White Paper

You Think Ransomware Is Your Only Problem? Think Again

Sponsored by: Druva

Phil Goodwin
September 2022

IDC OPINION

Data resilience is an imperative for every organization where information access is a competitive differentiator. Cybercrime — and especially ransomware — has become the most feared IT-related event — and is the greatest threat to data resilience. Organizational leaders of all types understand that ransomware can cause extreme damage to the organization's ability function and, in some cases, even survive. Ransomware is not just an IT issue but a situation involving the highest levels of management, including the CEO. Ransomware attacks can be so significant that they trigger a disaster response using traditional disaster recovery (DR) tools and methods. Because traditional DR is not designed for a cyberattack response, recovery from ransomware can last days, weeks, or even months before a fully operational state is resumed.

Many factors complicate data resilience. First, data is spread across the core, cloud, and edge, with the potential for mission-critical data in each repository requiring organizations to address each repository fully. Second, with data spread across the organization, data may be in silos with multiple data protection tools, processes, and policies opening risks and attack vulnerabilities. These same factors make ransomware recoveries especially challenging.

IDC research shows that more than 95% of organizations use the cloud for some part of their data protection. However, these implementations are often partial or limited in scope. Nevertheless, the direction is clear: IDC predicts that by 2025, 55% of organizations will have adopted a cloud-centric strategy toward their data protection.

To address these evolving threats and to consolidate and simplify data protection operations, organizations are rapidly adopting data protection solutions delivered as SaaS applications. IDC forecasts predict the data protection-as-a-service (DPaaS) market to reach $10.7 billion in 2022. Included in the DPaaS market is backup as a service (BaaS) and disaster recovery as a service (DRaaS), which are growing at a CAGR exceeding 19%.

Because cybercrime and data loss are such important topics, Druva engaged IDC to conduct independent research into ransomware preparedness, challenges, and threats. Druva wanted to learn how the approaches to ransomware are changing and whether common recovery efforts are effective. This research had a very interesting conclusion: *While organizational leaders believe they are fully prepared and have a high regard for their data protection tools and processes, the actual outcomes paint a very different picture.* A majority of organizations suffered significant consequences from ransomware attacks including long recoveries and unrecoverable data despite paying a ransom.

Are You Prepared?

Organizational leaders believe they are fully prepared and have a high regard for their data protection tools and processes, yet the actual outcomes paint a very different picture.

Findings supporting our conclusion include:

- 85% of organizations claim to have a cyber-recovery playbook for intrusion detection, prevention, and response, yet 46% of organizations have been successfully attacked by ransomware in the past three years.
- 92% said their data resiliency tools were "efficient" or "highly efficient," yet 67% of those hit by ransomware were forced to pay the ransom, and nearly 50% experienced data loss.
- 93% claim to have either fully automated or partially automated recovery tools to find the correct recovery point, yet the inability to determine the correct recovery point was cited as the number 1 reason for data loss. Moreover, corrupted backups were the number 2 reason for data loss. Clearly, there is a gap between what people believe their recovery tools can do and what they actually deliver.

The problems aren't that organizations don't take cyberattacks seriously or that they don't try to prepare; they most certainly do both in earnest. The root issues are that no one knows what they don't know: the commonly used do-it-yourself (DIY) approaches to cyberpreparedness are insufficient – recovery is limited to the experience of those implementing it – many of whom may have no experience with an actual attack response. Instead, a DPaaS-based approach to data protection and cyber-recovery leverages the expertise of the provider and the knowledge it has gained from hundreds or thousands of customer implementations and responses when those customers are attacked. Moreover, cloud-based DPaaS also provides the economic leverage of public cloud, and many tools not available with on-premises solutions alone.

