Enterprise Strategy Group™ by TechTarget

2023 RANSOMWARE PREPAREDNESS: Lighting the Way to Readiness and Mitigation

Christophe Bertrand, Practice Director
Dave Gruber, Principal Analyst

SEPTEMBER 2023

Research Objectives

Ransomware is widely considered a critical and existential threat to the viability of any business. Given the high frequency of attacks and the impacts of successful ones such as data and infrastructure loss, many organizations are left with damages that have an effect well beyond IT. Attackers often go beyond valuable data assets by undermining key infrastructure components and exposing significant gaps, including those in the backup infrastructure itself. IT leaders must understand that the nature of the threat goes well beyond just data and focus on protecting and further leveraging their backup and recovery infrastructure to de-risk and minimize business impact through advanced capabilities. Overall, most organizations should consider key features to improve their cyber-resilience as they continue to battle ransomware and other cyber-risks.

In order to gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 600 IT and cybersecurity professionals at organizations in North America (US and Canada) personally involved with the technology and processes associated with protecting against ransomware. The research results were further used to create a multidimensional model to evaluate organizations' progress over the last 18 months in preparing for these threats and identifying best practices.

This study sought to:

Understand the proactive and reactive measures organizations have in place to defend against the ransomware threat.

Examine the state of ransomware mitigation best practices across readiness, prevention, response, and recovery phases.

Segment the levels of ransomware preparedness for all key defense phases.

Identify the priorities and plans associated with mitigating the ransomware threat in the coming 12-18 months.

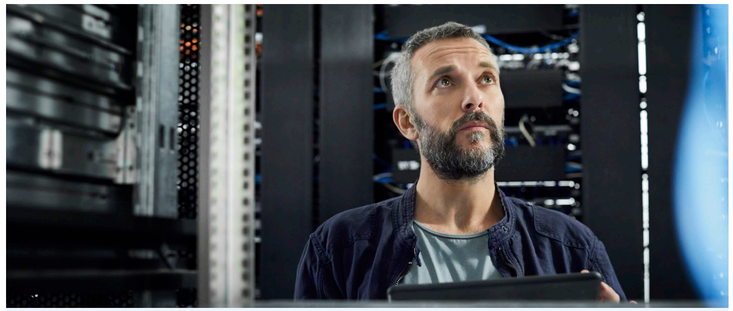
BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW

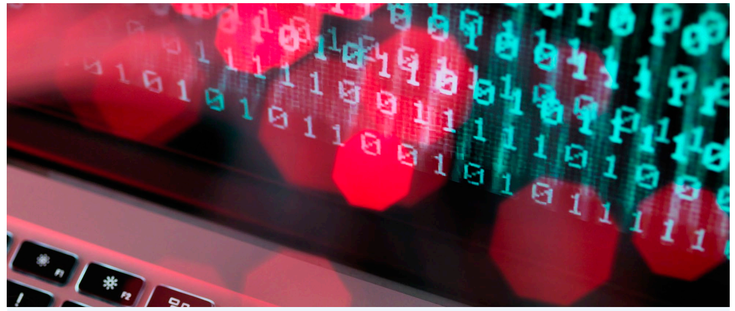
Ransomware Is the New Normal

PAGE 4



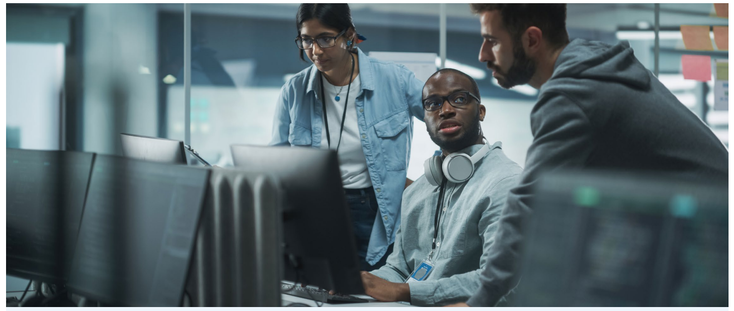
Ransomware Attacks Go Beyond Just Data

PAGE 10



Organizations Must Adopt Backup and Recovery Best Practices for Ransomware Preparedness

