being used by attackers.

Apply DNS and firewall rules: Block known command-and-control (C2) domains and IP addresses to cut off attacker communication.

These actions help limit the scope of the attack while preserving the environment for investigation.

Root cause analysis

Understanding how the attack occurred is critical to preventing recurrence:

Identify patient zero: Determine the first system or user compromised.

Determine the attack vector: Was the entry point a phishing email, an exposed RDP port, or a software vulnerability?

Map lateral movement paths: Analyze how the attacker navigated through the network to reach critical assets.

This analysis informs both remediation and long-term security improvements.

Eradication techniques

Once containment is achieved and the root cause is understood, the focus shifts to **removing the threat**:

- **Remove all malware artifacts** using trusted antivirus or EDR tools.
- **Reimage systems** where necessary to ensure complete removal of persistent threats.
- **Change all credentials**, especially high-privilege accounts like domain administrators, to prevent re-entry.

These steps ensure the environment is clean and secure before recovery and restoration begin.

VII. Recovery and restoration

System recovery

The recovery phase is where organizations transition from containment to restoration, ensuring systems are brought back online safely and securely.

Follow these steps to ensure a functional recovery:

1. **Prioritize critical systems** to restore essential business functions first.
2. **Verify backup integrity** to ensure data has not been corrupted or compromised.
3. **Identify the last known clean restore point** to avoid reintroducing malware.
4. **Gradually reintroduce systems to the network** to monitor for anomalies and prevent reinfection.

Post-Incident validation

Following system restoration, **post-incident validation** ensures that the threat has been fully eradicated. Activities include:

1. **Confirm full eradication** of ransomware and related malware through comprehensive scanning.
2. **Monitor for reinfection** using endpoint detection tools and network monitoring.
3. **Review logs** for any lingering indicators of compromise or suspicious activity.

Documentation and Reporting

Equally important is **documentation and reporting**. Be sure to keep a detailed record of the following:

1. **Create a detailed incident timeline** outlining key events, decisions, and actions taken.
2. **Fulfill regulatory notification requirements**, if applicable, to maintain compliance with legal and industry standards.

VIII. Post-incident activities

The conclusion of a ransomware incident does not mark the end of the response process. Instead, it initiates a critical phase focused on analysis, improvement, and compliance. Post-incident activities are essential for strengthening organizational resilience, fulfilling legal obligations, and ensuring that lessons learned are translated into actionable improvements.

Forensics and Analysis

A comprehensive **forensic investigation** should be conducted immediately following containment and recovery. This process involves a detailed examination of affected systems, logs, and network activity to determine the full scope of the attack.

The objective is to identify the **initial point of compromise**, the **methods used by the attackers**, and any **security weaknesses or vulnerabilities** that were exploited. These insights are vital for preventing recurrence and for informing both internal stakeholders and external authorities.

Lessons learned and retrospective

A structured **retrospective review** should be held with all relevant stakeholders, including IT, security, legal, communications, and executive leadership. This session—often conducted as a **tabletop exercise**—provides an opportunity to evaluate the effectiveness of the incident response, identify procedural gaps, and assess decision-making under pressure. Based on these findings, organizations should **update their incident response playbooks**, revise security **policies and technical controls**, and implement any necessary changes to tools or workflows. This continuous improvement cycle is essential for building a more robust and agile security posture.

Compliance and legal considerations

In the aftermath of a ransomware incident, organizations must carefully navigate a range of **regulatory and legal obligations**. Depending on the nature of the data affected and the jurisdictions involved, it may be necessary to **report the incident to regulatory bodies** such as those enforcing GDPR, HIPAA, or other industry-specific mandates. Additionally, organizations should conduct a **legal assessment of any ransom payments**, as such actions may have implications under local or international law.

A thorough review of **contracts, insurance policies, and liability exposure** should also be undertaken to ensure that all obligations are met and that future risks are mitigated.

Stakeholder engagement and coordination

Effective post-incident response requires coordination with a range of external partners. Organizations should maintain active relationships with:

- **Incident response firms** for forensic support and remediation guidance.
- **Cyber insurance providers** to ensure coverage is activated and claims are properly documented.
- **Legal counsel** to navigate regulatory requirements and assess legal exposure.
- **Local law enforcement or federal agencies** (e.g., the FBI or CISA) to support investigations and contribute to broader threat intelligence efforts

Conclusion

Ransomware is a matter of when, not if. Every component of the IT organization, from operations and security to risk management and backup administration, must be equipped to recognize, respond to, and recover from an attack. With ransomware actors increasingly targeting backup systems and legal restrictions potentially limiting ransom payments, organizations face the real risk of being left inoperable if they are unprepared.

This guide serves as a practical foundation for building ransomware resilience. It outlines the essential strategies and best practices needed to prepare for, respond to, and recover from an attack. However, resilience is not a one-time achievement—it is an ongoing commitment. We encourage readers to use this guide as a starting point, continuously assess their environments, and stay informed about emerging threats and evolving tactics. By fostering a culture of preparedness and continuous learning, organizations can stay one step ahead of ransomware and safeguard their operations against disruption.

How Object First Can Help

When—not if—ransomware strikes, the future of your business hangs in the balance. In that moment nothing's as critical as getting back up and running as fast as possible, without being hindered by unwanted complexity. Successful recovery depends on how you approach cyber resilience.

That's why we offer secure, simple, and powerful immutable backup storage. When your business, reputation, and career are on the line, Object First is your ultimate defense against ransomware.

With Object First, resilience is a given. We ensure security, reduce the risk of disruption, and enable growth for businesses and people.

To do this, we focus on making resilience as simple as possible. When security is complex, costly and difficult to implement, it's less likely to be effective. It's more error-prone. It's harder to find the right skilled people to manage, and harder to maintain. Ultimately, resilience becomes almost impossible to achieve.

When securing your backup data is simple, when you're fully confident in your last line of defense, then you have the freedom to focus on what really matters—accelerating strategic growth, building your teams, and even spending more time outside of work.

That's why we designed Object First with security and simplicity in mind. We removed the friction and automated the complexity. You don't need to be a Linux or security expert. There's no complex manual integration. No constant, complicated updating. No concern that your backup storage won't scale with your business. No wondering if your data will be secure or if you will recover after an incident.

We're the first and only out-of-the-box immutable backup storage purpose-built for Veeam—so it fits seamlessly into your Veeam environment and performs when it matters most.

Simplicity doesn't come at the expense of security—it strengthens it. Your backup data is absolutely immutable leveraging S3-native object storage and Zero Trust best practices, and security is proven by 3rd party testing. We enforce Zero Access to perform destructive actions: even with the most privileged credentials, no one—neither cybercriminals nor insiders—can alter or delete data. So you don't just hope you're resilient, you know you are.

With Object First, you and your team are ready to lead—focusing on innovation and growth, not troubleshooting your backup storage.

We're the simplest way to get the most out of Veeam. We make enterprise-grade cyber resilience achievable as the ultimate defense against ransomware—with no security expertise required.

Because when resilience is this secure, simple and powerful, you and your organization are Simply Resilient.

Object First. Simply Resilient.

OBJECT FIRST

Simply Resilient for Veeam

Learn More at ObjectFirst.com