White Paper

The State of Ransomware and Disaster Preparedness: 2022

Sponsored by: Zerto, a Hewlett Packard Enterprise company

Phil Goodwin
May 2022

IDC OPINION

The demand for data has never been greater, and yet the stress and risk to data integrity and availability have never been greater. Malware, data loss from exfiltration, and ransomware are pervasive. Simultaneously, evolving regulatory requirements demand higher standards of data governance and management. An IDC primary research survey across North America and Western Europe, conducted for this paper and sponsored by Zerto, a Hewlett Packard Enterprise company, highlights the need for effective disaster recovery responses. In this research, 79% of respondents indicated they had activated a disaster response within the past 12 months, with 61% of those responses triggered by ransomware or other malware. Indeed, 60% of respondents said they had experienced unrecoverable data during that same time, substantially more than the 43% response rate to the same question a year earlier.

IDC research has found that 60% of organizations have taken steps to be "data-driven" — that is, they have implemented tools and methods to utilize data more effectively to make decisions faster and with greater accuracy and certainty. For those organizations genuinely pushing to become data-driven, the key foundational element is, obviously, data availability. Without data availability, effective data use simply is not possible. Data availability has a number of aspects, starting with online access. Organizations that suffer disproportionately high downtime, whether planned or unplanned, will be at a competitive market disadvantage relative to those companies that have "always-on" systems. Data loss, often regarded as the cardinal sin of data protection, further erodes an organization's ability to harness the power of data. Data loss can lead to lost customers, lost revenue, lost opportunity, and staff overtime.

Previous generations of data protection software and storage systems simply did not have the capability to prevent data loss or downtime. Organizations had to accept data loss and downtime as unavoidable. Even in this most recent research, 94% of organizations reported unplanned downtime. With separate IDC research showing the cost of downtime averaging $250,000 per hour (across all industries and organizational sizes), this situation has become increasingly unacceptable as the consequences become more costly and severe. Thus, IT organizations are looking for solutions that can drive down service-level agreements (SLAs) (i.e., recovery time objective [RTO]) and data loss SLAs (i.e., recovery point objective [RPO]) to near zero, equating to no downtime and no data loss.

The proliferation of applications and the associated increase in data creation are complicating the effort to keep data always available. Organizations use a variety of interleaved data protection products (backup and recovery software, snapshots, mirrors, and replicas) along with disaster recovery (DR) strategies as a means to ensure data recovery in the event of any failure. However, new

applications at the core, in the cloud, and at the edge create data that is structured, unstructured, and containerized; this data resides in geographically dispersed object storage services such as AWS S3 and Azure Blob. As a result, IT organizations are facing ever-increasing complexity in providing data protection and disaster recovery.

Our research also indicates that more than 80% of new applications will be deployed in the cloud or at the edge. Most cloud applications will be either software as a service (SaaS) or cloud-native containerized applications. SaaS application data, in particular, can create a data management gap. Because of this move to cloud, IDC predicts that by 2025, 55% of organizations will have shifted to a cloud-centric data protection strategy. Although data will continue to be protected at the core, in the cloud, and at the edge, we believe that enterprise data protection and DR will be managed from the cloud.

IDC PREDICTION

By 2025, 55% of organizations will have migrated their data protection systems to a cloud-centric model to centrally manage core, edge, and cloud data protection from the cloud.

In early 2022, IDC conducted a research study sponsored by Zerto, a Hewlett Packard Enterprise company, to learn about the evolving requirements for ransomware recovery and disaster recovery and how organizations are dealing with emerging challenges. The top IT priorities include:

- IT transformation (ITX)
- Cloud-first IT strategy
- Cloud-based disaster recovery

Other key findings from the research:

- Cloud-native apps, hybrid cloud backup and hybrid cloud archive are the top 3 technology priorities.
- Ransomware is 2.5 times more likely to cause a disaster declaration than a natural disaster (though hardware and software failures are the leading causes of disaster declarations).
- Software failure (56%) and hardware failure (47%) were the top 2 reasons for causing a DR response.
- Backup reliability was the number 1 challenge cited for backup and recovery operations.