PAGE 14



Ransomware Recovery Solutions Need to Deliver on Wide-Ranging Requirements

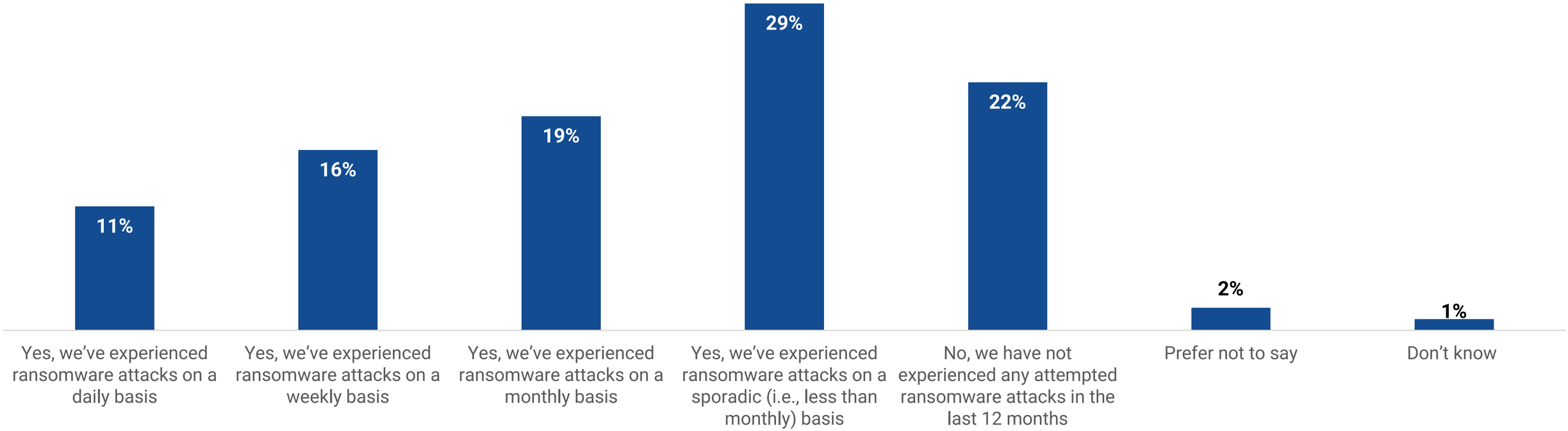
PAGE 20

Ransomware Is the New Normal

Ransomware Is Not a Matter of If, But When

In today's digital age, ransomware has become an alarming and prevalent issue that most organizations have encountered within the last 12 months. Regardless of whether the attack was successful, the reality is that it's not a matter of *if* an attack will occur, but rather *when* it will strike. Therefore, it's crucial to acknowledge that ransomware poses a significant and immediate threat that cannot be ignored, and immediate action must be taken to combat it.

Frequency of attempted ransomware attacks over the last 12 months.



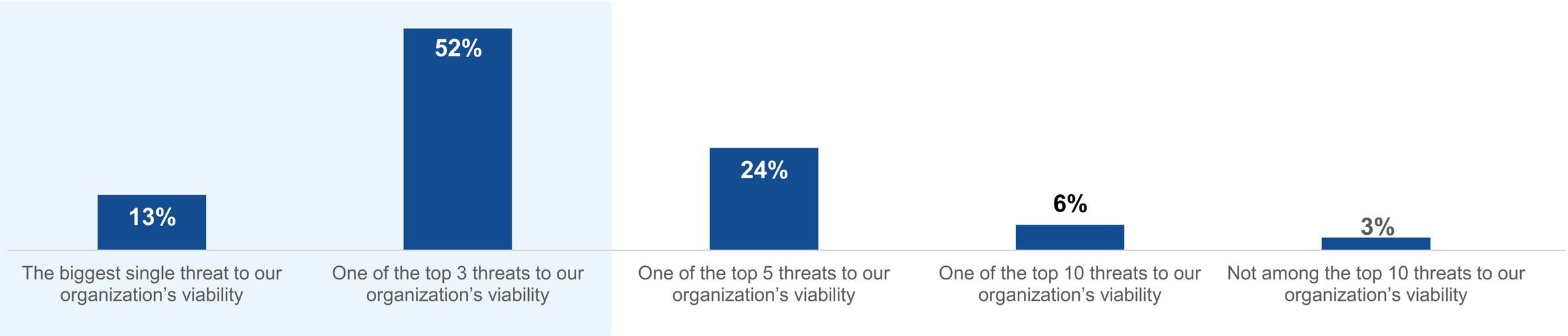
BACK TO CONTENTS

“Nearly two-thirds (65%) of respondents consider it **one of the top three most serious threats to the viability of their organization.”**

Vast Majority Rank Ransomware as a Top Threat to the Viability of Their Organization

Ransomware is a significant threat that can potentially devastate organizations. In fact, nearly two-thirds (65%) of respondents consider it one of the top three most serious threats to the viability of their organization. To address this issue, it’s crucial to first comprehend its impact. So, despite being a relatively new issue in the world of technology and IT, it’s encouraging to see that business leaders have recognized its severity. This realization has spurred efforts to find solutions.

Ransomware as an overall threat to organizational viability compared to all other potential risks.

