



Enterprise Strategy Group | Getting to the bigger truth.™

The Long Road Ahead to Ransomware Preparedness

Christophe Bertrand, Practice Director
Dave Gruber, Principal Analyst

MARCH 2022



Research Objectives

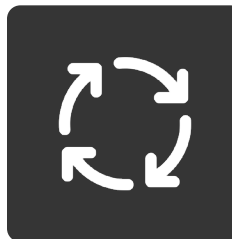
The ransomware threat is a top-of-mind issue for so many organizations; however, few feel totally prepared for an attack. Without an industry reference architecture or blueprint for ransomware protection, organizations are building their own strategies and processes to respond. But with ransomware protection included with so many different security and data protection solutions, many are confused about the scope of what is to be included, who is responsible for the implementation, and who needs to be involved in the conversation.

In order to connect the dots between those organizations that feel most prepared and the specific strategies and plans they are using to get there, with an eye on defining best practices, ESG surveyed 620 IT and cybersecurity professionals personally involved with the technology and processes associated with protecting against ransomware attacks at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada) and Western Europe (UK, France, and Germany).

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.


KEY FINDINGS

CLICK TO FOLLOW



Ransomware attacks are pervasive and having an impact.

PAGE 4




Readiness is essential to ransomware mitigation, yet significant gaps exist for most.

PAGE 8



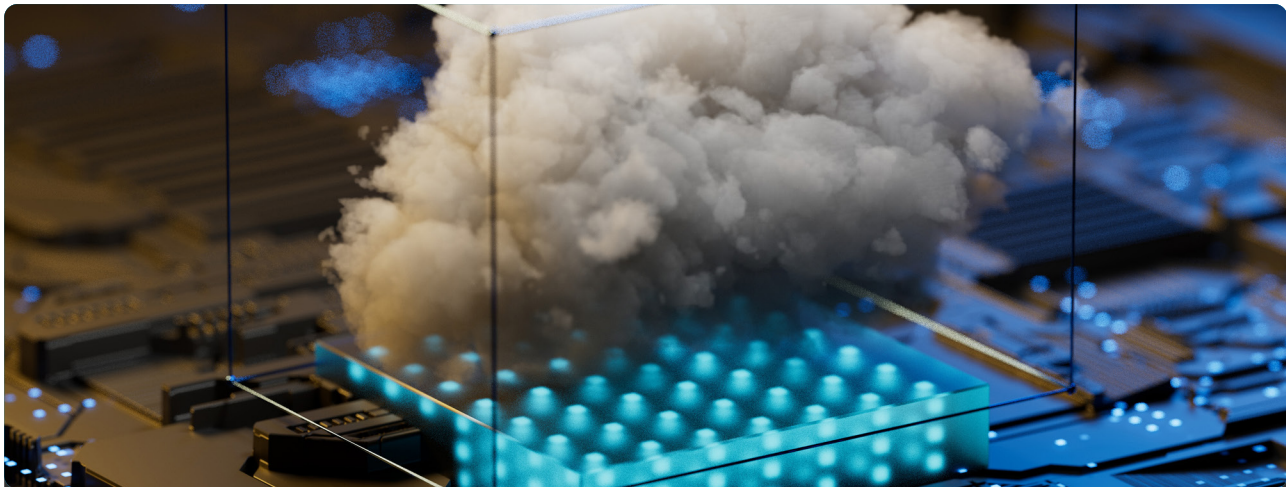
Most have prioritized investments in and focus on prevention.

PAGE 13



Skill shortages and a dependence on internal resources for response posture put many at risk.

PAGE 16



While hybrid backup is common, recovery is not a guarantee.

PAGE 20



RPO and RTO gaps separate the most advanced in business continuity.

PAGE 25



Ransomware Attacks Are Pervasive and Having an Impact

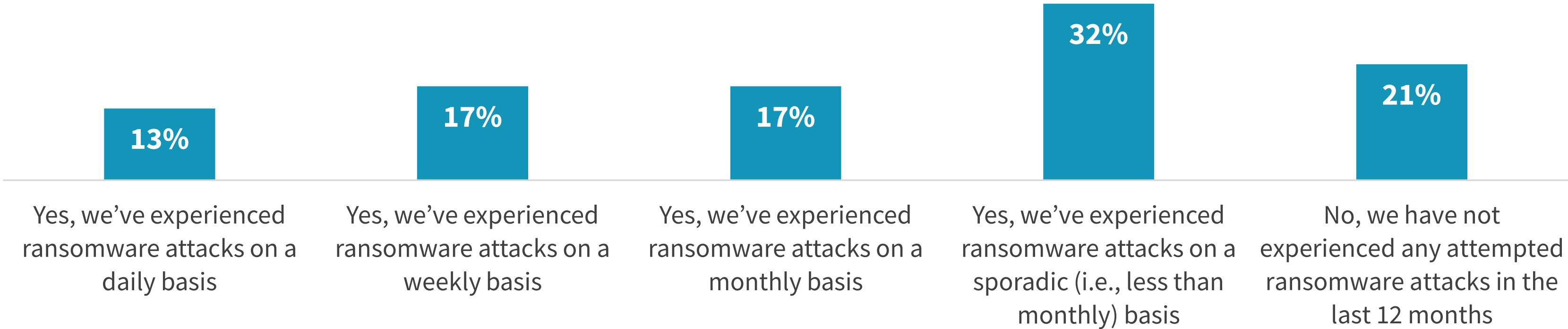
Ransomware Attacks Are Frequent and Having an Impact

Ransomware attacks make the news on a regular basis, so it should come as no surprise that respondents confirm the regular frequency with which they occur. Indeed, 79% of respondent organizations report having experienced a ransomware attack within the last year, and among that population, with nearly three-quarters report that they have been financially or operationally impacted by these attacks, making them “successful.” It should also be noted that 1 in 3 organizations report having been successfully hit more than once, making ransomware both a significant and recurring source of business disruption.

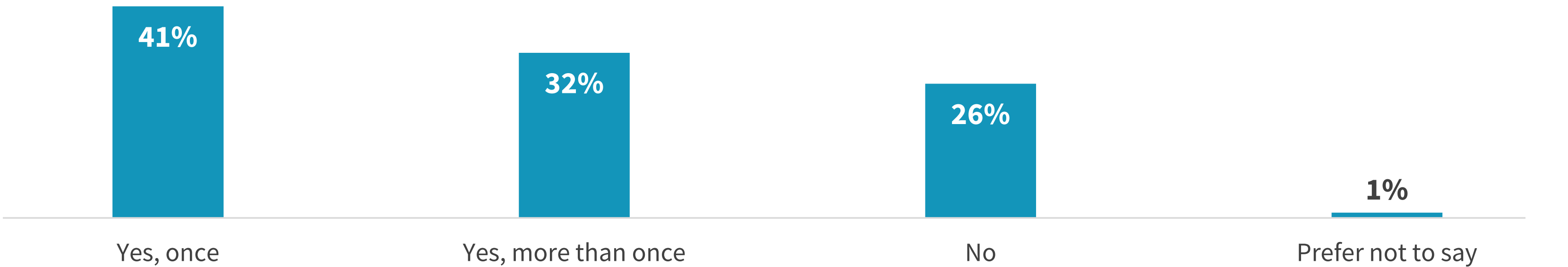


79%
of respondent organizations report having experienced a ransomware attack within the last year.

| Attempted ransomware attack frequency over the past 12 months.



| Successful ransomware attacks over the past 12 months.



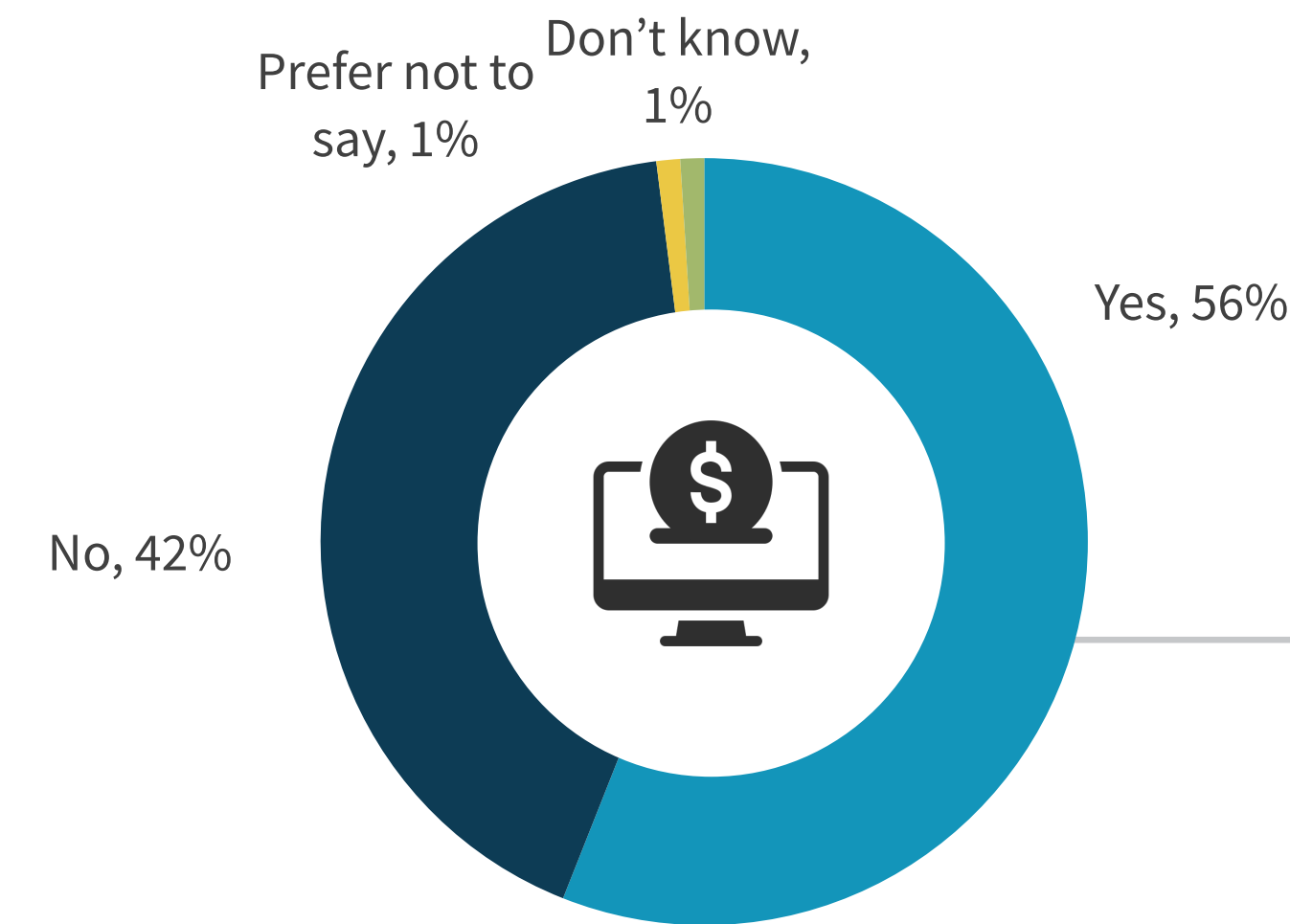
Paying Ransom Doesn't Guarantee Data Recovery

More than half (56%) of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems. However, it's not necessarily a solution that works effectively as paying the ransom does not guarantee the recovery of data. Indeed, only one in seven reported getting all their data back post payment. So, paying the ransom encourages further "bad behavior" in the form of demanding additional ransoms, and fails to guarantee seamless business resumption overall, including recovering from data loss and other operational consequences.



