White Paper

The State of Disaster Recovery and Cyber-Recovery, 2024–2025: Factoring in AI

Sponsored by: Zerto

Phil Goodwin
August 2024

IDC OPINION

Data protection strategies and systems are constantly evolving, as are the systems they protect and the threats organizations face. Cyberattack methods "mutate" over time as attackers seek new ways to exploit defensive weaknesses. Moreover, the changing regulatory landscape, often geographically specific, demands new data management protection policies.

Data protection strategies and systems must support the organization's business requirements. Foremost among these is maximizing data availability — the resource upon which business operations and competitive posture depend. To maximize data availability, IT teams must minimize downtime and data loss. More mature organizations measure and track data availability service-level agreement (SLA) for data availability. These SLAs addressing downtime, recovery time, and acceptable data loss, such as RPO and RTO, are becoming shorter and stricter as businesses depending upon data demand ever-better service levels. In the early days of data protection, systems were primarily limited to backup/recovery (B/R) software to move data to tape. However, B/R alone is insufficient for disaster recovery (DR) or cyber-recovery (CR). B/R is foundational to all data protection and resilience efforts, yet it is not enough to meet the more complex needs of DR, which may involve moving application services and data to a second site. This requires asynchronous or synchronous data replication, replicated infrastructure, application failover/failback processes, and operational process runbooks. CR builds upon B/R and DR technology and processes with additional requirements for malware detection, forensic analysis, cleanroom recovery, and more. Speed is of the essence regardless of the nature or cause of the recovery.

The sudden rise to the prominence of artificial intelligence (AI) adds to the requirements for data protection and cyber-resilience solutions in two ways. First, AI can be used to improve protection and resilience operations. This may include infrastructure optimization, dynamic process development such as runbooks, malicious activity detection, and AI-driven recovery. Second is the need to protect the AI models themselves. This includes AI learning modules and inputs, chain of custody verification to avoid capturing proprietary information, compliance to ensure sensitive information is properly protected, and malware detection and recovery.

For all the hype and promise of AI, it remains nascent in data protection and cyber-resilience and is often limited to anomaly detection. To assess the current state and impact of DR, CR, and AI, Zerto engaged IDC to conduct an independent assessment of the industry. We wanted to determine where IT organizations are today in developing DR and CR systems and their perspective on AI for data protection and their priorities in the next 12-24 months and addressing gaps in current solution

deployments. This IDC white paper intends to help IT leaders assess where their organizations are relative to the industry and provide insights on improving their strategies and operations.

METHODOLOGY

This IDC white paper highlights key findings from a recent market survey sponsored by Zerto to assess the state of modern data protection, disaster recovery, cyber-recovery, and AI. The survey was conducted worldwide with 504 respondents or organizations having 500 employees to more than 10,000 employees with representative samples of 18 industries; no industry was represented by more than 9% of respondents.

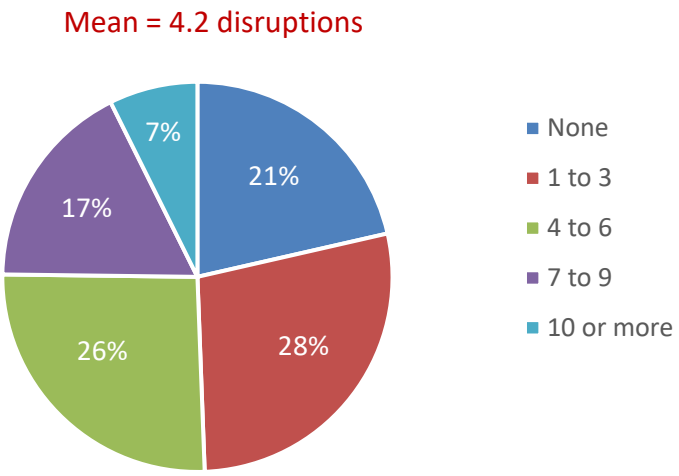
SITUATION OVERVIEW

Data loss has been an issue since the dawn of computing, but cyberattacks have made that risk greater than ever before. Some organizations, especially financial institutions, may need to deflect thousands of attacks per day. Yet no organization of any size, industry, or geography is immune from cyberattack. Successful attacks penetrate defenses or events that cause business disruption and demand the undivided attention of the ITOps and SecOps teams. To understand the magnitude of the problem, we asked respondents to tell us how many data-related business disruptions requiring an IT response occurred yearly. According to these respondents, organizations across the board average 4.2 data disruptions yearly (see Figure 1).

FIGURE 1

Data-Related Incidents per Year

Q. *Within the past 12 months, how many data-related business disruptions (including cyber-related, e.g., ransomware) has your organization experienced (i.e., loss of access to at least one application)?*



n = 504

Base = all respondents

Notes:

The data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

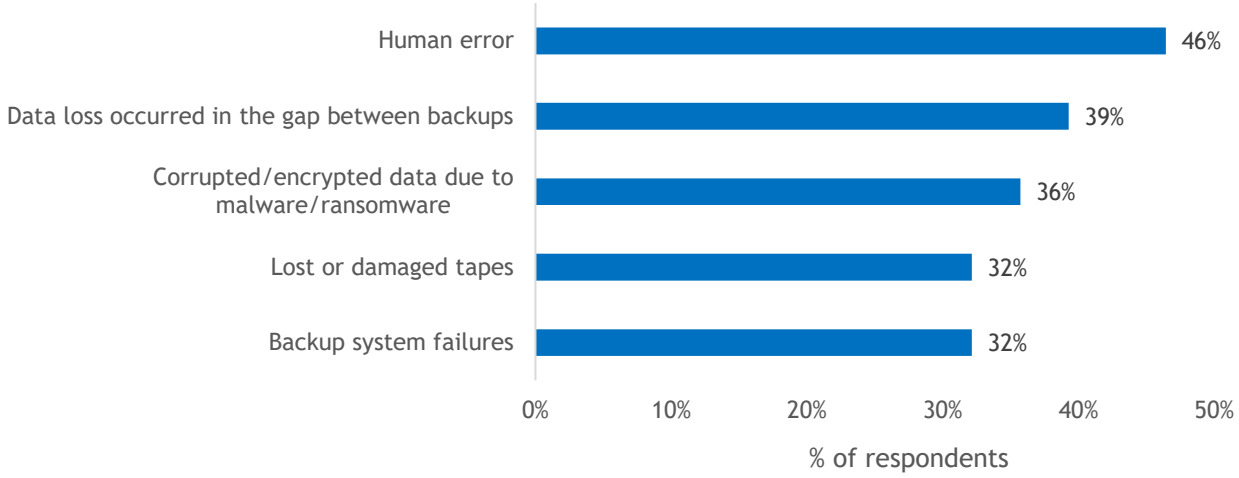
When we drilled in further and asked respondents about the impact of these events, loss of employee productivity was the top response (49%). Direct loss of revenue was a distant second in the list of impacts (29%). Although reputation damage was cited as an impact, it was relatively far down the list, with 16% citing major reputational damage. We find that as ransomware attacks have become commonplace, the stigma of attack has diminished, save for a few especially high-profile attacks. Instead, more mundane, business-oriented impacts are most significant. Separate IDC research pegs the average cost of downtime at $970,856 per year for planned and unplanned downtime across all industry's geographies and organizational sizes (see *Average Hours and Cost of Datacenter Downtime,* IDC #US51053921, July 2023). However, it does not include extraordinary events such as ransomware or the average ransom paid of $166,000 per event (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* November 2023).