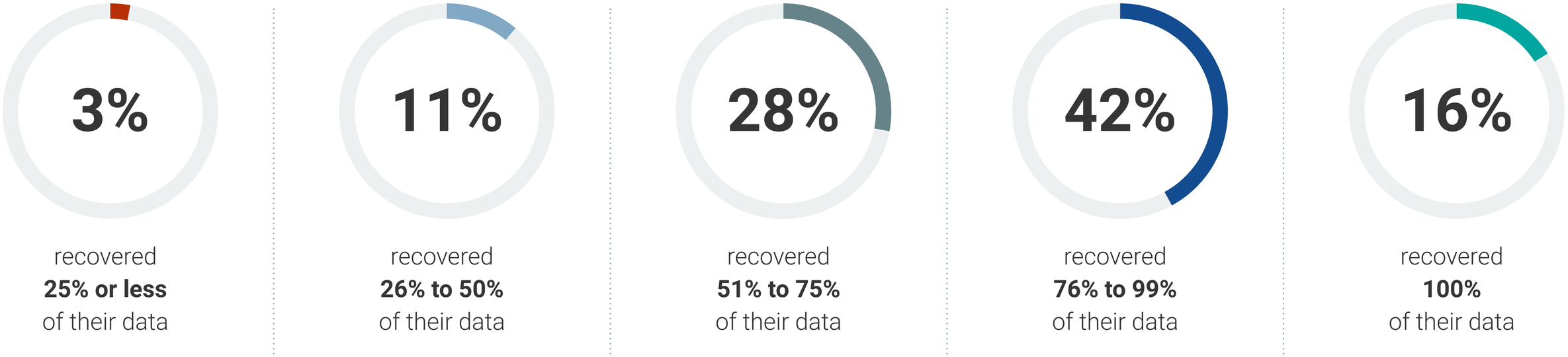


BACK TO CONTENTS

Typically, Not All Data Is Recovered

When ransomware strikes and is effective, the main goal is to recover data and minimize losses. This is because data losses not only lead to non-compliance but also pose a risk of losing crucial business transactions. Unfortunately, the current reality is bleak as only one in seven report they were able to *fully* restore their data after a successful ransomware attack. This highlights the need to reengineer recovery processes for ransomware attacks.

| Percentage of data organizations were able to recover after a successful ransomware attack.



BACK TO CONTENTS

Despite Recovery, a Window of (Valuable) Data Is Often Lost

The currency of data protection is reflected in recovery points. Unfortunately, only one in five organizations can recover their data to a production-like state. The majority of them will lose a valuable window of data, with more than half losing only minutes of data. This can result in significant losses for large-scale operations. In today's competitive and regulated business environment, these levels are unacceptable and pose a significant business risk.

Actual recovery point after a successful ransomware attack.

22%
We were able to recover to a state seconds prior to the attack (i.e., seconds of data were lost)

37%
We were able to recover to a state minutes prior to the attack (i.e., minutes of data were lost)

27%
We were able to recover to a state hours prior to the attack (i.e., hours of data were lost)

8%
We were able to recover to a state a day prior to the attack (i.e., a day of data was lost)

5%
We were able to recover to a state multiple days or more prior to the attack (i.e., multiple days of data were lost)

BACK TO CONTENTS

Attacks Hurt Organizations in Many Ways

Attackers employ many different techniques and targets to motivate payment, resulting in various impacts with potentially profound repercussions for the victim organizations. While it's not surprising that more than half cite data exposure (53%) and/or loss (51%) as effects of ransomware, the ramifications of a successful attack can significantly hamper operational processes and cause impacts to the internal and external supply chain, affecting employees and customers. These impacts are just too deep and broad to be ignored. Data or access to it is the prize, and extortion of exposure is in play.

| Ways in which successful ransomware attacks impacted organizations.

53%
Data exposure

51%
Data loss

46%
Operational disruption

42%
Direct impact to employees/ customers/partners

36%
Financial loss

33%
Compliance exposure

29%
Reputational damage

26%
Third-party liability/legal action

BACK TO CONTENTS

Ransomware Attacks Go Beyond Just Data

Infrastructure Configuration Data Is at Risk, Too!

While nearly six in ten organizations report that regulated data, often in the form of personally identifiable information, was impacted by successful ransomware attacks, sensitive configuration data is also at significant risk of compromise. This is because attackers understand that without critical infrastructure components in working order (e.g., networking, access/login, etc.), organizations' key processes are effectively disabled. Affecting the infrastructure at its core is a very effective way to stop production in its tracks. This means that IT professionals should consider both the business-related data and the infrastructure data equally in their preparedness efforts.

| Data classes affected by successful ransomware attack(s).

58%
Regulated data (i.e., personally identifiable information)

55%
Sensitive infrastructure configuration data

48%
Intellectual property (IP) data

40%
Mission-critical data

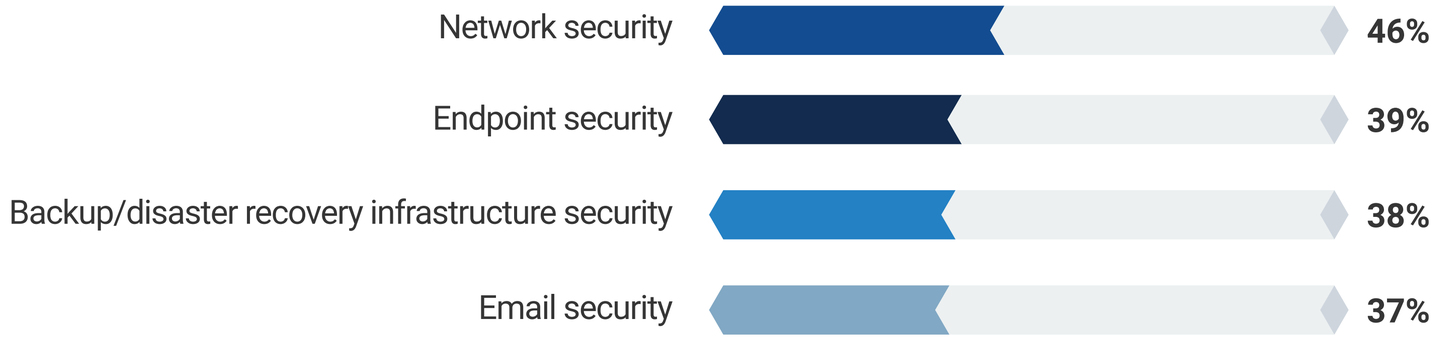
35%
Non-mission-critical data

BACK TO CONTENTS

Most Critical Preventative Controls (Unfortunately) Align With Biggest Gaps in Ransomware Preparedness

A variety of preventative security controls must be considered and are currently deployed by organizations in their fight against ransomware. The most salient ones also happen to be the controls that show the most gaps (i.e., technology, skills, and processes) today. While network security is the most commonly recognized deficiency in preparedness (reflecting the nature of our interconnected economy), those gaps in the security of endpoints and "traditional" email systems can significantly expand attack opportunities for cybercriminals as well. Also of critical importance is the backup and disaster recovery infrastructure: Without that in a fully functional state, no recovery can be undertaken, which is a perfect scenario for attackers seeking to optimize their profits. Protecting the "protector" is an area where there is work ahead for many.

