Insights

Executive Summary

Ransomware Trends 2024

US Federal Government

According to the 2024 Data Protection Trends Report:

- 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 report each year, the 2024 Ransomware Trends Report was commissioned to better understand the attacks, the recovery process, 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. However, respondents from the US federal government in this survey are expecting budget increases of:

6.6%
increase in budget for cyber prevention and detection technologies

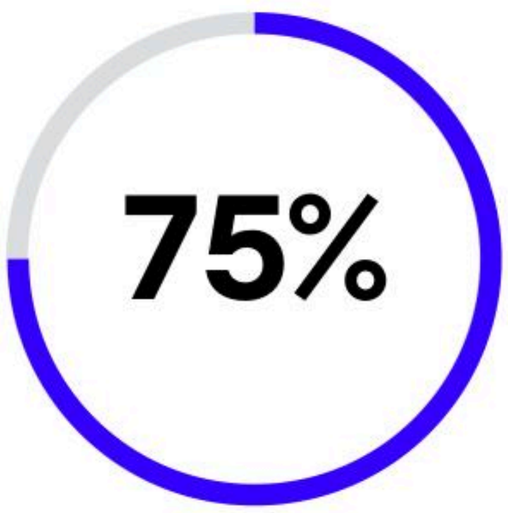
6.3%
increase in budget for recovery technologies such as backup and business continuity/disaster recovery (BCDR)

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. It's worth pointing out that these large increases in both cybersecurity tools and in data recovery technologies are related. Agencies increasingly recognize the requirement for hardened, clean backup copies, which include data that is 'survivable' against attacks and does not include malicious code.

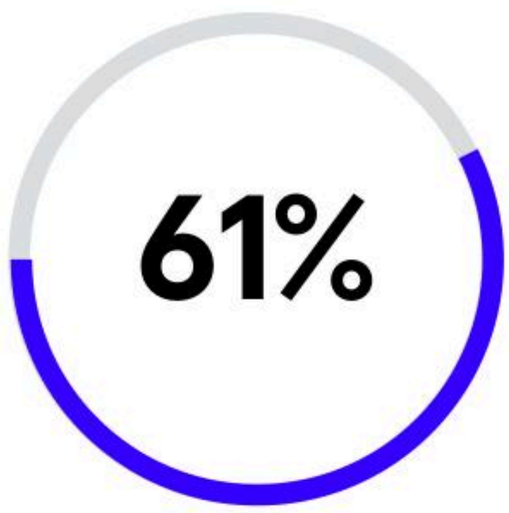
63% of Organizations Are Not Aligned

For the third year in a row, more than half of organizations — and a whopping 73% of federal respondents surveyed — believe that there is either a "significant improvement" or "complete overhaul" needed for organizations to be aligned between their backup and cyber teams.

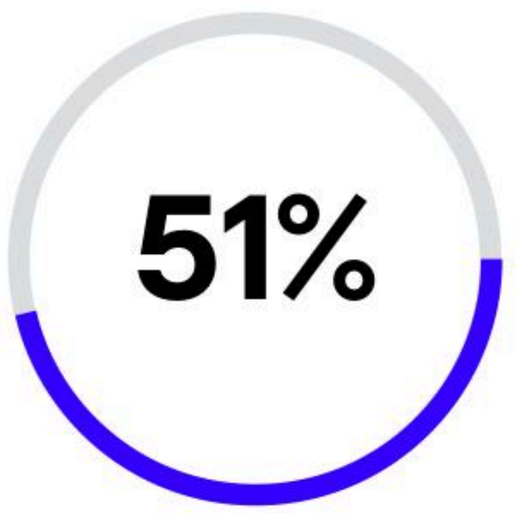
Globally, of the three roles surveyed, backup administrators were the least satisfied with the alignment of their teams.



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

Almost three out of four federal (civilian and DoD) organizations polled believe that major improvement is needed in coordination between cyber and backup teams. This reflects pressures being exerted by several factors:

- While federal agencies as a policy do not pay ransoms, this has not prevented threat actors from attacking federal organizations at virtually the same rate as private sector entities.
- The prevalence of cyber warfare in the Russia/Ukraine conflict and the importance of hardened backups for survivability of Ukraine's civilian and military systems has been repeatedly called out by the US intelligence community.
- The increasing focus on federal cyber resilience mandates, including zero trust strategies called out in EO 14028
- And most obviously, a global threat environment escalating constantly through attacks by both criminal actors and hostile nation-states

Together, these factors have made it clear, especially to data protection teams, that closer coordination between security and infrastructure operations is a critical priority.

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.