Unfortunately, data loss remains all too common for organizations. IDC's February 2024 *Zerto AI CR Data Protection Disaster Recovery Survey* asked respondents what the primary causes of data loss were (see Figure 2).

FIGURE 2

Reasons for Data Loss

Q. Which of the following were responsible for the data becoming unrecoverable?



n = 56

Base = respondents who indicated that their organization had experienced an event that resulted in unrecoverable data

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

While ransomware gets all the current attention, keep in mind that human error remains a major cause of data loss. Aside from human error, we found it significant that backup-related errors were cited in about one-third of cases where data was lost, including corrupted backups due to ransomware, backup system failures, and lost or damaged tapes. While human error will always be an issue, in the modern era, backup-related issues should be rare. Organizations that do not achieve 96% success on backup/restore operations should evaluate their systems for improvement, and organizations that lose data due to tape failure are likely not following the basic 3-2-1 backup best practices.

Perhaps because of the reported backup failures, 28% of respondents in this survey told us that backup modernization was among their top 3 IT initiatives for the next 12 months. When asked about the most important criteria when selecting backup and DR tools, the top response was "breadth of solution" (30%). Speed of recovery was a close second (29%), in fact, within the survey's margin of

error. Clearly, respondents understand the need for solutions that address common data recovery scenarios, such as human error, and the need for comprehensive solutions to address DR and CR. Organizations need solutions to meet SLAs to provide the fastest recovery with the least data loss.

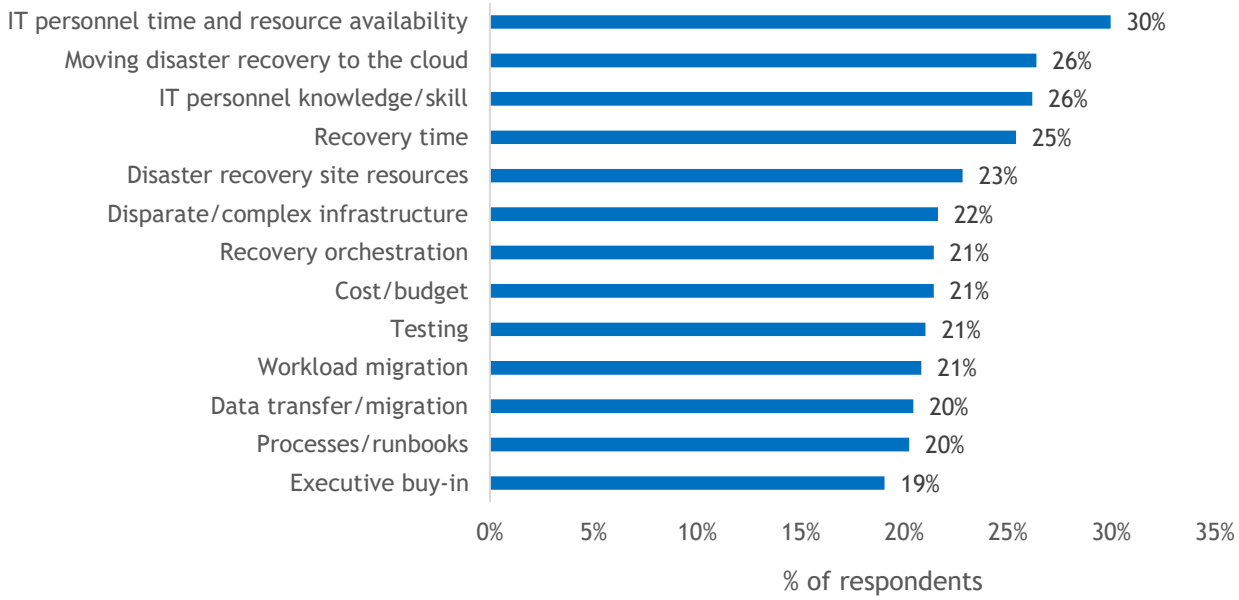
Although technology is an important part of any resilience solution, people and processes are equally important. Our survey found that the people aspect is a significant challenge for many organizations. When we asked respondents to tell us their top 3 biggest challenges for disaster recovery, "IT personnel time and availability" was at the top of the list (30%). Figure 3 graphically presents the details.

As noted in Figure 3, the second-most- cited DR-related challenge was moving DR to the cloud. This likely bolsters the perspective that "breadth of solution" is highly important. Organizations need solutions that support hybrid cloud architectures and multicloud environments. In fact, this survey also showed that although 90% of organizations use cloud for some aspect of their data protection, more than 58% of organizations protect fewer than half of their applications using cloud DR.

