veeam

The SMB Guide to Ransomware Recovery

Table of Contents

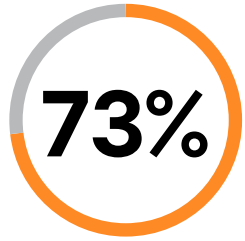
The SMB Guide to Ransomware Recovery

Introduction

Ransomware remains one of the biggest risks for businesses of every size. Attacks happen every day and can bring operations to a standstill within minutes. The costs add up fast — downtime, data loss, reputation damage, and financial penalties.

According to a 2025 Coveware Quarterly Report, **about 73% of organizations impacted by ransomware have fewer than 1,000 employees**, showing that small and midsized businesses face the same — and often greater — risk as large enterprises.

The Veeam 2025 Risk to Resilience Report shows a small but meaningful improvement: **the percentage of companies impacted by at least one ransomware attack that resulted in encryption or data exfiltration declined slightly from 75% to 69% year over year**. That's progress, but it also means nearly seven in ten organizations still faced a successful attack underscoring the need for strong backup and recovery strategies across every business size.



73% of organizations impacted by ransomware have fewer than 1,000 employees

Ransomware impact dropped slightly, from 75% to 69%

The good news?

You can prepare. With the right data protection strategy, recovery can be fast, predictable, and effortless, so you can get back to business with confidence.

What Is Ransomware Recovery

Ransomware recovery is the process of restoring systems and data after an attack. It's about more than decrypting files, it's about getting operations running again quickly, safely, and completely.

Successful ransomware recovery depends on the strength of an organization's backup, data protection, and incident response processes. That means using immutable backups, verified recovery points, and well-tested plans that cover every workload.

For SMBs, the goal is to recover fast and keep your business running.

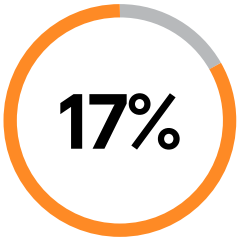
Understanding Ransomware Attacks

Ransomware doesn't discriminate against size or industry. In fact, most victims are small and midsized businesses that attackers see as easier targets with limited resources.

These attacks typically start with phishing emails, malicious downloads, or stolen credentials. Once inside, attackers encrypt critical data, exfiltrate sensitive files, and demand payment to restore access.

The **Veeam 2025 Risk to Resilience Report** shows that paying a ransom doesn't guarantee recovery: **17% of organizations paid but still couldn't recover their data, while nearly one quarter recovered without paying at all.**

Attackers target what matters most — your data. Understanding how ransomware spreads is step one. The next is building a recovery plan that ensures your data can't be held hostage.



17% of organizations paid but still couldn't recover their data

nearly one quarter recovered without paying at all

Best Practices for Ransomware Recovery

There's no shortage of credible guidance on cybersecurity, and it's worth knowing where to find it. Many government agencies and national cybersecurity centers offer valuable documentation, monitoring support, and even direct assistance if your data is found circulating on the dark web.

Instead of just reading those frameworks or blueprints, the following sections focus on real life experience and practical advice drawn from the field.

It's highly recommended that every organization review these regulations and frameworks to protect customer information:

Global Frameworks and Standards

- **NIST Cybersecurity Framework (CSF)** — Strategic risk management framework.
- **NIST SP 800-61** — Incident response playbook.
- **ISO/IEC 27001 and 29100** — International standards for information security and privacy.
- **PCI DSS** — Payment card industry security standard.
- **HIPAA** — U.S. healthcare data protection.
- **GDPR** — EU data protection regulation.
- **MITRE D3FEND Framework** — Defensive techniques mapped to adversary tactics.
- **RE&CT Framework** — Response and countermeasure taxonomy.

Regional and Sector-Specific Frameworks

European Union

- **DORA (Digital Operational Resilience Act)** — Financial sector resilience.
- **NIS2 Directive** — Network and information systems security.

Australia

- **ACSC Essential Eight** — Cybersecurity maturity model.

Japan

- **APPI (Act on the Protection of Personal Information)** — Privacy law.
- **Basic Act on Cybersecurity** — National cybersecurity policy.
- **FSA Cybersecurity Guidelines** — Financial sector guidance.

South Korea

- **PIPA (Personal Information Protection Act)** — Privacy regulation.
- **ISMS Certification** — Mandatory security management system.
- **Electronic Financial Supervisory Regulation** — Financial services cybersecurity.

India

- **Digital Personal Data Protection Act (DPDP), 2023** — Privacy law.
- **CERT-In Guidelines** — Incident reporting and cybersecurity directives.
- **RBI Cybersecurity Framework for Banks** — Financial sector requirements.
- **Information Technology Act, 2000** — Foundational cybersecurity law.

Learning from these frameworks and regulations helps you stay informed, respond faster, and recover smarter when an attack happens.

Under a Ransomware Attack

Once an attack is underway, here's how it typically presents.

The first sign is usually losing access to files or systems — suddenly, you can't open documents, apps crash, or shared drives go blank. In some cases, screens are locked completely.

