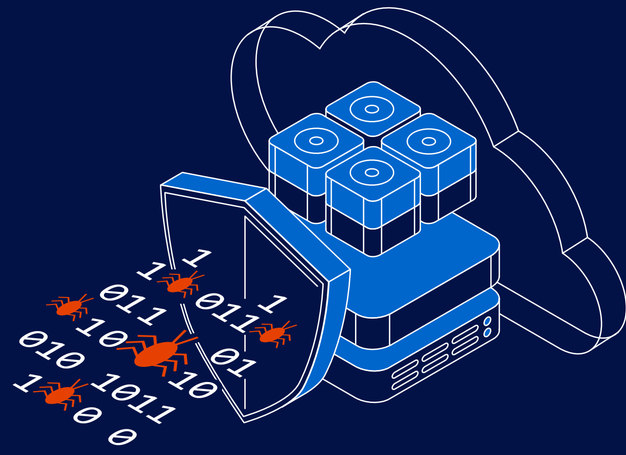
VEEAM

2022

# Ransomware Trends Report



# Contents

# Introduction

In January 2022 an independent research firm surveyed over **1,000** unbiased IT leaders about the impact that ransomware had on their environments, as well as what their IT strategies and data protection initiatives are moving forward. Respondents came from organizations of all sizes from over **16** different countries across APJ, EMEA and the Americas.

All respondents must have experienced at least one cyberattack in 2021, and most actually experienced at least two attacks over that period. On average, about half (**47%**) of their data was encrypted by ransomware, and vulnerability was pervasive across all parts of a hybrid- or multi-cloud architecture.

This is the first broad, ransomware-related market study conducted on Veeam's behalf. The survey was developed to understand the organizational threat, operational impact, financial impact and shift and/or adoption of mitigation practices.

**This report is presented in four sections:**

**1.0** **RANSOMWARE PERVASIVENESS AND FREQUENCY**

**2.0** **REMEDIATION METHODS AND OUTCOMES**

**3.0** **IMMUTABILITY AND AIR GAP**

**4.0** **ORGANIZATIONAL ALIGNMENT BETWEEN CYBER, BACKUP AND BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR)**



# About the research

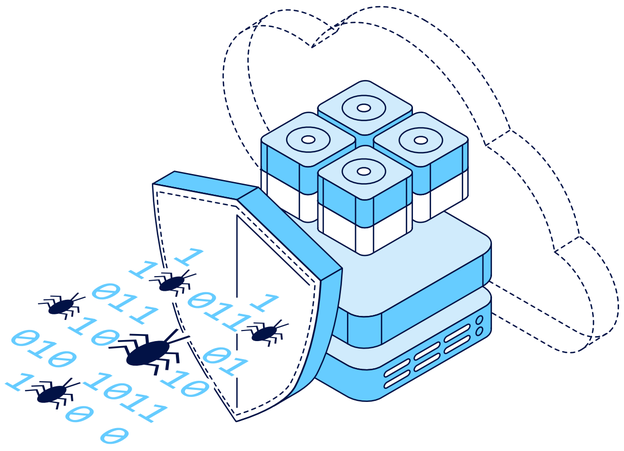
**This research report summarizes the learnings of 1,000 organizations, all of whom had been attacked by ransomware, including:**

- **400 security professionals**
  Operators of cybersecurity detection or prevention technologies
- **200 IT operations**
  Primarily focused on production IT system delivery
- **200 backup administrator**
  Operators of data protection mechanisms and processes
- **200 CISO or other equivalent IT executives**
  Responsible for cybersecurity preparedness

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. We provide a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. To learn more, visit www.veeam.com

Questions about these research findings can be sent to StrategicResearch@veeam.com

# 1.0
# Ransomware Pervasiveness



1.1

# Ransomware is inevitable

According to a another independent research project, the 2022 Data Protection Trends report, **76%** of the **3,393** surveyed organizations suffered at least one ransomware attack, while **24%** either avoided attacks or **were unaware** that an attack occurred.

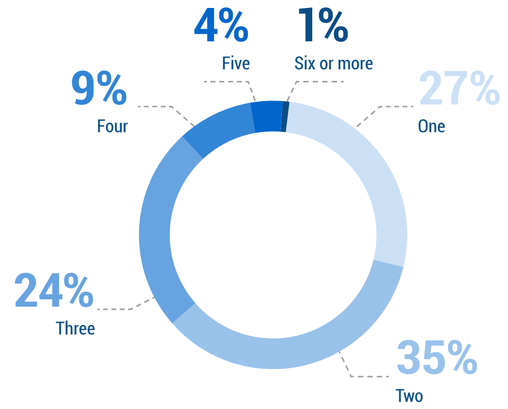
Organizations responding to this independent survey must have experienced at least one ransomware attack in 2021, revealing at least two important truths:

- Only about one in four (**27%**) organizations suffered just one attack, presumably with bad actors attempting to return for more ransom.
- Organizations of all sizes appear relatively equal in the persistence of attacks from small-to-medium-sized businesses (SMBs) (**100–249** employees) to large enterprises (**>5,000** employees). Said another way, just like any other disaster (fire/flood), ransomware attacks are universally pervasive.