FIGURE 3

Top 3 DR Challenges

Q. What are your organization's top 3 biggest challenges with respect to disaster recovery?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

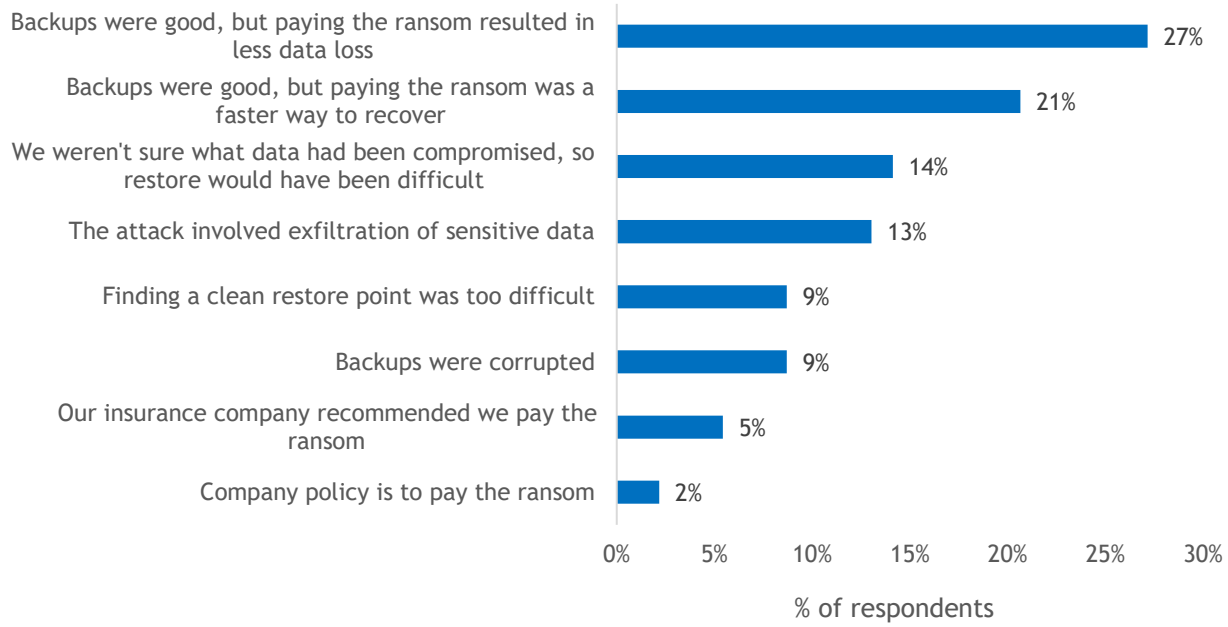
Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

IT organizations must respond to an average of 4.2 incidents per year (refer back to Figure 1). When we delve into the nature of these events, we learn that one involves ransomware, on average. An IDC research, separate from this survey, has found that only 31% of organizations can fully recover from ransomware without paying ransom. Moreover, according to the survey conducted for Zerto, 48% of companies that paid the ransom were often from organizations with clean backups. We wanted to learn why organizations would pay a ransom even when they can fully recover their data (see Figure 4).

FIGURE 4

Reasons for Paying Ransom with Clean Backup

Q. Indicate the primary reason your organization paid that ransom.



n = 92

Base = respondents who indicated that their organization paid a ransom for malicious attacks that required IT response

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

As this data illustrates, roughly a quarter of organizations felt that paying the ransom would result in a faster, more complete recovery than their data restoration capabilities. While it can't be determined if the root cause was poor processes or inadequate technology, it is likely a bit of both because process and technology go hand in hand. Even if processes are at the root, they often must make up for a lack of technology, such as manual effort in the place of recovery orchestration software. Modernizing

technology and updating processes may avoid these situations. Furthermore, IT leaders should take steps to adequately test and audit their recovery capabilities, as these capabilities should never be inferior to ransom payment.

Effective cyber-response requires a well-coordinated organization. Unfortunately, according to this research, senior management and the ITOps teams often view cyber-recovery as having different priority levels. Findings from this survey showed that only 36% of organizations have coordinated DR and CR systems and plans. Our findings also showed that while 9% of senior business management respondents and ITOps teams saw cyber-recovery planning as a number 1 priority, only 6% of senior IT managers saw it with the same priority (a statistically significant difference). And, whereas only 10% of ITOps respondents saw it as a top 3 priority, twice as many senior business and IT managers (20%) saw it as such a priority. This illustrates a "too common" disconnect between different parts of the organization and between senior management and IT teams.

FUTURE OUTLOOK

There is no question that AI is generating a tremendous amount of interest in almost every industry and organization type. For data protection and cyber-recovery, AI has several potential applications:

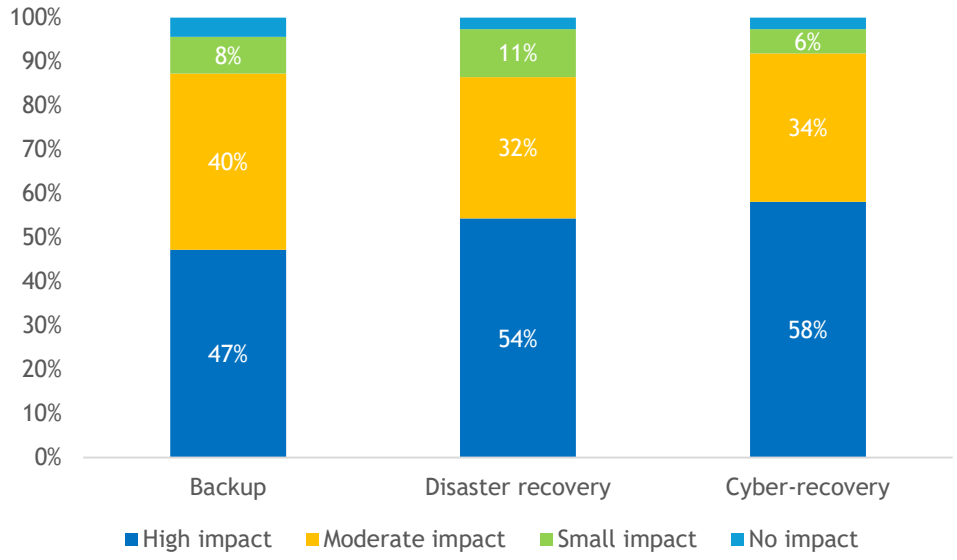
- Backup infrastructure optimization
- Runbook development
- Threat detection
- Dynamic recovery orchestration
- Recovery point determination

Based on our survey results, respondents clearly agree about AI's potential. Nearly half (47%) of respondents think that AI has "high potential" for backup over the next 24 months, while more than half feel the same way regarding AI and DR (54%) and CR (58%) (see Figure 5).

FIGURE 5

Expected Impact of AI for Backup, DR, and CR

Q. How do you expect AI to impact your backup, DR, and cyber-recovery capabilities within the next 24 months?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

Of the three major types of AI (generative, behavioral, and predictive), most respondents feel that predictive AI will be the most impactful. Behavioral AI will be able to detect anomalous human behavior, such as compromised credentials, which is one of the most common methods for attackers to gain system access and detect rogue employees. Interestingly, GenAI was expected to have the least contribution to data protection and cyber-resilience in the next 12 months (22%) compared with behavioral AI (41%) and predictive AI (37%).

