2023 GLOBAL REPORT

RANSOMWARE TRENDS

Lessons learned from 1,200 victims and nearly 3,000 cyber attacks

veeam

Ten questions that you didn't want to ask... and the answers are worse than you want to know.

Introduction

According to the 2023 Data Protection Trends Report, 85%* of organizations suffered at least one cyber attack in the preceding twelve months; an increase from 76% experienced in the prior year.

To better understand the preparedness and recoverability of cyber attacks, an independent research firm conducted a blind survey of 1,200 unbiased IT leaders whose organizations suffered at least one ransomware attack in 2022. Organizations of all sizes from 14 different countries across APJ, EMEA and the Americas were represented.

The survey asked about the impact that ransomware had on their environments, as well as what their IT strategies and data protection initiatives are moving forward. While analysts forecasted growth in overall IT spending for 2023 between 4.5%** by IDC and 5.4%*** by Gartner, respondents in this survey expect their cyber security (preventative) budgets to grow by 5.6% and their data protection (remediation) budgets to grow by 5.5% in 2023.

ABOUT THE RESEARCH

This is the second annual survey of organizations who suffered cyber attacks with a key focus to compare the view-points of four different roles that are involved in cyber-preparedness and/or mitigation:

37%
Security professionals

21%
CISO or other IT executive stakeholder

21%
IT operations generalists

21%
Backup administrators

Questions about these research findings can be sent to StrategicResearch@veeam.com

* 2023 Data Protection Trends Report, January 2023, n=4,200
** IDC, Technology to Scale the Digital Business: The Golden Era of IT; Innovation to Automation, Doc #DR2023_GS1_CDP, March 2023
*** Gartner, Forecast Analysis: IT Spending, Worldwide, February 2023

60% of organizations need significant or complete overhauls between their backup and cyber teams

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

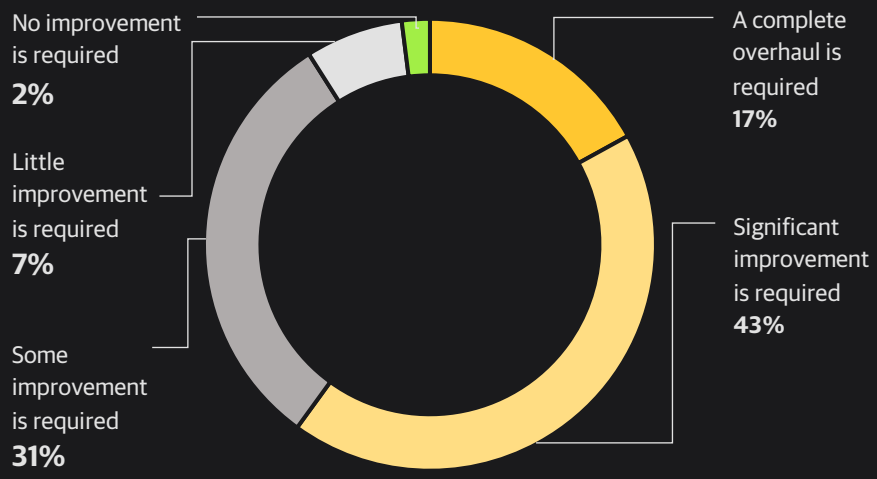
One of the consistent findings of this research over the past two years has been that those roles closest to the challenges of cyber events are often the least satisfied with the partnering between the teams.

Those believing their teams' alignment needs either 'significant improvement' or a 'complete overhaul' include:

- **70%** of backup administrators
- **59%** of security professionals
- **62%** of IT operations
- **51%** of CISO or IT execs

FIG 1

How much improvement do you believe is required in order for your organization's IT backup team(s) and your cyber-security team(s) to be fully aligned?
n=1,200



The most common element of an incident response playbook is a good backup

87% of organizations have a risk management program that drives their security roadmap or strategy. That said, only **35%** believe their program is working well, while **52%** are seeking to improve their situation and the remaining **13%** do not yet even have an established program.