While not charted, respondents to this survey reported an average of **47%** of their data being encrypted by ransomware.

This should scare every IT leader!

**Figure 1.1** How many ransomware attacks has your organization suffered in the last 12 months? (n=998)




## 1.2

# Don't click that!

The most common entry point for a cyber attack is still phishing emails, malicious links, or a website that has dubious underpinnings. In considering the old mantra, "go with what works" it is unfortunate that even in 2022 with all the global awareness of ransomware and corporate training available, this is still the leading cause.

That said, there is plenty that IT professionals can do through increased diligence in patch-testing, credential management, role-based controls, etc. As a positive, only **1%** of respondents stated that they were not able to identify the entry-point; inferring that there have been improvements in monitoring and investigation tools across the security stack, as well as overall ransomware prevention strategies.

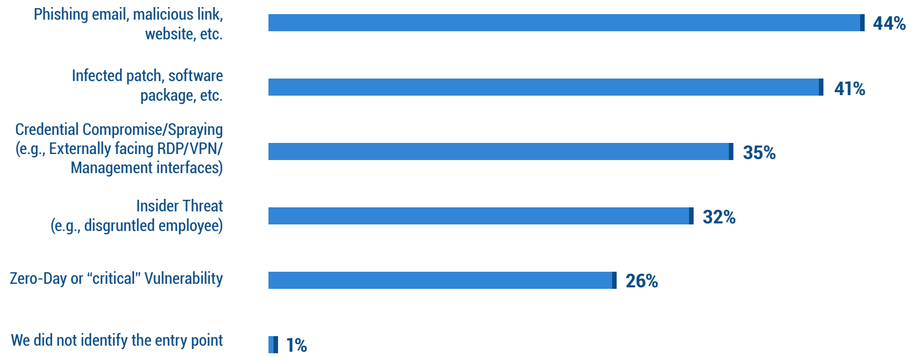



**Figure 1.2** How did ransomware enter your organization's IT environment? (n=1,000)

## 1.3

# Targeted platforms

Today's attacks may start with a user's mistake, but once bad actors are in the environment, specific mainstream platforms are often targeted, most notably:

- **Backup repositories** were targeted in **94%** of attacks and at least some of the repositories were impacted in **68%** of cyber events.
- **Specific production platform or application types** were targeted in **80%** of successful ransomware attacks, presumably based on known vulnerabilities within common platform types, such as mainstream hypervisors and operating systems or wide-spread workloads like NAS filers or database servers.

This alone should drive broader conversations within IT, so cyber security isn't just the delegated to the security team; database administrators should also help ensure that database servers are secure and administrators should help ensure hypervisors are patched, that Windows updates are routinely run, etc.

This is why immutability and air gap matters

**Figure 1.3** Did the threat actor attempt to modify/delete **backup repositories** as part of their ransomware attack? (n=1,000)

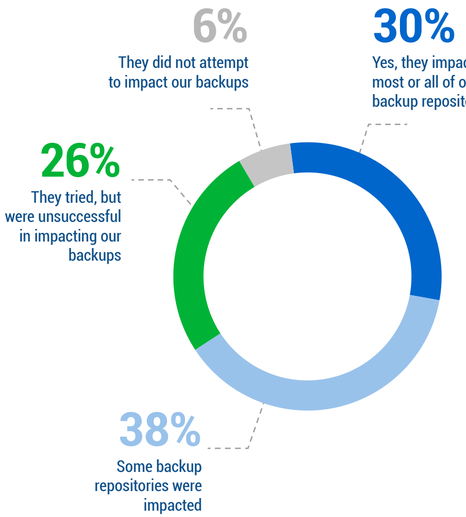
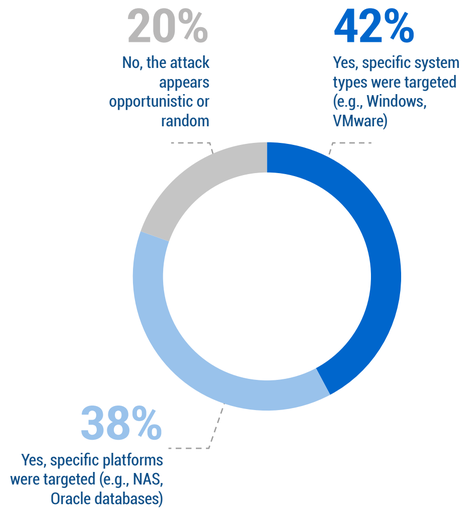