METHODOLOGY

This study included a primary research survey based on the following demographics:

- Worldwide scope with a total of 505 respondents, evenly divided between regions:
  - **North America:** United States and Canada
  - **Europe:** United Kingdom and Sweden
  - **Asia/Pacific:** Australia, Singapore, India, and New Zealand
- Representative samples from 20 different industries (The three largest representations were manufacturing, banking, and information technology, with none making up more than 15% of total responses.)
- Small and medium-sized enterprises up through large-scale enterprises:
  - 35% having 250–1,500 employees

    - 32% having 1,501–5,000 employees
    - 33% having 5,000+ employees
- Respondents representing IT practitioners up through C-suite respondents including CIO, CTO, and COO

SITUATION OVERVIEW

Data resilience, for the purposes of our survey, was defined as the practice of making data available within the organization. As such, it is central to any sort of disaster or cyber-recovery and requires a coordinated effort of people, process, and technology. Data resilience is about ensuring data survival in the face of any threat because, without data resilience, application recovery and normal business operations simply are not possible.

It is said that hindsight has perfect vision, so our survey was designed to learn about common organizational preparation, the perspective of IT leaders regarding their data resilience capabilities, and the practical outcomes of their efforts.

Cyberattack recovery success can be measured by three KPIs:

- The ability to fully recover encrypted or deleted data without paying a ransom
- Zero data loss in the process of recovering the data
- Rapid recovery as defined by applicable service-level requirements

When a recovery fails to meet these criteria, then the organization may suffer financial loss, loss of reputation, permanently lost customers, and reduced employee productivity.

Although this survey generated more than 90 different data points, this white paper focuses on the key findings of the survey. These results should help organizational leaders better assess their own preparations and benefit from the hindsight experience of others.

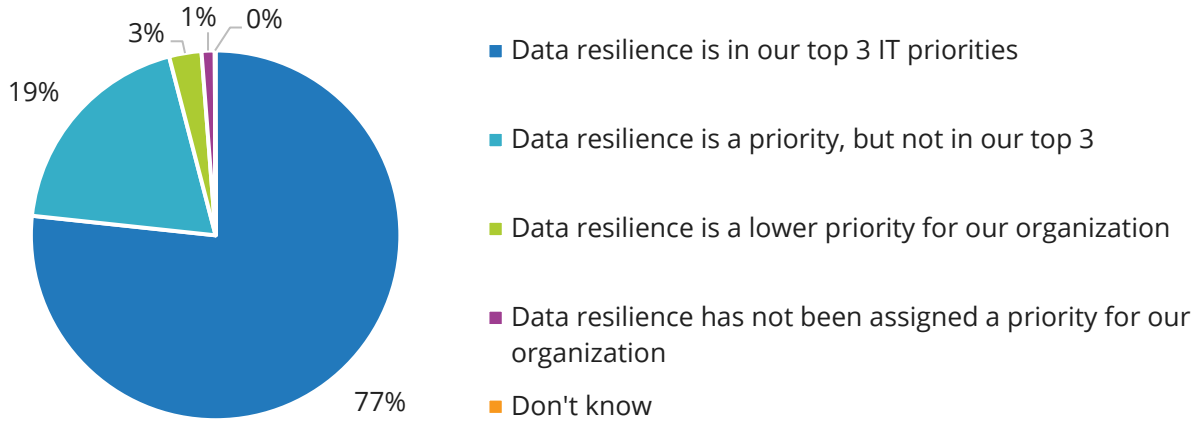
Survey Findings

Key Finding Number 1 — Organizations Take Data Resilience Seriously

To begin our research, we wanted to establish the current environment and respondent perspective. Thus we asked respondents a series of questions about their perspective on data resilience. We established the definition of data resilience as described previously and asked respondents to tell us where data resilience fits as an organizational priority. As shown in Figure 1, 77% indicated that data resilience is a "top 3" priority, while 19% said it was a priority but not in their top 3. Only 3% said it was not a priority, while 1% didn't know.

FIGURE 1

Data Resilience as a Priority



n = 505

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

Separate IDC research finds that more than 90% of organizations operate in a hybrid cloud environment and more than half in a multicloud environment. Therefore, we wanted to know what role the cloud plays in data resilience efforts. In this case, 55% of respondents indicated plans to use third-party BaaS or DRaaS solutions. Of the remaining 45%, 8% will use hybrid solutions and the remainder will continue to primarily use on-premises backup.