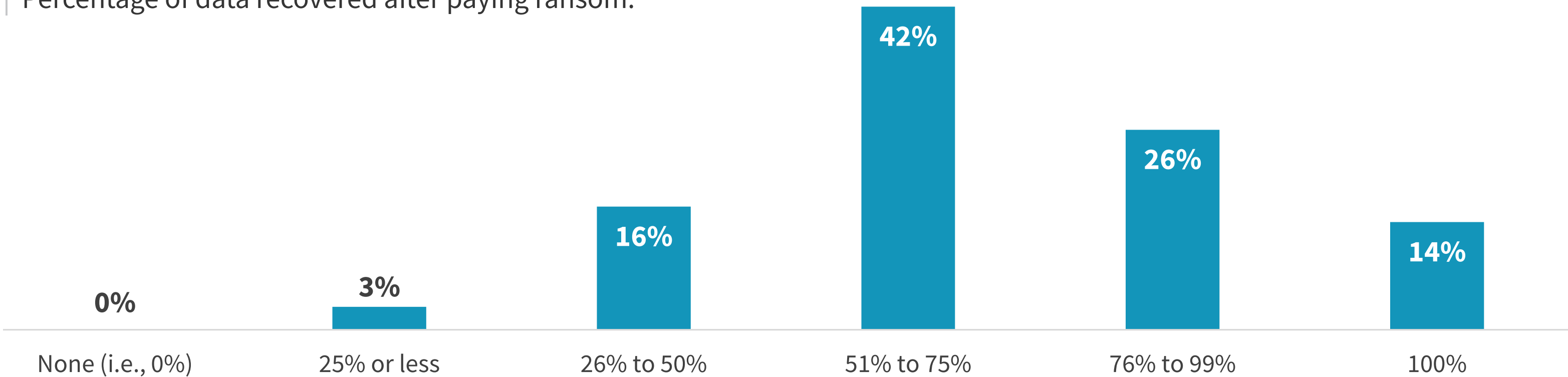
ONLY 1 IN 7
reported getting all their data
back post payment.

Have organizations paid ransoms resulting from successful attacks?



“ More than half
of organizations that have been
victimized by a successful ransomware
attack at some point admit to having
paid a ransom to regain access to data,
applications, or systems.”

Percentage of data recovered after paying ransom.



Storage and Cloud Are Most Common Ransomware Targets, and Vulnerable Software and Misconfigurations Are Most Common Points of Entry

Cyber criminals have become more sophisticated in their attacks over time and leverage many different targets to optimize their efforts. Storage systems and cloud are the most common targets across the board, but it should be noted that networks and IT infrastructure in general, as well as data protection infrastructure specifically, are also atop the target list. By disabling all or part of the IT infrastructure, cyber criminals disrupt IT and business operations with the objective of shutting business down for all practical purposes. It also means that they don't necessarily have to go after data assets. If you can't run your systems and applications, you are out of business, just as if you had no usable data. Interestingly, while it could easily be assumed that ransomware primarily comes from email or unsafe web browsing, the reality is different: Vulnerable software and misconfigurations are the most likely points of entry.

| Areas of IT environment impacted by successful ransomware attack(s).



40%
Storage systems



39%
Cloud-based data



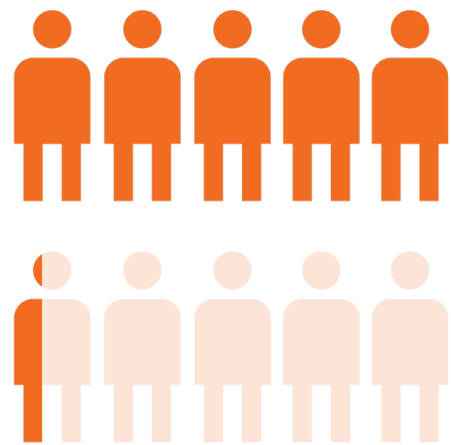
37%
Networks or connectivity



36%
Key IT infrastructure



36%
Data protection infrastructure



53%

of victims of successful ransomware attacks report that this included sensitive infrastructure configuration data.

| Initial point of compromise for successful ransomware attack(s).



36%
Application software vulnerability



33%
Systems software vulnerability



31%
Application user permissions and misconfigurations



31%
Misconfiguration of externally exposed device



27%
Email

Readiness Is Essential to Ransomware Mitigation, Yet Significant Gaps Exist for Most



Most *Believe* Their Ransomware Preparedness Has Improved, with Further Prioritization and Investment Planned

Almost all respondent organizations believe their ransomware preparedness is stronger today than it was two years ago, with 52% identifying their position as much stronger. This is not surprising as ransomware has become much more than just an IT priority for many organizations. In fact, more than three-quarters (79%) say that ransomware is a top five overall business priority, clearly stemming from the heightened importance to executive teams and even boards of directors. Given the highest levels of attention that ransomware posture is receiving, it follows that 82% plan to invest in further strengthening it in the coming 12-18 months.

Preparedness to mitigate the impact of ransomware.



- **52%**
Our preparedness position for ransomware is much stronger today than it was two years ago
- **47%**
Our preparedness position for ransomware is somewhat stronger today than it was two years ago

Importance of ransomware preparedness for executive team and/or board of directors.



- **26%**
The most important business priority
- **53%**
One of the top 5 business priorities

Expected spending on ransomware preparedness over the next 12-18 months.

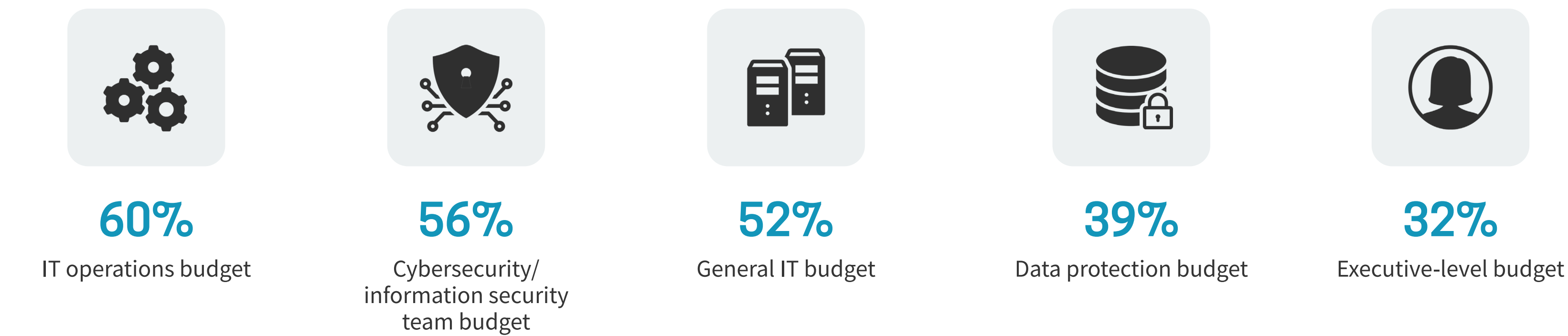


- **35%**
Increase significantly
- **47%**
Increase slightly

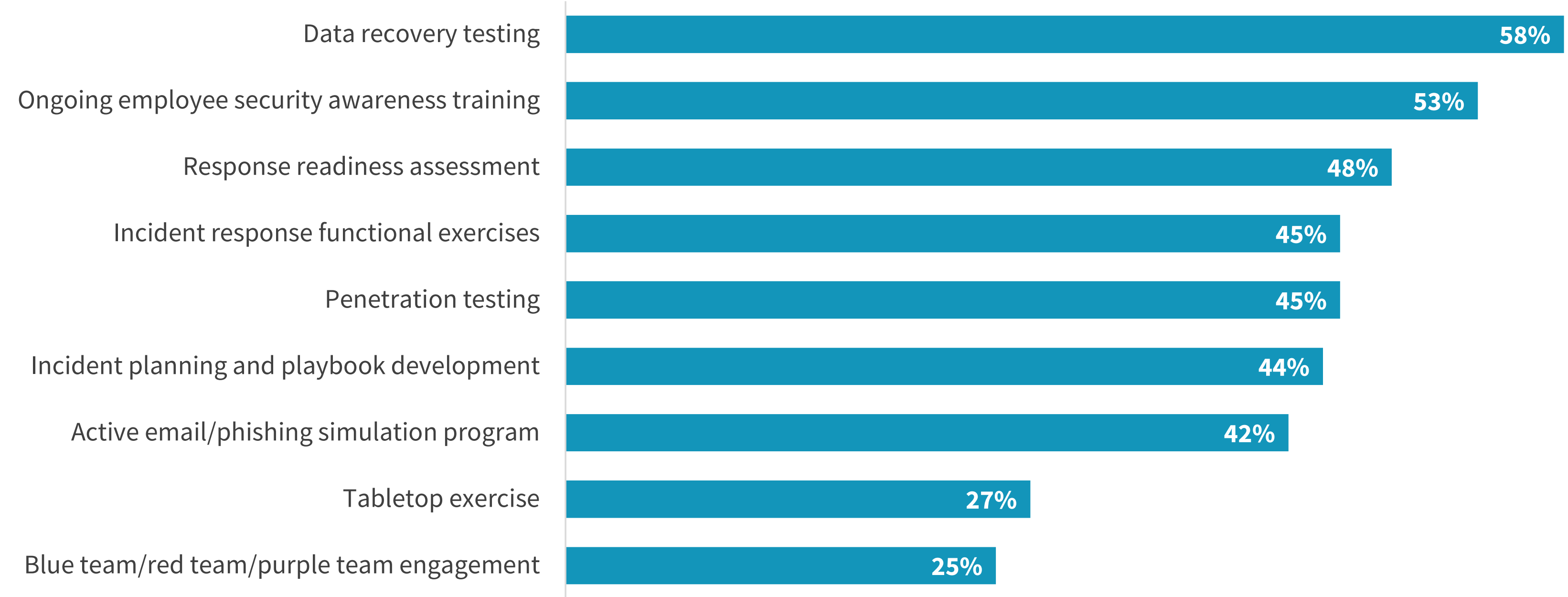
Ransomware Readiness Is a Team Sport

Ransomware readiness is a team sport, with preparedness investments coming from a combination of IT, security, and data protection groups. A majority report additional investment from centralized ransomware budgets. Investments are used for a diverse collection of preparedness activities, including hardware, software, services, insurance, data protection, readiness testing, functional exercises, employee security awareness training, playbook development, penetration testing, and more.

Groups that contribute funding to technologies for ransomware readiness.



Ongoing ransomware preparedness activities and processes.