**Figure 1.4** Did the ransomware attack appear to focus on specific **applications or platforms**? (n=1,000)



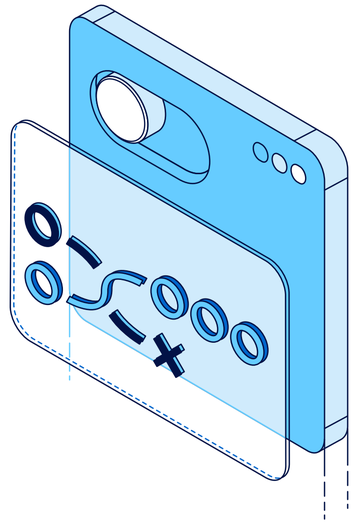
## 1.4

# The Veeam Perspective

Ransomware has democratized data theft, since targeted data only needs to have enough value to the victims that they're convinced to pay ransom to recover that data. This model of ransomware has been successful despite increased investments in defensive security technologies. Veeam believes that secure backup is your last line of defense against ransomware. Our software-defined approach means there is no lock-in into proprietary hardware and it works with your existing architecture, both on-premises and in the cloud. Veeam is committed to helping you minimize downtime and data loss, so that you never have to pay a costly ransom.

To learn more visit: https://www.veeam.com/ransomware-protection.html

# 2.0 Remediation Methods



2.1

# Ransom: Was it paid? And did it help?

One of the more notable statistics in the survey is that half (**52%**) of those with encrypted data paid the ransom and were successful in recovery. However, one in four organizations paid the ransom but were still unable to recover their data, while nearly as many were able to recover **without paying a ransom**.

This final element is why data protection companies are so focused on ransomware scenarios. That said, when ransoms were paid, the majority (**72%**) of organizations used some form of insurance. Beating ransomware by utilizing insurance could be harder for organizations moving forward, based on how they responded when asked about cyber insurance:

- **57%** have cyber insurance that includes ransomware coverage
- **30%** have cyber insurance, but ransomware is excluded from coverage
- **13%** do not have cyber insurance

This should be everyone's goal

**Figure 2.1** Did your organization pay ransom to recover its data? (n=1,000)

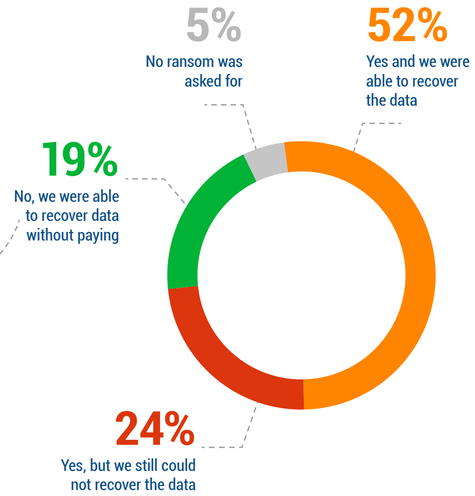
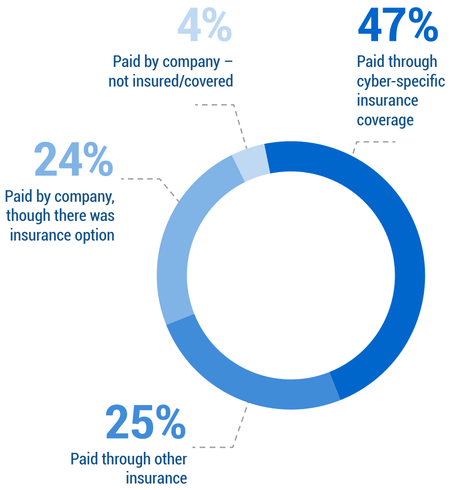



**Figure 2.2** How did your organization pay for the ransom? (n=1,000)



## 2.2

# Remediation takes longer than you think

Most cyberattacks occur when bad actors covertly move throughout your environment after an initial vulnerability is discovered, with goal of doing as much damage as possible. On average, **47%** of data was encrypted according to survey respondents.

The pervasiveness of the attack increases the likelihood that victims will pay a ransom, not just due to the value of some datasets, but to relieve the massive challenge of remediating significant portions of their infrastructure.

While many organizations were able to start their remediation activities in the same or following day, those respondents cited that their recovery journey took (on average) **18** days to complete. This is presumably due to not only the scale issues of addressing what was affected, but also the necessary diligence to confirm that restored systems were "clean" before being put back into production.