Top four preventative security controls that play the **most critical** role in protecting against ransomware.



Top four biggest gaps in ransomware preparedness programs.

BACK TO CONTENTS

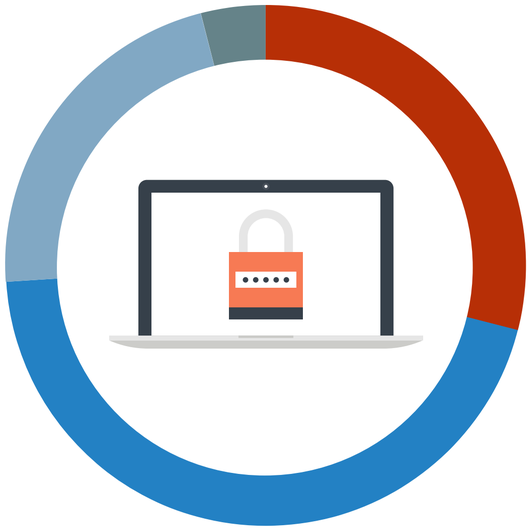
ONE IN THREE

express serious concerns about the security of their backups.

Broad Awareness That Backups Are a Target

A significant number of IT leaders are rightly worried about the security of their backup and recovery infrastructure. In fact, almost one in three (29%) express serious concerns. This level of concern can be beneficial as it will likely prompt necessary investments in defensive measures and enhancements to recover data, systems, and infrastructure.

Level of concern that data protection copies could also become infected or corrupted by ransomware attacks.



29%
Very concerned

45%
Somewhat concerned

22%
Not very concerned

4%
Not at all concerned

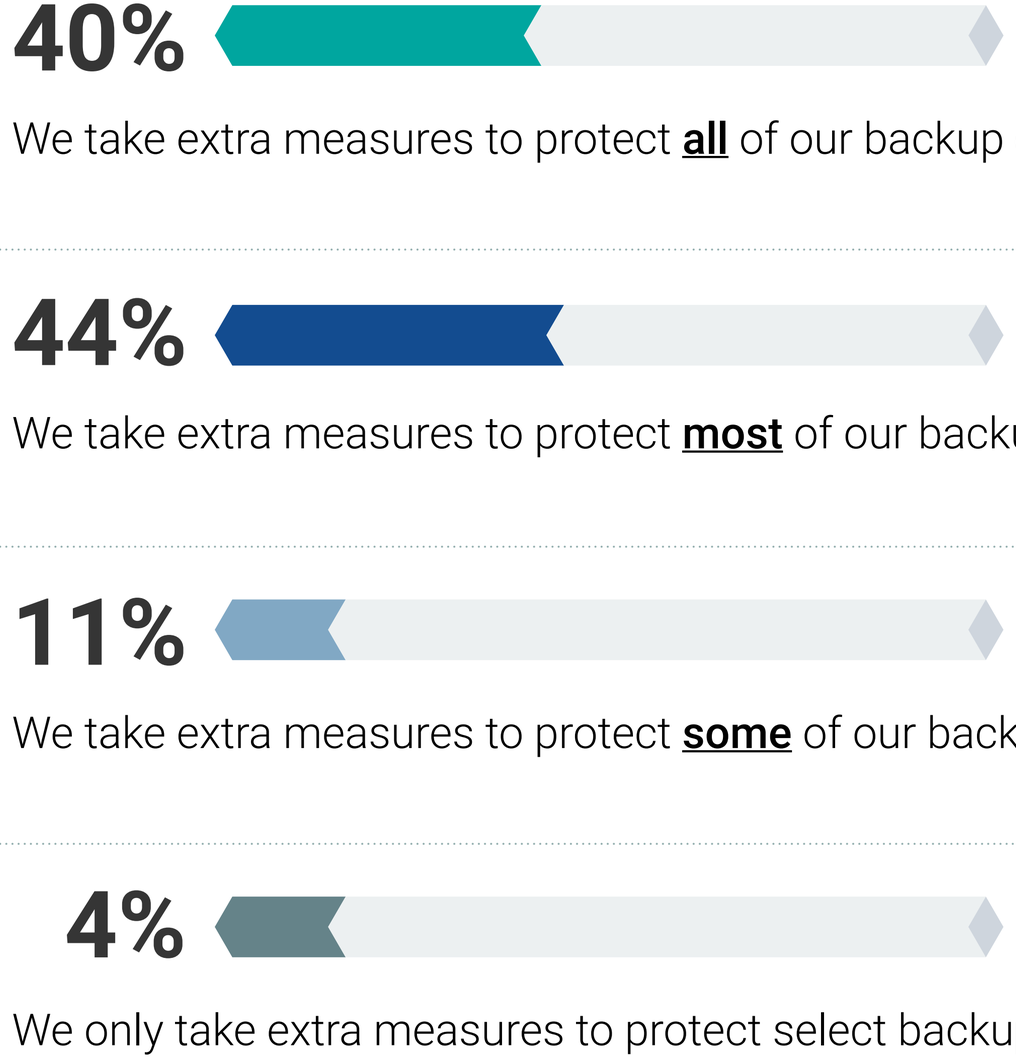
BACK TO CONTENTS

Organizations Must Adopt Backup and Recovery Best Practices for Ransomware Preparedness

