2023 EXECUTIVE SUMMARY

RANSOMWARE TRENDS

NORTH AMERICA EDITION

According to the 2023 Data Protection Trends Report, 85% of organizations suffered at least one cyberattack in the preceding twelve months; an increase from 76% experienced in the prior year. To better understand the preparedness and recoverability of cyberattacks, an independent research firm conducted a blind survey of 1,200 unbiased IT leaders whose organizations suffered at least one ransomware attack in 2022 — including 350 for North America.

This is the second annual survey of organizations who suffered cyberattacks with a key focus to compare the viewpoints of four different roles that are involved in cyber-preparedness and/or mitigation: Security professionals, CISO or other IT executives, IT Operations generalists and backup administrators.

The full 2023 Ransomware Trends Report is available at https://vee.am/RW23.

"IT takes a village" … but organizations aren't aligned

While many organizations may ***say*** that 'ransomware is a disaster' and therefore include cyberattacks within their Business Continuity or Disaster Recovery (BC/DR) planning, the ***actual*** interaction between the teams leaves much to be desired.

55%

believe either 'significant improvement' or 'complete overhaul' is needed between the Cyber and Backup teams.

42%

believe their risk management program is working well, with the rest either seeking improvement or do not have a program yet.

That said, there is alignment on two areas: budget and playbooks. For 2023, cyber (prevention) budgets grew by **5.5%**, while backup (remediation) budgets grew by **5.5%**. Beyond that, when asked about Incident Response Teams and how organizations plan on dealing with the inevitability of cyberattacks, the most common elements of the 'playbook' in preparation to recover are:

- Clean backup copies, which one might presume includes data that is 'survivable' against attacks and does not include malicious code.
- Recurring verification that the backups are recoverable.

Cyber insurance can help … if you can get it

Globally, **77%** of ransoms were paid by insurance, with **75%** of cyber-victims in North America paying via insurance. But cyber-insurance is becoming harder and more expensive, with **20%** of organizations stating that ransomware was now specifically excluded from their policies. While those with cyber insurance saw significant changes in their last policy renewals:

75%

saw increased premiums

42%

saw increased deductibles

13%

saw coverage benefits reduced

Paying the ransom does not ensure recoverability

What might surprise some people is that even though most respondents paid the ransom, many of them actually had 'do not pay' policies from either their corporate management or a governmental regulation. That said, even paying the ransom is not a guarantee that you'll be able to recover.

63%

paid the ransom and could recover data

19%

paid the ransom but could not recover data

14%

did not pay the ransom because they recovered from backup

Sadly, the global statistic that **16%** of organizations that were able to recover themselves without paying is down from **19%** in last year's survey.

To recover without paying, your backups must survive

In at least **93%** of cyber-events, the criminal attempted to attack the backup repositories, which effectively negates any other options other than paying the ransom.

76%

of organizations lost at least some of their backup repositories during the attack

34%

of backup repositories were lost when the cyber-villain was able to affect the backup solution

When you first get attacked, you have two choices: pay or restore-from-backup. By attacking the backup solution, the cyber-villain is removing one of their victims' choices.

The secret to survivable backups is immutability

There are other best practices such as securing the backup credentials, automating the cyber detection scans of backups, auto verifying that backups are actually restorable, etc., but a key tactic is to ensure that the backup repositories cannot be deleted or corrupted. This is 'immutability' and can be enacted throughout the data protection lifecycle:

82%

of organizations use immutable cloud repositories

64%

of organizations use immutable disk storage

And when it comes to survivable media, it is hard to be more 'air-gapped' than a tape cartridge that is removed from its drive and stored on a shelf. In fact, **47%** of data is still written to a tape at some point in the data protection strategy.

The secret to recoverability is portability

Like in any other disaster (e.g., fire, flood, tornado), one key strategy decision is ***'where will we recover to?'*** — meaning that if the production servers are compromised, you'll need new ones. While larger organizations may have multiple datacenters with 'cold' servers standing by, many do not, so it is not surprising that most survey respondents had a hybrid plan:

66%

of organizations plan to recover to cloud-hosted infrastructure or DRaaS

81%

of organizations plan to recover to servers within a datacenter

It is notable that the intent to recover to servers within a datacenter could include:

- Cold-servers that were standing by, such as the dual-datacenter model.
- Acquiring new servers if supply chains permit.
- Simply wiping and re-using the original servers, assuming they aren't taped off for forensics or law enforcement.

Since the two statistics add up well beyond 100%, it is heartening that most organizations' BC/DR and cyber resiliency strategies include both location types, depending on the crisis.

Do not re-infect during recovery

Like the doctor's motto of "Do no harm" is the mindset of not reintroducing the malware or cyber-infected data into the production environment during restoration. With other disasters (e.g., fire/flood), the data in the backups, replicas and snapshots, is valid to immediately begin recovering with. Unfortunately, one of the many complexities in cyber warfare is that the data immediately prior to receiving the ransom demand is likely compromised too.

So, it is important to thoroughly scan data during the recovery process.

This is not always an easy task, based on whether the data protection solution offers integration with detection technologies (during backup, restore or both), as well as some kind of 'staging' or 'sandbox'. When asked to the cyber-victims within the survey:

- **44%** first restored to an isolated test area or 'sandbox' before reintroducing to production.
- **35%** restored to production and then immediately scanned.
- **12%** restored and then simply monitored behaviors.
- **9%** had no means of preventing reinfection.

Concluding remarks from the research

Based on lessons learned from the **1,200** attack experiences within this survey, most organizations today employ a few key technologies in preparation for the next assault:

- **Immutable storage** within disks, clouds and air-gapped media, to ensure survivability.
- **Hybrid IT architectures** for recovering to alternative platforms like any other BC/DR strategy.
- **Staged restorations**, to prevent re-infection during recovery.

Questions related to this research data and insights can be directed 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 provides organizations with resiliency 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 give businesses peace of mind their apps and data are protected and always available so that they can keep their businesses running. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 82% of the Fortune 500 and 72% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers, service providers, and alliance partners. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeam-software and Twitter @veeam.

Scan to learn more about Veeam ransomware solutions