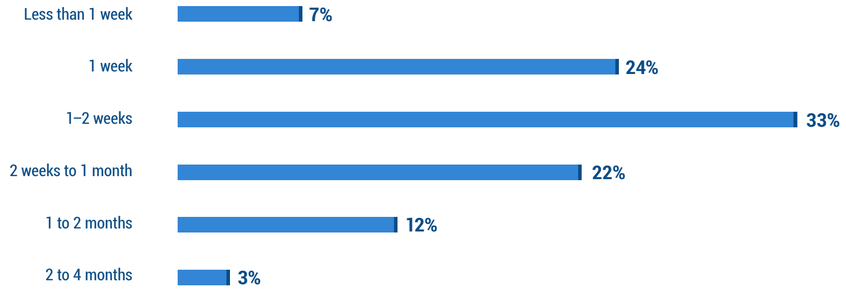



**Figure 2.3** How long after the attack was your organization able to begin restoring data from its backups? (n=998)

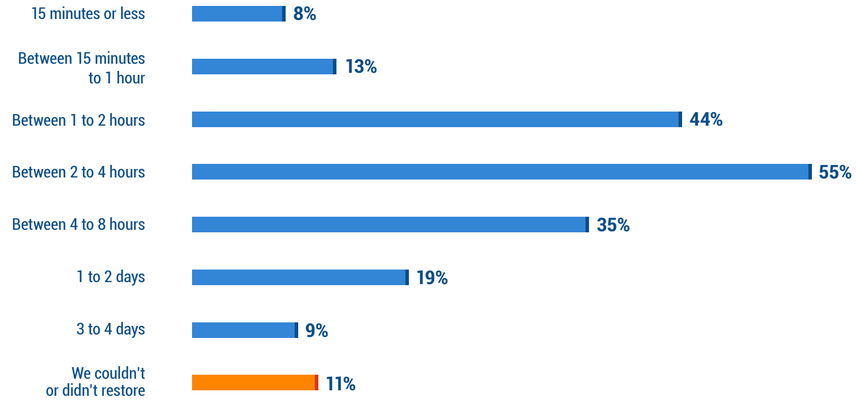



**Figure 2.4** How long did the entire remediation/recovery take before the organization at large would say the event was over? (n=998)

2.3

# Key to success: Use clean backups

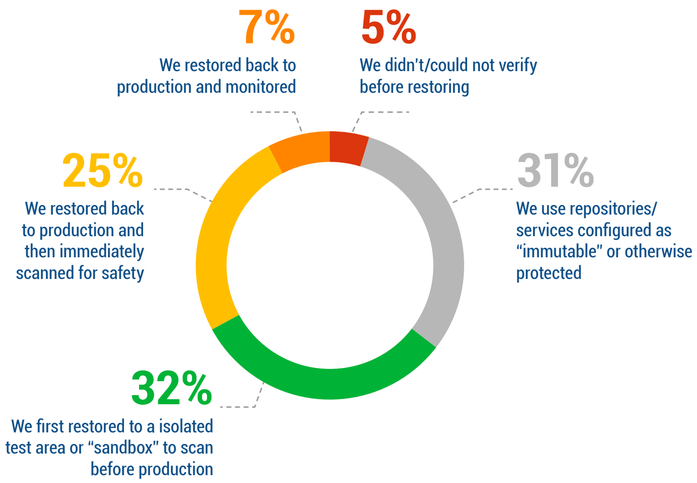
It is important to understand the difference between protecting backup repositories and ensuring that data is clean within those repositories; protecting the repository does not ensure that a repository's contents are free of malware.

When asked about assurance of clean restores, nearly a third (**31%**) of organizations relied on immutability, which does **not** ensure that the data within your repository is safe. **If you remove the immutability option**, we saw that:

- **46%** of organizations first restored to a sandbox
- **36%** of organizations restored directly to production and then immediately scanned for safety
- **18%** of organizations restored directly back to production, without being able to verify safety

While the best option for restoring data after a ransomware attack is to restore to an isolated area, test for infection and reintroduce that data back into the production environment, less than half of organizations do that (or have the capability to do so).

**Figure 2.5** How did the organization ensure that system data/backups were clean prior to restoration? (n=719)



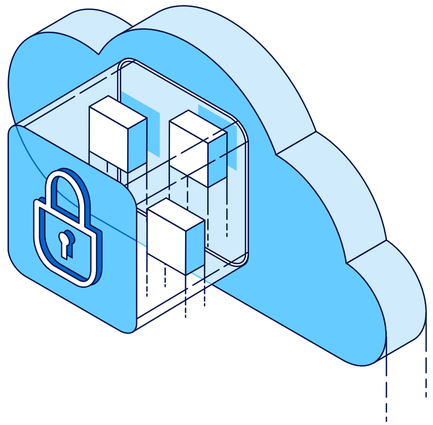
## 2.4

# The Veeam Perspective

Modern ransomware protection requires an integrated security architecture that can stretch from endpoints to network and the cloud to detect, correlate and remediate attacks. Your remediation options are essentially either recovering from backups or paying a ransom. The challenge is, just "restoring from backup" oversimplifies the process and causes many organizations to make assumptions about their backup and recovery capabilities, which often leads to data loss. To avoid the worst-case scenario, Veeam believes that having a plan in place that includes verified, tested and secure backups that can be restored quickly is the key to surviving modern attacks like ransomware. It's important to always remember that your backup infrastructure is part of your overall cybersecurity defense plan and can be the final option for getting back to, or staying in, business.