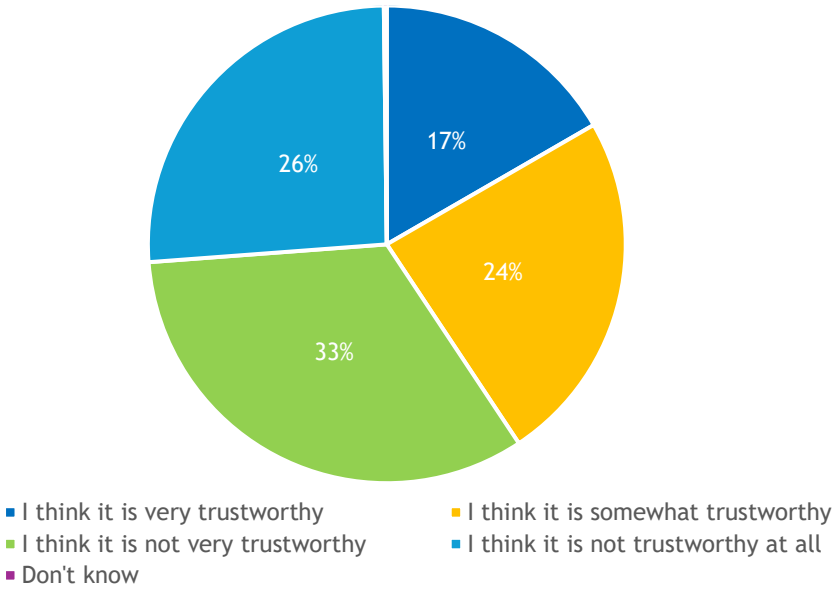
Without doubt, AI has significant promise for improving all aspects of data protection. Yet there is a dark side: Cyberattackers are using AI to more effectively penetrate cyberdefenses. Despite this trade-off, a plurality of respondents to our survey are generally positive about the future outlook. Of the total respondents, 40% believe AI is a greater benefit than a threat; 28% believe it will deliver equal benefit and threat, while only 15% believe it will have greater threat than benefit. The remaining 17% said it is too soon to tell.

Yet most survey respondents appear to be cautious about all the perceived potential for AI. Only 41% indicate they feel it is "very" or "somewhat" trustworthy, while 59% feel it is "not very" or "not at all" trustworthy. Despite the hype, these results indicate that AI adoption is more likely to follow the traditional technology adoption curve than rapid wholesale adoption. We believe it will be adopted on a use case basis as vendors introduce capabilities and IT organizations gain trust and identify tangible benefits to their organization (see Figure 6).

FIGURE 6

Degree of Trust in AI for Data Protection and Cyber-Recovery

Q. To what degree do you have trust in the current state of AI for data protection and cyberprotection?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

CHALLENGES/OPPORTUNITIES

Backup, DR, and CR require different technological, process, and human capital capabilities. While B/R may be foundational to all data recovery, it alone is insufficient for fast, effective DR or CR. Although the market offers numerous solutions, the fact is that they are hard to compare, given various competing capabilities. IDC suggests that organizations set and monitor service-level requirements to

ensure compliance. Frequent testing of recovery, DR, and CR is essential to preparedness. These testing protocols should include tabletop exercises and virtual and physical testing. To the extent that data protection and recovery products can assist with this testing, they can ease the burden on IT staff.

No vendor can offer every feature or function to satisfy all situations or scenarios. Cyber-recovery, in particular, is complex and involves solutions required from several sources. IT organizations should look for vendors with healthy, complementary ecosystems of products that can create a whole solution for their organization. Most organizations have hybrid cloud and multicloud applications, so selecting a vendor to address these environments is necessary.

CONCLUSION

Modern ITOps teams must be prepared to respond to a wide range of data threats and loss scenarios. While most data recoveries are routine and adequately addressed by backup/recovery software, B/R alone is not enough to address the unique requirements of disaster recoveries or cyber-recoveries. Nevertheless, B/R is foundational to DR, which in turn is foundational to CR. While the research in this survey showed that only 36% of organizations have coordinated DR and CR plans, those that do so will spend less on technology purchases and training while delivering faster recoveries.

The absolute certainty of data survival is table stakes for any data recovery, regardless of data loss event. Beyond that, this survey illustrated that IT organizations also highly value both speed of recovery and the granularity of data recovery. Faster recovery means less downtime, better worker productivity, and minimized organizational impact. Granular data recovery means minimal data loss, especially when using continuous data protection capabilities that deliver an RPO measured in seconds. With the combination of data integrity, speed of recovery, and minimal data loss, organizations should never be faced with the need to pay ransom to get their data back.

AI is in an obvious hype cycle. This survey found that many respondents believe that it has the potential to deliver significant benefits to data protection systems and processes, yet it is also clear that AI has not yet crossed the threshold of trust. AI is a complicated technology very much in the early stages of development and with limited deployment. While we believe AI will ultimately live up to the promise, we expect it to hew to the more common technology adoption cycle over a period of years as it proves itself on a use case by use case basis and satisfies IT buyer's requirement for trust.