Regardless of what you call your program or team that is chartered with planning against cyber events and preparing for how the organization will deal with them, the most common elements of the 'playbook' in preparation against a cyber attack 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

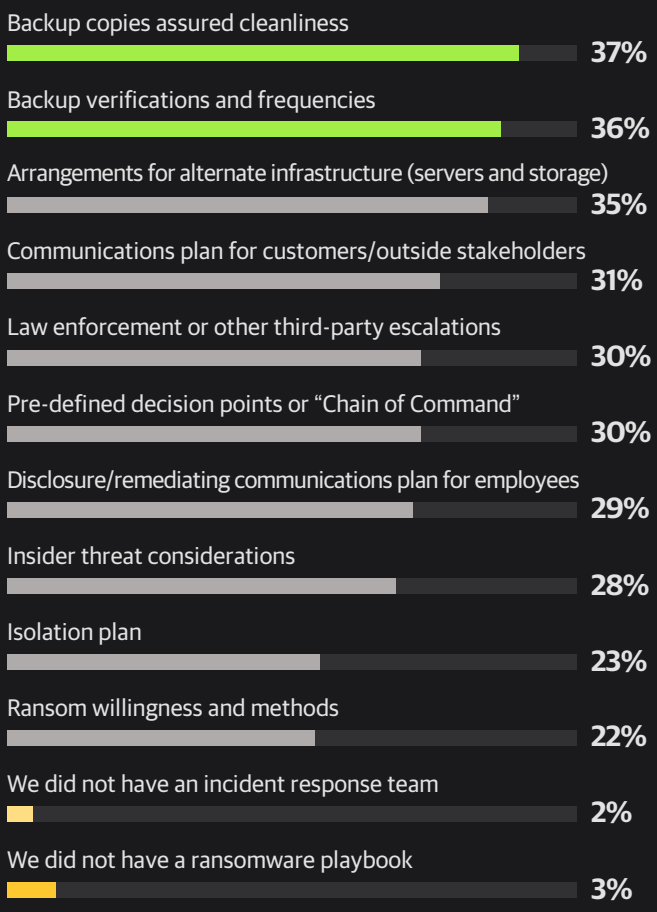


FIG 2

Prior to the incident, did your incident response team have a defined ransomware response playbook which incorporated any of the following?
n=1,200

77% of ransoms were paid by insurance, but that is becoming harder and more expensive

In 2022, paying the ransom via insurance was an option for **96%** of cyber victims, with half of all respondents using cyber-specific insurance.

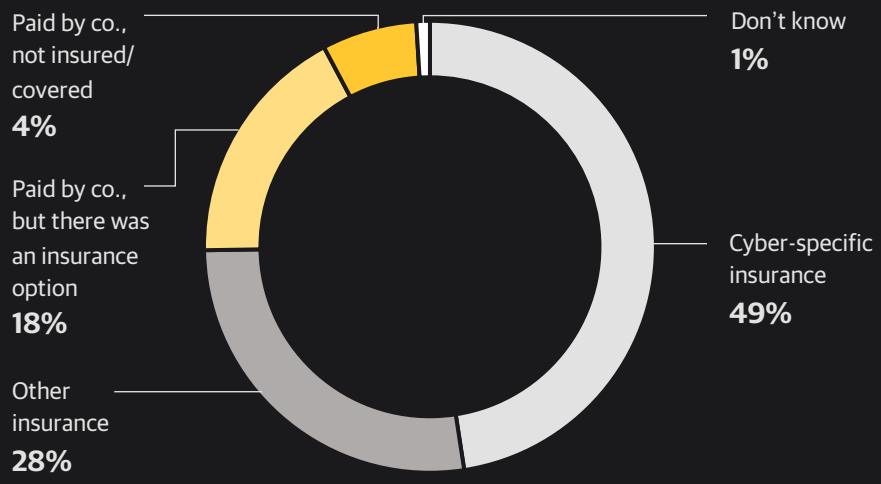
Interestingly, **28%** used insurance that was not cyber-specific, while **18%** chose not to use insurance that was available to them. These options might increasingly become the norm, as insurance becomes more expensive or less available, like homes that cannot acquire flood insurance due to increasing storm frequency.

In fact, **21%** of organizations stated that ransomware was now specifically excluded from their policies. While those with cyber insurance saw changes in their last policy renewals:

- **74%** saw increased premiums
- **43%** saw increased deductibles
- **10%** saw coverage benefits reduced

FIG 3

How did your organization pay the ransom?
n=914



80% of victims paid the ransom, but many still could not recover

The right answer ought to be "We did not pay, since we were able to recover our data," but only **16%** of organizations responded that way, which is slightly down from **19%** in last year's survey.