To learn more visit: https://www.veeam.com/blog/ransomware-recovery-what-you-need-to-know.html

# 3.0 Immutability and Air Gap



3.1

# What you should do before: Test often, test better

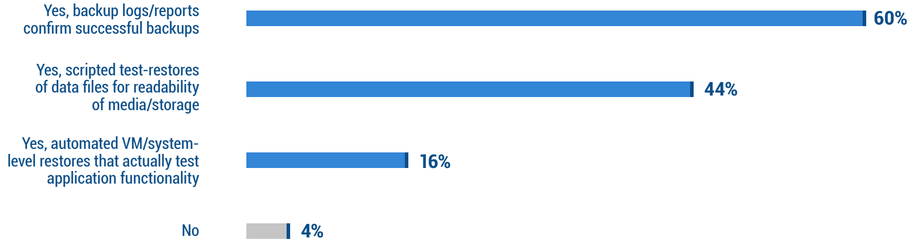
According to the 2022 Data Protection Trends Report, the second most common driver behind changing backup solutions was to improve solution reliability. As stated in that report, you cannot restore what you did not successfully back up.

Unfortunately, **only one in six** organizations test whether their backup solutions can restore by actually restoring and verifying their data. Every experienced backup professional has a horror story in which their software's logs claimed no errors and yet the media was unreadable, some dependency wasn't tested, the source was corrupted, etc.

The idea of integrating some type of isolated sandbox into the data protection architecture is even more important when considering not only automated validation for recoverability, but also for staging restores to test for clean data as described in **Figure 3.1.**

Why would you trust a log file or media-read test? If you are depending on the ability to restore, test it routinely.

**Figure 3.1** Does your organization do automated recovery verification or validation of backups and/or replicas? (n=396)



## 3.2

# Lots of options for immutability and air gap

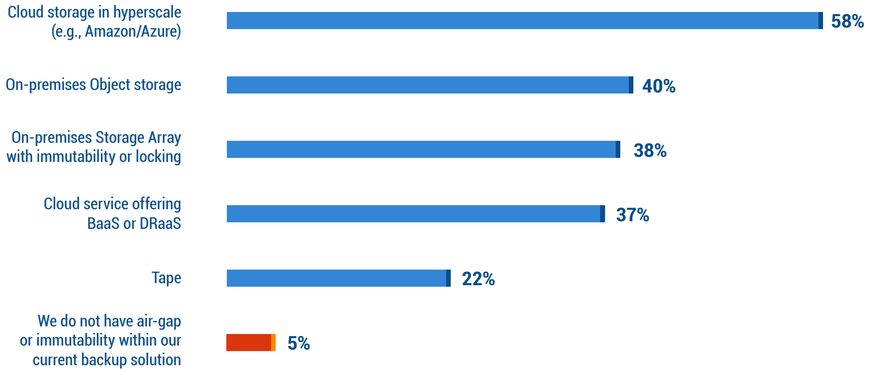
Building off **Figure 1.3** and the importance of assuring that backup repositories cannot be affected by cyber attackers, the good news is that 95% of organizations now use at least one method of retaining isolatable backup data.

With so many combinations, it is notable that:

- **74%** of organizations use some kind of cloud-service (i.e., hyperscale storage or a managed service)
- **67%** of organizations use some kind of on-premises storage (on-premises)

Also, in addition to tape's persistent usage as a low-cost, extended long-term retention medium of choice, it is also used by more than one in five organizations as an air gapped repository. Considering the rising costs associated with cyber attacks, plus the investment put into production systems to accommodate the ever-increasing demands on IT today, the low total cost of ownership (TCO) of tape is making it favorable for organizations of all sizes.

**Figure 3.2** Which offline, air-gapped or immutable backup repositories does your organization use? (n=396)



## 3.3

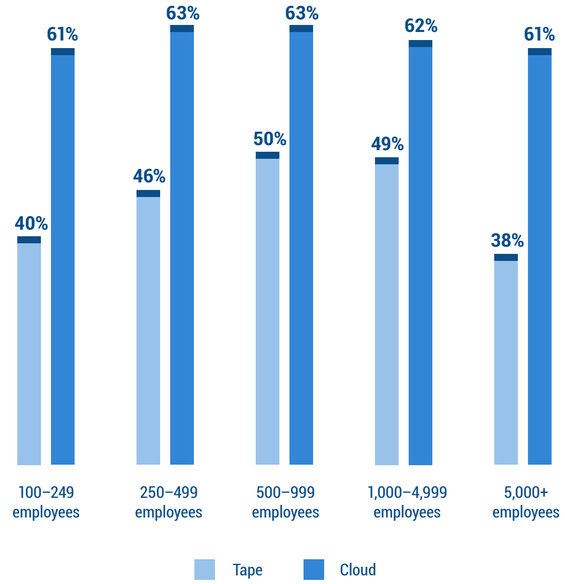
# A closer look at offsite mediums

Unfortunately, not all cloud services offer immutability (yet). Just as important, not all tape solutions would be considered air gapped if the tapes didn't leave the robotics and could be erased in a cyberattack.

