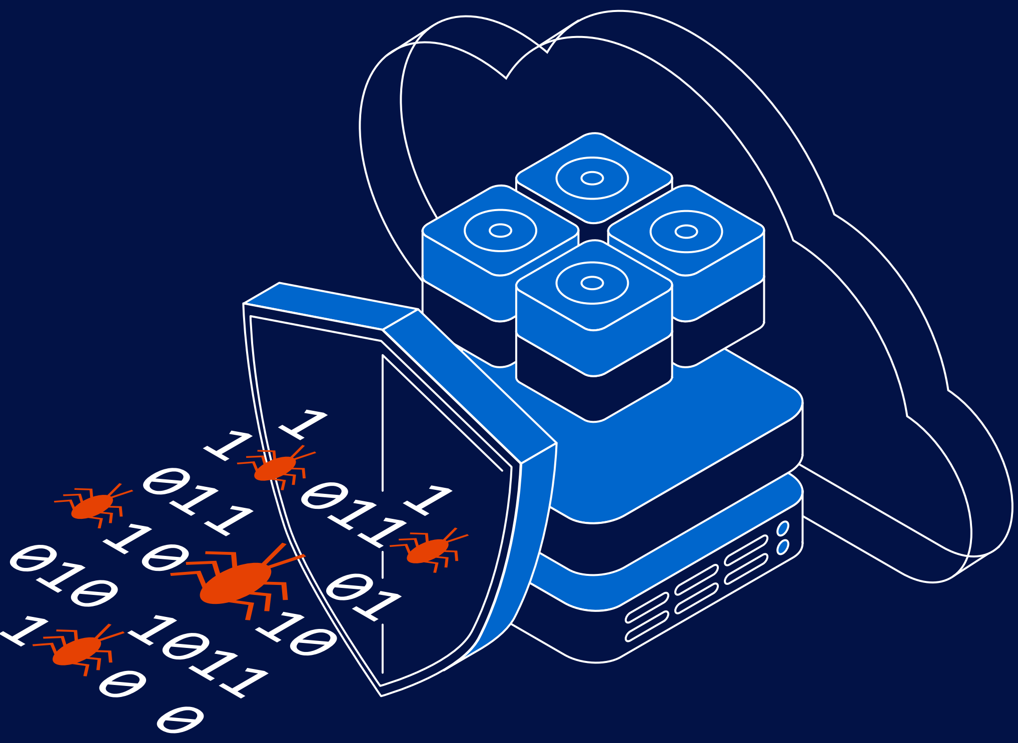
VEEAM

EXECUTIVE BRIEF

2022

Ransomware Trends Report

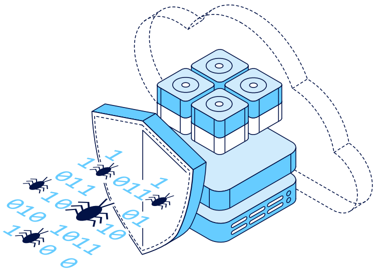
EMEA EDITION



In January 2022, an independent research firm completed a survey of 1,000 unbiased IT leaders regarding the impact that ransomware had within their environments, as well as their remediation methods and future facing strategies. Responses came from members of one of four professions (i.e., CISOs, security professionals, backup administrators and IT operations) and represented organizations of all sizes across 16 different countries from APJ, EMEA and the Americas – including 300 from EMEA.

An earlier research report from the same research firm showed that **76%** of organizations experienced at least one cyberattack in 2021, and **24%** either weren't attacked or were unaware of the intrusion. To learn more, a second survey was conducted where respondents had to have experienced at least one cyberattack in 2021; while most actually experienced at least two attacks over that period. One of the most alarming statistics from these 2021 cyberattacks was the fact that organizations acknowledged that they were only able to recover **69%** of their data. Overall, these results revealed at least three key areas of discovery:

- The effectiveness and pervasiveness of bad actors
- Key attributes of a successful remediation strategy
- Opportunities for improvement between the teams responsible for proactive prevention and reactive remediation



This executive brief summarizes findings from the full 2022 Ransomware Trends Report, which can be downloaded at http://vee.am/RW22.

The effectiveness and pervasiveness of bad actors

Even with the global awareness of ransomware and malware, plus the ever-increasing vigilance of IT teams, the most common entry point for ransomware continues to be users accidentally clicking malicious links, visiting insecure websites or engaging with phishing emails, according to **44%** of survey respondents worldwide and **46%** in EMEA. That said, far too many cyber criminals also gain access through infected software packages and compromised credentials.