Prevention Extends to Data Protection Infrastructure

As organizations have become aware of the vulnerabilities in their data protection processes for backup and recovery, many are taking extra precautions to safeguard their backup copies, which are crucial for recovery in case of a crisis. Currently, 40% of organizations are protecting all their backup copies, which should be considered the ideal approach. Although it's not the majority, it's worth noting that another 44% are implementing similar measures for most of their backups. These practices are highly recommended to enhance the chances of successful recovery from a ransomware attack.

Extent to which organizations take additional specific steps to protect their backup copies.

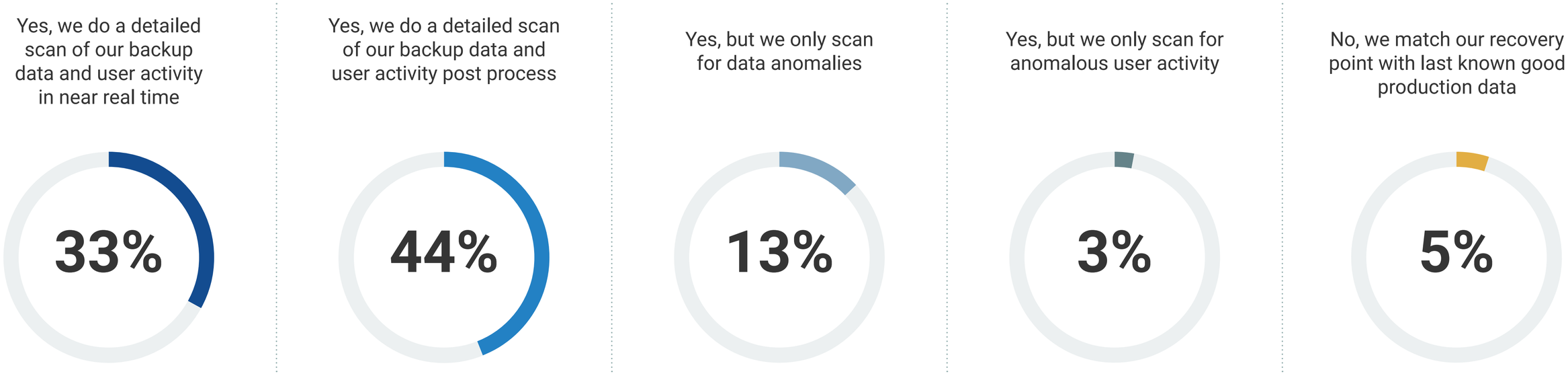


BACK TO CONTENTS

Backup Scanning in Near Real Time More Popular with Enterprises

Many organizations use a technique called backup scanning to identify any suspicious files or executable code. This process can be done in real time or near real time, providing quick results and triggering signals for defensive actions. It can also be carried out as a post-backup process that examines the backup data and reports back to other components of the cybersecurity system. It's important to scan as thoroughly as possible. While real-time scanning is preferred for early detection, post-process solutions may be more practical for larger systems due to performance or cost reasons. Both approaches have their advantages, and around 80% of organizations use backup scanning, which is a positive sign for improving ransomware preparedness.

Can organizations analyze backup images for data anomalies and anomalous user activity?

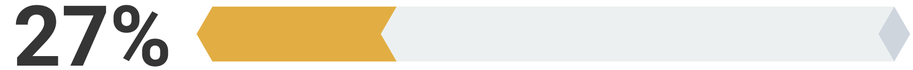


BACK TO CONTENTS

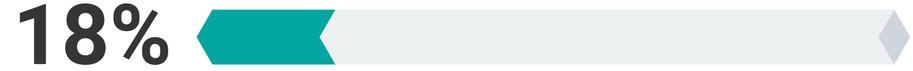
Air-gapping Seen as a Viable Protective Strategy

To ensure the maximum security and protection of backed up data, air-gap backups should be stored in volumes inaccessible by default to any applications, databases, users, or workloads currently operating in the production environment. Such data storage can only be accessed during protected and vetted backup sessions. This is a crucial best practice to prevent cyber-attackers from exfiltrating or destroying backup data. Despite the importance of this solution, only slightly more than one in four (27%) organizations have deployed it at this point. While 18% are in the process of testing and deploying an air-gapped solution, which confirms it is seen as a viable strategy, there is still much work to be done in the market overall to ensure that the vast majority have it in place.

Usage of air-gap solutions to protect storage capacity and mitigate the effects of ransomware events.

