veeam Insights

Ransomware Trends Report

2024

CEO Letter

Welcome to the 2024 Ransomware Trends Report

Veeam's goal is to relentlessly advance data and cyber resilience to keep your business running. As modern data threats continue to evolve almost daily, so does modern data protection. That's why at Veeam, we lead the charge in cyber resilience by offering the best data protection combined with rapid ransomware recovery. The secret to organizational resilience is not only putting in place the right protection, but if the worst happens being able to recover rapidly.

Today's landscape is fraught with challenges, including geopolitical tension and unrest, burgeoning cybercriminal capabilities, and shortages in cybersecurity expertise. These factors contribute to elevated cyber risk in an increasingly data-driven and interconnected world. This has heightened the need for senior management to understand, manage, and mitigate risk in an era of rapid digital evolution. Insights are critical, and that is why I am thrilled to share the findings of this year's Ransomware Trends Report with you.

This year, the Ransomware Trends Report dives deeper into key areas relating to:

- Scale, breadth, and impact from the 1,200 who experienced cyberattacks
- Importance of organizational alignment during preparation as well as remediation
- Technologies that matter for implementation before as well as usage during the recovery of cyberattacks

At Veeam, we believe that building data resilience is equal parts protection and recovery. And so, the goal of this research is to help lead organizations towards a more strategically aligned modern data protection and recovery plan.

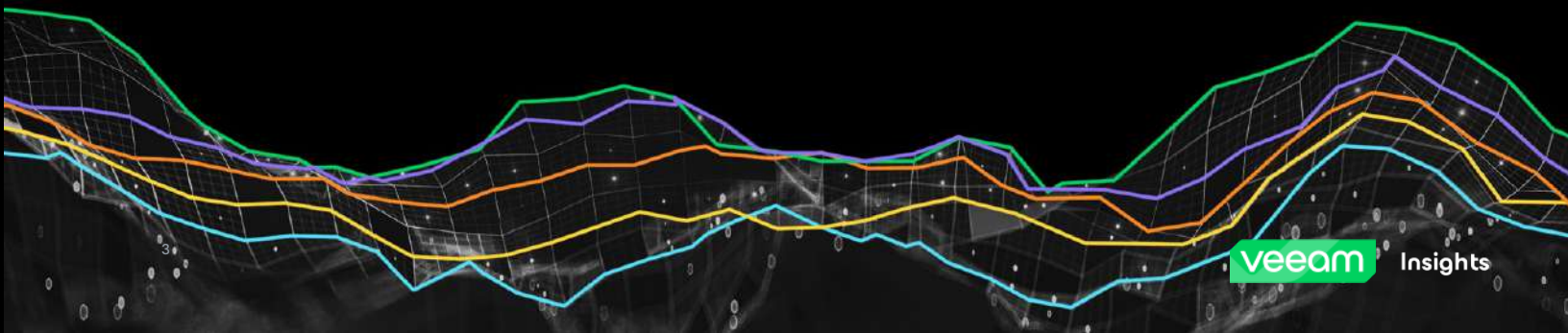
About the Report

Each year, Veeam contracts independent research firms to survey IT leaders and implementers on various data protection topics. The surveys are intentionally not just Veeam customers, but a broad representation of the market. This is to ensure that Veeam continues to develop solutions that understand top trends around where the market is headed. The results of the surveys affect our product strategy and go-to-market methods, and hopefully help organizations engage in deeper conversations with colleagues and teams as they continually consider modernizations to their data protection and cyber-resiliency strategies.

This year's report surveyed 1,200 respondents — comprised of CISOs (or executives with similar responsibility), security professionals, and backup administrators — whose organizations suffered at least one ransomware attack in 2023 to assess different perspectives in the united fight against ransomware.

Introduction

Ransomware continues to be a major reason that organizations experience business interruption. In the event of a ransomware attack, production data isn't the only victim, and the losses won't only be financial. Threat actors now aggressively pursue an organization's backups, recognizing that these are critical to recovery efforts. The 2024 Data Protection Trends Report revealed that **75%** of organizations get hit by cyberattacks, and most report getting hit more than once. In face of this, organizations must worry about the impacts such an attack will have on their reputation, productivity, insurance costs, and total financial impacts for the company — all of which can lead to data loss and, ultimately, a loss of trust from stakeholders. Protecting against complex risks means implementing modern, comprehensive security measures across all domains. This includes strategically aligned initiatives between IT and security teams, which have proven to ensure cyber resiliency across all attack surfaces — including your backup data.



Targets and Impacts of Ransomware Attacks

Bad Actors Will Target Your Backups

As the value of your backups continues to grow, so does the number of bad actors coming after them. In fact, backup repositories are targeted in **96%** of attacks, with bad actors successfully affecting the backup repositories in **76%** of cases.

On average, 37% of backup repositories were affected by a successful attack.