After gaining the ability to navigate within an organization's environment, most attackers **(80%)** seek out mainstream systems with known vulnerabilities, including common operating systems and hypervisors, as well as NAS platforms and database servers. One of the more interesting insights that came from this survey was whether certain facets of a hybrid or distributed IT infrastructure may be more (or less) vulnerable to cyberattacks. When organizations were asked about which parts of their environments had been encrypted, they said:

- **48%** suffered encryption of servers within their datacenters
- **49%** suffered encryption of platforms within their remote offices
- **46%** suffered encryption of cloud-hosted server instances

In EMEA, **47%** of datacenter servers, **50%** of remote offices and **44%** of cloud instances were impacted. Perhaps more alarming is the effectiveness of attackers to proactively destroy their victim's data backup repositories, as seen in **Figure 1.1**.

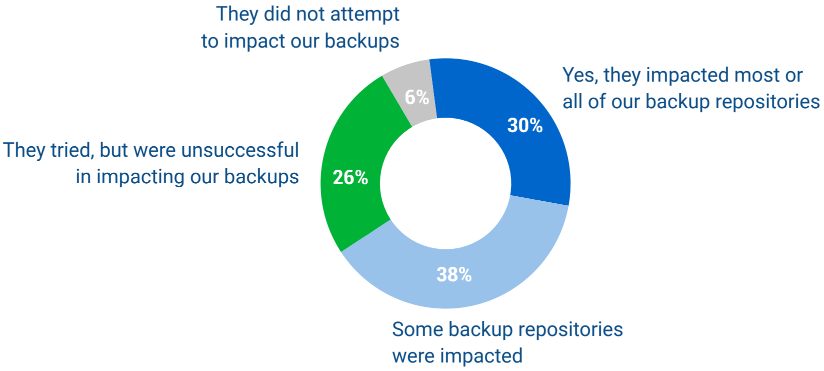


Figure 1.1

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

Make no mistake, cyber villains are "selling" the ability to retrieve their victim's data. The victim's likelihood to pay the ransom is significantly increased if restoring from backups is no longer an option. That reality is even more interesting when considering whether organizations paid the ransom if they were successful in recovering their data **(Figure 1.2)**.

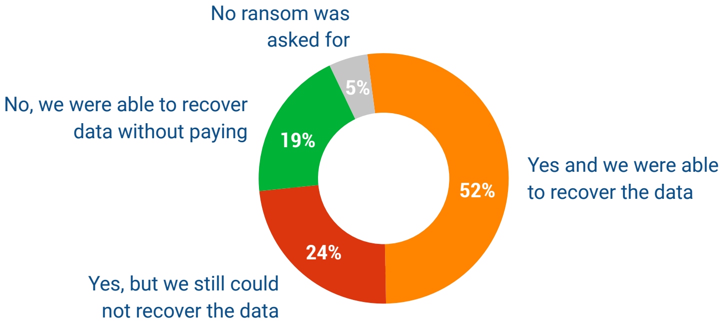


Figure 1.2

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

Figure 1.2 reveals a few key points that everyone should pay attention to:

- In barely half of the attacks, the organizations paid the ransom AND were able to recover their data.
- Meanwhile, one in four **(24%)** organizations paid the ransom, BUT were still not able to recover their data.
- Most notably, one in five **(19%)** organizations did NOT pay the ransom but were able to recover their data anyway.

Said another way, almost as many organizations were able to recover without paying as there were that paid but could not recover. In EMEA, **22%** were able to recover without paying the ransom. This is why data protection companies are so focused on ransomware scenarios — so that the other **78%** of cyber victims can also say they recovered without paying.

88%

of ransomware attacks attempted to infect backup repositories, and **75%** of those attempts were successful

Key attributes of a successful remediation strategy

With that in mind, it is not surprising that so many organizations use at least one type of immutable or air-gapped backup repository in hopes of attempting to recover their own data **(Figure 1.3)**.