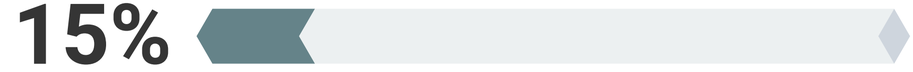


27% Yes, we have deployed this type of solution



18% No, but we are engaged in the process of planning/testing this type of solution

34% No, but we are interested in investing in this type of solution



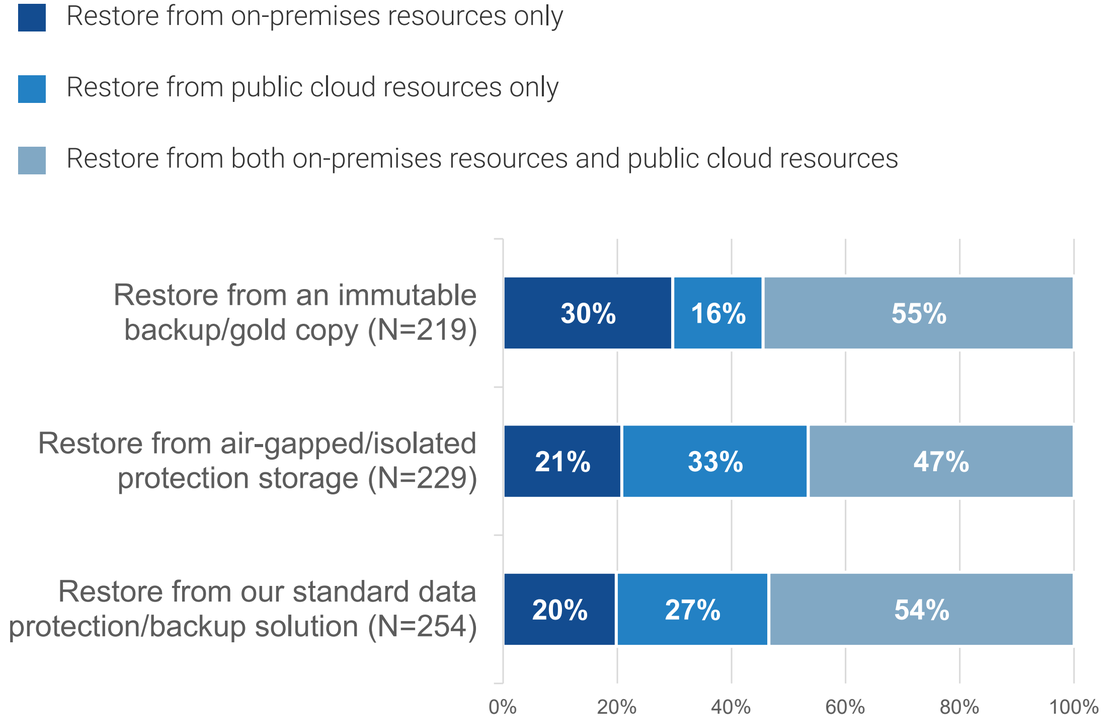
15% No, and we have no immediate plans to invest in this type of solution

BACK TO CONTENTS

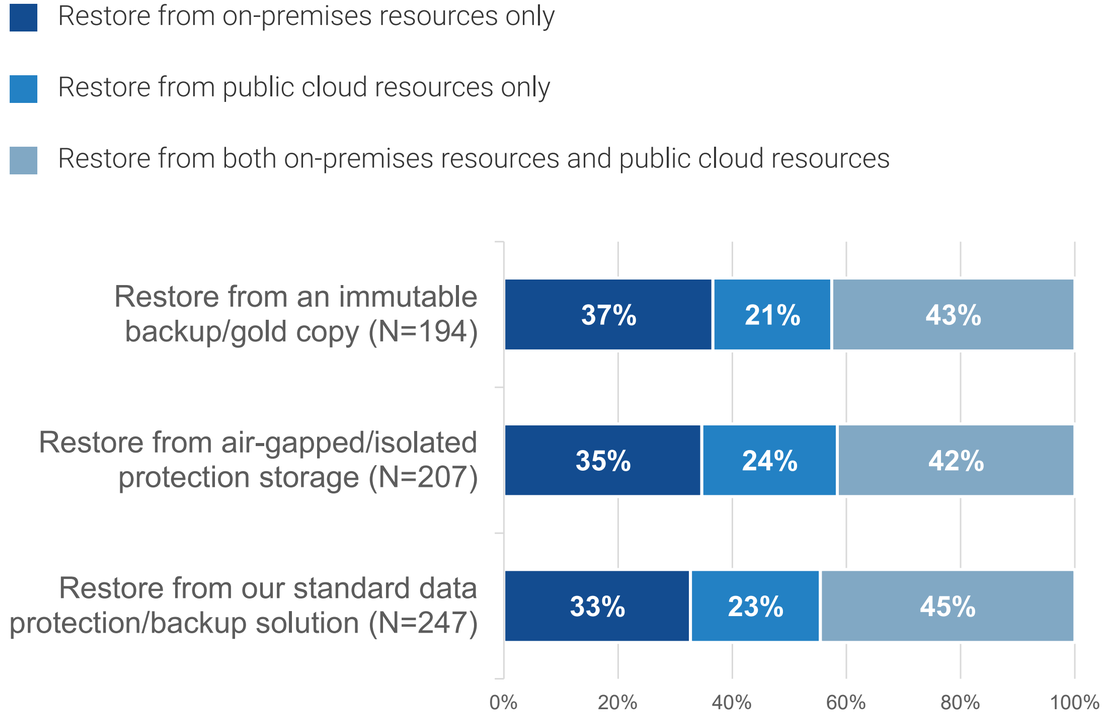
Growth of Immutable, On-premises Backups

Ensuring the security of data is crucial, and two key measures to achieve this are air-gapping (previously discussed) and immutability. Immutability refers to the prevention of any deletion or alteration of volume, application, or database data. Depending on an organization's needs, immutable backup/recovery solutions can be deployed on premises, in the cloud, or both. Comparing 2022[1] and 2023, it's clear that backup topologies have evolved, with more organizations gravitating to pure on-premises approaches. On-premises topologies offer a first line of defense and faster large restores due to leveraging local networking and storage infrastructure. Additionally, compliance-related regional requirements may influence this trend. Organizations seem to increasingly favor a "first line of defense" for on-premises environments.

