Enterprise Strategy Group by TechTarget

SHOWCASE

JANUARY 2025

Proactive Ransomware Response Plans Play a Vital Role in Ensuring Cyber Resilience

Scott Sinclair, Practice Director, and Todd Thiemann, Senior Analyst

Abstract: Ransomware and other cyber incidents rank among the top threats to business viability and are now poised to become even more potent and prevalent in the age of AI. Achieving optimal resilience requires a combination of people, process, and technology that facilitates preparation before an incident, streamlines investigation, and facilitates rapid recovery. To help combat ransomware threats, Veeam provides a comprehensive approach to cyber resilience that facilitates collaboration before, during, and after incidents while avoiding the "grey areas" between participants that can inhibit a rapid response.

Understanding the Cyber Recovery Conundrum

Ransomware is widely considered a critical business threat, with 65% of enterprises rank it as a top three threat to the viability of their organization.[1] Recent incidents such as Change Healthcare, Colonial Pipeline, and Ascension Health demonstrate the substantial business risk presented by ransomware attacks. Given the high frequency of attempted attacks and the impacts of successful ones, many organizations are left with damages and interrupted operations that go well beyond IT.

Attackers often go beyond valuable data assets by undermining key infrastructure components and exploiting security gaps, including those in the backup infrastructure itself, as the ransomware can often reside dormant for long periods of time to maximize its impact on backups. CIOs, CISOs, IT and security leaders, and their teams must understand that the nature of the threat goes well beyond just data and focus on protecting and further leveraging their backup and recovery infrastructure to remove risk and minimize business impact through advanced capabilities.

According to research from Informa TechTarget's Enterprise Strategy Group, 75% of respondents reported that their organization had been the victim of a ransomware attack within the 12 months leading up to the research study. Of those enterprises that suffered a cyberattack, 37% suffered multiple successful attacks in that timeframe.

Attacks involving ransomware typically have two significant elements: 1) ransomware that encrypts enterprise data and 2) data exfiltration that enables further extortion by threatening to make the data public. Threat actors try to extort their victims in both cases and—frequently—in the same attack.

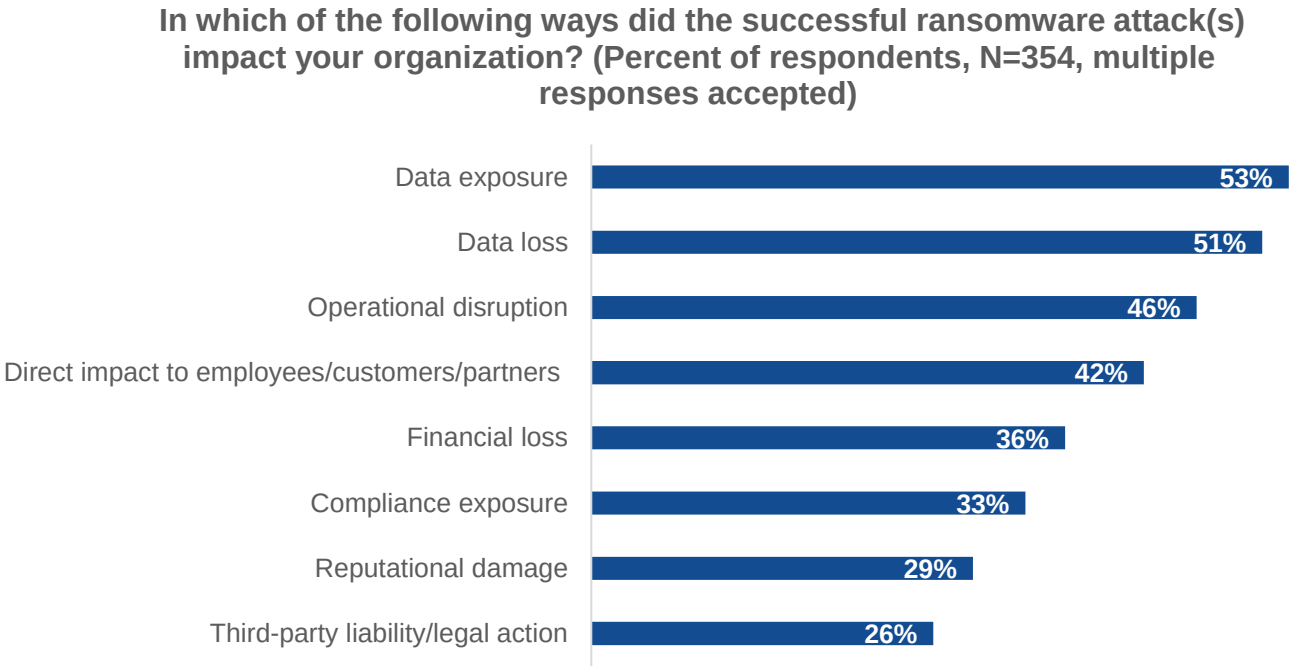
Ransomware has manifold impacts on the organization, with data exposure, data loss, and interrupted operations leading the list alongside compliance risk and the cost of business interruption (see Figure 1).