METHODOLOGY

IDC surveyed 509 respondents from medium- to large-scale organizations. The demographics of the survey included:

- 70% North America, 30% Western Europe
- Representative sample across all industries, with no industry represented by more than 15% of respondents
  - Manufacturing (14%), financial services (13%), retail (13%) and information technology (13%) as the top verticals in representation
- 70% IT leaders, 30% business leaders
- Results weighted by GDP

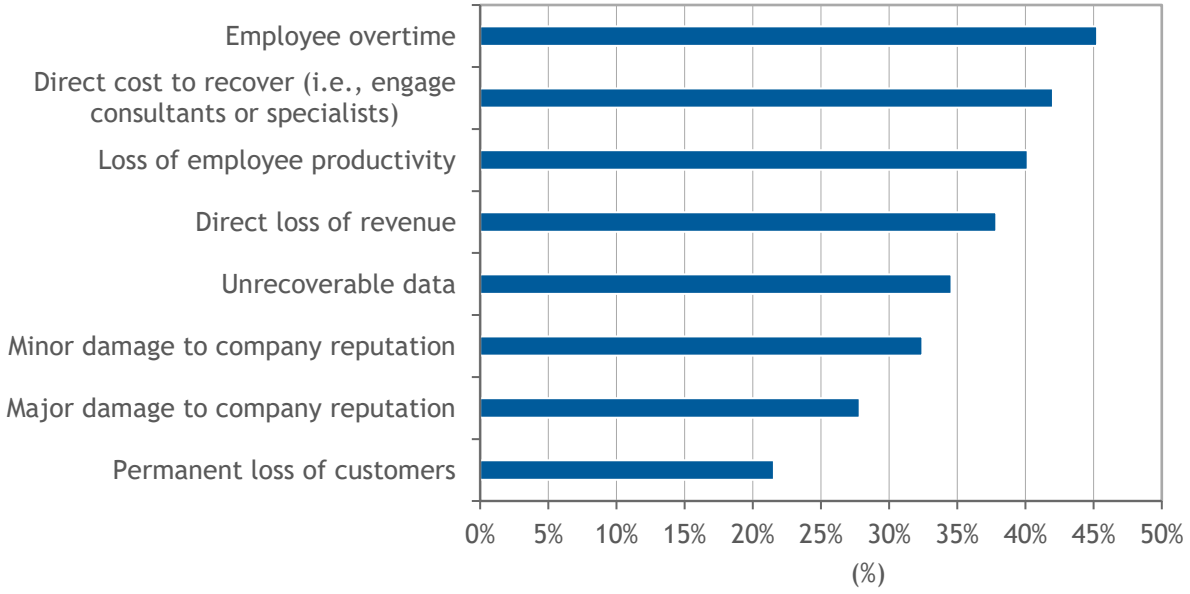
SITUATION OVERVIEW

The threats to data are increasing, and the consequences are becoming more serious. Attacks from bad actors have become nearly ubiquitous. Respondents reported an average of 19.3 attacks (all types) and 2.3 ransomware attacks in the past year. Furthermore, from this survey we learned that 93% of organizations have suffered a data-related business disruption during the past 12 months, and 68% of respondents have suffered four or more such disruptions. Unfortunately, with so many attacks, the chances of a successful attack become very high. Of the respondents that reported being attacked, 83% indicated that at least one attack had resulted in data corruption. Of even greater concern, 60% of respondents have experienced unrecoverable data within the past 12 months.

These statistics concerning ransomware/malware attacks are stunning. Attacks are common, and the odds of being a victim seem to be a matter of when, not if — and perhaps even how often. The impact on organizations of these attacks can be profound, as reported to us by those who had been victimized. The consequences of data corruption primarily affect people, as respondents told us that employee overtime, lost employee productivity, the direct cost of recovery (i.e., the engagement of consultants or specialists), and unrecoverable data were the most significant issues. However, other significant consequences do occur, as shown in **Figure 1**. From **Figure 1**, we can see that other consequences suffered include lost revenue, damaged company reputation, and permanent loss of customers. Put together, the consequences of disruption affect all aspects of the company, both internal and external.