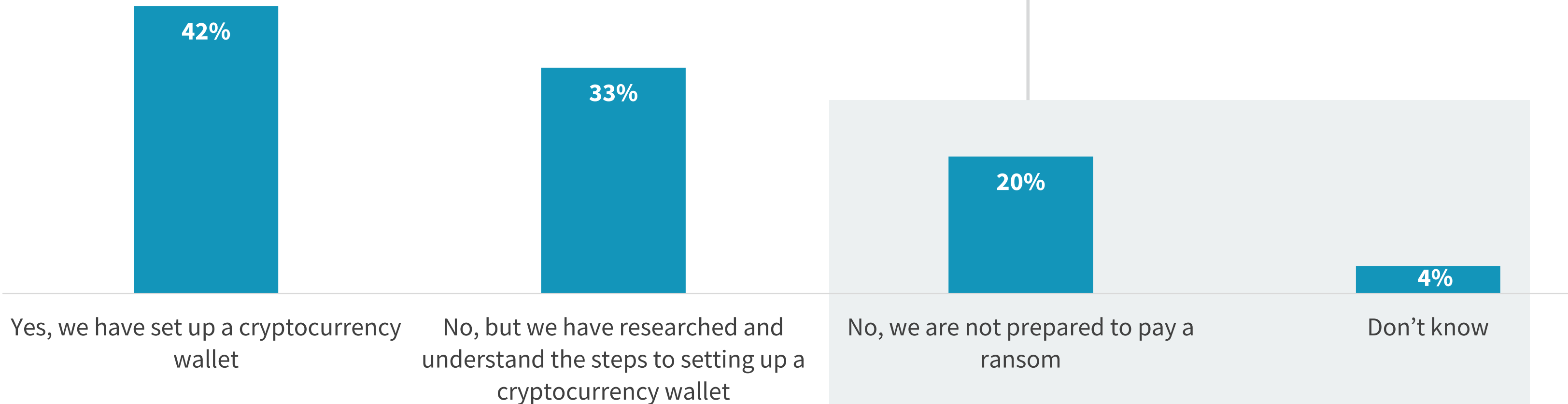


Using Cryptocurrency Measures to Pay Up Faster

When the decision to pay a ransom is made, speed matters when it comes to restoring operations. Because ransoms typically are required in cryptocurrency, preemptively understanding how to move funds through a cryptocurrency wallet in advance of an attack enables IT organizations to potentially minimize the impact of payment times. For many, this means having a cryptocurrency wallet set up and ready to utilize. For others, just understanding how is enough. Notably, nearly a quarter seem to be unprepared to pay a ransom.

“ Nearly a quarter seem to be **unprepared to pay a ransom.**”

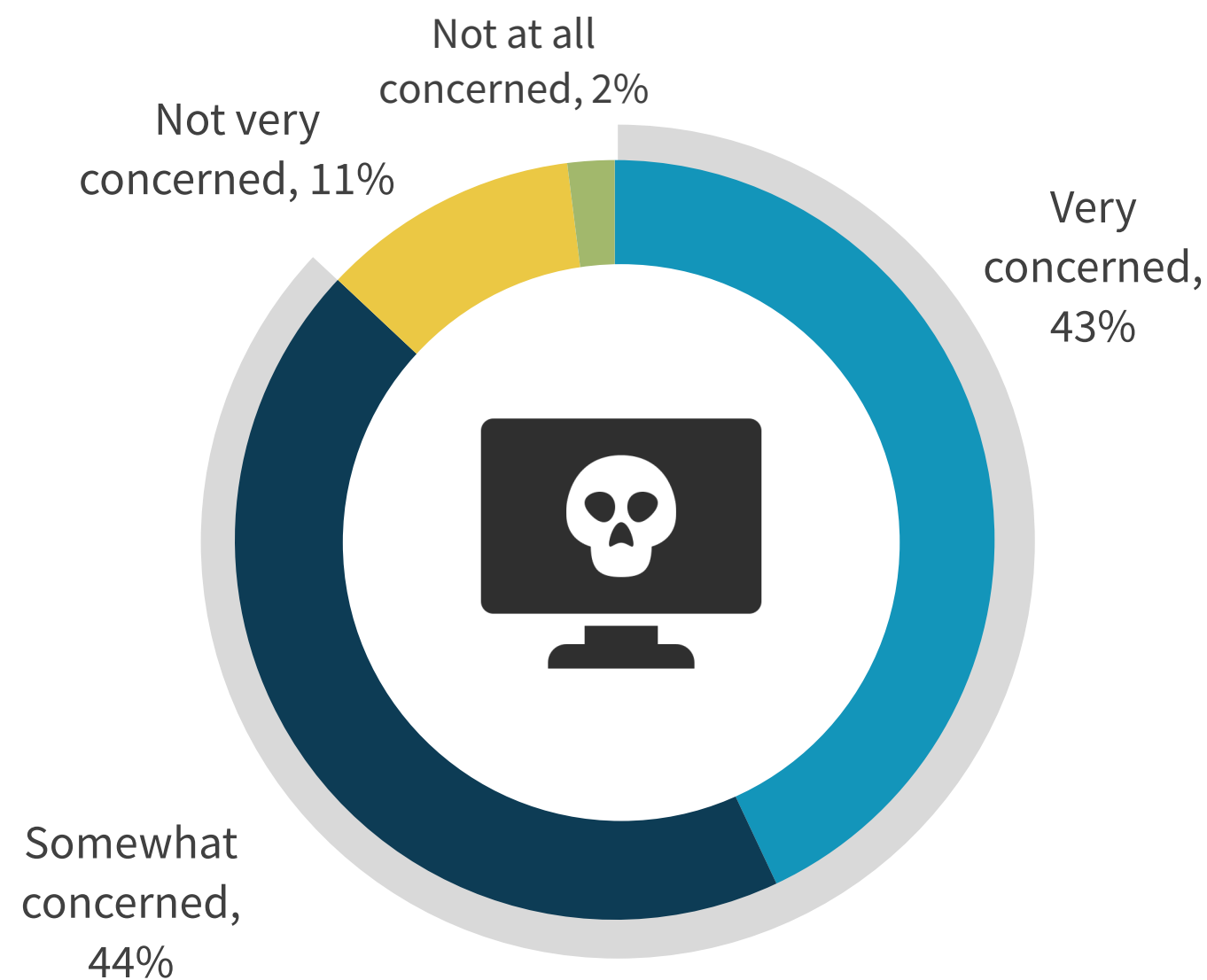
Do organizations preemptively have a cryptocurrency wallet to pay ransoms?



Major Concern that Backups Could Become Ransomware Targets, Driving Demand for Third-party Backup Integrity Validation

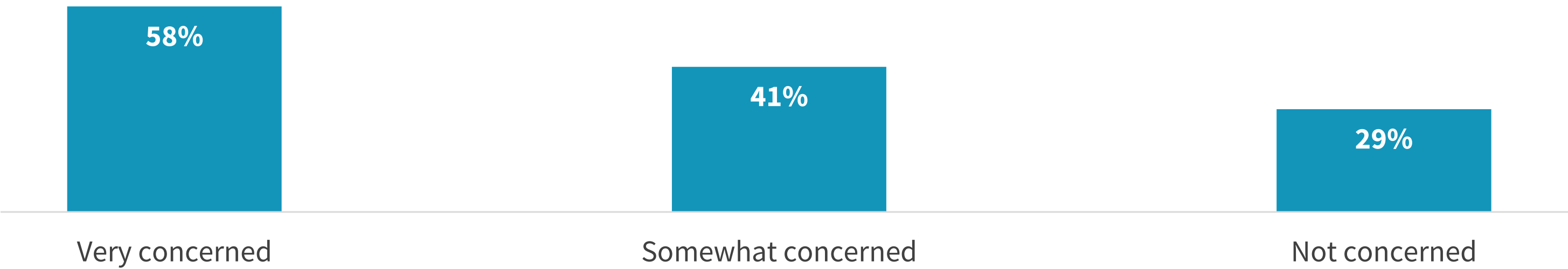
When primary data gets corrupted or lost, backup copies are traditionally leveraged for recovery purposes. This has made the backup infrastructure a very desirable target for cyber criminals since it is a key tool that can mitigate or negate data-related attacks. By taking out the defenses, attackers are optimizing their chances of success. IT leaders understand this situation, and it generates significant levels of concern. Indeed, nearly nine in ten organizations are concerned that their backup copies could be corrupted by ransomware attacks, with 43% saying they are very concerned. And this apprehension is driving action as those who are very concerned are twice as likely (59% versus 29%) as those with no concerns about corrupted backup copies to leverage third-party tools that validate the integrity of backups to ensure that they are usable for recovery.


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



47% leverage a third-party tool to automate data backup restoration, configuration, and validation.

Percentage of organizations that leverage a third-party backup validation tool based on level of concern that data protection copies could become infected.



A woman with dark hair is seen from the side, sitting at a desk. She is using a silver laptop with her left hand on the keyboard. In her right hand, she holds a black smartphone. The phone's screen is on, showing a lock screen with a blue padlock icon and the text "Your device is blocked!" and a circular arrow icon. The background is a blurred office environment.

Most Have Prioritized Investments in and Focus on Prevention

Most Valued Ransomware Prevention Controls

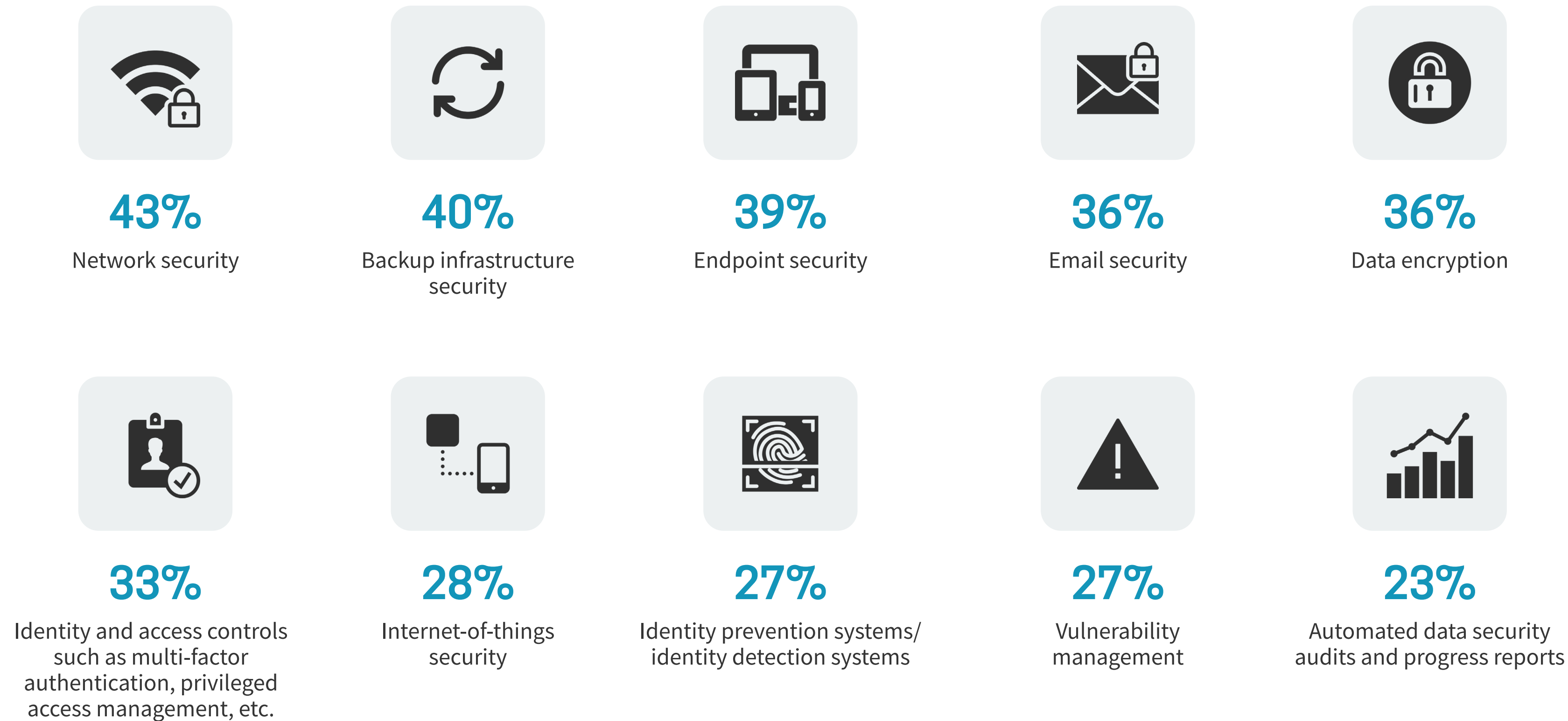
Threat vectors considered most important to implement preventative controls on include network, endpoint, email, and identity. Not surprisingly, reflecting the concerns of IT leadership and highlighting the critical role of backups in business resumption, backup infrastructure security ranks very high. “Protecting the protector” is critical for the recovery phase of successful ransomware attacks.