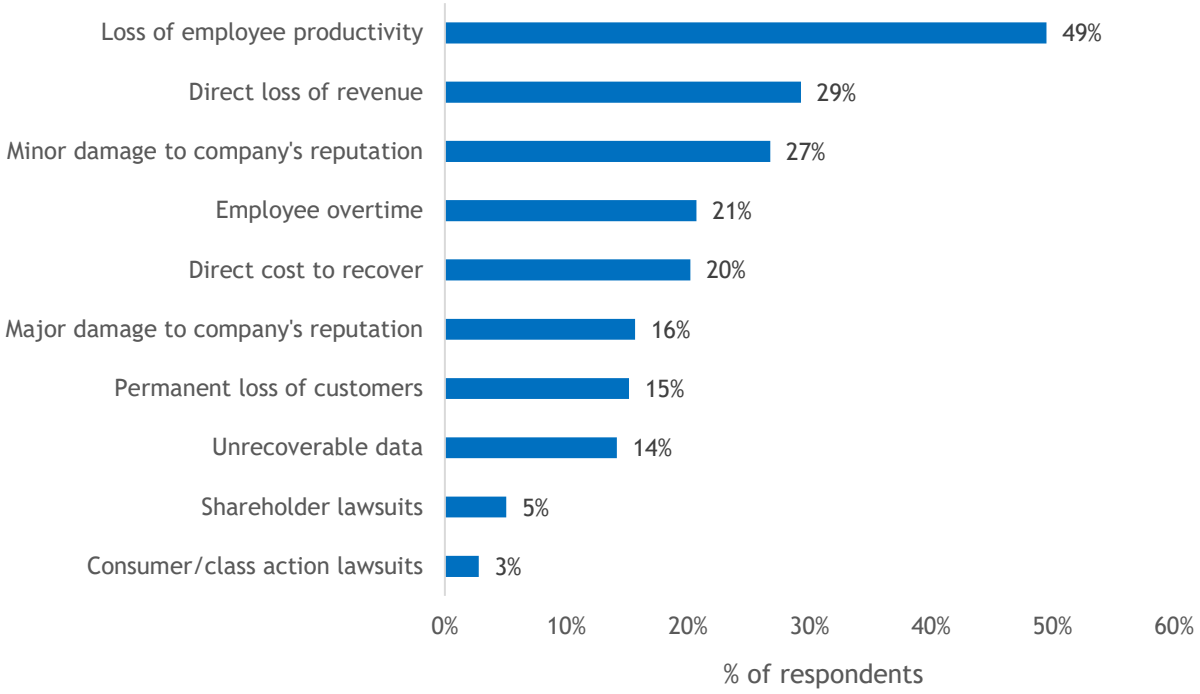
APPENDIX

Figures 7–16 represent additional results from this custom survey.

FIGURE 7

Data-Related Business Disruptions

Q. Within the past 12 months, when data-related business disruptions (including cyber-related) have occurred, what have been the consequences?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

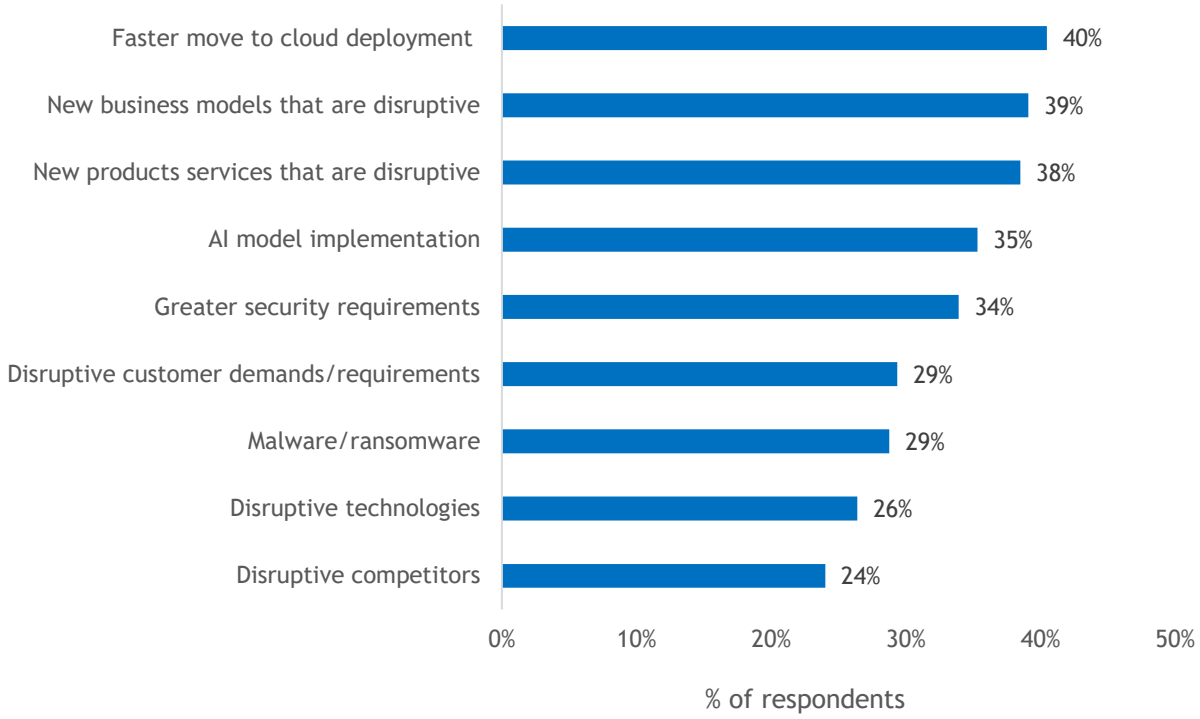
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 8

Drivers of Data Availability Approach

Q. During the past 12 months, which of the following circumstances, if any, has made your organization rethink its data availability (backup and disaster recovery) strategies, schemes, or systems?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

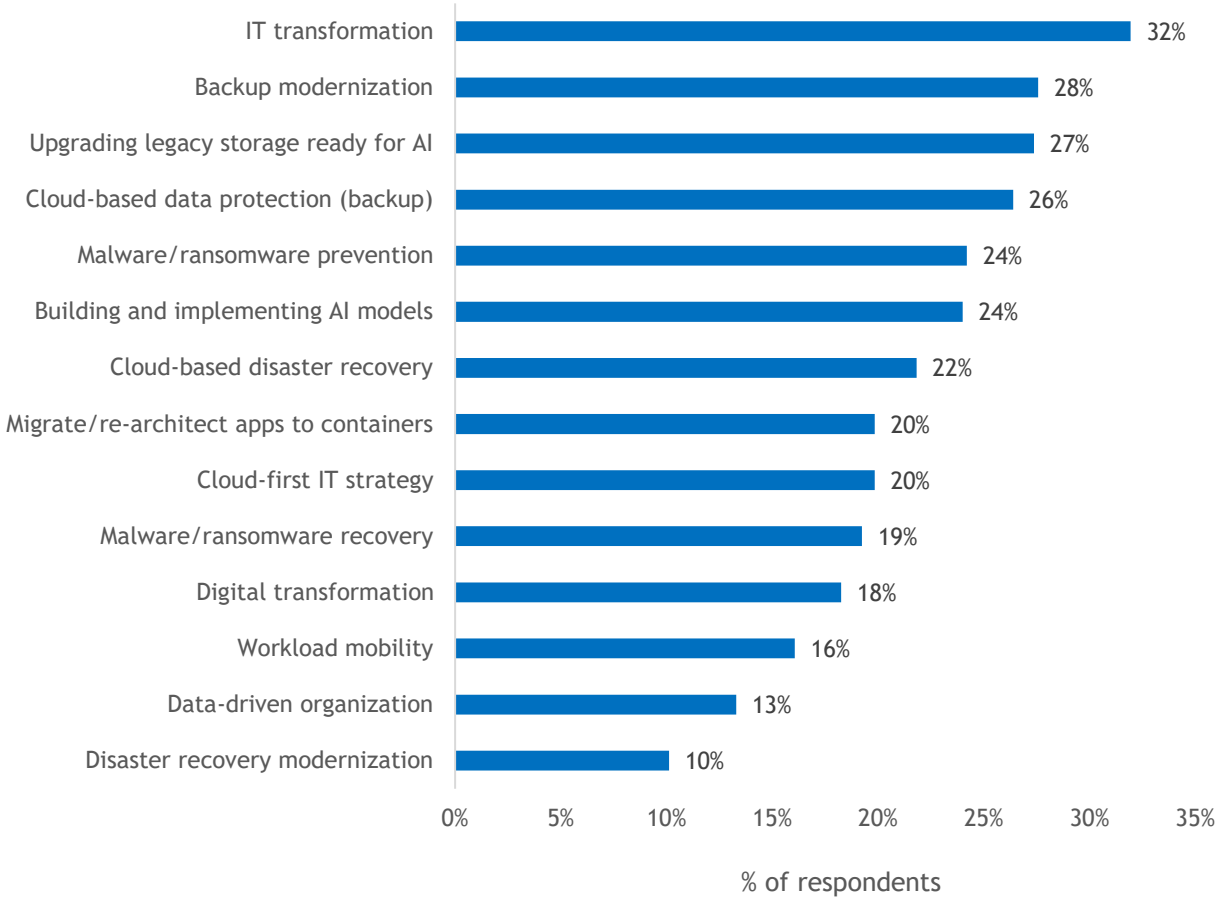
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 9