Restore point approach in **2022.**



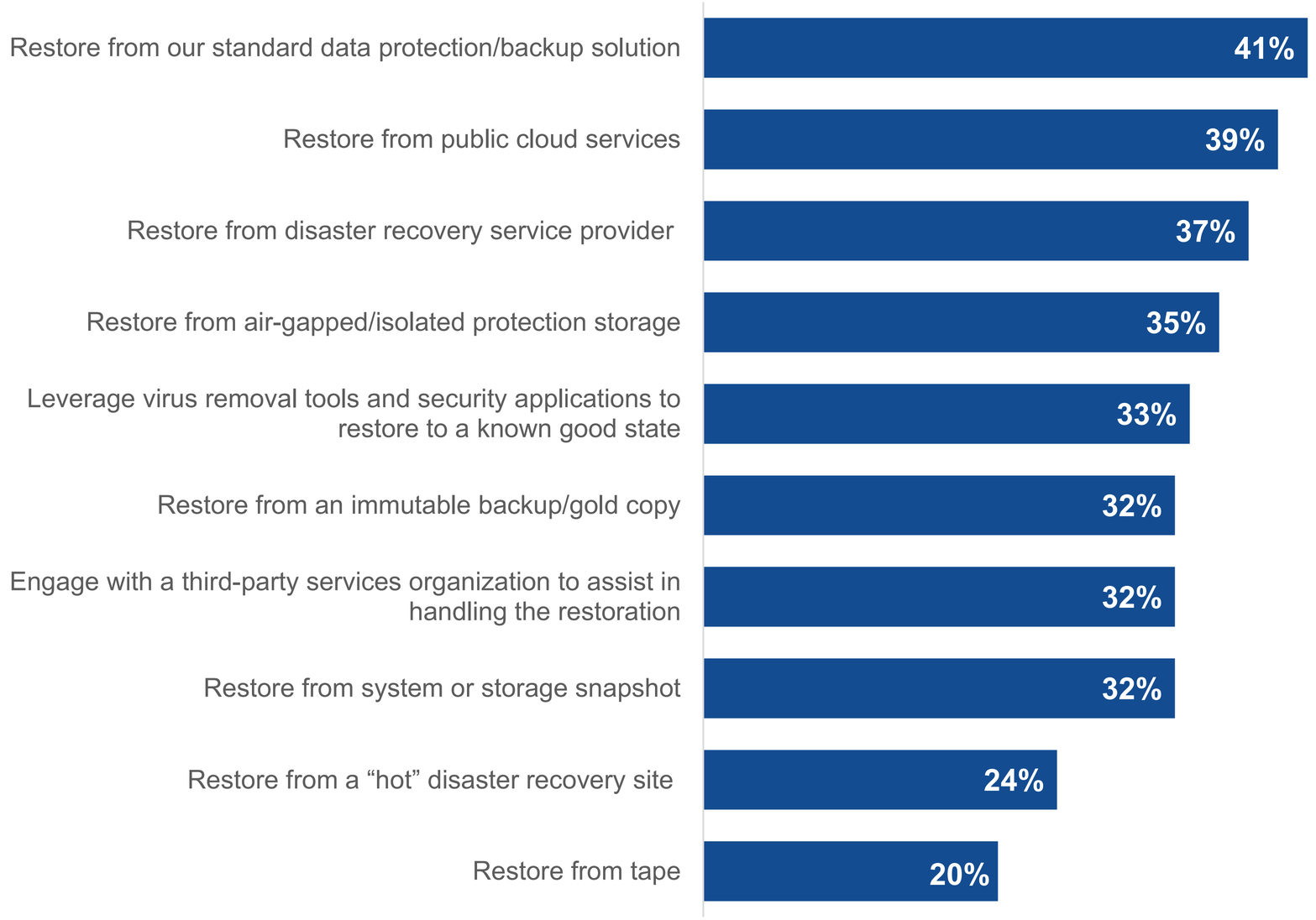
Restore point approach in **2023.**



 1 Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness,* June 2022.

BACK TO CONTENTS

Planned method of recovery for the impacted applications and data of a successful ransomware attack.



Recovery Strategies Vary Based on Multiple Factors

Ransomware can affect many different parts of the operation in a variety of ways, which means that organizations have to consider a number of recovery scenarios and strategies in order to optimize their recovery capabilities and service levels. Data and applications are disseminated across a hybrid infrastructure today, and many techniques and capabilities are available to recover data, metadata, and applications. It should be noted that the plurality of respondents are naturally turning to the backup and recovery mechanisms already in place as the planned method of recovery. While having access to multiple mechanisms may contribute to complexity if not carefully planned, this can be turned into an advantage. IT leaders must turn to vendors and implementation service providers for advice. This is also an opportunity for market education on best practices.