Despite software vulnerabilities being reported as the most common entry point for ransomware attacks, vulnerability management appears far down the list of what most consider most important to ransomware preventions. This is exacerbated by the fact that more than half (52%) of organizations report gaps in their vulnerability management programs.



52%
of organizations believe they have gaps in their vulnerability management programs.

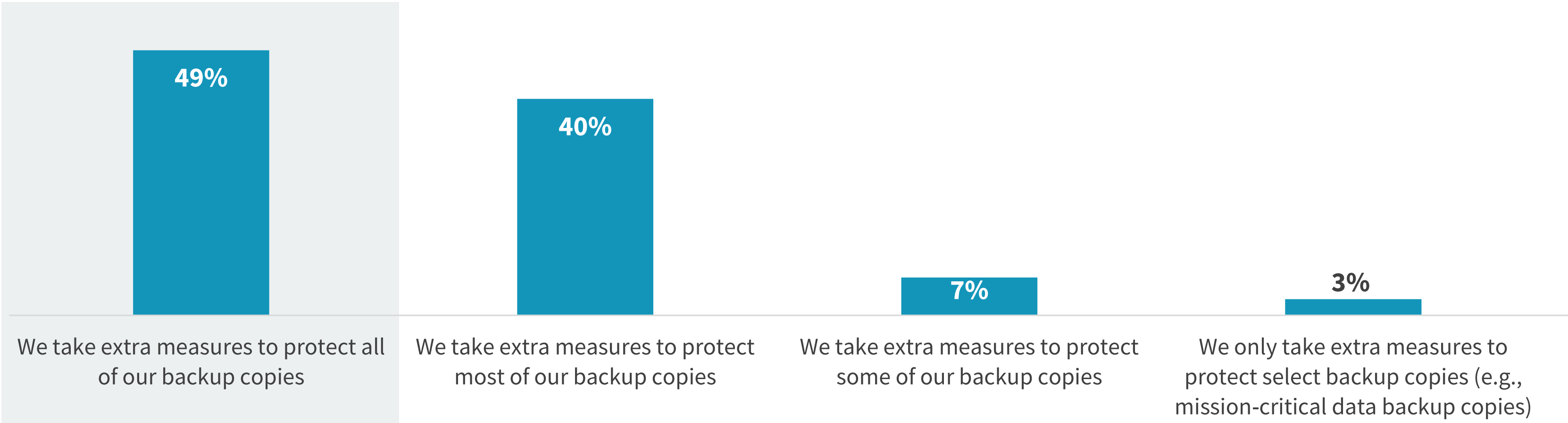
| Most critical preventative security controls for protecting against ransomware.




Protecting Backup Copies Is a Key Prevention Tactic

Protecting backups has now become the norm in light of ransomware attacks specifically targeted at these workloads/processes. As has already been established, most organizations are concerned about backup copies being targeted by ransomware, and many leverage third-party tools to validate their backup copies in addition to security controls to protect their backup infrastructure. In a perfect world, organizations would protect all their backup copies since it's virtually impossible to predict what might be needed in terms of recovery with so many varieties of attacks, data loss interdependencies, etc. While the trend toward backup protection is encouraging, there is still significant room to grow overall with only 49% reporting that they take extra measures for all their backup copies.

Extent to which backup copies of data are protected against ransomware attacks.



“There is still significant room to grow overall with only 49% reporting that they take extra measures for all their backup copies.”

A woman with long dark hair, wearing a grey long-sleeved shirt and a black headset, is sitting at a desk in a dimly lit office. She is looking at a large computer monitor that displays a dark-themed code editor with lines of white text. Her hand is resting on her chin, suggesting a thoughtful or focused expression. In the background, another person is visible working at a desk, and the office environment is softly lit with natural light from a window on the right. A small red horizontal line is positioned above the text on the left side of the image.

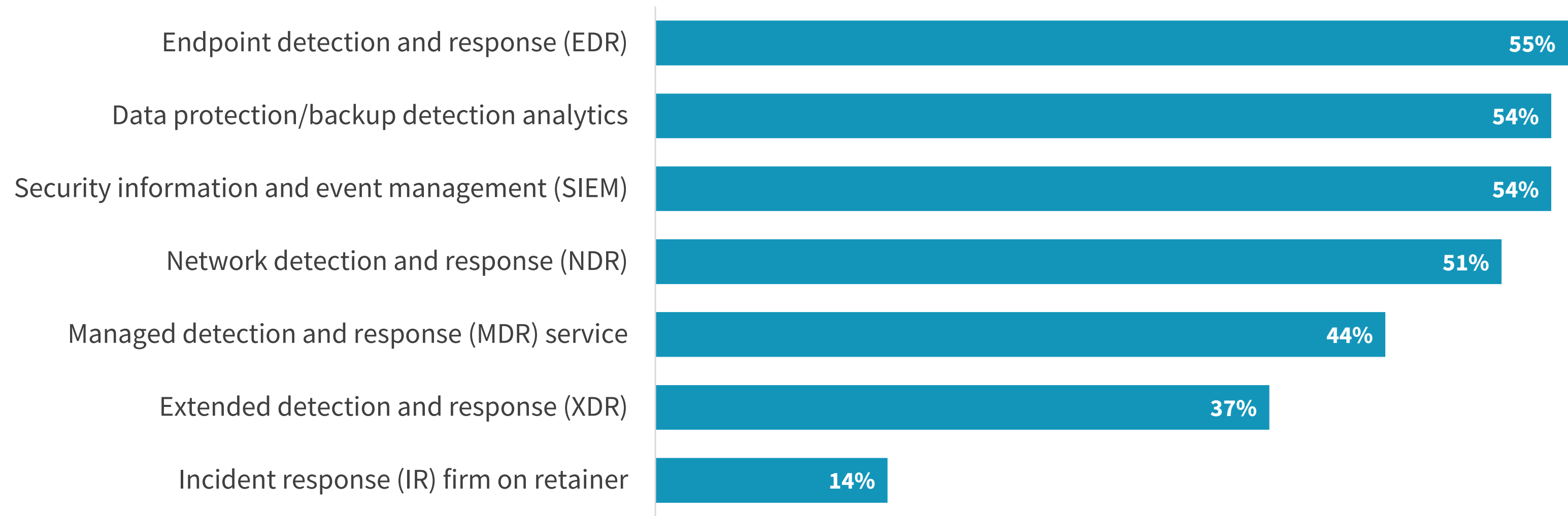
Skill Shortages and a Dependence on Internal Resources for Response Posture Put Many at Risk

Detection and Response Mechanisms Are Critical across All Vectors, though Most Depend on Internal Resources for Response Activities

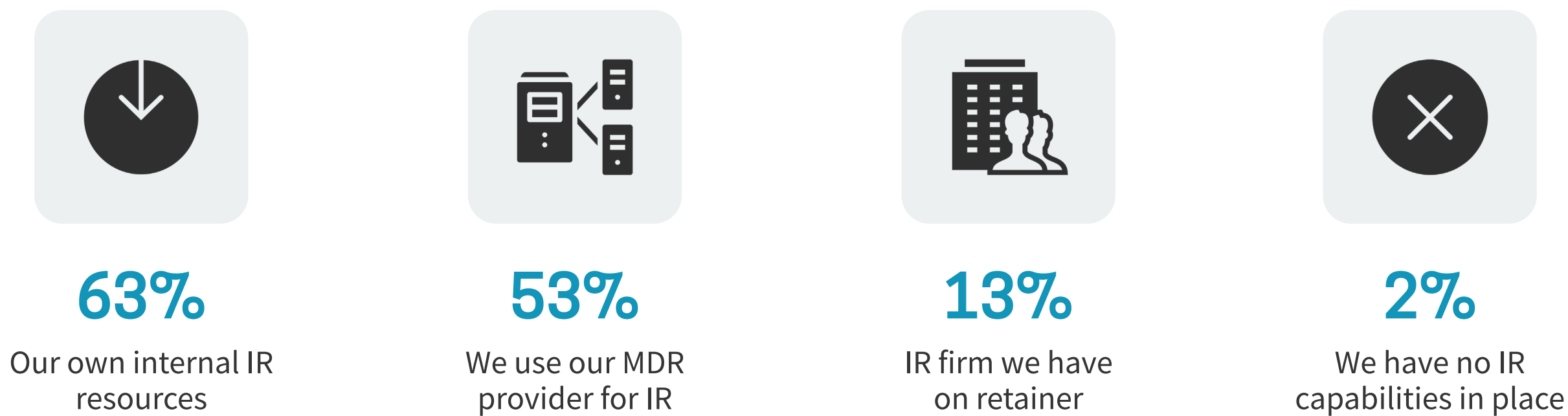
Investments in detection and response mechanisms and services are core to ransomware response activities, with more than half already leveraging these mechanisms, from the endpoint out to the network. Even XDR investments are quickly gaining traction, with more than one-third already reporting active use.

While the majority of organizations do have some kind of incident response (IR) capabilities in place, only 14% have formal retainer agreements with IR firms. Two-thirds of organizations are staffing response functions with their own incident responders, while half are also depending on managed detection and response (MDR) providers to help. MDR has quickly become a core strategy for security teams to overcome skills and coverage shortages.

Mechanisms in place to help detect and respond to an active ransomware attack.