Leading IT Initiatives

Q. In the next 12 months, which of the following IT initiatives are the top 3 priorities for your organization?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

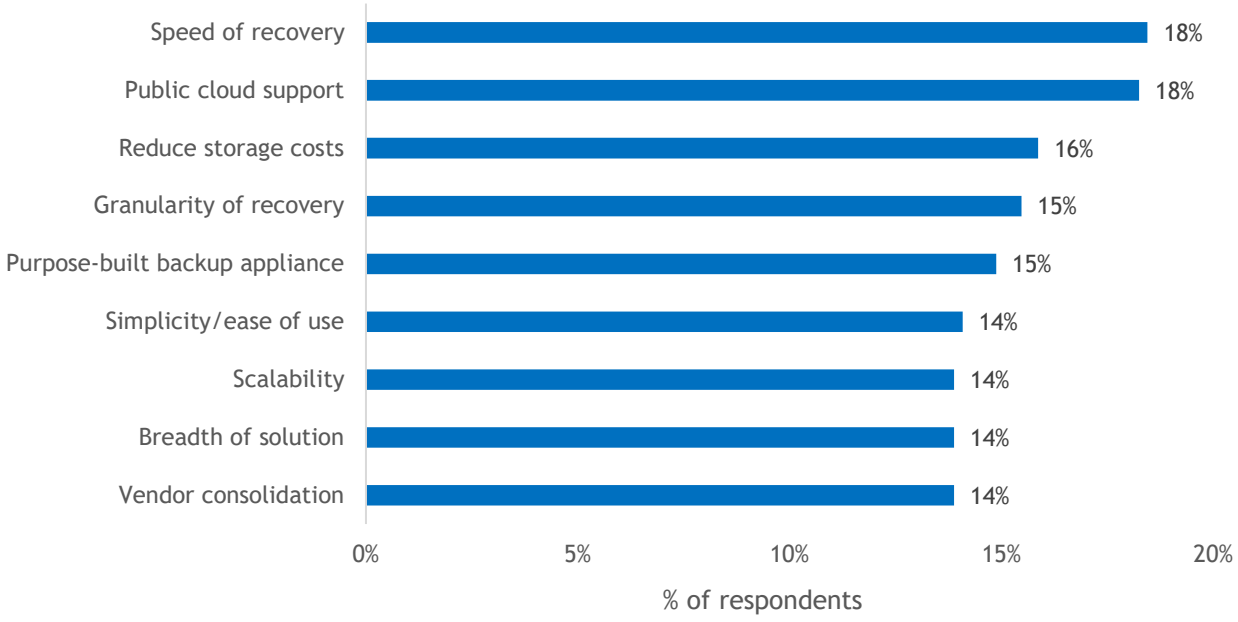
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 10

Disaster Recovery Decision Criteria

Q. *What are your organization's three most important decision criteria when choosing a disaster recovery solution?*



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

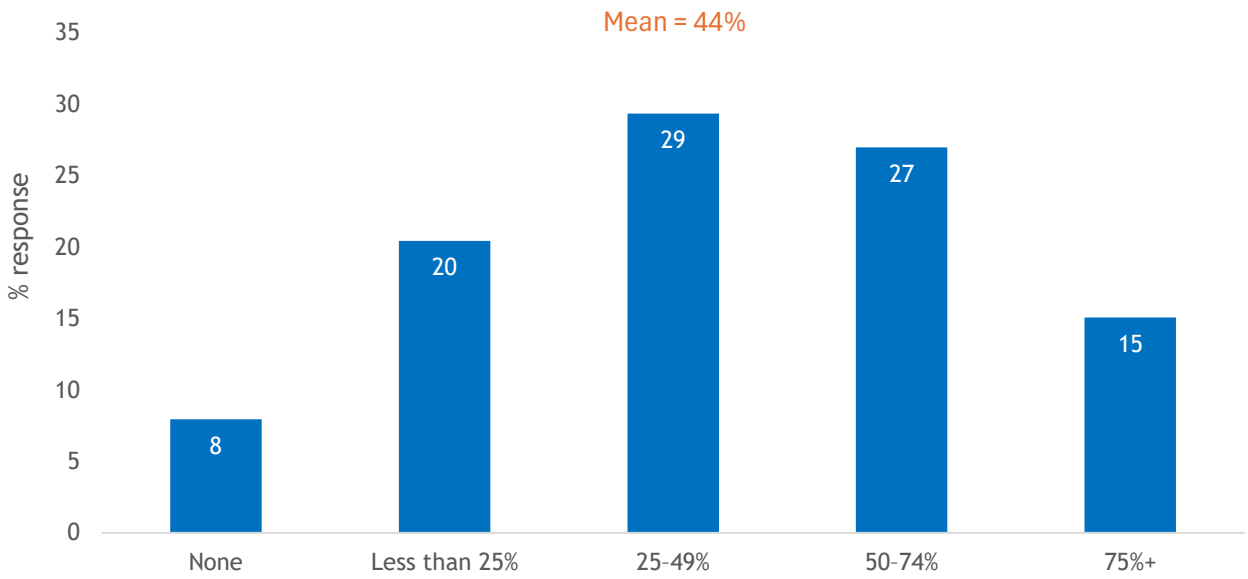
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 11