That said, most organizations use a combination of cloud services and/or tape to complement an on-premises disk-based backup solution. When asked about what percentage of their data is stored on each off-premises type:

- **62% of organizations' data is put into a cloud service at some point** in its data retention or protection lifecycle, with nearly equal usage across all sizes of organizations.
- **45% of organizations' data is stored on a tape at some point** in its lifecycle, though **Figure 3.3** reveals less tape usage by SMBs and large enterprises than mainstream organizations in between. While smaller organizations likely lean toward easier modern cloud services, large enterprises are likely more selective on long-term retention strategies based on regulatory concerns and scale challenges.

**Figure 3.3** In addition to whatever disk-based backup solution you are running, what percentage of your production data is also backed up to **tape** and/or **cloud**? (n=396)



## 3.4

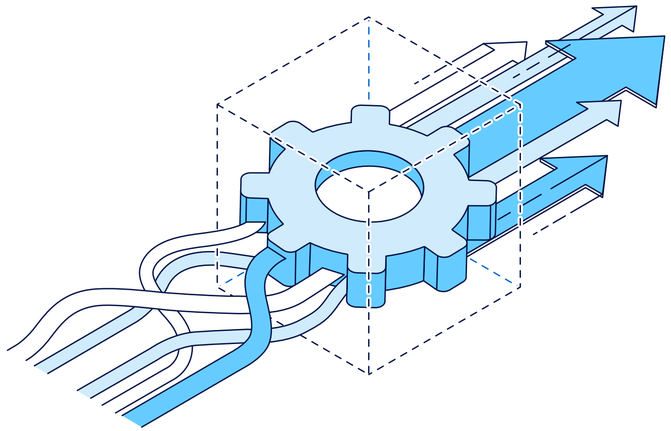
# The Veeam Perspective

Verified and tested backups are the first step to any successful recovery. Veeam's SureBackup® pioneered automated backup verification and is a key capability behind ransomware resiliency. SureBackup automatically brings up servers and applications in a network-isolated environment and executes health checks that include application verifications such as executing specific Microsoft Active Directory or SQL commands to ensure application integrity.

For many years, Veeam has advocated for the 3-2-1 Rule as a general data management strategy. The 3-2-1 Rule recommends that there should be at least three copies of important data, on at least two different types of media, with at least one of these copies being off site. As the threat of ransomware has advanced, Veeam has emphasized that at least one copy of data should be air-gapped, offline or immutable. This modern application, called the 3-2-1-1-0 rule, is one of the most important concepts that an organization can implement to be better prepared to fend off and remediate cyberthreats.

To learn more visit: https://www.veeam.com/blog/beat-ransomware-with-double-play-immutability.html