BACK TO CONTENTS

Ransomware Recovery Solutions Need to Deliver on Wide-ranging Requirements

The Ransomware Preparedness Top Ten ‘Recovery Solution RFP’

When considering the technology and features currently needed in the market, it is apparent that any solutions implemented must have a wide range of capabilities across many disciplines. The ten most desired ransomware recovery capabilities among IT professionals include those related to backup and recovery infrastructure, with a focus on protection and recovery features. It’s important to note that no single vendor offers a one-size-fits-all solution, and instead, an ecosystem of technologies and vendors must come together to create integrated solutions that meet the diverse needs of organizations.

Important considerations when selecting a ransomware recovery solution.

35%
Data encryption (at rest and/or in flight)

34%
Ability to protect SaaS data

34%
Ability to detect ransomware in data copies/backups

33%
Integrated cloud services capabilities

32%
Ability to recover to any point or location

31%
Ability to protect endpoint devices

31%
Ability to protect virtual machines

31%
End-to-end recovery services

30%
Protected/immutable data copies/backups

30%
Continuous data protection/ replication/journaling

BACK TO CONTENTS

COHESITY

Cohesity is a leader in AI-powered data security and management. We make it easy to secure, protect, manage, and get value from data — across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring malicious behavior, and rapid recovery at scale. Cohesity solutions can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

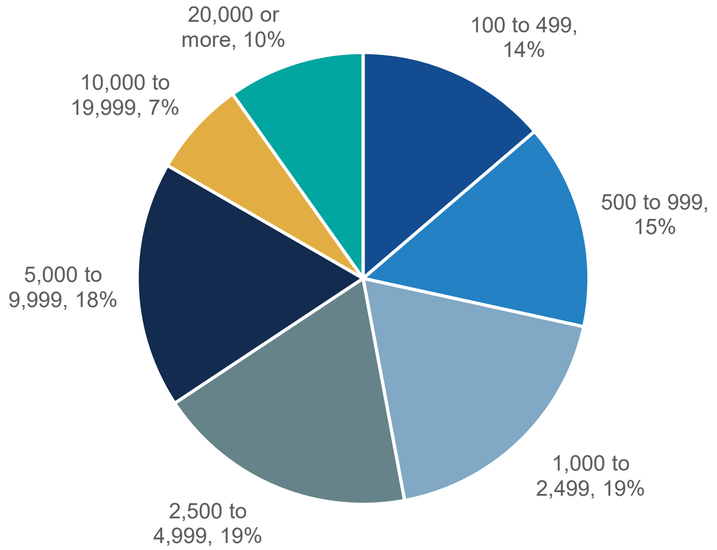
Cohesity ransomware recovery

Research Methodology and Demographics

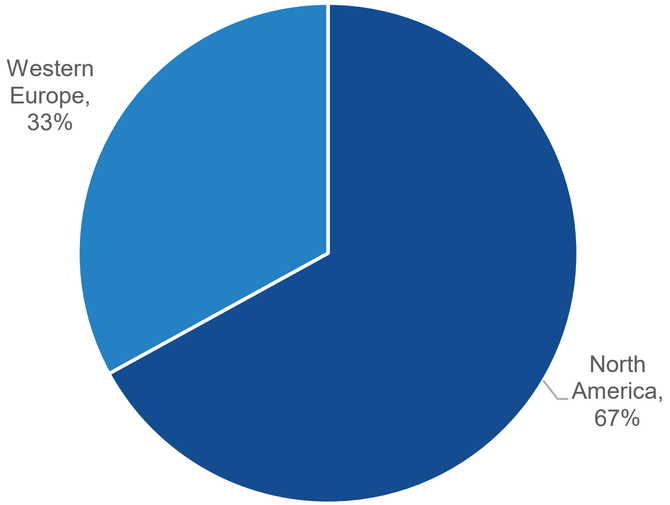
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) and Western Europe (UK, France, and Germany) between May 22, 2023 and June 15, 2023. To qualify for this survey, respondents were required to be involved with the technology and processes associated with protecting against ransomware. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 600 IT and cybersecurity professionals.

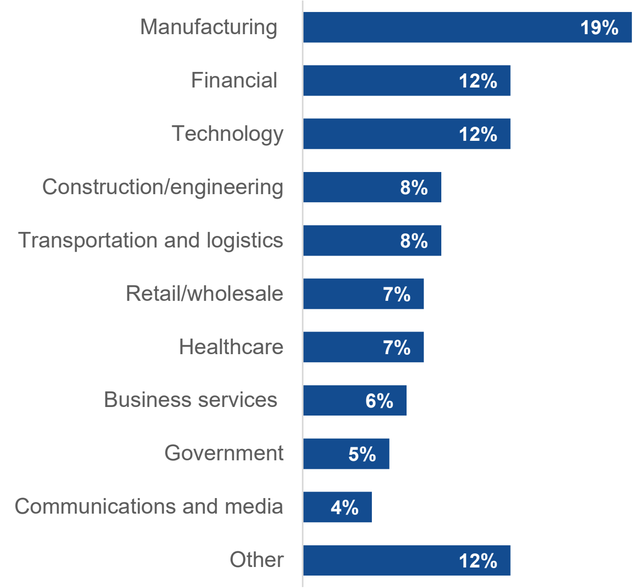
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY REGION



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.