FIGURE 1

Consequences of Data Disruptions



Source: IDC's *Worldwide State of Data Protection and Disaster Recovery Survey*, sponsored by Zerto, January 2022

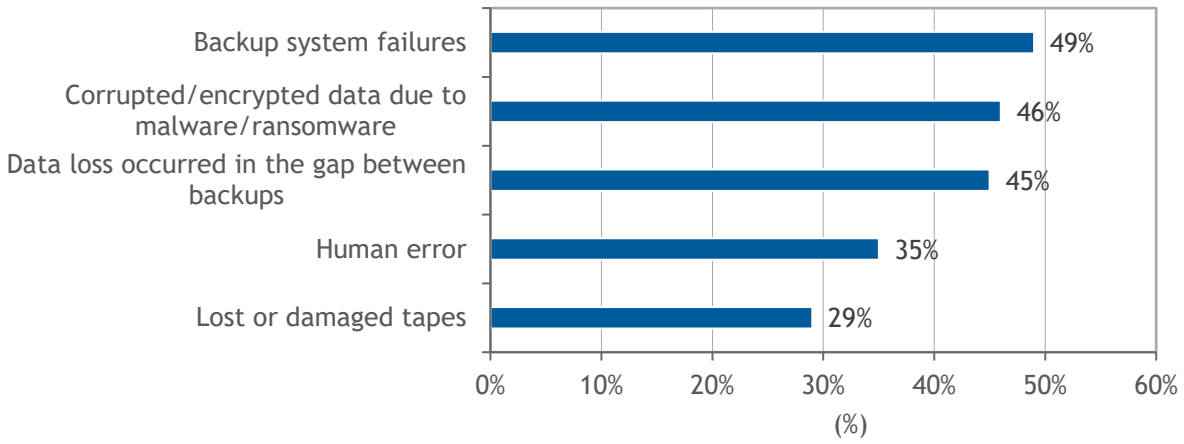
Notes: Managed by IDC's Quantitative Research Group. Data weighted by country GDP. Multiple dichotomous table – total will not sum to 100%. Use caution when interpreting small sample sizes.

As noted previously, data-driven companies simply cannot afford data loss, yet more than half (60%) of the respondents reported having experienced unrecoverable data in the previous 12 months. For those organizations that had experienced unrecoverable data, we asked them to tell us the reasons behind those losses. **Figure 2** shows the results.

It is noteworthy that two of the top 3 reasons in **Figure 2** relate directly to the backup system itself and were experienced by large percentages of respondents. The number 1 reason, backup system failures, is particularly concerning. Backups are generally considered to be the last backstop against data loss. Moreover, there is a general assumption that backup/recovery systems are reliable. The number 2 reason, corruption or encryption due to malware/ransomware, was cited by nearly half of the respondents (46%). Even this cause indirectly relates to the failure of backup systems: Clearly, the backup system for these respondents in these instances was not up to the challenge of recovering data from the ransomware attack. If organizations can deploy more reliable backup systems, with more frequent and more granular backups, then it is entirely possible that they can eliminate the top 3 reasons for unrecoverable data. In this regard, continuous data protection (CDP) may offer the most promise, as it nearly eliminates the gap between backups and does not rely on traditional backup windows for success.

FIGURE 2

Reasons for Unrecoverable Data



Source: IDC's *Worldwide State of Data Protection and Disaster Recovery Survey*, sponsored by Zerto, January 2022

Notes: Managed by IDC's Quantitative Research Group. Data weighted by country GDP. Multiple dichotomous table – total will not sum to 100%. Use caution when interpreting small sample sizes.