It is worth noting that **41%** of organizations have a "do not pay" policy, while **43%** of organizations do not have a policy to pay or not. That said, **80%** paid.

Unfortunately, while **80%** of respondents acknowledged paying, one fourth of them still could not recover their data even after paying the ransom. Can you imagine sending the bitcoin, but the decryption tool didn't work (or wasn't given at all)?

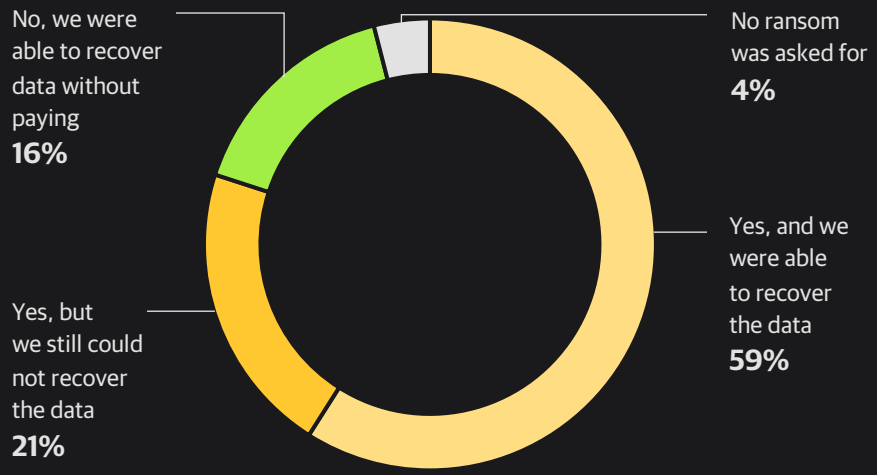
There are two probable reasons why the ransom was paid:

The **ransom was paid** with insurance money, instead of by organization, as covered in FIG 3

The backup repositories were also affected by the cyber attack, so **no recovery option was possible**. This is covered in FIG 6

FIG 4

Did your organization pay ransom to recover its data?
n=1,149



45% of production data was affected by a cyber attack

This is unfortunately consistent with last year's **47%** affected statistic, with no reason to assume future attacks won't result in a similar catastrophic amount of data loss or impact.

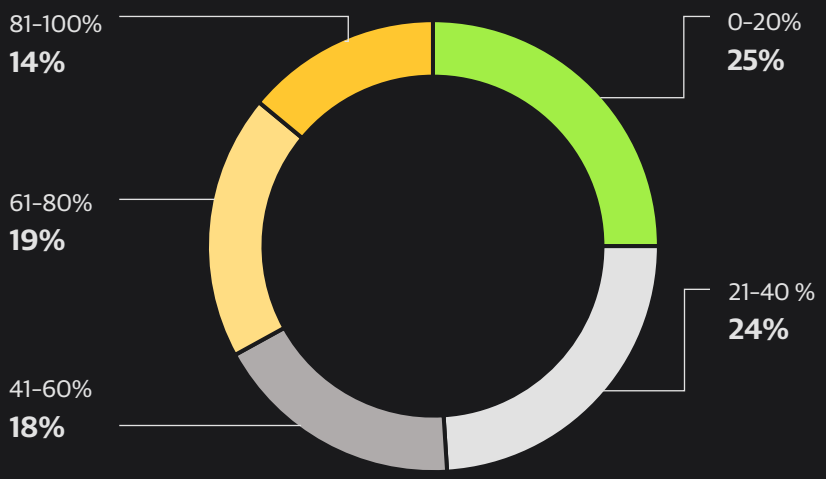
On average, organizations stated that **45%** of their production data was affected by the cyber attack. In looking at the extremes, **25%** had a small portion (<20%) of their data affected, while **14%** had nearly all (>80%) of their data affected by the attack.

Unfortunately, only **66%** of the affected data was recoverable. This calculates that **15%** of the organizations' production data was unrecoverably lost.

As an aside, cyber victims were also asked of their confidence before and after the attack. In hindsight, only **59%** considered themselves 'prepared' — and even then, the results did not vary greatly on how impactful the attack was.

FIG 5

What percentage of your organization's production data do you estimate that the ransomware attack successfully affected or encrypted?
n=1,200



Cyber villains were able to affect the backup repositories in 75% of attacks

Said another way, one in four organizations had backups to restore from, which is down from last year when one in three organizations had survivable backups.