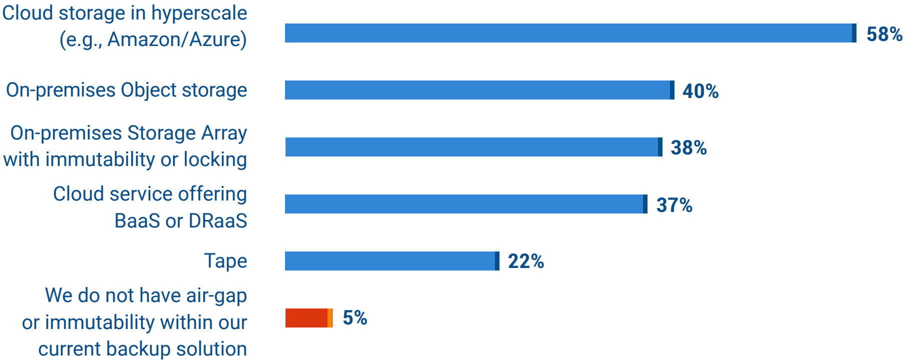


Figure 1.3

Which offline, air-gapped, or immutable backups repositories does your organization use? (n=398)

In fact, while only **5%** of organizations have less than one immutable tier within their data protection framework, many use multiple. This implies that their backup data is immutable throughout its lifecycle:

- **74%** use cloud repositories that offer immutability
- **67%** use on-premises disk repositories with immutability or locking
- **22%** use tape that is air-gapped

84%

of organizations rely on backup logs or media readability to assure recoverability; meaning only **16%** routinely test by restoring and testing functionality

After ensuring that their repositories are less likely to be disrupted, the next step is ensuring that clean data can be restored back to the production environment. For nearly half of these surveyed organizations, this is accomplished by first restoring to a sandbox or an isolated area, to test the safety of the data prior to reintroducing it to the production environment **(Figure 1.4)**.

This best practice of isolation and “staged restore” occurs in **46%** of organizations worldwide, and **52%** by organizations in EMEA. Another best practice that was revealed by a minority **(16%)** of organizations was the importance of proactively testing the recoverability of data with automated verifications of real restores, instead of relying on backup logs or media tests.

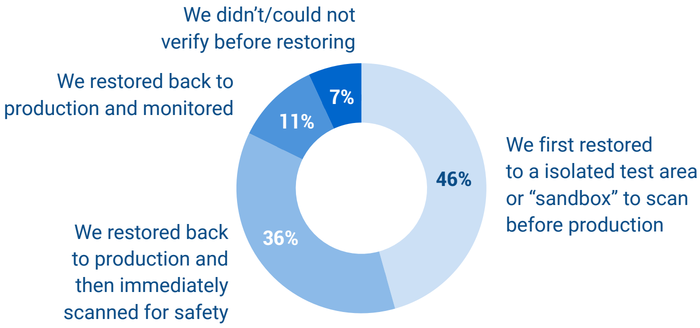
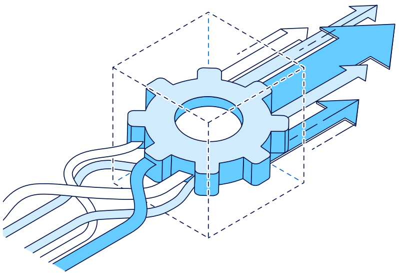


Figure 1.4

How did the organization ensure system data/backups were “clean” prior to restoration? (n=555)

Opportunities for improvement across the organization



While the technologies described above are indispensable in combatting the **$50 billion**[1] annual impact of the ransomware industry, the real power to defend or mitigate cyberattacks comes from the expertise of various teams and their alignment with each other. From a strategy perspective between organizations' cyber-preparedness and their overall BC/DR preparations, we found:

- **23%** claim a completely unified strategy
- **58%** are mostly integrated between the two initiatives
- **17%** are somewhat integrated
- **2%** are completely disconnected

While the **strategies** seem mostly (i.e., **81%**) aligned, or **84%** by organizations in EMEA there is apparently a significant disconnect between the **teams** responsible for cybersecurity and those responsible for backup **(Figure 1.5)**.