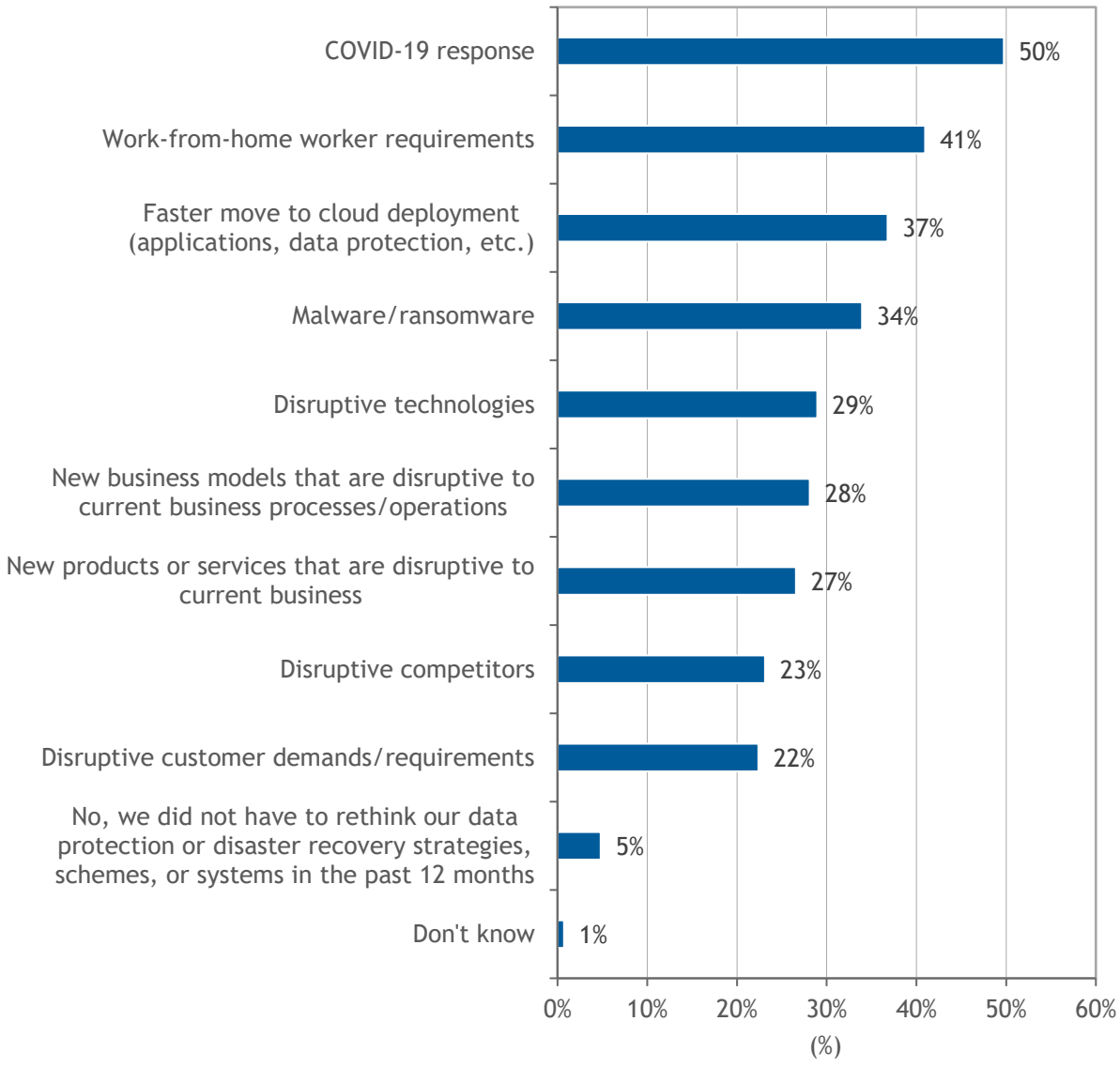
From this survey, we confirmed that the current most common RPO is 1–4 hours, as in past surveys. However, the most common RTO is now also 1-4 hours, much shorter than the 4–8 hours in prior surveys. Given the cost of downtime and the disruption that data unavailability causes, organizations are becoming less tolerant. While we cannot correlate specific SLAs to instances of data loss, we believe it is fair to conclude that the given SLA for respondents with data loss was not adequate to prevent the loss — nor, at the very least, to ensure the recovery. Organizations must rethink availability SLAs based on new digital business models and market expectations. Because 45% of respondents said that data loss occurred in the gap between backups, taking measures to reduce the

RPO in particular can reduce the gap between backups from hours to seconds, thereby reducing the chances for data to be lost.

As with our prior survey, the 2022 version took place during the COVID-19 pandemic. The pandemic has caused many organizations to rethink their data availability strategy, as seen in **Figure 3**.