In fact, bad actors targeted the backup repositories in at least **93%** of attacks in 2022, nearly identical to the **94%** of repositories that were targeted in 2021.

The respondents who stated that "some," "most" or "all" of their repositories were affected (FIG 6), FIG 7 reveal that on average, **39%** of backup repositories were affected.

Combining those statistics means:

75% likelihood that backup repositories affected

When affected, **39%** of repositories unusable

This will result in roughly **one third** (29%) of restores not being viable.

FIG 6

Did the threat actor attempt to modify/delete backup repositories as part of the ransomware attack? *n=1,200*

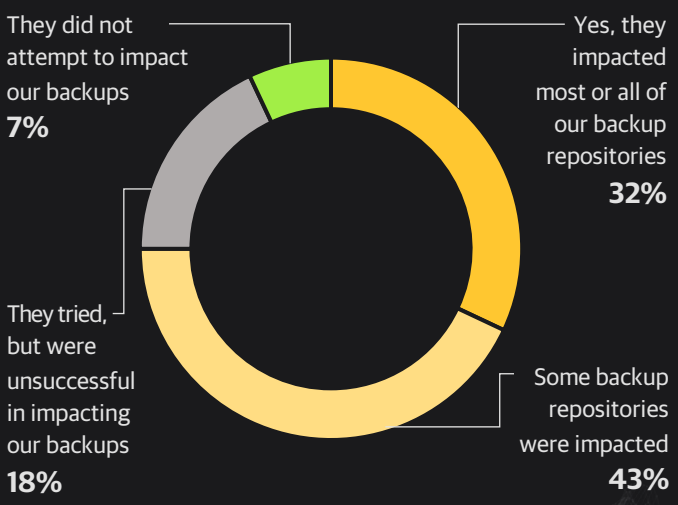
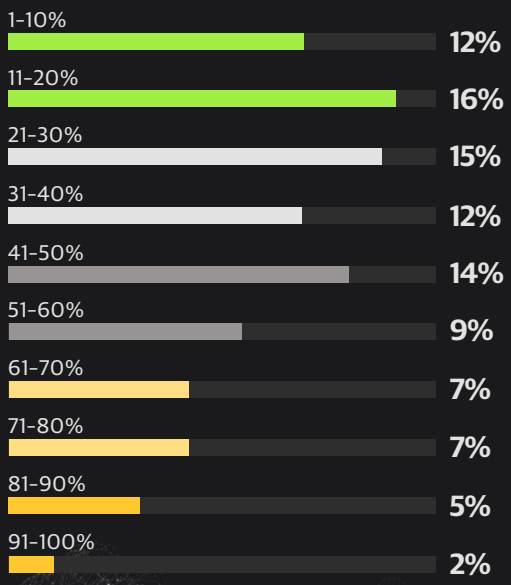


FIG 7

What percentage of the backup repositories did the cyber attackers modify or delete? *n=900*



It takes at least 3 weeks to recover (per attack) — after triage

Like any disaster, recovering a wide range and number of IT systems takes time. Respondents to the survey estimated that it took them **3.3 weeks** from when they earnestly began until they considered their recovery efforts essentially "complete." BUT there was a recognized caveat:

If you are recovering from fire, you immediately start recovering the burnt servers.

If you are recovering from flood, you immediately start recovering the wet servers.

In both cases, the last known backups or replicas are trusted to begin recovery immediately.

But when you recover from ransomware, there is an unpredictable amount of time to:

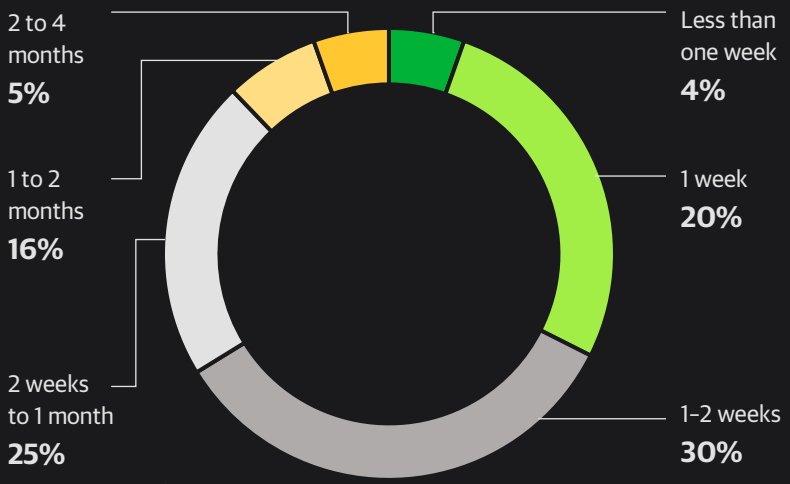
Identify which servers are infected

Determine that the backup/replica versions are not also affected or might reintroduce malware

Only after you know those criteria can you *start* to recover, after which the process will take an average of 3+ weeks.