> Unprotected backup is troubling to even think about and should be avoided at all costs. In today's modern age, clean, safe, and recoverable data — including effective protection from ransomware attacks — is a key of factor to organizational success.
>
> Aleh Sadaunichy,
> Network & Architect Manager,
> Lyreco

The Ransom is Only **32%** of the Financial Impact the Organization Will Experience

When thinking of the costs associated with a cyberattack, prevention fees, detection fees, recovery services, the cost of business interruption, and the ransom itself are often the first things to come to mind. While the cost of remediating the incident does play a role, it does not reveal the full scope of the damage dealt to an organization. Out of all the responses to this year's survey, only one in nine organizations **(11%)** stated that ransom payment was the significant majority of the overall financial impact to their organization. For the rest of the cyber victims, the overall financial impact was appreciably more than 'just' the ransom itself, including damage to brand image, loss of productivity, and increased pressure on their IT teams. Additionally, these factors can have impacts on your people and teams.

Respondents to this survey reported that the ransomware attack affected their individual roles, as attacks contribute to increased workload and stress levels, decreased work-life balance, a lessened sense of job security, and an overall feeling of burnout.

Some impacts of the attack to organizational roles:

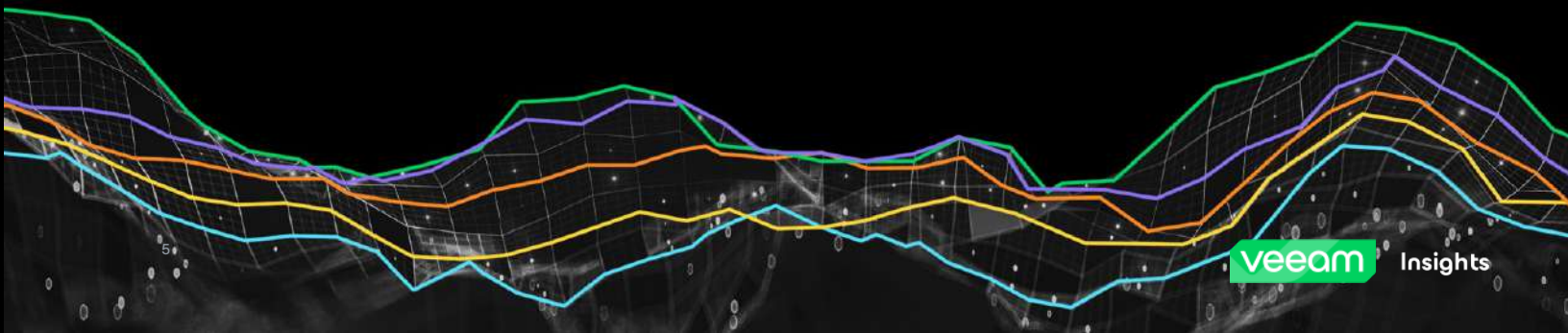
40%
Increased stress

31%
Decreased work-life balance

28%
Disciplinary action or loss job security

45%
Increased workload

Coveware, leaders in Incident Response, shared that the average ransom payment in Q4 was $568,705



Cyber Insurance Isn't the Answer

Insurance can be costly. While it's an aspect of what needs to be done, it is not, however, the end-all-be-all solution, and should not be used as a replacement for cybersecurity measures. With ransomware on the rise, access to coverage is expected to diminish, as cyber insurance continues to change in response to ever-increasing claims. At the time of their last renewal, respondents reported that:

73%
of their organizations experienced an increase in their premiums

44%
had their deductible increased

14%
saw their coverage benefits reduced

When it comes to paying the ransom to restore your organization's data, there isn't an easy *"to pay or not to pay"* answer. While the majority of organizations *did* have a policy, there were

nearly equal sentiments towards paying (47%) versus not paying (36%).

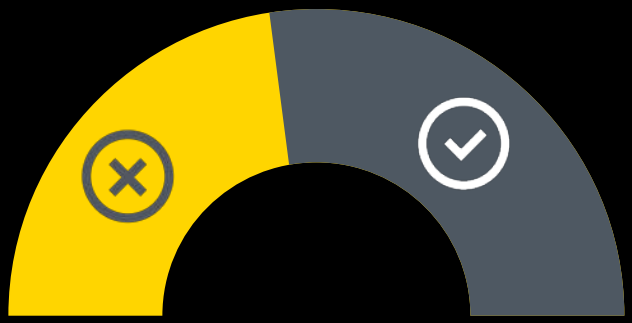
For organizations who were asked to pay a ransom to recover their data in 2023, **86%** could have used insurance to cover the cost — however, only **65%** chose to do so. The other **21%** chose to not use their insurance, paying the ransom without making a claim.

However, for some organization, insurance and payment policies ended up not mattering at all. ***One in three organizations still could not recover their data even after paying.*** This leaves your organization's ability to restore data safely from your own clean databases as one of the few options capable of ensuring full data recovery.

43% of Affected Data Won't be Recoverable.

Two of the most alarming statistics from the 1,200 survey respondents and their experiences in 2023 were:

- On average, cyber victims reported that they were unable to restore **43%** of whatever data was affected by the ransomware attack.



- Contrary to popular belief, datacenter servers, branch office resources, and cloud-hosted data all showed similar infection and encryption rates by the time the attack was finished. Said another way, if your cloud-hosted data is as easy for your users to access as your on-premises servers, it is just as easy for bad actors to affect once they're inside your environment.

Collectively, these statistics emphasize the criticality of ensuring comparable protection and assured recoverability across all platforms in a hybrid-cloud strategy — particularly as workloads move from one hypervisor to another or from one cloud to another.

The Cost of Team Misalignment

Backup and Cybersecurity Teams Aren't Aligned

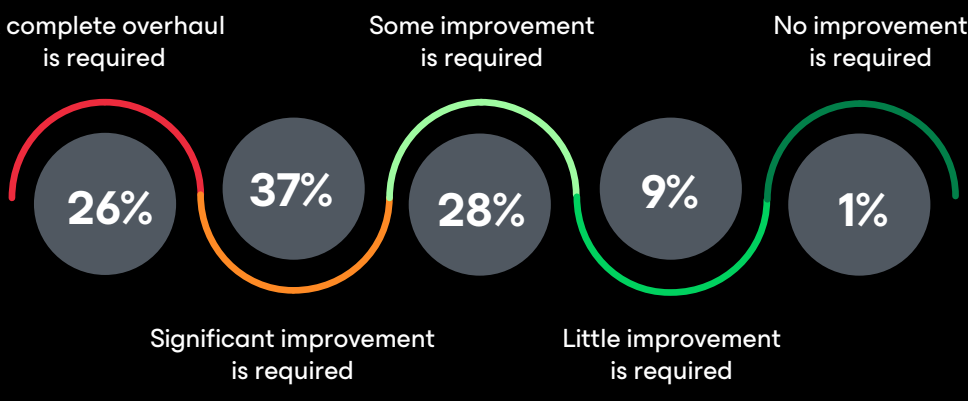
Recovery from a ransomware attack is a team sport. But it turns out that IT, security, and leadership teams — as well as myriad other teams such as legal, compliance, and procurement — aren't as aligned as they want to be.

For the third year in a row, more than half of organizations (**63%**) believe that there is either a "significant improvement" or "complete overhaul" needed for their organizations to be aligned between their backup and cybersecurity teams. It is worth noting that of the three roles surveyed backup administrators were the least satisfied with the alignment of these teams. This suggests that backup, while important, may not be as involved in the preparedness strategy as organizations ought to consider.

Looking deeper, the survey then asked why teams were not better aligned, to which the most common response was **a lack of integration between backup tools and cybersecurity tools.**

> The secret formula to combat ransomware? Collaboration between Security and Infrastructure teams.
>
> Bobby Stojceski,
> CSO, Penske Australia & New Zealand

How much improvement is required in order for your organization's IT Backup team(s) and your Cybersecurity team(s) to be fully aligned?



Who Gets Called In?

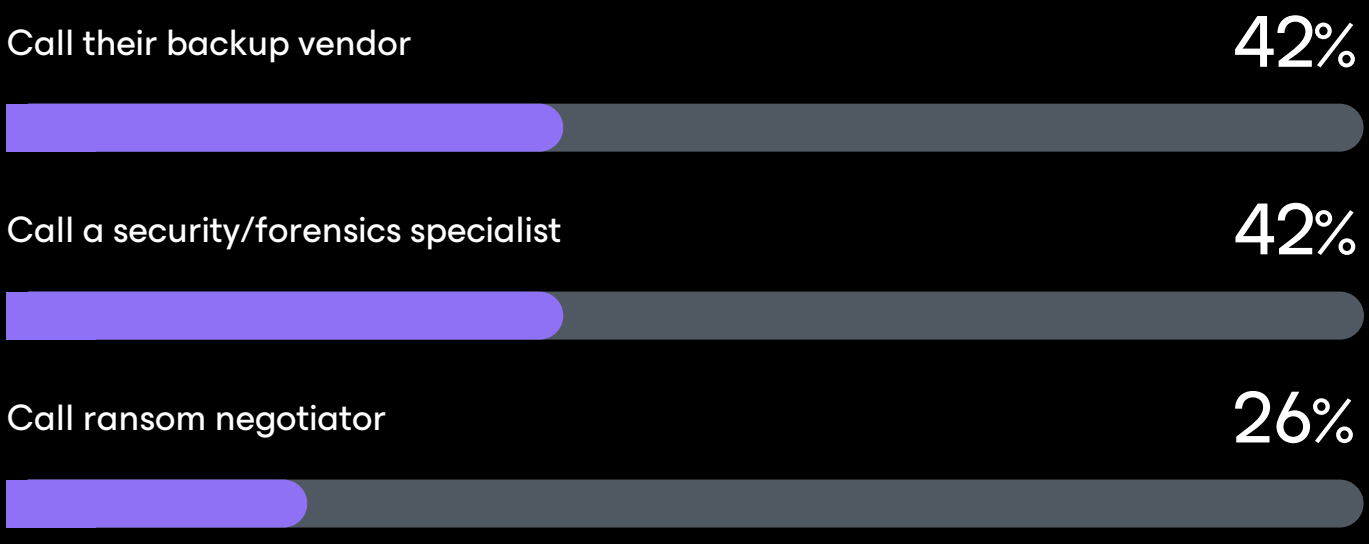
Three teams were nearly tied for first place when respondents shared who they called first in the event of a ransomware attack. IT Backup Teams, C-suite members, and Cybersecurity Teams were all top ranking for the internal calls. When it comes to partner teams who were called in, respondents stated that backup vendors, security vendors, and forensics specialists were all on the list.

It is worth noting that **94%** of the organizations surveyed stated they also pre-identified third parties that would be involved during the recovery process. This is a positive sign, showing that organizations are already implementing well-rounded strategic initiatives to better align across IT and security, thus better protecting themselves from ransomware.

When Incident response is a critical focus area of oncoming regulation in the EU due to the increasing frequency, complexity, and impact of cybersecurity incidents on essential and digital services. This emphasis ensures that entities are not only prepared to handle incidents effectively but also contribute to the overall cyber resilience of the European Union.

Andre Troskie,
CISO EU, Veeam

Did your organization engage any third parties as part of remediating the ransomware attack?



Don't Re-Infect During Recovery

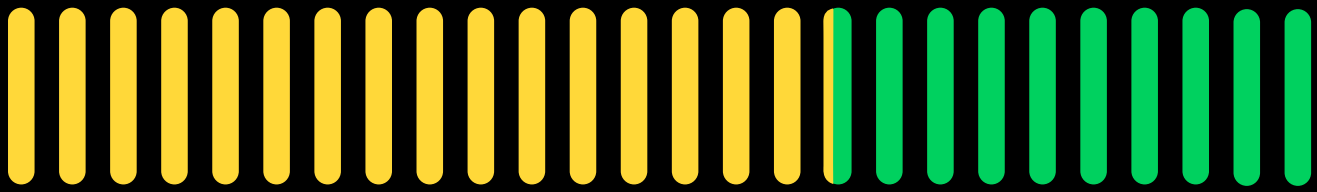
Upon initial discovery of a cyber event, containment is always the first step. After which, restoration attempts can begin. Unfortunately, this often places an inordinate amount of pressure on your organizations and employees to resume IT functionality as quickly as possible. It is not surprising that, in their haste to resume work as quickly as possible, **63%** restored directly back into their production environment without some type of quarantine or other scanning method during recovery.

By not being coordinated on proper scanning and testing of backup environments, your organization runs the risk of bringing ransomware back into your system.

Encryption of files is the most common form of impact observed. This may include forensics logs and artifacts as well that may inhibit an investigation.

63% restored directly back into their production environment

37% use a quarantine or sandbox



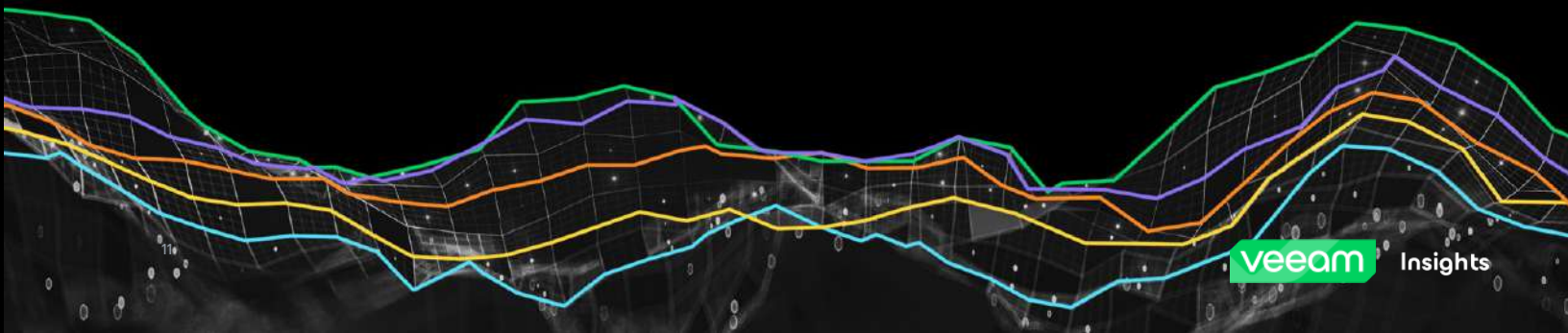
How to Better Prepare against Ransomware

Importance of a "Good Backup"

Of those surveyed, at the time of the attack, **95%** of organizations had a predefined incident response team with a predetermined plan for when a cyber event occurred. It is notable that the two most common parts of their backup process were the assurances of **clean** and **recoverable** data.

If you and your organization have a plan in place to recover your data safely — without being reliant on paying a ransom and hoping for the best — it is crucial to be sure that data is, in fact, recoverable. Assurance that your data is safe from bad actors and not at risk of reinfection critically involves predetermining a safe place for it to go, as well as isolation and mitigation strategies in the event of an attack. Said another way, ensuring recoverable data across both production and protection architectures that embrace Zero Trust principles is critical to your organization's survival.

> When in the digital battlefield, system backups are the last line of defense. Cyberattackers know this, and they've homed in on undermining these crucial fail safes. As CIOs, we must treat backups not as mere copies, but as strategic assets.
>
> John O'Neill Sr.,
> CIO, Molded Fiber Glass Companies



Plan on a Secondary Site for Recovery

Many organizations noted that a good portion (**31%**) of their infected servers were not able to simply be *"wiped and restored"* for myriad reasons. As such, it is important to plan for alternative infrastructure to be used to recover from a cyberattack like any other large-scale disaster.

These statistics emphasize that many organizations are planning an "either/or" strategy with at least one cloud destination, as well as some on-premises options, depending on which servers were affected, the location, or the scale of the attack.

> The big four impacted industries remained static quarter over quarter: Professional Services, Healthcare, Consumer Services and Public Sector. As we've noted in past reports, ransomware is, and has always been, an industry-agnostic crime.
>
> Bill Siegel,
> CEO, Coveware

Data gathered showed that 75% of organizations' plans include being able to recover to cloud-hosted infrastructure, and 86% of plans include leveraging physical infrastructure (original, new, or in another datacenter).

Did your organization pay ransom to recover its data?

4%
No ransom was asked

15%
No, we were able to recover data without paying

27%
Yes, but we still could not recover the data

54%
Yes, and we were able to recover the data

The Most Important Preparation is the Assurance of Recoverable Data

It was well established in this survey that many organizations are laying the necessary groundwork to have a resilient modern data protection and recovery plan. That said, it is heartening to see organizations embrace the industry-standard 3-2-1 rule of having multiple media types, regardless of whether those media types are or are not immutable. This yields two key considerations for 2024:

Most organizations have some amount of backup repositories being immutable (resistant to cyberattacks), with

85% of respondents using cloud storage that can be made immutable while…

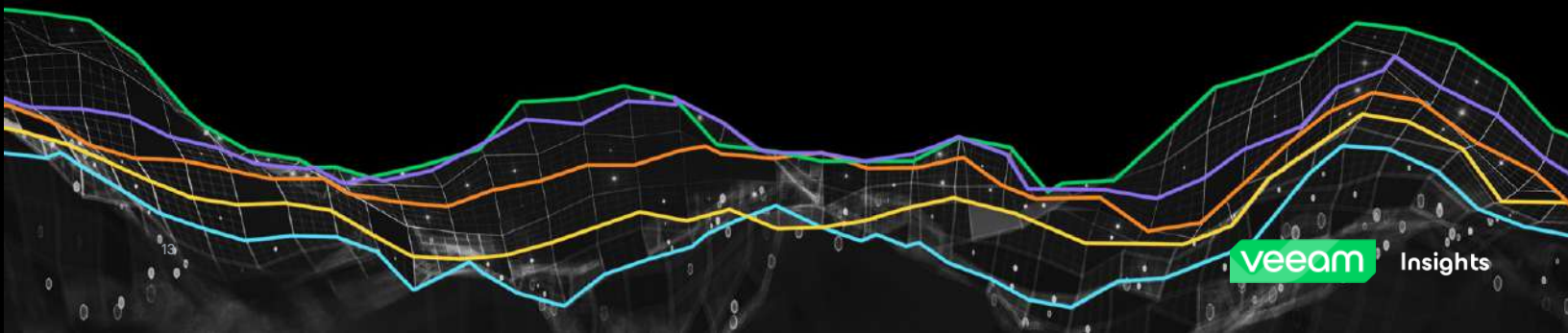
75% using local disk storage that can be locked down.

Beyond immutability, physical separation as part of the 3-2-1 rule continues whereby in addition to whatever disk repositories are on-premises.

47% of production data is still retained on tape, while…

54% is also replicated to cloud storage

These architecture decisions emphasize the importance of flexibility of where the recovery data will come from and the earlier statistics of where organizations intend to recover to.



Recommendations

Ransomware attacks will happen — regardless of prevention technologies or employee awareness training. Through the strategic alignment of **IT and security teams** and the implementation of robust security measures and technologies to ensure clean, secure, and recoverable backups, organizations will be better prepared to bounce forward from a ransomware attack by implementing the following best practices:

1. Help IT teams and security teams work better together

One of the most revealing trends in this report is the fractured strategy, tool sets, and organizational alignment between executive leadership, the security teams responsible for prevention and detection, and the backup teams tasked with protection and recovery.

In some organizations, especially those that handle large volumes of sensitive data, a cross-functional committee may oversee backup and disaster recovery planning. This committee typically includes representatives from IT, security, legal, and business units to ensure all perspectives are considered in the backup strategy.

2. Plan ahead

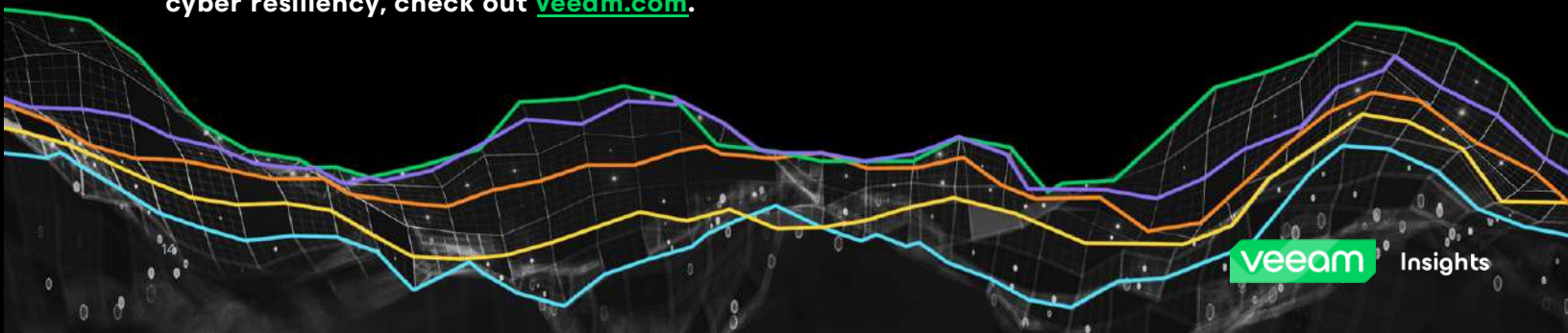
The attack will be worse than you imagined and cost more than you're expecting. Organizations should make cyber preparedness plans that include broadening the use of immutable repositories, isolation and authentication of backup systems, and verifying the recoverability of the backups within the organization to ensure the established SLAs.

Modern organizations should employ an incident response playbook or plan that allows for cross-team collaboration with the goal of utilizing a diversified immutable portfolio of disks, tapes, and clouds. And finally, being able to recover to both on-premises and cloud hosted infrastructure gives an organization its best potential to survive what could be an existential threat.

3. Ensure your backups are clean and reliable

Similar to any disaster or cyber preparedness strategy, even daily backups require routine testing to ensure their viability on your worst day. For cyber resilience in particular, organizations need to test not only the recoverability of their backup data, but also the assurance of its cleanliness through immutable repositories.

For more information and data protection and cyber resiliency, check out veeam.com.



Charts

*Charts not pictured but available for download here: https://vee.am/RW24charts

FIG 01

Did the threat actor attempt to modify/delete backup repositories as part of the ransomware attack?

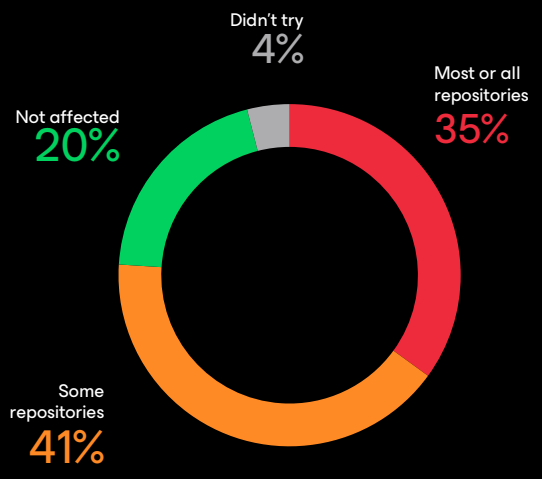


FIG 03

How did your organization pay for the ransom?

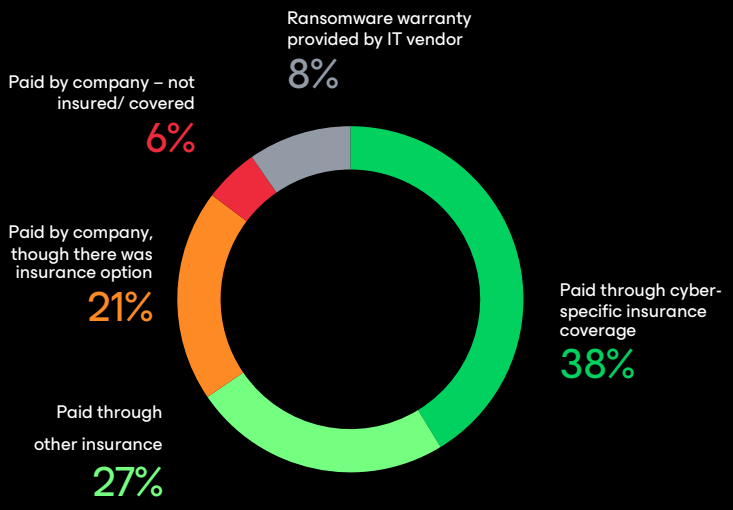


FIG 02

As a percentage, what was the total financial impact of the ransom payment?

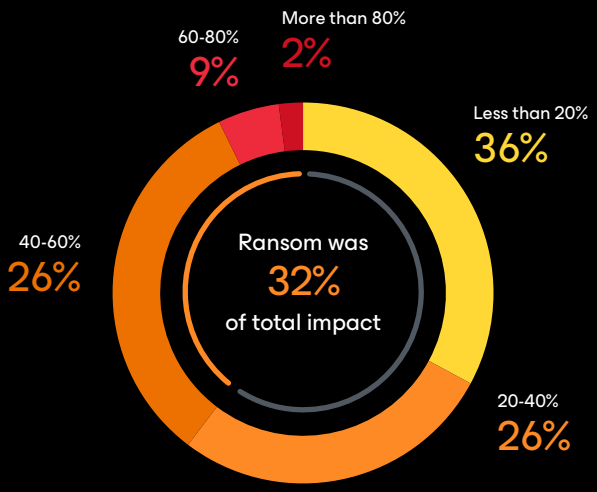


FIG 04

What percentage of your organization's production data do you estimate that the ransomware attack successfully encrypted?

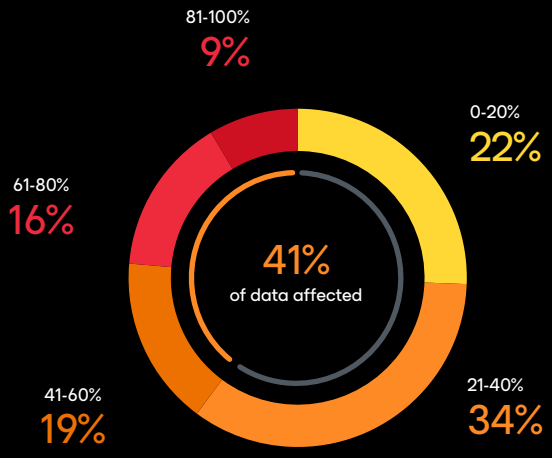


FIG 05

How did the organization ensure system data/backups were "clean" prior to restoration?

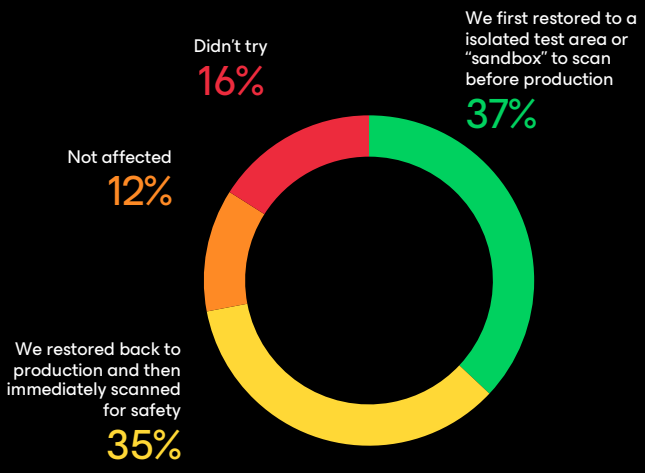


FIG 06

For your organization's more recent server recoveries from ransomware, where did you recover your data to?

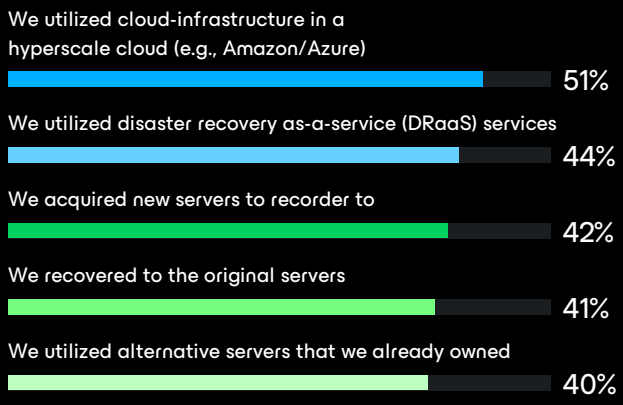


FIG 07

Prior to the incident, did your incident response team have a defined ransomware response playbook which incorporated any of the following?

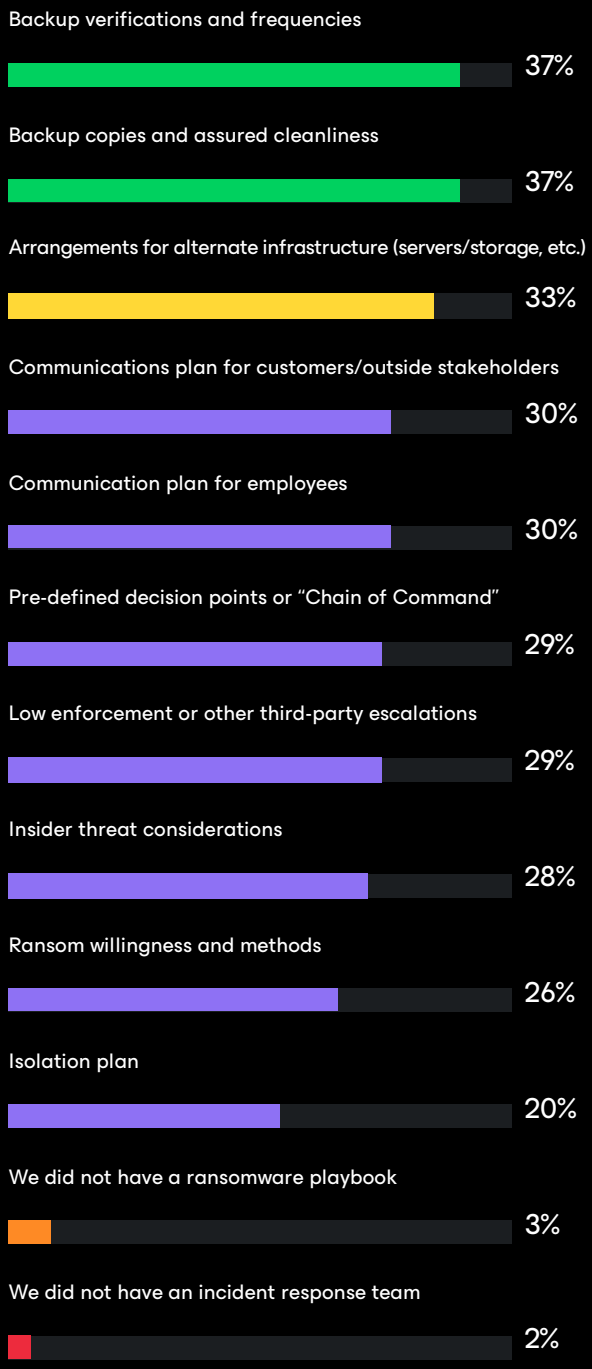
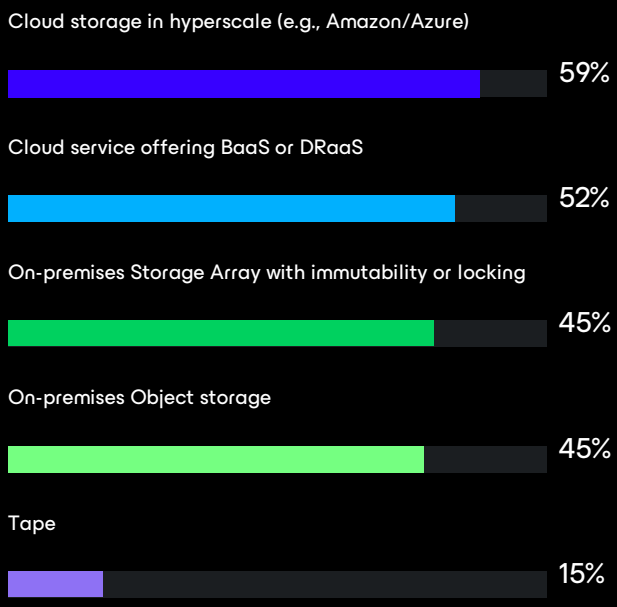


FIG 08

When a cyberattack happens in your organization, which teams are among the first to be actively engaged?

FIG 09

Does your organization utilize offline air-gapped or immutable backups using the following systems?



This data was surveyed by an independent research firm in early 2024 and then curated by two former industry analysts, previously from ESG and Gartner, with a combined 70 years in data protection. For questions related to the research methodology, its usage, or the insights: StrategicResearch@veeam.com.

Jason Buffington
VP, Market Strategy
@JBuff

Dave Russell
SVP, Head of Strategy
@BackupDave

veeam Insights