Other attacks are less obvious. If data is being exfiltrated, everything may appear normal while information is quietly stolen. Only when the ransom note appears, sometimes as a text file among encrypted data, other times as an email, does the full scope become clear.

Whether it's obvious or silent, every ransomware attack follows a pattern. Recognizing it early helps you protect what matters and start recovery sooner.

Immediate Response

After discovering an attack, take a breath, assess the situation, and act deliberately.

Avoid disconnecting systems immediately. Interrupting encryption mid-process can damage files and make recovery harder.

Bring in your internal IT or security team right away. If you don't have in-house expertise, contact a trusted external partner. Notify your legal counsel and, if you have one, your cyber insurance provider as soon as possible.

Maintain secure backups of essential documents, such as your cyber insurance policy, ensuring they are accessible from multiple locations or stored offline to prevent loss in the event of system encryption.

Activate your communication plan. Use predefined channels to keep leadership, employees, and partners informed without spreading panic.

Containment

Once the situation is stabilized, shift your focus to containment by stopping the spread of the attack and preserving evidence.

Mobilize your response team, including forensics specialists if available, and begin collecting all artifacts related to the incident. Gather ransom notes, samples of encrypted files, and any suspicious executables or scripts. These materials will help your team understand what happened and how far the attack has spread.

Stay methodical. Containment is about control, not panic.

Key steps for initial containment include:

- Identify affected systems and data.
- Change all admin passwords immediately.
- Isolate infected endpoints from the network.
- Review your recovery time (RTO) and recovery point (RPO) objectives.
- Communicate internally through secure, pre-defined channels.
- Review your cyber insurance policy and notify your provider if required.

A segmented network and well distributed architecture make it easier to isolate affected systems and keep critical operations running.

Assessment

After containment, the next step is a clear assessment by understanding what was affected, how it happened, and what can be recovered.

Start by identifying what kind of encryption or file changes occurred. In some cases, files may only be renamed, not actually encrypted, which means recovery could be faster than expected.

Attackers range from organized criminal groups to opportunistic individuals using common ransomware kits. Understanding their methods helps estimate the level of damage and the complexity of recovery.

Before beginning any restoration, confirm that your backups are clean and malware-free. Restoring from an infected backup can restart the attack.

Expert support, such as from **Coveware by Veeam**, can help you evaluate artifacts, validate backups, and forecast recovery timelines based on a complete assessment of the evidence.

A structured assessment gives you a clear picture of what is recoverable and what steps to take next.

Negotiation with Threat Actors

Engaging with threat actors doesn't necessarily mean paying a ransom. It can also be an opportunity to gather insight into how the attack occurred. Some threat actors may share details about the vulnerabilities they exploited, which can help guide remediation.

Always assume any communication could become public, so keep it factual and professional. Never share internal or sensitive information.

Even if both parties agree to terms, there's no guarantee that decryption keys will work, or that stolen data will be deleted. Experience and data from **Coveware by Veeam** show that paying a ransom does not ensure recovery, where some groups provide faulty tools or fail to follow through.

Negotiation can take time but use that window to advance your recovery efforts and prepare to restore operations as quickly as possible.

Recovery

When it comes to recovery, having clean backups is essential. It's equally important to evaluate how long the recovery will take. Consider how much downtime your operations can sustain, how much data you can afford to lose, and what resources you have available.

Depending on the situation, some systems may need to be rebuilt. This process could take anywhere from a few days to several weeks.

Document your recovery priorities ahead of time, just as you would in an incident response playbook. Identify which systems and data are most critical to your business. During negotiations or restoration, you may decide to recover only the highest priority assets first while less critical data is recovered later or lost entirely.

It's essential to know what matters most. Determine which assets are critical enough to justify immediate recovery efforts or even decryption costs, because restoring those first will help you bring the rest back online sooner.

Recovery involves many considerations — from time and cost to data importance — but clear priorities and clean backups make the process faster, safer, and more predictable.

Restore Data From Veeam Backups

Once recovery priorities are set, the next step is restoring data using the right tools.

With **Veeam Data Platform**, there's a choice for recovery between restoring to original servers or to isolated clean rooms. This second option provides an opportunity to clean up, verify, and test recovery in an isolated environment.

Veeam Data Platform offers a variety of restoration options to ensure data resilience and recovery across different environments.

Instant VM Recovery

Restore entire virtual machines to different environments such as VMware vSphere, Hyper-V, Azure, and Amazon EC2 from backups in minutes.

Bare Metal Recovery

Restore an entire system from scratch, including the OS, apps, settings, and data, to the same or different hardware.

Storage Snapshots Recovery

Automate data recovery for VMs hosted on storage systems, eliminating intermediate restore and manual operations.

Continuous Data Protection

Disaster recovery solution providing near-continuous replication to minimize data loss for mission-critical workloads.

Instant Database Restore

Quick recovery for SQL and Oracle databases by publishing the database directly from its backup files.

Instant File Share Restore

Publish a point-in-time version of a file share as a read-only SMB (Server Message Block) share, providing immediate access to files without a full restore.

Object Storage Restore

Restore data from object storage backups, including whole buckets or containers, from a specific restore point, and multiple object versions.