FIG 8

How long did the entire remediation/recovery take before the organization at large would say the event was "over"?
n=1,200



82% use immutable clouds, 64% use immutable disks, and tape still matters in 2023

Only **16%** were able to recover instead of paying the ransom (FIG 4). To do that, they had to have recoverable data within the repositories.

Less than **25%** of victims stated that their backup repositories were not affected by the attacker (FIG 6). The way to do that is immutability or air gapping, so that the backup repositories are not malign-able by the cyber villain.

For 2023, only **2%** of organizations do not have immutability in at least one tier of their backup solution, with many reporting that they have immutability or air gaps across multiple tiers. In 2023, it is very achievable for backup data to be immutable across its entire data protection lifecycle, including short-term disk, within BC/DR capable clouds and long-term tape storage.

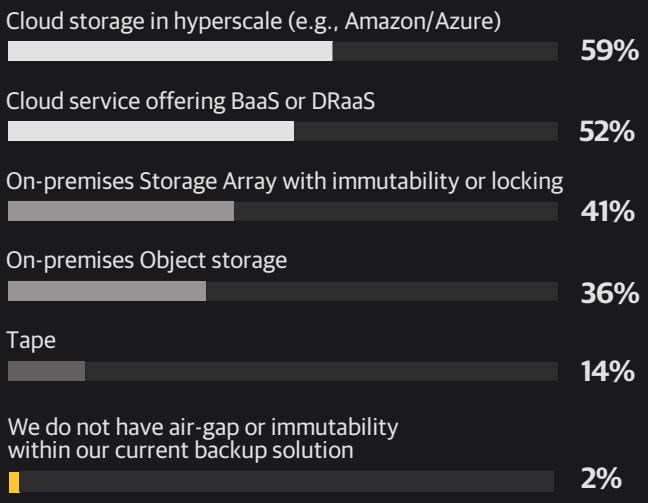


FIG 9

Does your organization utilize offline, air-gapped, or immutable backups using the following systems?
n=500

56% of organizations run the risk of re-infection during restoration

When respondents were asked how they ensure that data is 'clean' during restoration, **31%** stated that they rely on immutable repositories — which while this is a best practice, it does not guarantee 'clean' data.

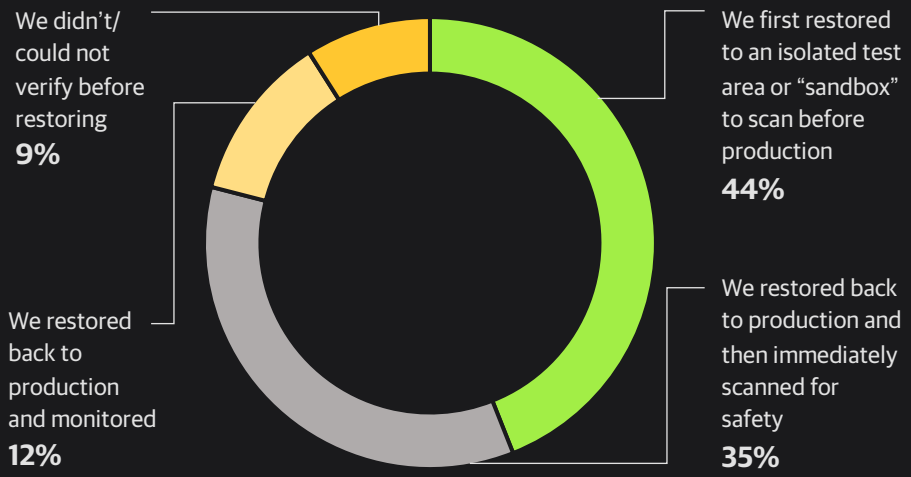
This is analogous to ensuring a leak- and tamper-proof bottle; which is not the same as ensuring that the contents within the bottle are safe or non-poisonous.