# 4.0 Organizational Alignment



## 4.1

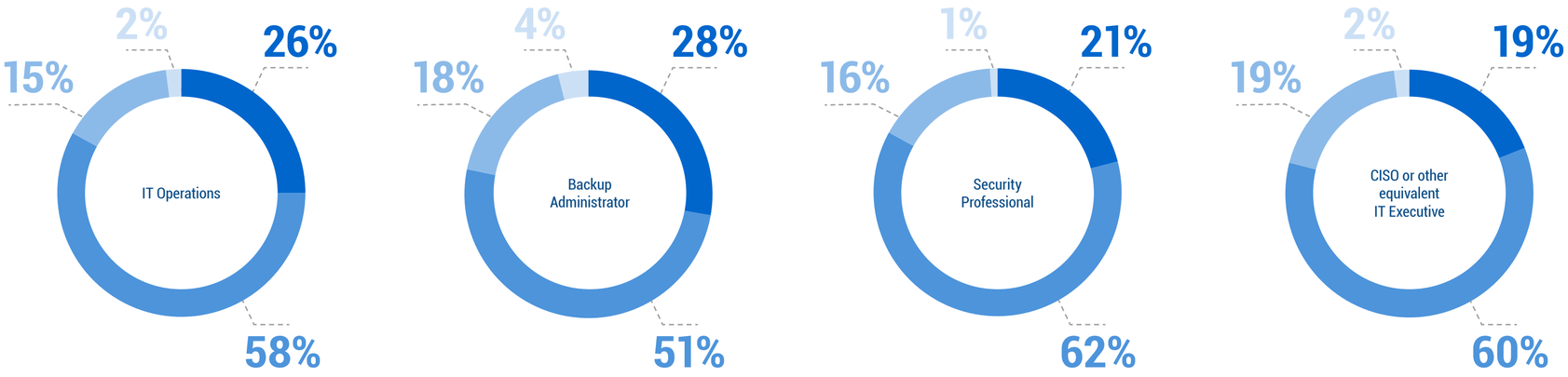
# Ransomware is a disaster

According to **3,393** IT Leaders and Implementers surveyed within the 2022 Data Protection Trends Report, seven out of eight organizations are well aligned in their strategies for cyberattacks and other disasters like site crises, fire/flood, etc.:

- **40%** of organizations claim a single and unified strategy
- **48%** of organizations are mostly integrated
- **11%** of organizations are somewhat integrated

While that survey came from IT generalists, this survey asked the same question to those who specialize in some aspect of cyber-preparedness and have faced **the hard lessons that come with being successfully attacked by ransomware**. Through those four lenses, while the overall sentiment is similar, those closer to security practices (i.e., security professionals and CISOs) noted a greater disparity between cyber strategies and business continuity/disaster recovery (BCDR) strategies than those further from the security initiatives.

**Figure 4.1** To what extent are cybersecurity strategies part of your organization's BC/DR strategy, or are they handled separately? (n=1,000)



## 4.2

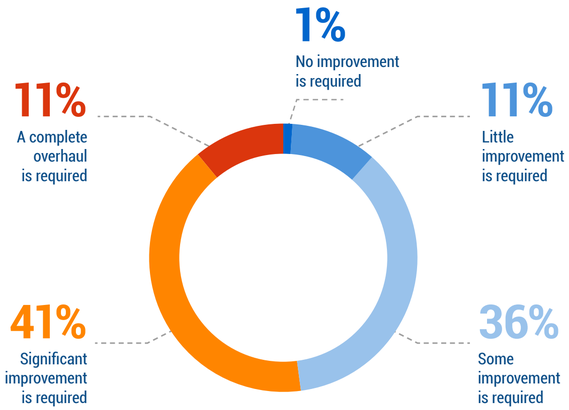
# Alignment between cybersecurity and backup teams is insufficient

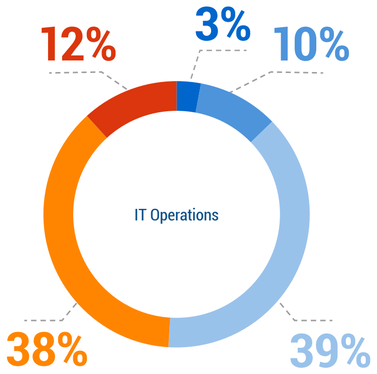
While **Figure 4.1** assessed the alignment between cybersecurity strategy and BC/DR strategy, **Figure 4.2** ask the four respondent groups about the more pragmatic alignments between backup teams and cybersecurity teams.

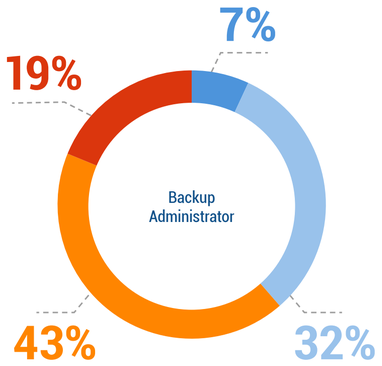
Overall, about half (**52%**) of respondents believed significant improvement or a complete overhaul was necessary for cybersecurity and IT backup teams to collaborate successfully. However, there is a second story that persists across many of the questions in this survey when broken down across these four personas.

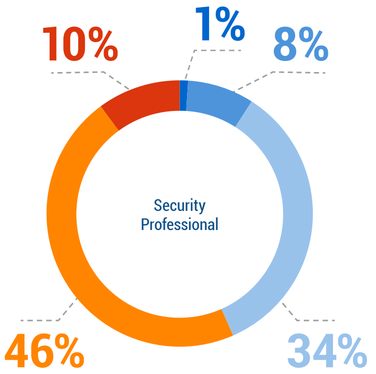
Notice that professionals **closer to the problem** (i.e., backup administrators and security) **see a greater need for improvement** than those further from the details (i.e., IT operations and CISO/executives). This trend continues throughout the survey data, which shows that **the more you know, the more concerned you are** about your organization's ability to survive a ransomware or other cybersecurity event.