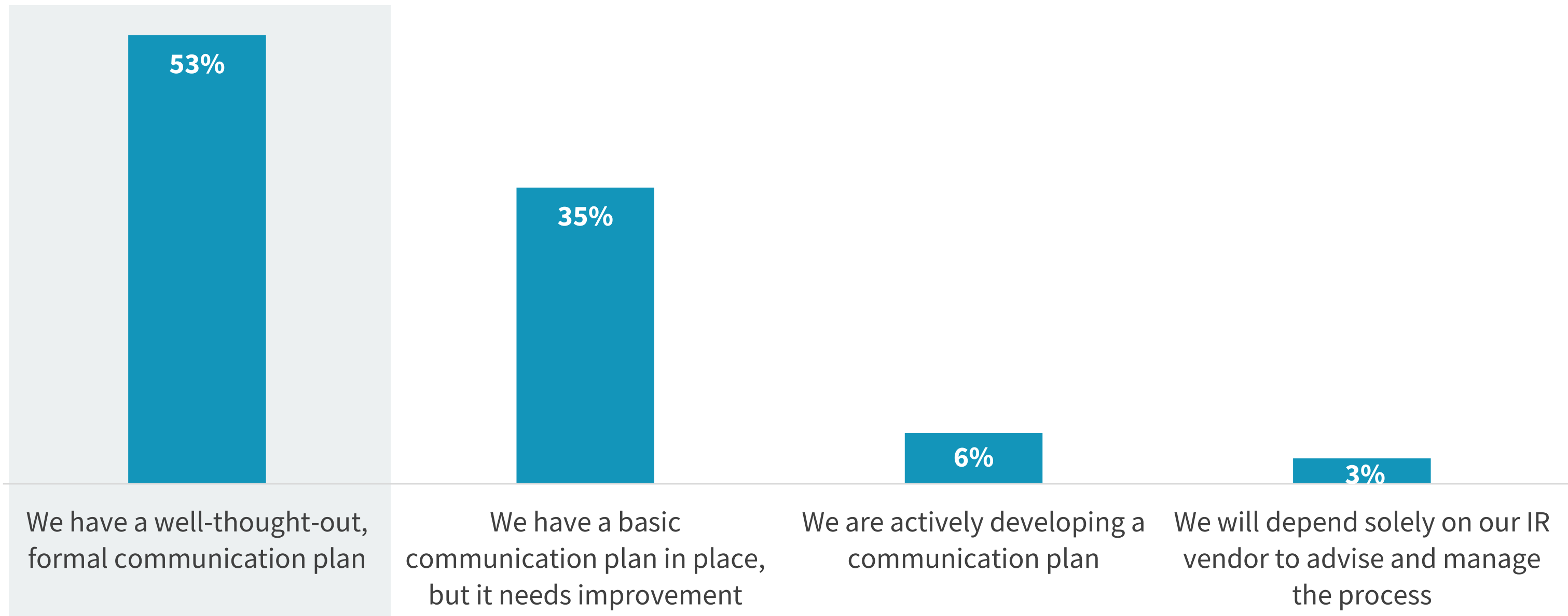
Who handles incident response in the event of a ransomware attack?



More Than Half Have Formal Communications Response Plans

Rapid internal and external communications play a critical role as ransomware attacks play out, and more than half (53%) report that they are prepared with a well-thought-out, formalized communication plan. However, the remainder of organizations indicate that their communication plans either need improvements or to be developed.

Communication response plans made to prepare for a ransomware attack.



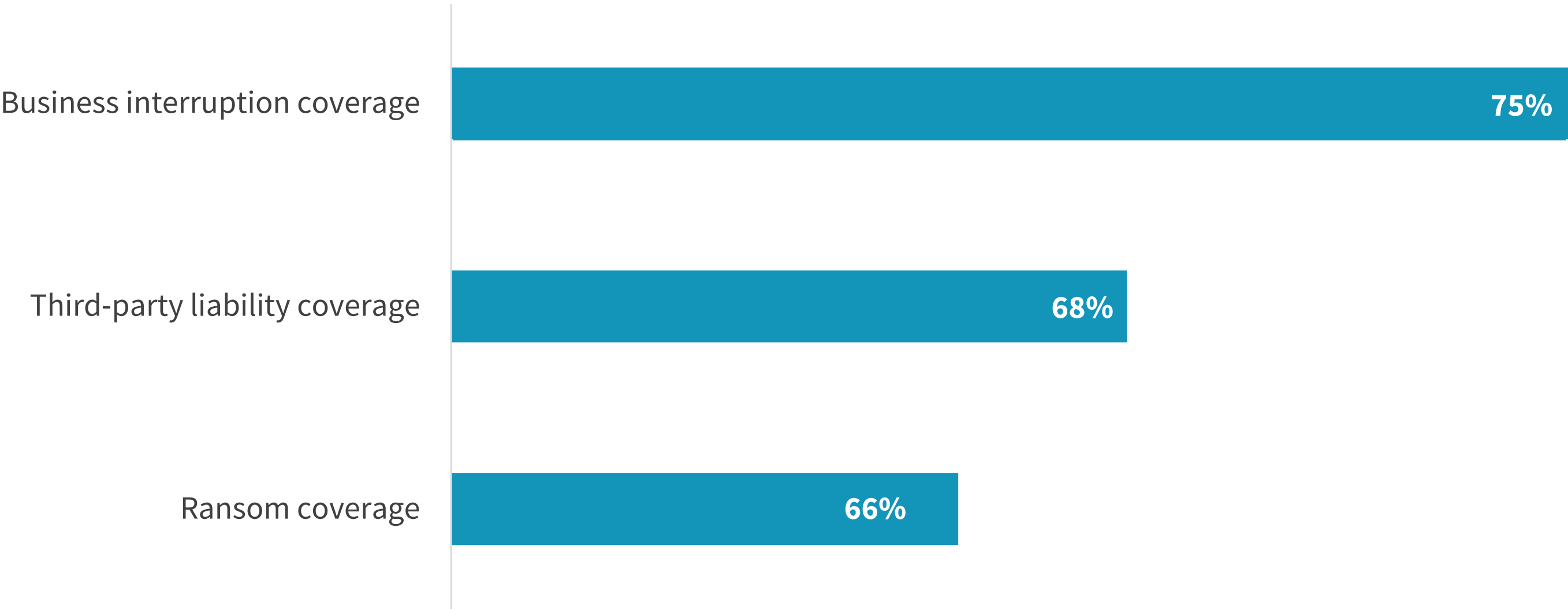
“More than half (53%) report that they are prepared with a well-thought-out, formalized communication plan.”

Organizations Currently Using Cyber Insurance as a Preemptive Ransomware Measure Taking a Varied Approach

Cyber insurance continues to grow in popularity to help mitigate financial impacts, with more than one-third (35%) of organizations reporting they currently purchase cyber insurance as a ransomware mitigation tactic. Cyber insurance offerings vary widely, meaning that the insured must make bets on where coverage is needed most. Among those organizations that currently own policies, coverage for business interruption and ransom payments are most popular, but those most prepared also invest significantly in third-party liability coverage to mitigate the long-tail impact of ransomware attacks.

“More than one-third (35%) of organizations report they currently purchase cyber insurance as a ransomware mitigation tactic.”

Type(s) of cyber insurance to which organizations currently subscribe.



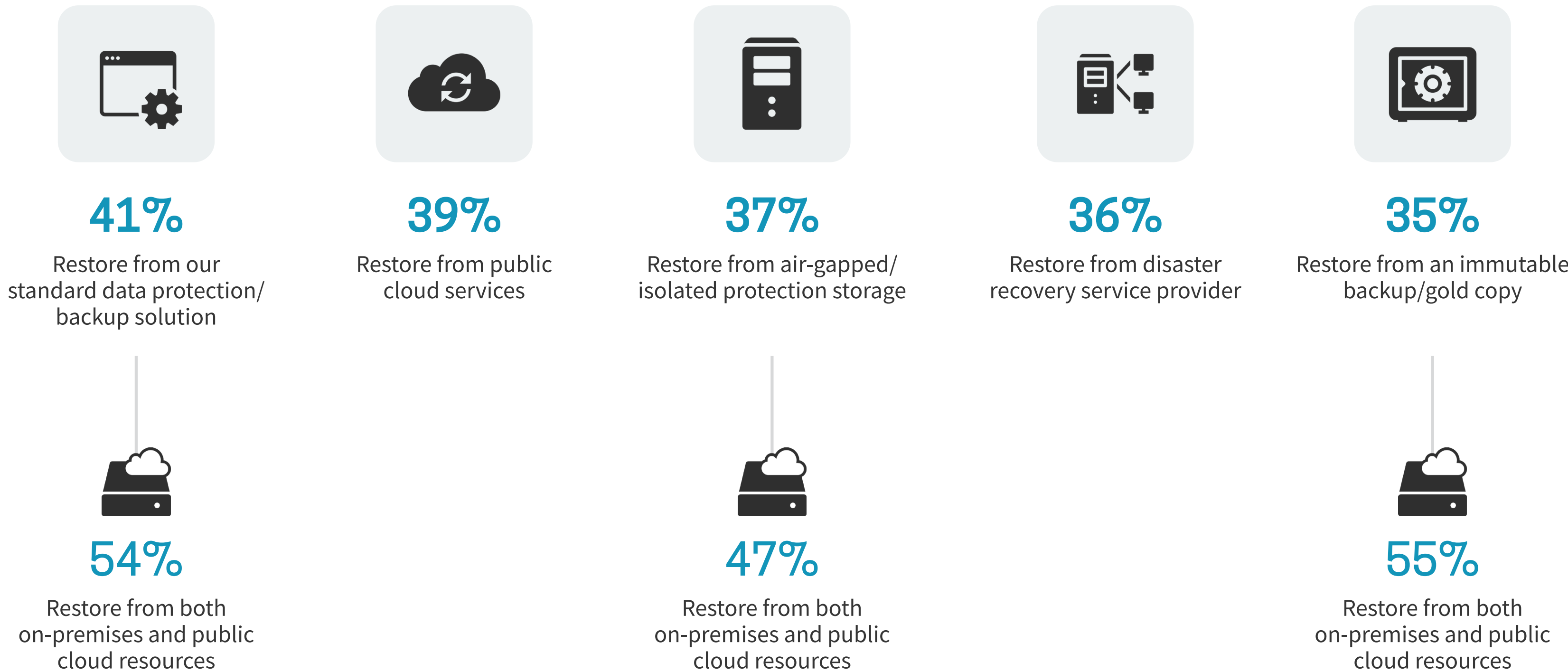
The background is a dark, futuristic digital environment. A large, billowing white cloud is the central focus. Below it, a glowing blue grid of light points stretches across the floor. A transparent wireframe cube is positioned in the upper right, with a thin blue line extending from its top right corner towards the bottom right. In the lower right, there are faint, glowing blue circuit-like patterns. On the left side, a short, thick red horizontal line is visible.

**While Hybrid Backup Use Is
Common, Ransomware Recovery
Is Not a Guarantee**

Backup Is King for Cyber Recovery Overall, with Hybrid Recovery Methodologies Favored

Backup is king for cyber recovery overall as it tops the list of methodologies that organizations would leverage should they become victims of a successful ransomware attack (a successful attack meaning that data is compromised and needs restoring to a “clean state”). The advent of cloud in the past few years is very visible in this context as public cloud infrastructure has become a destination of choice for backups. It should also be noted that in order to mitigate the ability of cyber criminals to “reach” backups (to make them targets), many organizations are favoring emergent best practices such as restoring from air-gapped/isolated protection storage or restoring from an immutable or “gold” copy of data. This means that IT leaders will be looking for these capabilities in their current and future backup solutions, which must be hybrid to support on-premises, cloud-only, or a combination of deployment topologies.

| Planned method(s) of recovery from successful ransomware attack for impacted applications and data.