Key Finding Number 2 — Organizations Think They Are Prepared

Perhaps it's human nature to believe that, as an organization, one is prepared. After all, competent, qualified staff are putting in their best efforts, and if anyone believed they were deficient, they would be taking corrective action. We asked a series of questions regarding the respondents' perspective on their preparedness. We previously noted that 93% of organizations believe they have partially or fully automated means of recovering the right data. Other results to related questions were almost equally positive:

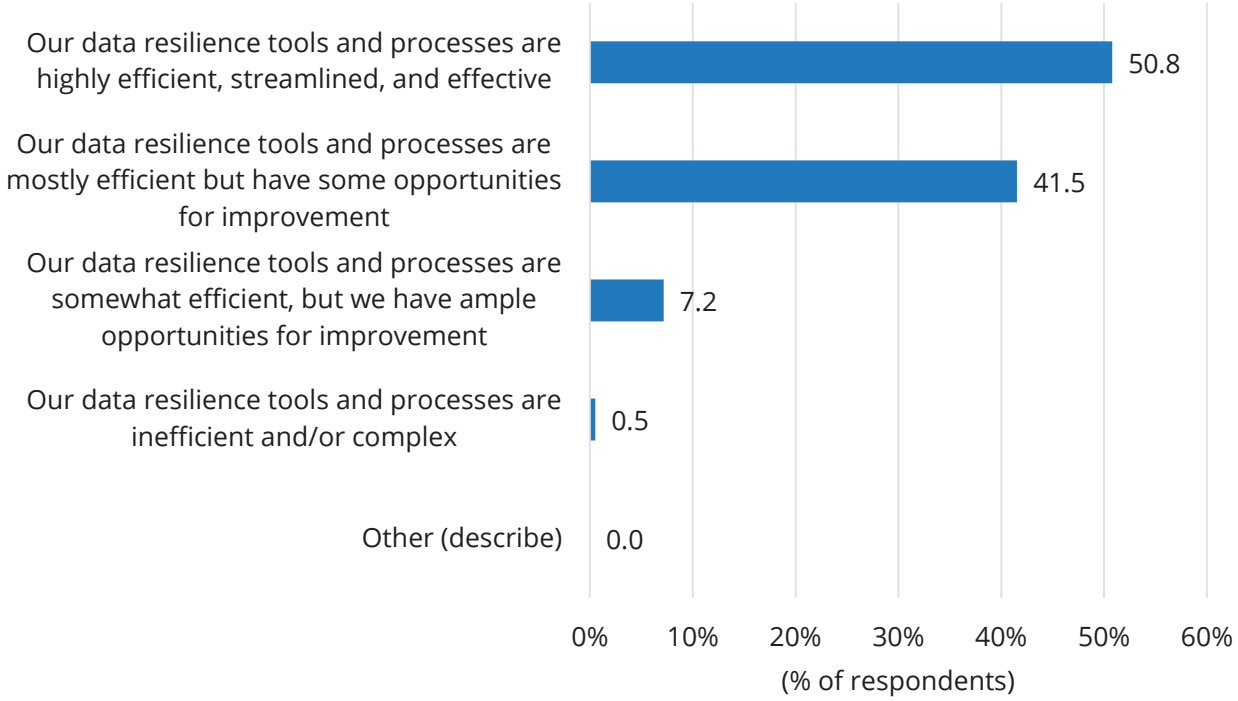
- 85% of respondents indicate they have a formal cyber-recovery playbook. Obviously, the quality of playbooks may vary significantly between respondents, and this question cannot assess that quality spectrum. However, the high response rate makes clear that some level of effort to create a playbook has been undertaken by the vast majority of organizations.
- 92% of respondents say their data resiliency tools are "efficient" or "highly efficient" (see Figure 2). Errors, accidents, system malfunctions, and internal or external attacks are always a

threat to data availability. