veeam Insights

Executive Summary

Ransomware Trends 2024

United States Edition

Provided by

element four
TECHNOLOGY SERVICES

According to the 2024 Data Protection Trends Report that surveyed IT leaders and implementers across 10 countries around the world:

- Only 25% of organizations believe they were not hit by ransomware in 2023
- 49% attest they were hit between one and three times that year
- 26% of organizations stated they were hit four or more times

Due to the high attack rates shown in this unbiased report each year, the Ransomware Trends Report was commissioned to better understand the attacks, the recoveries, and the lessons learned by using a double-blind anonymous survey of vetted IT leaders with firsthand experience with those cyberattacks to dig deeper through additional research: The 2024 Ransomware Trends Report.

Inside 2024 Ransomware Trends

The 2024 Ransomware Trends Report is the third annual publication of unbiased research conducted by a team of independent analysts surveying anonymous but vetted organizations who suffered at least one successful cyberattack in the preceding 12 months. Each year, this report curates 1,200 responses with an intentional breakdown of roughly 400 individuals in three key roles that are responsible for part of an organization's cyber resiliency strategy:

- **CISO or senior executive:** Responsible for an organization's cyber resiliency strategy
- **Information security professional:** Responsible for the prevention and detection of cyber events
- **Backup administrator:** Responsible for ongoing protection and recovery of IT data

Ransomware continues to be a growing concern for everyone in the IT industry. Gartner is globally forecasting a 3.5% planned increase in overall IT budgets for 2024. Respondents from EMEA in this survey are expecting budget increases of:

6.5%

increase in budget for cyber prevention and detection technologies

6.5%

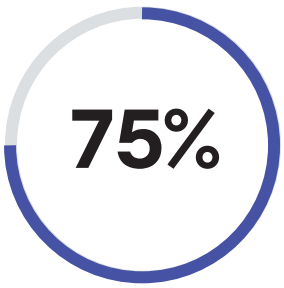
increase in budget for recovery technologies such as backup and business continuity/disaster recovery (BCDR)

Overall IT spending is up, increasing cyber resiliency budgets to nearly double the overall increase in IT spending. Thus, backup and cyber investments are taking "more than their share" of the increased IT investments while other areas are being deprioritized to address cyberthreats. Clean backup copies, which one might presume includes data that is 'survivable' against attacks and does not include malicious code.

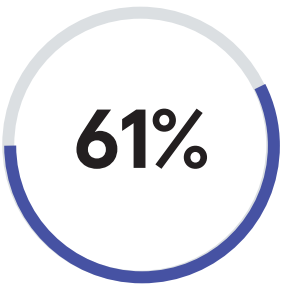
63% of Organizations Are Not Aligned

For the third year in a row, more than half of organizations — 57% in United States — believe that there is either a "significant improvement" or "complete overhaul" needed for organizations to be aligned between their backup and cyber teams.

Globally, of the three roles surveyed, backup administrators were the least satisfied with the alignment of their teams.



of backup admins believe a complete overhaul of their system is required



of security professionals are looking for changes in their organization

of CISO or other equivalent executives have concerns relating to their organizational alignment

It'll Take a Village to Recover

According to survey respondents, the two teams most often notified to kick off remediation efforts are the executives responsible for prevention and remediation and the IT backup team. This is quickly followed by cybersecurity experts and the organization's overall risk management team.

94% of the organizations surveyed stated they also utilized third parties during their recovery process, with these four types of experts being the most commonly engaged:

- **Security software vendors**
- **Backup software vendors**
- **Security specialists for forensics**
- **Resellers, partners, or service providers**

Expect to Lose 18% of Your Data from a Cyberattack

Two of the most impactful statistics from the 1,200 global lessons we learned in 2023 are:

of production data was successfully encrypted by bad actors in last year's attacks

of the affected data was recoverable after being encrypted in a ransomware attack

Unfortunately, if only 59% of your data was recoverable, then 41% was not; therefore, 16% of your production data was irrecoverable. Organizations of all sizes participated in this survey and surprisingly revealed that neither the size of their organization, nor their locale had a significant effect on their attack or recoverability rates. All organizations got hit roughly the same amount the world over and faced a similar amount of damage.

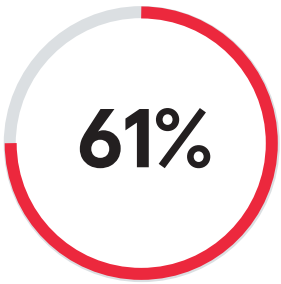
Organizations may also be surprised to find that there was not a significant variation between data center effects found in remote offices vs. branch offices, or even on data hosted in a public cloud vs. a private one.

Did You Pay? Did It Work?