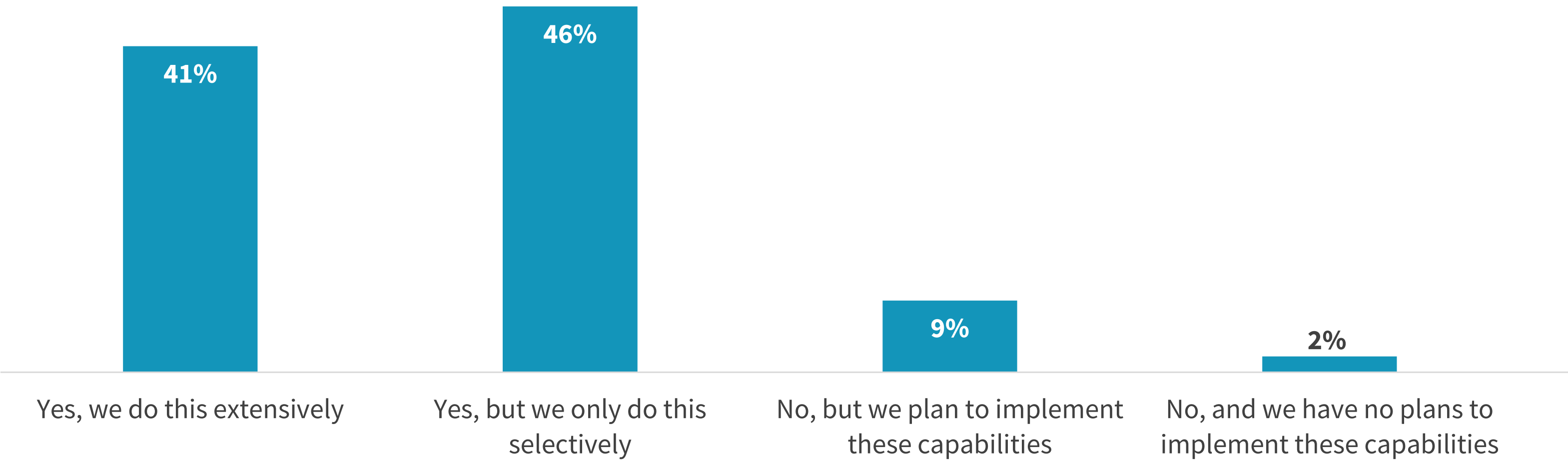


Granular Data Restores Preferred over Full Rollbacks

The ability to perform granular data restores versus full rollbacks is widely leveraged, though some organizations use these capabilities in a more extensive manner when it comes to ransomware processes. This best practice relies on the backup and recovery solution having the capabilities to pinpoint specific files, virtual machines, etc., rather than forcing a larger and potentially elongated recovery. Another aspect to consider is that granular recoveries allow for the exclusion of suspicious components and might help in speeding business resumption by excluding “dirty” data while allowing only the “clean” data to be used. Although for maximum effect, this capability might require automation and integration with ecosystem solutions beyond backup.

“The ability to perform granular data restores versus full rollbacks is widely leveraged.”

| Ability to perform granular data restores.

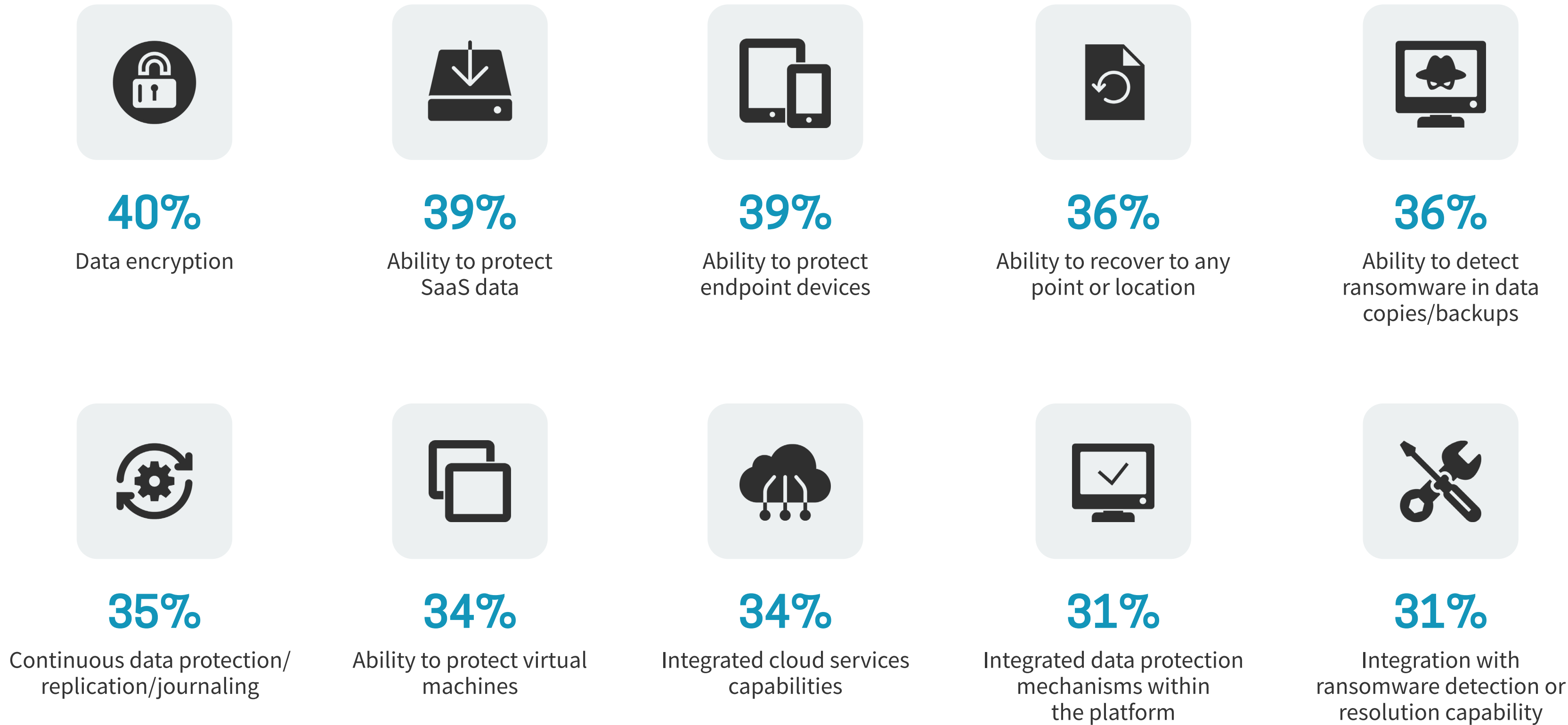


Ransomware Recovery ‘RFP’ Highlights Cloud and Ecosystem Integration

IT leaders have identified key areas of capabilities they require in the selection of a ransomware recovery solution, which is often powered by a backup and recovery solution. These requirements are very diverse in terms of technologies and capabilities that must work in unison.

Data governance and compliance best practices have placed a focus on the protection of data from unauthorized views or use, making encryption a “go-to” set of technologies, as evidenced by its place atop the list of considerations. The data could still be stolen or made unusable, but at least it would not be in the clear. Additional key recovery requirements reflect the evolution of modern IT infrastructure that heavily relies on SaaS data and endpoint devices as well as the need for flexibility with the ability to recover to any point or location to better adjust to the various anatomies of ransomware attacks. Also, securing backups is another concern and requirement expressed by many: Detecting ransomware in backup copies is a likely item on the RFP list as well.

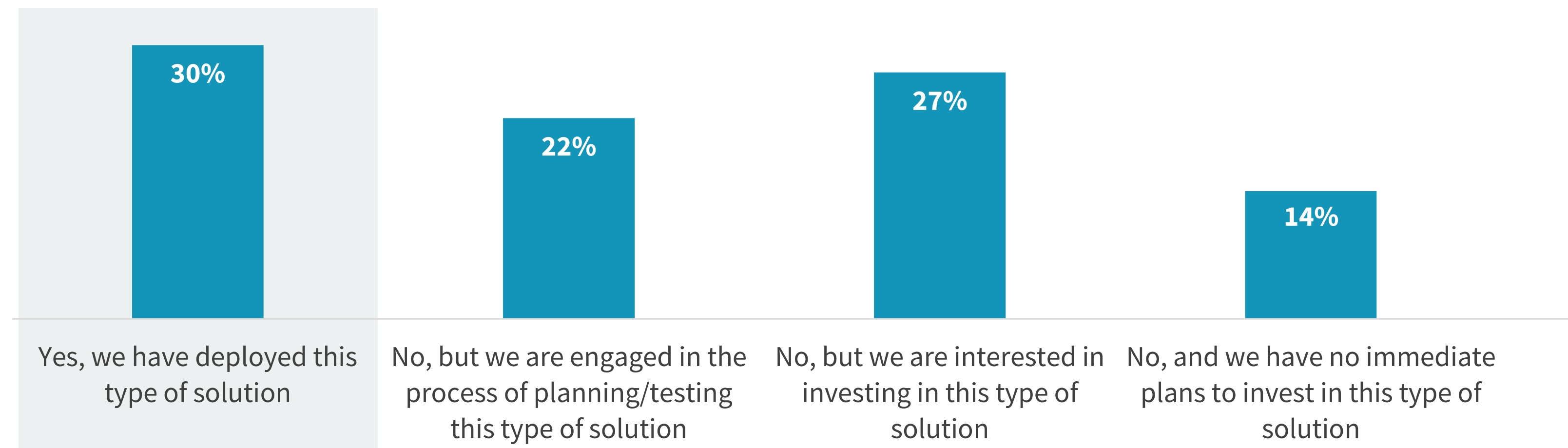
| Top ten important considerations for ransomware recovery solutions.



Less than One-third Have Deployed an Air-gapped Solution

In order to successfully reduce backup data destruction risks, air-gapping is a “must have” technology. Air-gapping is a best practice that has proven itself, allowing the backup or recovery copies to be physically and logically separated from the rest of the network (multiple topologies exist). The intent and net effect is to make the backups impossible to reach by attackers: Copies can be preserved from destruction and are fully usable in a recovery effort. Surprisingly, only 30% of organizations have deployed this type of solution today, providing cyber criminals with many opportunities. This demonstrates how much more maturity the market needs to acquire solutions like air-gapping to mitigate the substantial risks associated with backup/recovery data.

Usage of air-gapping to mitigate the effects of ransomware.



“Only 30% of organizations have deployed this type of solution today, providing cyber criminals with many opportunities.”

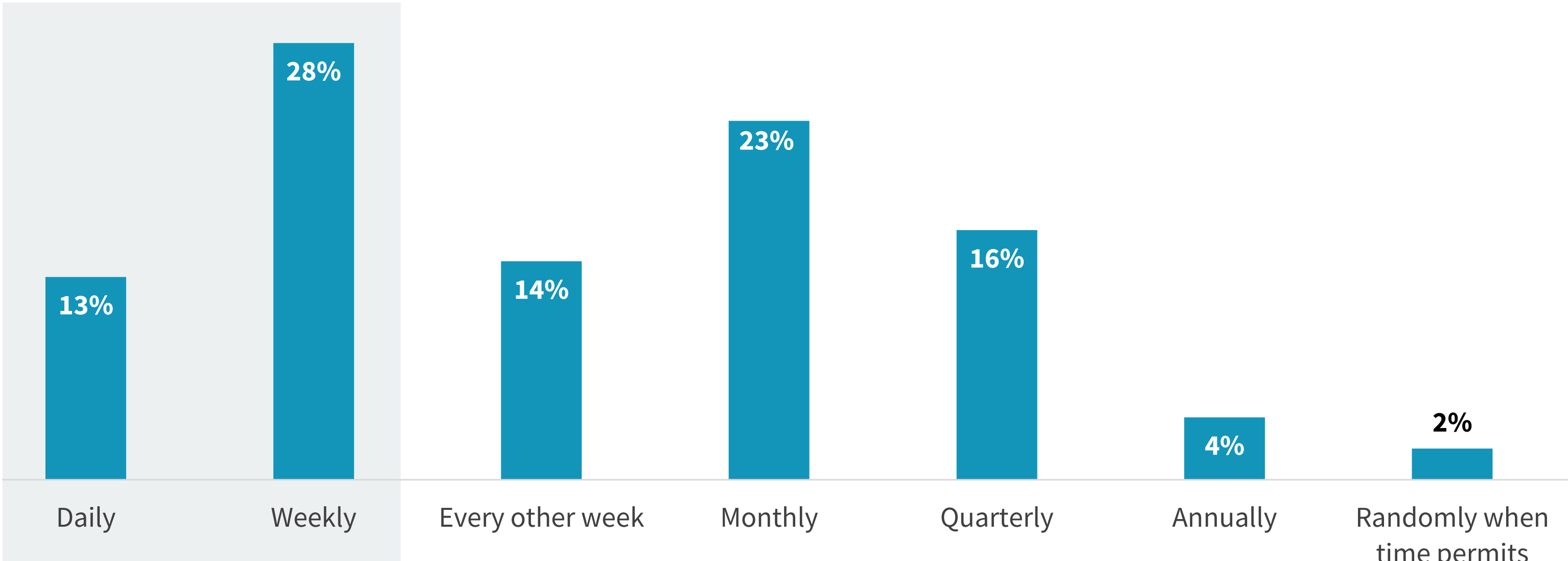
RPO and RTO Gaps Separate the Most Advanced in Business Continuity



Data Restoration Test Frequency

In the space of disaster recovery, practice makes perfect. The more organizations practice their processes, the better they will be at resuming business and IT activities in a timely fashion. One key element is to focus on data recoverability; after all, no data, no business. Testing the ability to restore from data protection and recovery solutions is therefore critical. However, with only 41% of organizations testing weekly or more frequently, the testing cadence appears to be too low to sustain the current influx of attacks and their consequences. There may be specific reasons: Ransomware data restoration is not as straightforward as a “normal” recovery, unless the data in the backups has been analyzed and deemed “clean.” And with the many types of attacks that exist, it may be hard to plan and test for all the possible scenarios. However, very frequent testing is still preferable, and the market seems to be lacking maturity in this dimension. This offers vendors a great opportunity to help automate and simplify these processes.

| Frequency of proactively testing the ability to restore data from data protection and recovery solution.

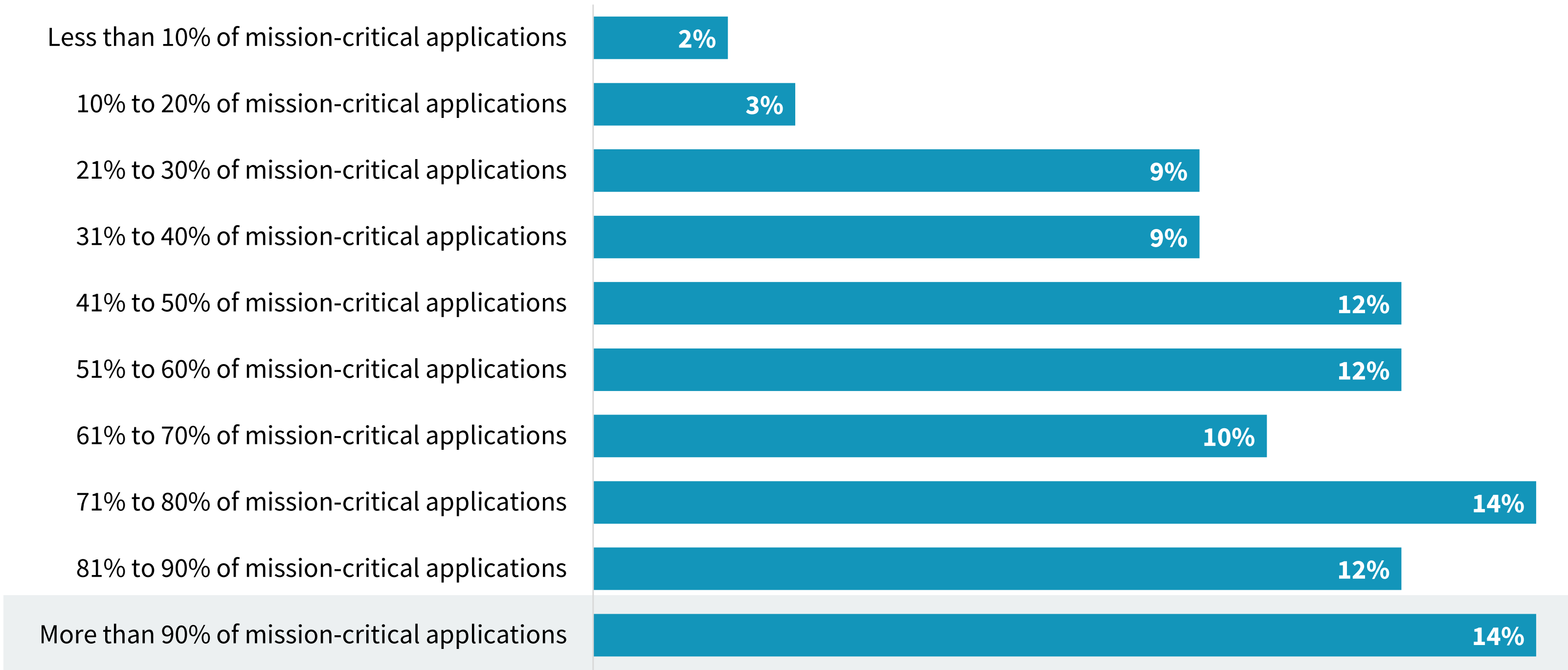


“Only 41% of organizations are testing weekly or more frequently.”

Underwhelming Mission-critical Application Protection Posture

There is a mission-critical data protection gap in the market today when it comes to ransomware preparedness. It is substantial and explains why attacks can be so successful and disruptive. In order to be prepared, one would expect that organizations would try to protect all of their mission-critical applications and associated data sets. After all, these are mission-critical for a reason: They power the business. It may be hard in a very dynamic environment to get to 100% protection at all times, but today, only 14% report protecting more than 90% of their mission-critical applications. Look no further for disruption opportunities. This is another indicator of how immature or unprepared the market is overall.

Percentage of mission-critical applications protected by a solution that can ensure there is always a copy of uncompromised data from which organizations can restore.

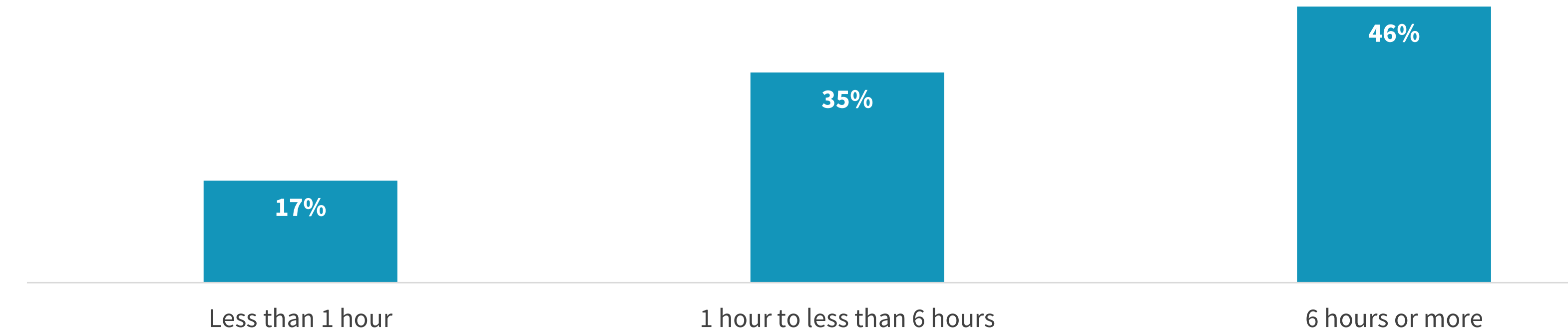


“Only 14% of organizations report protecting more than 90% of their mission-critical applications.”

Visible RTO and RPO Gaps Exist When It Comes to Ransomware

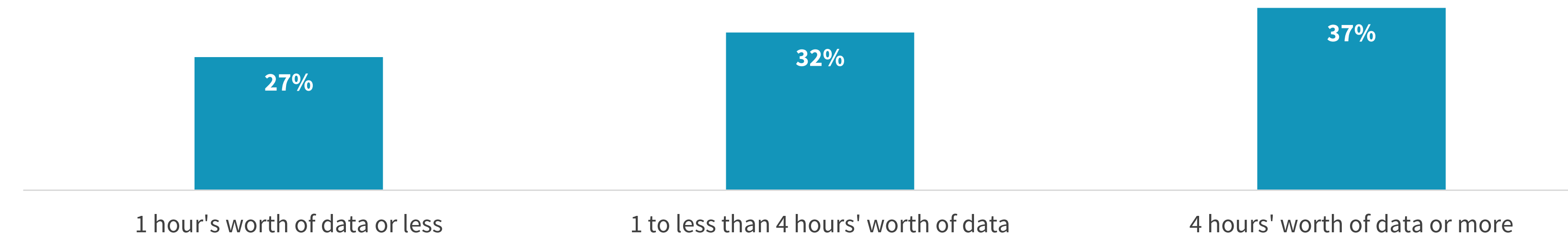
Recovery time objectives (RTOs) highlight how quickly organizations can recover from the resulting downtime of a ransomware event. Ransomware generates hours of downtime and business disruption and often comes with significant consequences like lost business, negative publicity, and compliance exposures, among others. More advanced organizations do better and can get back on their feet faster than the least prepared. When comparing to other service level agreement (SLA) benchmarks for traditional interruption events, ransomware RTOs are more elongated. The complexity of attacks and remediation mechanisms, including the need to engage with many different parts of the organization that may follow poorly coordinated incident response and disaster recovery processes, are likely reasons. This makes ransomware recovery a top business issue.

| Speed with which organizations can recover from a ransomware event and resume mission-critical functions.



Recovery point objectives (RPOs) matter greatly: Every lost bit of data is money and may represent a key transaction that can never be reproduced. Losing data is like throwing money out the window in layman’s terms. Overall, organizations are reporting that they are likely to lose hours of data with more advanced organizations being more apt at recovering data faster. Compared to traditional RPOs for “normal” disaster recovery, it is very clear that the complexities associated with ransomware recoveries are having a significant impact on best practices SLAs, exposing organizations to the potential of significant losses and consequences. In a “perfect” world, no transactions would be lost, or at least only a few minutes’ worth. Yet for ransomware, the threshold changes to hours. This is probably why executive management sees ransomware as a top business issue and not just an IT issue.

| Data organizations can afford to lose when recovering from a ransomware event.



Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers’ ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

LEARN MORE

ABOUT ESG

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.