FIGURE 3

Reasons for Rethinking Data Availability Strategies



Source: IDC's *Worldwide State of Data Protection and Disaster Recovery Survey*, sponsored by Zerto, January 2022

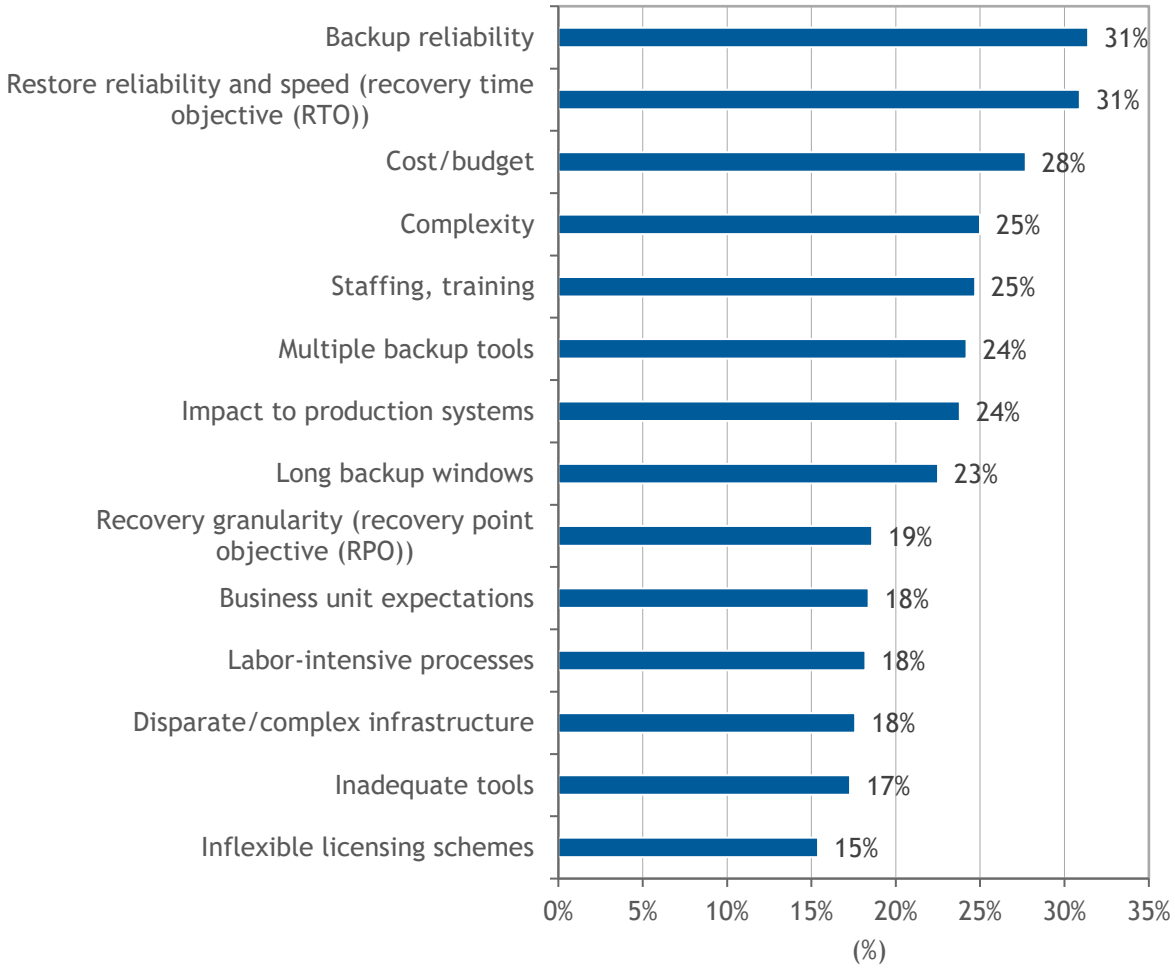
Notes: Managed by IDC's Quantitative Research Group. Data weighted by country GDP. Multiple dichotomous table – total will not sum to 100%. Use caution when interpreting small sample sizes.

The COVID-19 pandemic and work-from-home (WFH) responses are certainly related. Separate IDC spending data shows that organizations are spending more to move to the cloud faster as a result of the pandemic. The pandemic stimulated a great deal of urgency for adaptive projects, yet ransomware is often immediately behind those priorities.

With failed backups as the top reason for unrecoverable data, it is instructive to delve into the biggest challenges faced by IT organizations with respect to backup and recovery. This data is seen in **Figure 4**.