Cloud Utilization

Q. *What percentage of your organization's applications utilize the public cloud for backup or disaster recovery?*



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

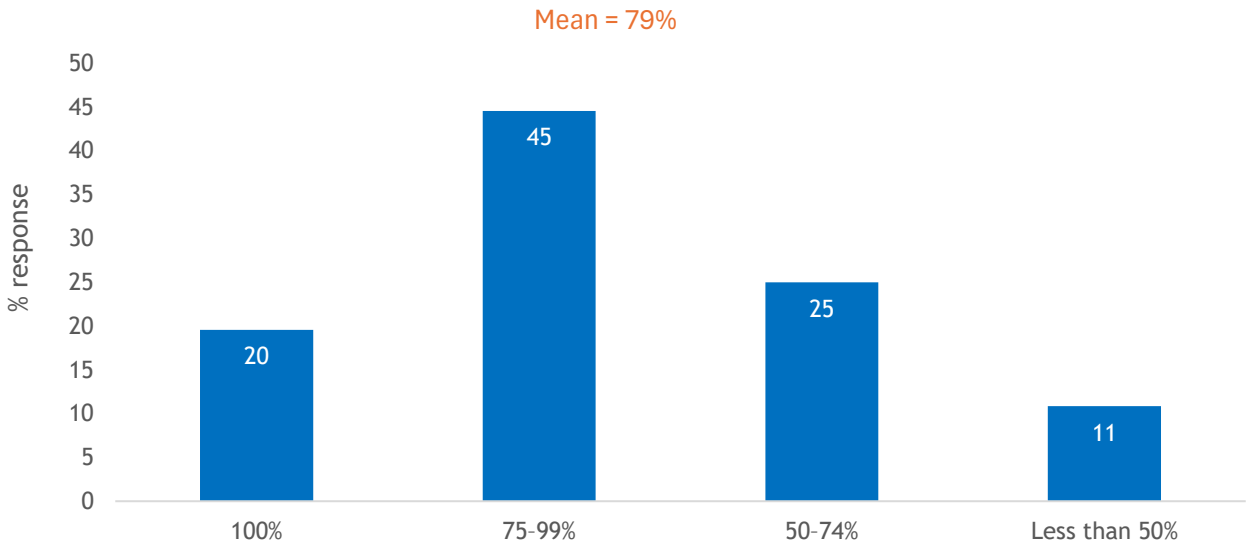
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 12

Post-Ransom Data Recovery

Q. After having paid the ransom, what percentage of your data was recovered?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

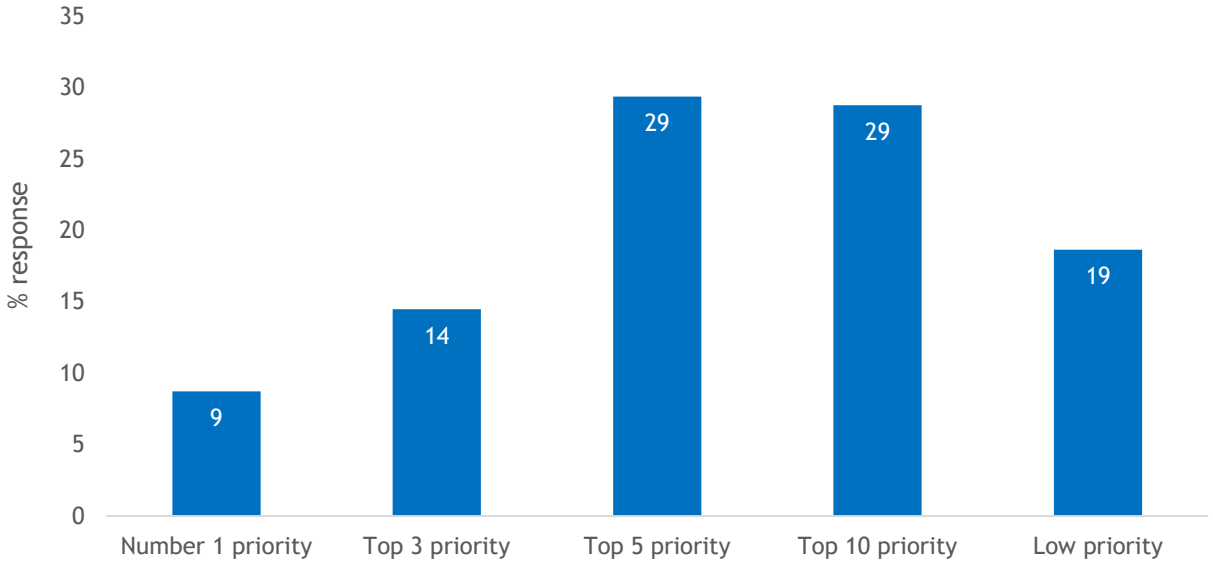
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 13

Ransomware Prioritization

Q. Where does ransomware/cyber-recovery planning fit into your organization's priorities?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

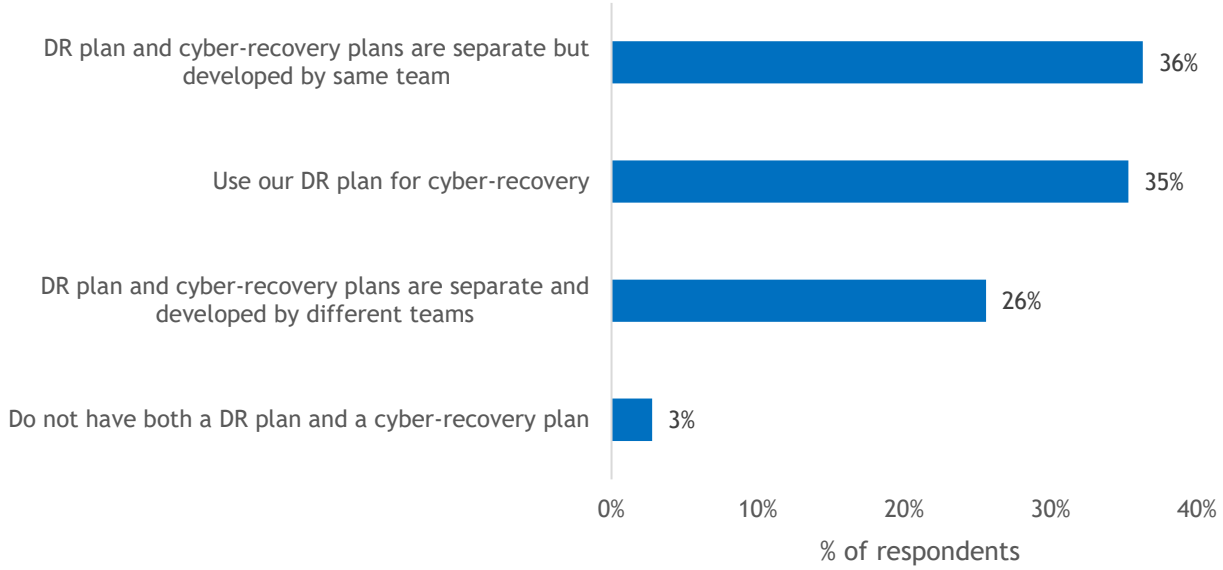
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 14