[1] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023. All Enterprise Strategy Group research references and charts in this showcase are from this report unless otherwise noted.

This Enterprise Strategy Group Showcase was commissioned by Veeam and is distributed under license from TechTarget, Inc.

© 2024 TechTarget, Inc. All Rights Reserved

Figure 1. Ransomware Attacks Hurt Organizations in Multiple Ways



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The recovery time to reach full operations from the point of ransomware attack detection is a key metric that needs to continually be driven down. A prolonged recovery time can lead to financial losses due to operational disruptions and may contribute to lasting reputational damage that can affect a firm's success and market position.

As with many IT challenges, cyber resilience requires a combination of people, process, and technology to ensure optimal recovery. Existing approaches to cyber resilience often fall short in one or more of the following:

- **Inadequate backup and recovery technology.** Backup systems with undetected malware infections can end up reinfecting systems during recovery.
- **Lack of clean rooms** for testing, quarantining data, and facilitating clean recoveries.
- **Lack of ongoing professional services** to maintain and improve the cyber-resilience posture.
- **Lack of communication and collaboration** between IT and security teams and between the enterprise and service providers.
- **Unestablished or inadequately tested combination of people, process, and technology.** Organizations need to implement the right backup and recovery technology by providing immutable backups and by ensuring that the IT and security teams are trained and processes are in place for incident response and rapid recovery.

The weakness or absence of any one element can hinder cyber recovery and lead to lengthy and incomplete recovery. Organizations must address all five if they wish to achieve optimal resilience.

The Veeam Approach to Cyber Resilience

Veeam provides a comprehensive approach to cyber resilience and facilitates collaboration before, during, and after incidents. It also provides best practices to prepare for incidents and ensures that security and IT teams have a common plan and approach.

The Veeam Cyber Secure solution includes the following key elements:

- **Veeam Data Platform** provides the foundation for data protection and data resilience, with all the enterprise data protection for backups and recovery, plus security features including:
  - **Inline malware detection** identifies threats during backup.
  - **Integrations via Incident API and with SIEM tools** help enterprises with visibility to investigate and identify threats earlier. Integrations via API can trigger backups and recovery before the malware appeared.
  - **Backup Immutability** provides secure, encrypted backups that cannot be altered, deleted, or re-encrypted.
- **Onboarding support, including design and implementation services** so Veeam experts can help establish the right foundation, including architectural design and deployment of backup strategy, for the Veeam Data Platform using best practices tailored to a customer's specific needs.
- **24x7 incident response** with a 15-minute service-level agreement that provides continuous ransomware incident response.
- **Negotiation, settlement, and decryption services,** as needed, from experienced negotiators on cyber extortion to help enterprises make informed decisions step by step.
- **Post-incident and insurance documentation** so enterprises can perform a post-mortem to navigate the post-incident process, ensure compliance, and support insurance claims.

The Veeam solution helps users protect their organizations before any attack occurs, quickly respond during an incident, and recover operations promptly following the attack.

Conclusion

As business enters the era of AI, the expectation is that ransomware attacks will become increasingly more frequent and more potent. In recent Enterprise Strategy Group research, IT decision-makers were asked to identify the IT initiatives that have become significantly more important to their organization's future over the past two years. Cybersecurity was the most commonly cited response, with 59% of respondents saying it had become significantly more important, beating the second most common answer, artificial intelligence, data science, and machine learning, which was cited by 44% of respondents.[2] Organizations will be unable to achieve their goals in 2025 and beyond if the foundation of their business is unsecured.

Ransomware presents a threat to not only the consistent operation of business, but to the long-term viability of enterprise organizations. The impacts that result from a ransomware attack often scale far beyond financial considerations, damaging both brand and customer perception. And given how lucrative successful ransomware attacks are for the perpetrators, the expectation is that attacks will only increase in frequency moving forward. This dynamic underscores the importance of having clean backups and tested recovery across workloads and technologies for on-premises, cloud, and hybrid environments.

[2] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

Enterprises must invest in a comprehensive approach to cyber resilience in order to best protect against and recover from a ransomware attack. A comprehensive approach to cyber resilience must go beyond just backup and recovery technology; the best plans and platforms must also help foster and ensure collaboration across security and IT teams. Organizations need to ensure plans are in place—and that those plans are being regularly exercised—to put their best foot forward before, during, and after an incident.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com