FIGURE 4

Biggest Challenges Regarding Backup and Recovery



Source: IDC's *Worldwide State of Data Protection and Disaster Recovery Survey*, sponsored by Zerto, January 2022

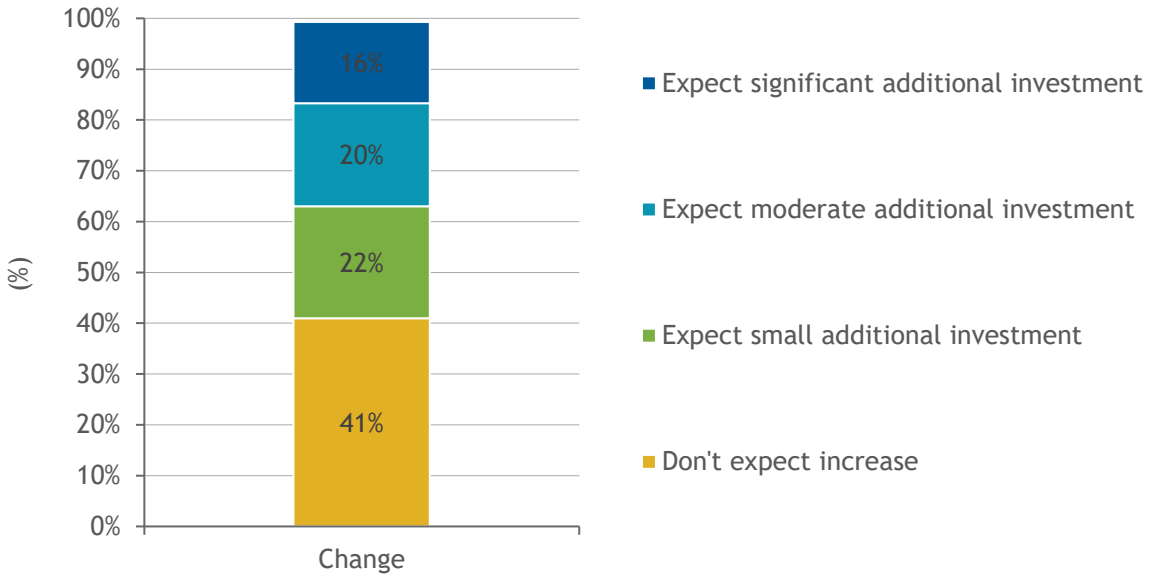
Notes: Managed by IDC's Quantitative Research Group. Data weighted by country GDP. Multiple dichotomous table – total will not sum to 100%. Use caution when interpreting small sample sizes.

The data indicating that backup reliability and restore reliability are the top challenges to backup/recovery is rather damning. One would presume that modernizing these systems would be a priority. Indeed, when we asked respondents about their top technology deployment priorities in the next 12 months, cloud-native apps was number 1 (29%), but it was followed by hybrid cloud backup (28%), hybrid cloud archive (27%), and cloud-based disaster recovery as a service (DRaaS) (27%).

However, with budget/cost next on the list of challenges, it would appear that spending the necessary money to modernize may be a problem. Based on the data seen in **Figure 5**, it appears that budget could be a challenge for a plurality of organizations, with 41% expecting no budgetary increase. On the other end of the group, more than a third (36%) expect to spend moderately to significantly more.

FIGURE 5

Backup and Disaster Recovery Expectations over the Next 24 Months



Source: IDC's *Worldwide State of Data Protection and Disaster Recovery Survey*, sponsored by Zerto, January 2022

Notes: Managed by IDC's Quantitative Research Group. Data weighted by country GDP. Numbers may not sum to 100% due to rounding. Use caution when interpreting small sample sizes.

Often, the problems that are priorities for DR track along with backup and recovery. However, that was not the case in this year's survey when we asked respondents for their top DR challenges overall. For these issues, IT personnel skills/knowledge was the number 1 issue (34%), along with IT personnel time/resources (34%). Cost/budget was fifth on the list. Regarding cloud-specific DR issues, the responses were recovery time (39%), data transfer/migration (36%), and cost/budget (34%).

As with backup investment priorities, we asked respondents about their expectations for investments in staffing and training. Nearly one fourth (24%) of respondents expected to invest in training only, 19% expected to add staff, and a significant 41% expected to do both.