Disaster Recovery Approach

Q. How does your organization approach DR planning versus cyber-recovery planning?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

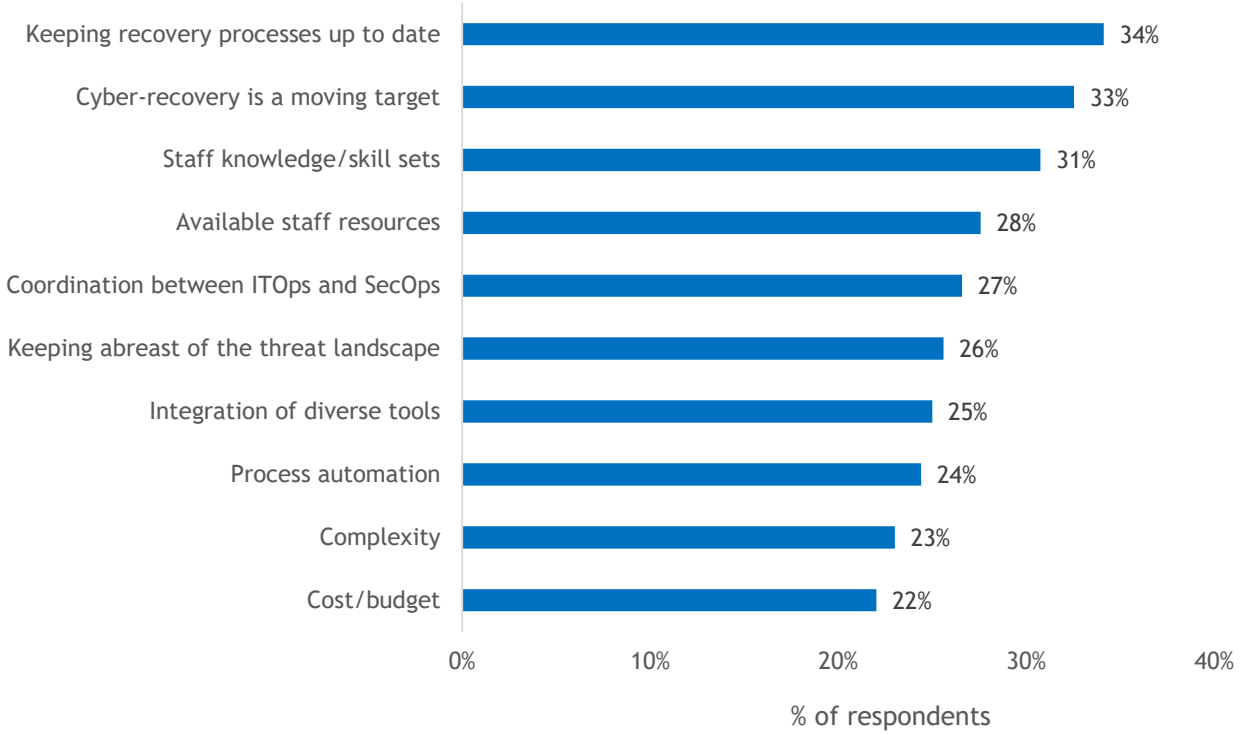
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 15

Cyber-Recovery Challenges

Q. What are your top 3 biggest challenges in developing and implementing cyber-recovery?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

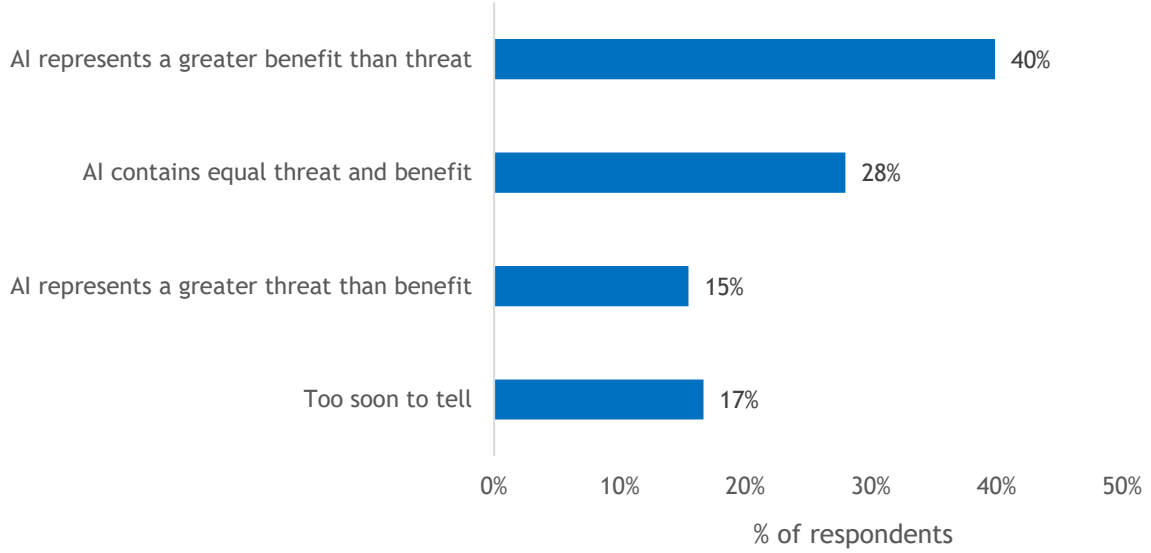
Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

FIGURE 16

AI — "Friend or Foe"

Q. Do you believe AI is a greater threat to the cyberlandscape or an opportunity to enhance the cyberlandscape?



n = 504

Base = all respondents

Notes:

Data is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Zerto AI CR Data Protection Disaster Recovery Survey,* February 2024

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com