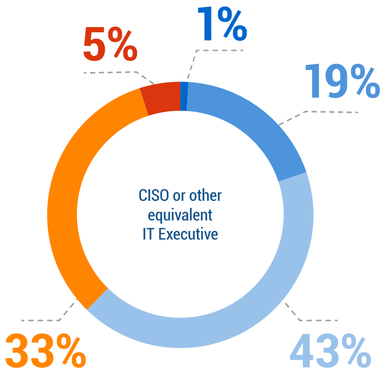
**Figure 4.2** How much improvement do you believe is required for your organization's IT backup team(s) and your cybersecurity team(s) to be fully aligned? (n=1,000)



# 4.3

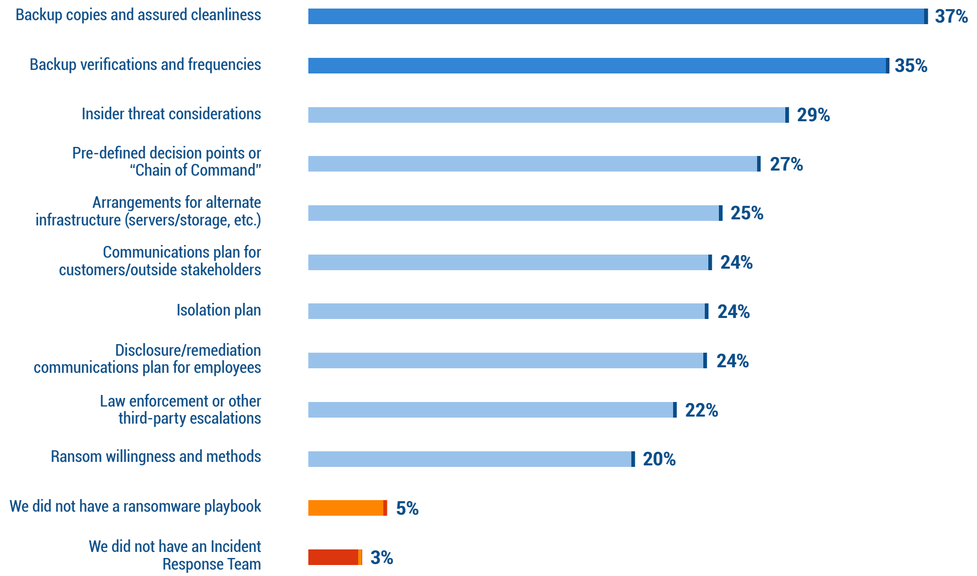
# What is in a Remediation Playbook?

Nearly all (**92%**) have a predesignated team for handling when ransomware attacks, including the identification of tools and policies to be enacted.

And while **1 in 4** (ranges from **20-29%**) organizations had some collection of escalation/isolation and ransom/remediation methodologies within their culture, the most common components within these strategies were:

- **Backup copies (plural),** presumably so that if one copy or media was encumbered, other recovery sources were available
- Processes to **assure the cleanliness** of the data as "safe" to recover from, presumably including both proactive media isolation (aka "air gapping") or sanctification (aka "immutability").
- Processes to **assure recoverability,** presumably including automated recovery tests to validate readable media and correct function of the restore software and hardware platforms.

**Figure 4.3** Prior to your last cyber event, did your organization's Incident Response Team have a defined ransomware response playbook that incorporated any of the following? (n=998)



## 4.4

# The Veeam Perspective

It's good news to see the continued alignment between BC/DR and cybersecurity teams. Veeam believes that the best way to reduce the risk of a cyberattack like ransomware is to have a comprehensive and tested disaster response plan. Solutions like Veeam Disaster Recovery Orchestrator allow you to create, document and automatically test your DR plans to prove that your data can be reliably recovered after an attack. Having and sharing disaster response plans with other security teams will help continually improve alignment between teams and provide a more holistic picture of your incident response process.

To learn more visit: https://www.veeam.com/blog/veeam-disaster-recovery-orchestrator-v5.html

# Summary

This analysis covers Veeam's first broad-based market study on the impact of ransomware. Based on the findings from these results from **1,000** independent IT leaders who persevered through at least one (or more) cyberattacks in 2021:

- When bad actors are effective in their cyber attacks, **47%** of an organization's data will be encrypted (across a wide range of production IT platforms) with only a **69%** recoverability rate, even after paying the ransom.
- One in four organizations was able to recover from their ransomware event by recovering from backups instead of paying the ransom. The three most important contributors to that success are:
  1. Immutable/air-gapped backup repositories
  2. Verifiably recoverable and assuredly "clean" data
  3. Orchestrated workflows for recurring testing and reducing the time of remediation
- While backup is inherent in most cyber recovery strategies, there is still significant improvement to be done between the cybersecurity, BC/DR, and IT backup teams.



Questions about these research findings can be sent to StrategicResearch@veeam.com

# About the authors

Jason Buffington
VP, Solutions Strategy

@JBuff

@jasonbuffington

Dave Russell
VP, Enterprise Strategy

@BackupDave

@backupdave

Julie Webb

Director,
Market Research & Analysis