Physical Machine Backup Restore

A full restore of the physical machine to its original hardware or new hardware.

Disk Recovery

Recover and export disks from backups.

Item Recovery

Recover VM files, guest OS files and folders, and application items.

File Level Restore

Enable granular recovery of individual files and folders from backups.

Cross Platform Recovery

Support recovery across multiple platforms, including VMware, Hyper-V, AWS, Azure and Google Cloud.

Quick Rollback

Allow fast recovery by restoring only the changed blocks since the last backup.

Cloud Platforms

Provide comprehensive restore options for major public clouds, with specific steps for restoring Amazon EC2 instances and Microsoft Azure VMs.

Orchestration at Scale and Veeam Support

Enable large scale recoveries to be orchestrated for Veeam Data Platform Premium users.

Plus, **Veeam Cyber Secure** can be added to any edition to ensure proactive cyber resilience through expert-led security assessments and prioritized incident response from Coveware, ensuring organizations can protect, prepare, and recover with confidence. These options help ensure recovery is fast, flexible, and verified across all workloads.

Professional Expert Incident Response

During a ransomware event, expert incident response is critical to containing the threat, minimizing disruption, and guiding key decisions.

Digital Forensics and Incident Response (DFIR) experts identify attack vectors, assess the scope of compromise, and restore systems while preserving forensic evidence.

Specialists such as **Coveware by Veeam** conduct a rapid impact assessment to identify affected systems, forecast outcomes, and shape response strategy.

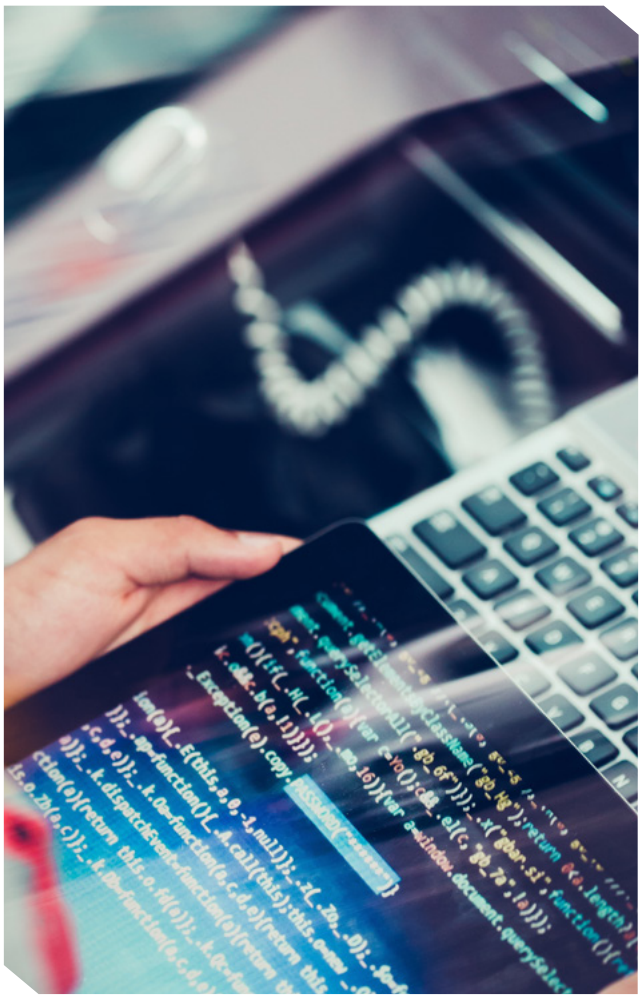
Forensic analysis follows, mapping attack methods, executed actions, and suspicious activity.

Threat actor attribution through **tactics, techniques, and procedures (TTPs)** helps predict escalation, assess data exfiltration, and ensure compliance with sanctions and regulations.

Encryption verification, using **Recon**, tests the integrity of the ransomware and evaluates recovery options such as decryptor availability or exploitable weaknesses before negotiation begins.

Reverse engineering expertise further enhances recovery efforts by validating encryption and assisting with decryption where possible.

Negotiation, when undertaken by professionals, can also yield intelligence that informs restoration and reporting.



An effective ransomware response relies on rapid assessment, forensic precision, and informed collaboration.

By leveraging experience, advanced tooling, and adversary insights, experts help organizations make confident decisions and restore operations with resilience.

Final Thoughts

After experiencing a ransomware attack, it is crucial to document lessons learned.

This process strengthens processes, updates plans, is equally important — through internal sessions, blogs, webinars, or collaboration with cybersecurity organizations — to help others strengthen their defenses.

The cybersecurity landscape offers a wide range of tools to provide multiple layers of protection. Implementing **multifactor authentication (MFA)**, enforcing **least privilege access,** and using modern **security tooling** are essential to preventing attacks. Even if an organization is compromised, these measures can help prevent lateral movement within networks and systems.

Expert assistance makes a difference. Your organization's finances and reputation are at stake, so bring professionals on board when needed.

Finally, regularly test your response plans and backup recovery procedures. Preparedness is the foundation of resilience against future attacks.

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it.

Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam.

Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.