FIG 9 looks at the kinds of immutable storage being utilized for 2023, while the remaining responses in FIG 10 show that **44%** of respondents complete some form of staging to re-scan data from the backup repositories prior to reintroduction into the production environment.

Unfortunately, that means that **56%** of organizations run the risk of re-infecting the production environment by not having a means to ensure clean data during recovery.

FIG 10

How did the organization ensure system data/backups were "clean" prior to restoration?
n=950



71% would recover to a cloud, 81% would use a datacenter

Like any BC/DR strategy, one of the key IT decision questions is "Where will the servers recover to?" including cloud-based and datacenter infrastructure.

For fire or flood, one presumes the original datacenter is unavailable. Cyber attacks may have the option to use the existing datacenter (with new servers) or even the original servers (wiped); but not always, depending on whether the original servers or facility are seized by law enforcement or other forensics is required.

In 2023, the most anticipated alternate site for ransomware recovery at scale was cloud-hosted infrastructure, closely followed by managed disaster recovery as-a-service (DRaaS) platforms; which makes sense considering the high percentage of organizations intending to use cloud-repositories as their immutable recovery source (see FIG 9).

Most organizations are flexible:

19% only plan to recover to a cloud

29% only plan to recover to on-prem servers

52% have plans that include both cloud and on-prem recovery options

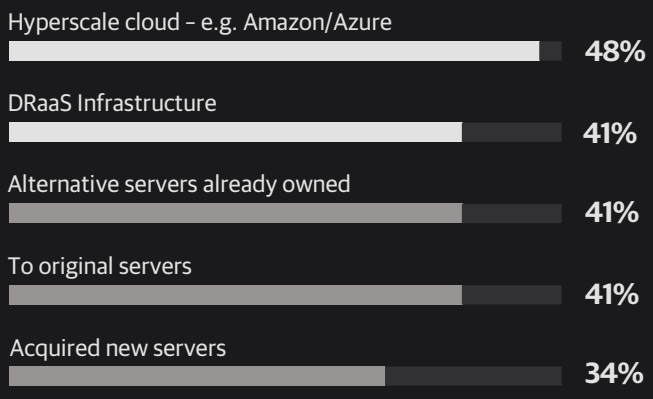


FIG 11

When recovering servers from ransomware, where do you recover your data to?
n=745

Summary of Lessons Learned

This analysis covers the opinions of 1,200 unbiased organizations who suffered at least one cyber attack in 2022:

Unlike potential natural disasters like fire or flood, being the victim of a cyber attack is much more probable than just possible. And when considering that on average, for each attack, an organization might expect to lose 15% of their production data, it is not surprising to see increased investments and prioritization of both cyber attack prevention and greatly increased remediation processes and technologies.

Said another way, a secure backup is the only alternative to simply paying the ransom.

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 and clouds, as well as air-gapped media, to ensure recoverable data.
- **Staged restorations**, to prevent re-infection during recovery
- **Hybrid IT** architectures for recovering the servers to alternative platforms like any other BC/DR strategy

Complementary Research

Data Protection Trends 2023

4,200 unbiased organizations across 28 countries

- Macro data protection drivers/trends
- Real-world downtime stats, DX considerations
- Cyber-strategies, containers and BC/DR

https://vee.am/DPR23

Cloud Protection Trends for 2023

1,700 unbiased respondents using at least one IaaS, SaaS or PaaS

- 3 XaaS, IT Ops and backup admin personas
- Backup drivers/methods for IaaS/PaaS/SaaS
- Adoption drivers for BaaS & DRaaS

https://vee.am/CPT23

Salesforce Protection Trends 2022

800 orgs managing SFDC across US, EU and APJ

- Salesforce devs/admins & backup personas
- Drivers & sentiments toward backing up SFDC

https://vee.am/SF22

For questions reach out to StrategicResearch@veeam.com

AUTHORS

The industry analyses of this data were authored by the following contributors:

Jason Buffington
VP, Market Strategy
@JBuff

Dave Russell
VP, Enterprise Strategy
@BackupDave

Julie Webb
Director,
Market Research
& Analysis

ABOUT VEEAM

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 that their apps and data are protected and always available to keep their businesses running.

TO LEARN MORE

Visit **www.veeam.com** or follow Veeam on LinkedIn **@veeam-software** and Twitter **@veeam**.

For questions on this research: StrategicResearch@veeam.com