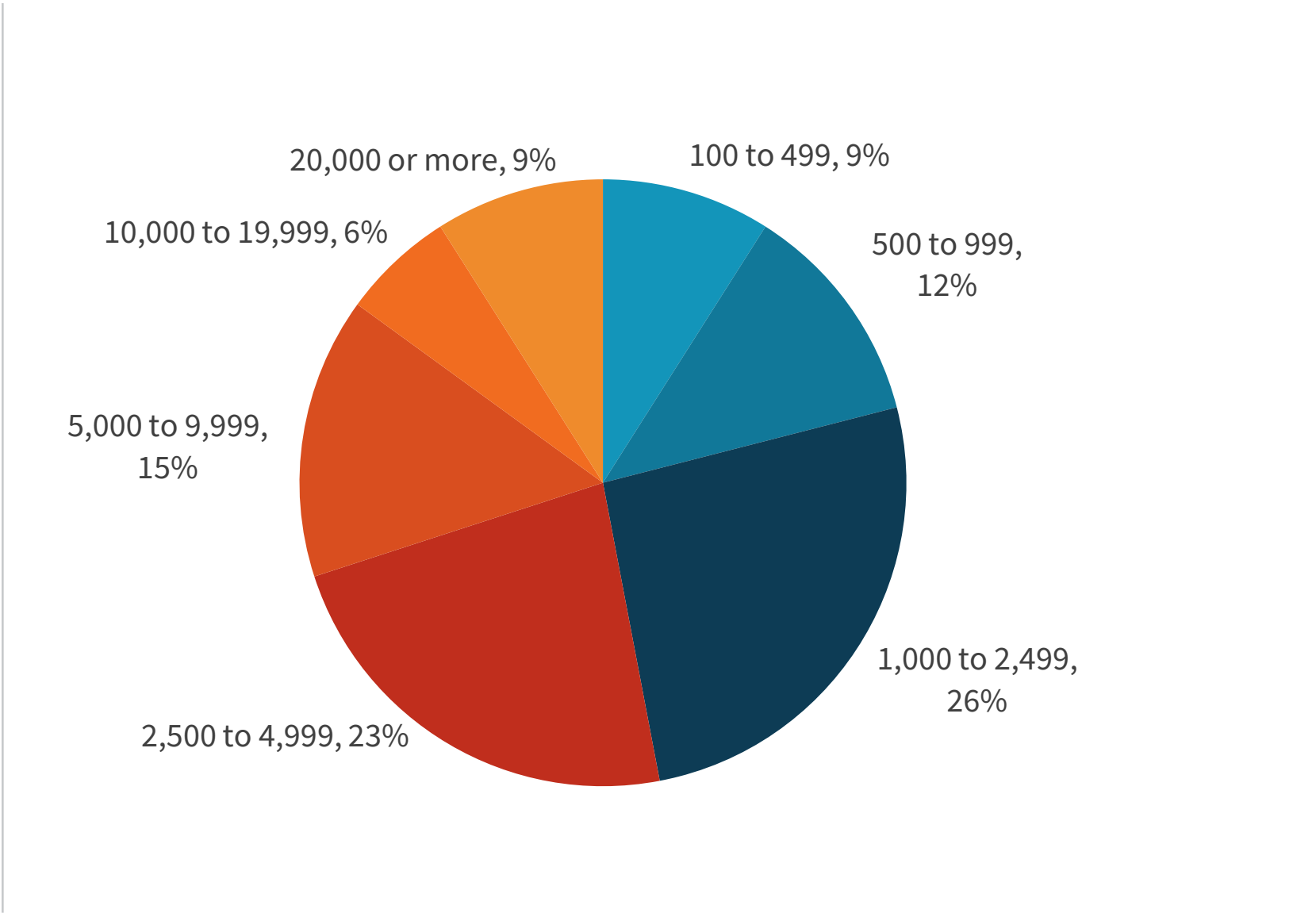


Research Methodology

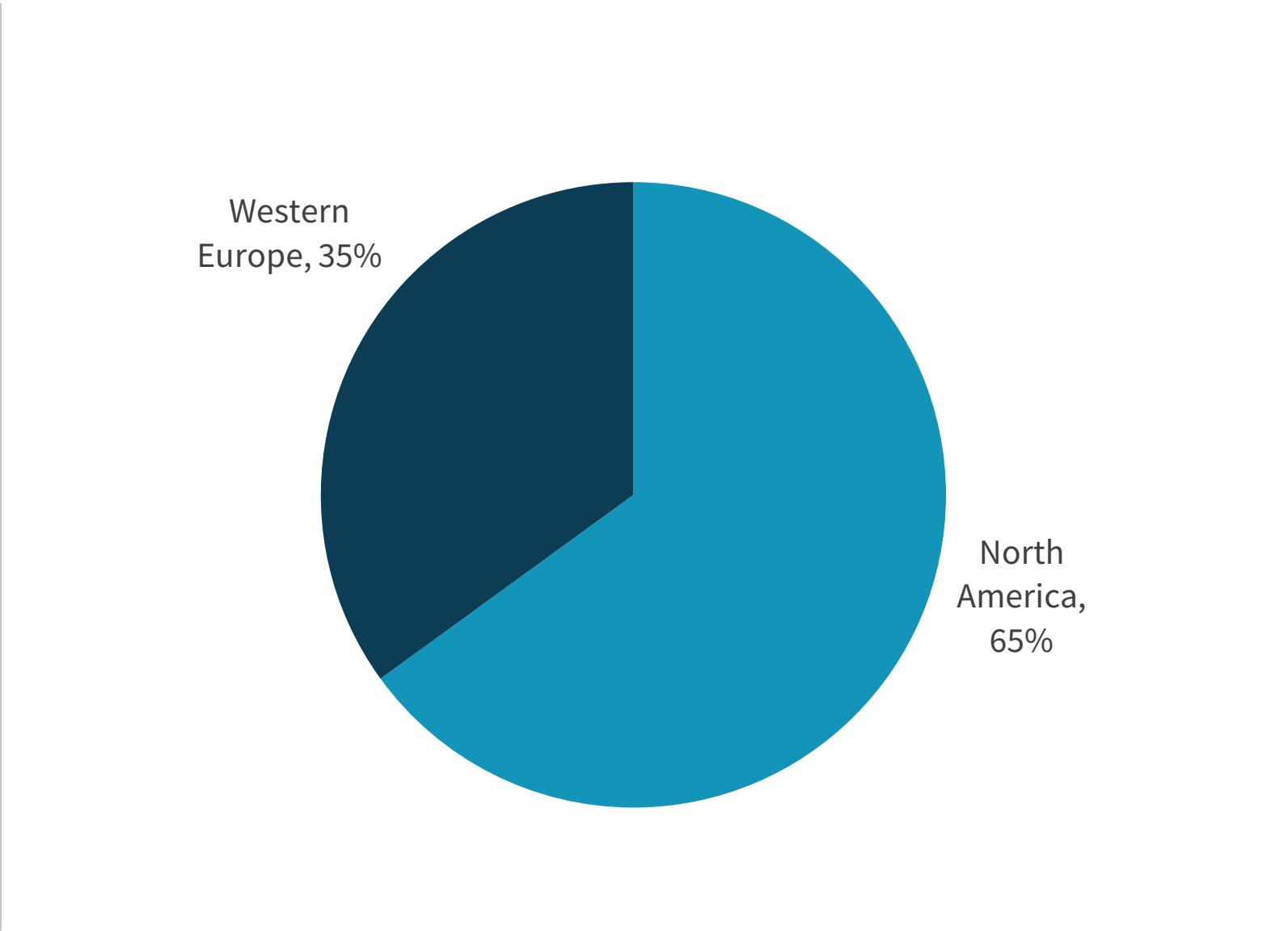
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America and Western Europe between December 21, 2021 and January 10, 2022. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally involved with the technology and processes associated with protecting against ransomware attacks. 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 620 IT and cybersecurity professionals.

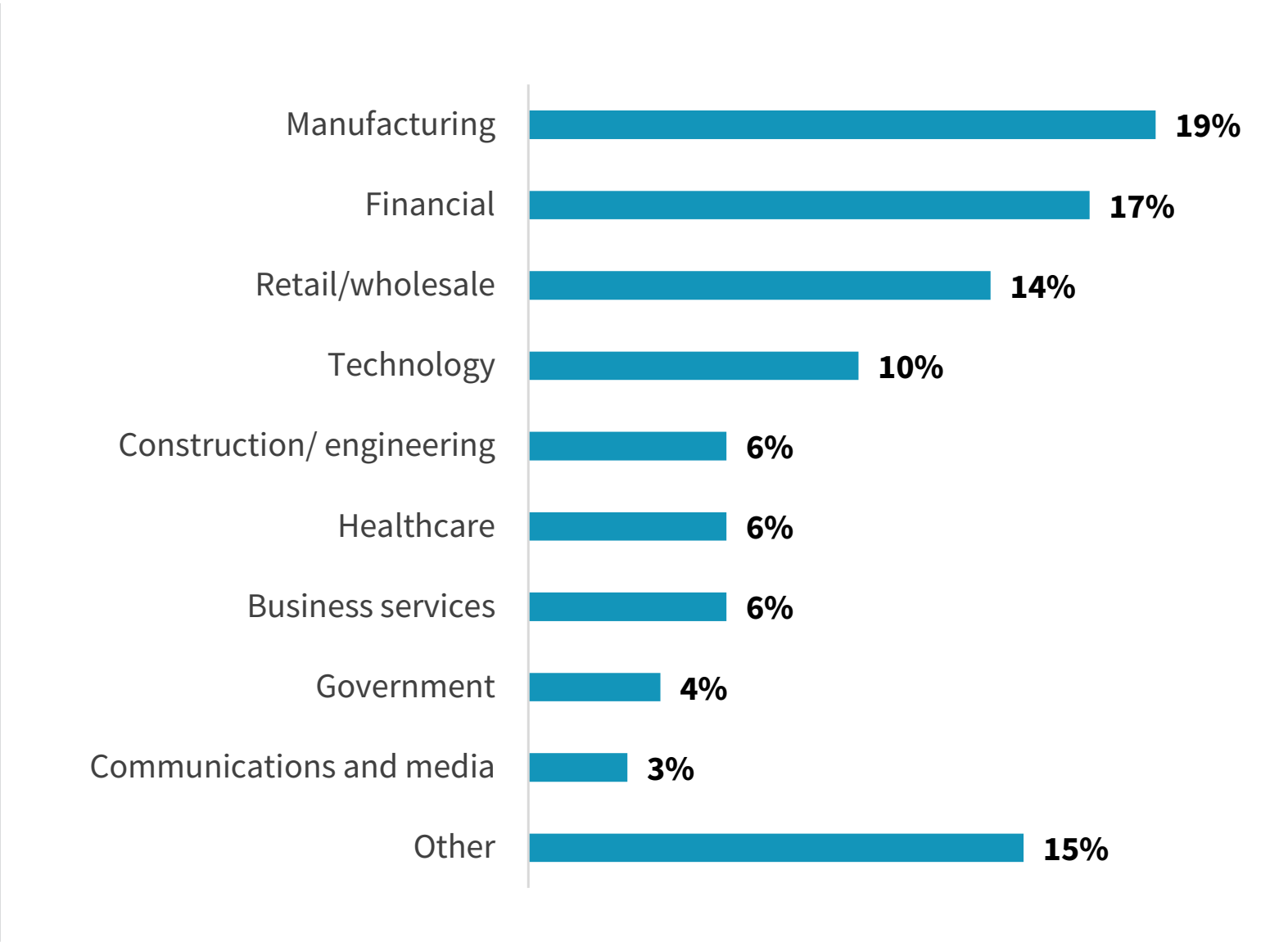
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY REGION



RESPONDENTS BY INDUSTRY



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



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.

© 2022 TechTarget, Inc. All Rights Reserved.