100% 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**

Federal respondents are clear: recovery from a cyber incident will involve not just your agency or command's personnel but also a cohort of outside experts. This has clear implications for incident response planning and exercises. Plans should be structured to make it easy to contact outside parties (even if all IT systems are offline). And response exercises should include the vendors and outside experts who will be called on during a genuine recovery.

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 57% of your data was recoverable, then 43% was not; so extending the math, on average after an attack 18% of 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.

These figures are particularly troubling in the context of US federal respondents. For many datasets and citizen services, federal agencies are the most trusted and most critical provider. There is potential for severe mission disruption if almost 20% of agency data is typically lost in a cyber-attack. For the warfighter on the tactical edge, the consequences are even more severe. Once again, these numbers point to:

- an urgent requirement for better coordination between security and data protection functions, and
- a need for rapid implementation of resilient data protection technologies for all production mission datasets.

Data in Every Environment is Affected

In the global sample, organizations may also be surprised to find that there was not a significant variation between ransomware effects found in remote offices vs. branch offices, or even on data hosted in the public cloud. This is in itself a significant finding, and it's one that many organizations haven't previously understood. Each year this survey asks respondents "What % of each type of production platform were affected by the last ransomware attack?" As in years past, in the global sample there is virtually no difference between data loss to a ransomware attack in any of these three environments.

However, the US federal statistics look quite different. Federal survey respondents who said "All or most data was affected":

Datacenter server data

Remote office data

Cloud-hosted platforms

In other words, among US federal respondents, a ransomware attack was more than twice as likely to affect all or most of their cloud-hosted data than to affect that much data in remote offices or on-prem datacenters.

This is a significant and troubling finding for federal IT leaders. It's still common for agencies to confuse the higher uptime stats for cloud services and platforms with true malware-resistant data protection. While it is true that hyperscale cloud providers offer impressive security and operational uptime, their shared responsibility models make it clear that the onus of data protection ultimately falls on the federal customer, not the service provider.

Federal IT and security leaders and practitioners urgently need to educate their teams on this facet of cloud data security. Yes, you still need good backups, even in the cloud.

There's More to an Attack than the Ransom

It is common to consider ransoms paid as a major financial loss component of malware attacks. 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 impact was substantially more than "just" the ransom itself. This is particularly true of federal agencies and US DoD branches and commands. Data loss and mission disruption here can lead to losses measured in lives rather than financial losses.

Returning to lessons learned from the Ukraine/Russia conflict, cyber attacks are now an established part of the modern battlefield. These attacks occur directly on military capabilities and targets, but they don't stop there. Critical infrastructure and financial resources are also virtually guaranteed to be attacked, extending the battlefield far from the tactical edge deep into America's critical infrastructure and citizen services.

Threat Actors Want Your Backups

In much the same way that your prevention team's playbook expects a clean and recoverable backup, the adversary'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. For US federal organizations, an average of 35% of backup repositories were affected by a successful attack. This figure maps exactly to that of the global sample, which was also an average of 35%.

64% Do Not Have a Recovery Plan

Malware attacks require recovery options that differ from other types of outages. Unlike data loss caused by misconfiguration or minor infrastructure failures, malware attacks generally require the ability to recover to alternate infrastructure and to sanitize restored data of malware before it goes back on the network. Unfortunately the data show that most organizations globally have not fully prepared for these requirements.

This explains why 36% of US federal organizations 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.

To put this requirement in perspective, the survey also asked federal organizations "Were any parts of your production IT infrastructure not allowed to be immediately wiped/recovered due to insurance, legal, or other forensics?" 19% of federal respondents replied that many, most, or all of their production systems were out of bounds for restore immediately after an attack due to ongoing digital forensics.

In other words, for roughly 1 in 5 US federal workloads restoring data in-place was not an option. After a cyber-attack, agencies need a clean offsite recovery area with secure backup data already in place to begin recovery efforts. Unfortunately for the 64% of responding agencies without an alternate site as part of their recovery plan, it's unlikely that these steps have been taken.

Given current supply chain constraints and the time that it takes to move backup data to the cloud or a net new environment, this will almost certainly lead to significant mission downtime. Federal IT and security leaders should also bear in mind that 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.

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 80% use hardened disks on-premises, and only 85% use immutable clouds.

Only 45% 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, 52% of production data is still retained on at least one tape while 60% is also replicated to a cloud.

This research brief is based on 1,200 survey responses in comparison to 200 respondents from the US Federal Government 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

Reach out for more details: veeam@marketplace.cgc.cloud

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 resilience, believes every business should control all their data whenever and wherever they need it. We're obsessed with creating innovative ways to help our customers achieve data resilience. We do that by offering purpose-built solutions that provide data backup, data recovery, data freedom, data security, and data intelligence. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.