FUTURE OUTLOOK

The research detailed in this study can be summarized by four key imperatives: a need for reliable backup; fast data recovery, regardless of whether it is a normal recovery or a DR scenario; assured recovery from ransomware/malware; and simplified backup and DR operations, to reduce staff time and effort. Organizations are clearly both willing and planning to make investments in these areas.

The fact is that common data protection technologies in use today are not able to reduce RPO and RTO to the levels needed by data-driven organizations. Snapshots, the most granular recovery technology deployed by most organizations, may be executed no more often than hourly, even for mission-critical applications, and may be executed as infrequently as every 4 or 8 hours. To be sure, some organizations will deploy snapshots every 15 minutes for their most sensitive applications. However, few will use snapshots at their highest frequency of every five minutes because of the required storage overhead and impact to applications that such a schedule would entail. Moreover, snapshots rarely factor into DR execution: Standard DR practice relies on backup copies or replication to move data. Because of the cost of synchronous replication in both bandwidth and infrastructure, this practice is reserved for only the most sensitive applications. Consequently, most applications recovered through DR processes have a 24-hour RPO.

IDC has identified an emerging trend toward the convergence of backup and DR, enabled by automated recovery workflows. As organizations leverage the cloud for data protection, adding workload migration and recovery orchestration can yield very low RTO and RPO. Using the cloud for these recoveries makes DR economical and rapid recovery of applications practical. We believe that as CDP, workload migration, and recovery orchestration merge in a hybrid cloud environment, organizations will no longer need to treat backup and DR as separate efforts. Container backup is another important requirement emerging for data protection. According to this survey, 56% of organizations have already deployed container-based workloads in production. We expect the majority of new applications to be cloud-native applications utilizing containers.

Container backup differs in important ways from traditional backup. Traditional backup captures the data and the virtual machine image (if applicable) only. With containers, where Kubernetes is the dominant orchestrator, backup capabilities must include the data, the system image, and the Kubernetes state to perform a restore. Moreover, the backup application must be able to capture persistent data and images and ignore transient data and images.

This survey also found that most organizations lack confidence in their current backup and DR solutions. Only 28% of respondents expressed 100% confidence in their backup system's ability to recover data, and 29% have 100% confidence in their DR solution to recover data, though both numbers are higher than in the previous survey.

Continuous data protection is a technology that is gaining traction in the industry. This technology, which is a part of backup solutions and not a standalone product, can significantly reduce the potential for data loss, regardless of cause, while reducing the time to recovery and simplifying recovery. CDP captures data changes as they are written so that the effective RPO is reduced to seconds, virtually eliminating the "backup gap" that was identified as a cause for data loss. Because of its granularity, CDP also helps organizations recover from ransomware attacks with minimal data loss and rapid recovery. Administrators can select a restore point just prior to the attack, thereby eliminating the trial and error of picking backup sets or snapshot versions to restore. In addition, CDP solutions enable

backup and DR with minimal data loss, especially when combined with recovery orchestration and workload migration.

CONSIDERING ZERTO, A HEWLETT PACKARD ENTERPRISE COMPANY

Zerto is designed to provide continuous backup, disaster recovery, data mobility, long-term retention, security, and compliance in a single integrated software-only scale-out solution. The solution is designed to protect virtual and container workloads, whether on-premises, cloud, hybrid, native, or multicloud. At the core of the Zerto solution is a continuous data protection engine that can reduce RPO to seconds with:

- Thousands of restore and recovery points, seconds apart, to recover enterprise applications without using snapshot copies or relying on backup copies that may be up to 24 hours out of date
- Application-consistent recovery for accelerated RTOs with quick and consistent recovery, even with complex multi-VM applications
- Instant journal-based recovery for a simple, granular recovery experience that doesn't impact production systems. This journaling technology can be used locally and remotely on premises across other sites and the cloud, thus enabling the fulfillment of the data protection 3-2-1 rule.
- Long-term retention for cost-effective and immutable storage on premises and in the public cloud. Data may be retained from months to years to assist with meeting compliance and data retention regulations.

Combining continuous backup, disaster recovery, and data mobility based on a foundation of CDP with near-synchronous replication, the Zerto solution is designed to provide a single software-only experience across all data recovery scenarios with the same mission-critical RPOs and RTOs for any workload. IT teams do not need to classify different workloads and treat them with different SLAs.

The Zerto solution does not rely on snapshot technology, either array-based or its own, so RPO is not limited by snapshot intervals, thus minimizing the risk of data loss and performance impact. The solution also includes backup and disaster recovery orchestration to automate and simplify operations and reduce human error, with a single, simple recovery experience. Users can leverage the same Zerto implementation for backup and then extend it to disaster recovery, migrations, and other use cases. Full recovery with built-in orchestration and automation removes many manual processes to simplify complex disaster recovery, backup, cloud migration, and data protection modernization projects. With a single user interface, administrators have centralized management and a common experience, whether on premises or in the cloud. The solution has flexible REST APIs to fully automate deployment and VM protection using ready-made examples. Nondisruptive DR and backup testing can validate recoverability, perform a migration dry run, or test against production replicas, with no production impact or disruption in protection.

Also included in the solution is an analytics engine with:

- Built-in dashboards and reporting, and access from desktop, tablet, or mobile devices for monitoring SLAs from any device
- Capabilities for forecasting future infrastructure needs with Zerto Resource Planner, for accurate infrastructure planning using the organization's own actual application data, and the ability to forecast required capacity and size protection needs for both protected and unprotected VMs

- Backup and DR reporting across all resources to ensure having timely, accurate data, whether for compliance and auditing or performance analysis

CHALLENGES/OPPORTUNITIES

The data protection market is highly dynamic and becoming more challenging due to the increasing application deployment schemes for core, cloud, and edge. Data is becoming more siloed and more disparate and is in the hands of more users than ever, making the protection and recovery of it more challenging. Because of the number of types of applications, deployment platforms, data, geographies, and more, it simply is not possible for any single product or platform to address all possible scenarios. Most IT organizations will be faced with the need to adopt multiple products, even when consolidation is desirable.

As a solution developer, Zerto is also faced with the task of choosing which scenarios it will address in its products. The company must focus on its core value proposition to stay ahead of its competition in these core areas. Zerto competes in a marketplace where IDC recognizes more than 44 vendor participants, many of which are multibillion-dollar firms with much larger R&D budgets. Zerto must ensure that it gets maximum "bang for the buck" when it invests in product development. However, having been acquired by HPE within the past 12 months, Zerto now has the backing of one of the industry's largest companies.

Containers will also emerge as a key growth market for data protection and DR products. Zerto, which recently introduced support for containers with Zerto for Kubernetes, must move quickly and aggressively to meet the emerging needs, as many competitors are now scrambling to address containers in what will become a highly competitive segment. Growth and market share gains for data protection software vendors are heavily dependent upon those vendors that are both participating in cloud ecosystems (e.g., AWS, Azure, GCP, IBM) and developing their own ecosystem of cloud service providers and managed service providers. Zerto has been one of the more successful companies in this regard, adapting to the changing landscape, which requires constant attention and product development.

CONCLUSION

Modernizing data protection, including backup and DR, is a high priority for many IT organizations. Cloud (i.e., hybrid cloud backup and archiving) and investment in cloud-based DR (DRaaS) are key ways in which organizations intend to modernize their data protection. Nearly every organization faces increased competition and challenges and must respond with data-driven decisions, digital business models, and operational efficiency. This means not only driving new business but also ensuring a better experience, without downtime and data loss for customers, partners, and employees. To that extent, it is an arms race among organizations constantly seeking an edge through greater data availability, usability, and reliability.

The complexity of application deployments, data types, governance requirements, and data dispersed across the core, cloud, and edge makes data management and availability a serious challenge for IT organizations to provide. The industry is responding to these needs with multicloud data management solutions that provide integrated backup, DR, recovery orchestration, policy management, and SLA tracking. CDP is among the latest introductions in delivering the capabilities needed to drive shorter recoveries with much less data loss. While CDP can help in common types of data recoveries across

backup and disaster recovery, it can also play an instrumental role in combating cyberattacks such as ransomware. By using CDP to return to a point just seconds or minutes prior to an attack, recoveries can be made quickly and with minimal data loss. We expect CDP to play a key role as organizations drive closer and closer to SLAs requiring zero downtime with zero data loss.

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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