Two key questions asked each year in this survey are:

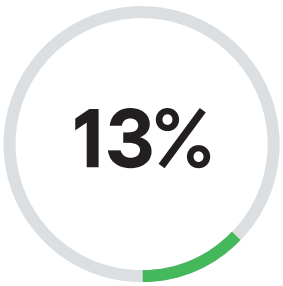
- **Did you pay the ransom?**
- **Were you able to recover?**

In 2023 within United States:



Paid and were able to recover their data from the attack

Paid but could not recover data lost in the attack



Recovered *without paying* the ransom that was demanded

The global results were similar:

- 54% paid and were able to recover their data from the attack
- 27% paid but could not recover data lost in the attack
- 15% recovered without paying the ransom that was demanded

With the remaining 2%, no ransom was asked for. These stats are notable namely because it shows that roughly **one in four organizations that paid the ransom still could not recover *even after paying*.**

There's More to an Attack than the Ransom

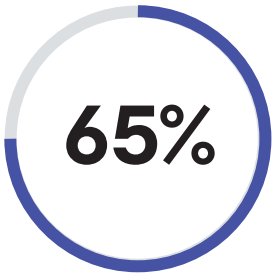
95% of organizations believe they have insurance, though 23% of those insurance policies specifically exclude ransomware. However, the costs of prevention, detection, recovery services, and the ransom itself are far from the only financial factors that can impact your organization in the event of a ransomware attack. In fact, out of all the responses to this year's survey, only 1 in 9 organizations (11%) stated that ransom payment made the significant majority of the overall financial impact to their organization. For the rest of the cyber victims, the overall financial impact was substantially more than "just" the ransom itself.

61% of Organizations Paid Their Ransom with Insurance

Regarding companies' internal policies in 2023, only a few organizations (18%) did not have a policy for whether to pay or not. While the majority of organizations did have a policy, there were ***nearly equal sentiments towards paying (51%) versus not paying (32%).***

Regardless of whether they had a policy or not, it should not surprise anyone that while only a minority of organizations had a policy to pay, 85% ended up paying. That said, 61% paid with insurance and another 21% had insurance but chose to pay without making a claim. This means that in 2023, 82% of organizations had insurance that they could have used for a cyber event.

These options will diminish as cyber insurance continues to change in response to ever increasing claims. At last renewal:



of organizations experienced a premium in response to the changing IT landscape

had their deductible increased due to ransomware and cyberattacks becoming more common

saw their coverage benefits reduced as insurance companies tried to protect themselves from the growing threat of ransomware

Cyber Villains Want Your Backups

In much the same way that your prevention team's playbook expects a clean and recoverable backup, the cyber villain's playbook intends to disable your ability to recover your own data. Unfortunately, in far too many attacks, the attackers are successful in removing your ability to save yourself. Thus, the data shows that only 13% of organizations recovered without paying. On average, 35% of backup repositories were affected by a successful attack.

67% Do Not Have a Recovery Plan

In 95% of all organizations — who had a team with a plan — the two most common aspects of their incident response playbook was the assurance of clean and recoverable data.

This explains why 36% of organizations in United States have an alternate infrastructure in their plan, which unfortunately means that the other 64% do not have a plan for where they will recover after a site-level crisis.

However, cyberattacks affect not only the organization and its teams, but the individuals caught most in the fray as well. Of those surveyed this year, the key personal effects included increased workload, stress, and other human factors which most organizations already struggle to balance or mitigate even on "normal" days.

The Attack Will Be Worse than You Imagined and Cost More than You're Expecting

With 40% of data affected by a cyberattack and only 59% of that affected data being recoverable, organizations can reasonably expect to lose 16% of data per cyberattack. Moreover, the ransom averages to make up only 38% of the overall financial impact while only 65% of the overall impact is in some way reclaimable through insurance or other means. This comes along with everything else going against the organization's bottom dollar budget.

2024 Is Not Immutable Enough

In 2024, it is not unreasonable that organizations would embrace immutable storage within their on-premises disk, complemented by immutable cloud repositories and air-gapped tapes. Unfortunately, even of those who have suffered at least one cyberattack in the past, only 70% use hardened disks on-premises, and only 89% use immutable clouds.

Only 54% of organization's overall backup storage is immutable.

That said, it is encouraging that organizations are embracing the industry standard 3-2-1 Rule of having multiple media types, regardless of whether those media types may be immutable or not. In 2024, in addition to whatever disk repositories are on-premises, 42% of production data is still retained on at least one tape while 50% is also replicated to a cloud.

This research brief is based on 1,200 survey responses, including 400 from United States, all of whom were unbiased IT leaders and implementers responsible for their organization's cyber-resiliency strategies, including CISO's, IT Security Professionals, and Backup Administrators. This survey was conducted in early 2024 and published in June 2024. The data was curated and sentiments were authored by two former industry analysts, previously from ESG and Gartner, with a combined 70 years in data protection.

Questions about this research and insights/assets published from it can be sent to StrategicResearch@veeam.com

The Veeam Perspective

Veeam® believes that secure backup is your best line of defense against ransomware. Veeam is committed to helping organizations minimize downtime and data loss, so that they never have to pay a costly ransom. Only Veeam provides the most recovery options on the market, and a truly portable data format, empowering you to recover, anywhere: from physical to virtual, between clouds or even the cloud to an on-premises data center. There's no one silver bullet to solve your ransomware problem, which is why Veeam takes a multi-layered approach to ransomware protection and recovery.
To learn more, please visit https://www.veeam.com/ransomware-protection.html

About Veeam Software

Veeam®, the #1 global market leader in data protection and ransomware recovery, is on a mission to empower every organization to not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 74% of the Global 2000, who 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.

element four
TECHNOLOGY SERVICES

Contact us to get started and manage Veeam
Element-4.com