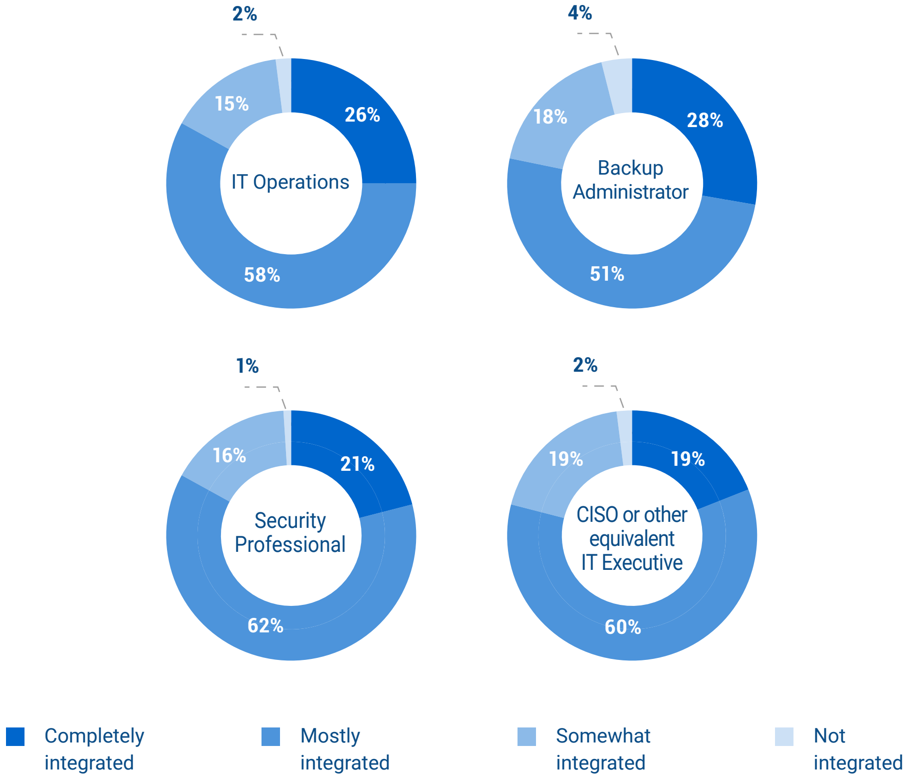


Figure 1.5

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

[1] Gartner, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

It appears that those closer to prevention (i.e., security professionals) and remediation (i.e., backup administrators) see an even greater need for improvement than those that are less aware of the interactions (i.e., IT operations or executives). That said, while there is improvement to be had between the functional teams, the broader group that's responsible for helping their organizations survive a cyberattack often referred to as the "incident response team" (IRT), does recognize verifiable recoverability and assured cleanliness of backup data as the most common component of their playbook **(Figure 1.6)**.

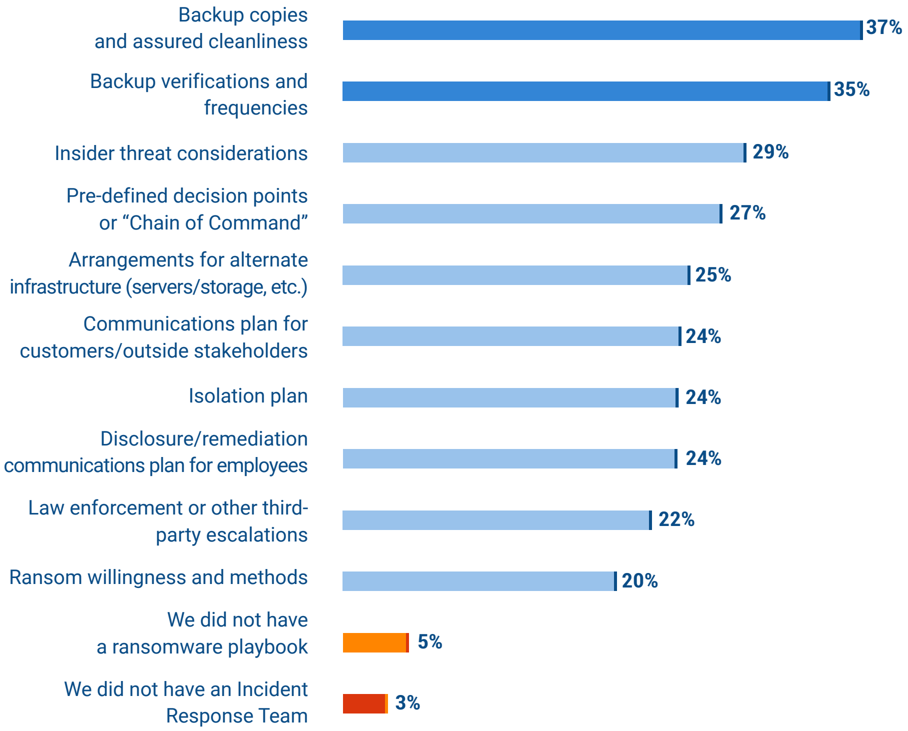


Figure 1.6

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)

The Veeam perspective

Ransomware has democratized data theft, since targeted data only needs to have enough value to the victims so they're convinced to pay ransom to recover that data. This model of ransomware has been successful despite increased investment 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 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**.

Click here to view the 2022 Ransomware Trends Report

Questions related to research data and insights can be directed to StrategicResearch@veeam.com

Also check out the 2022 Data Protection Trends Report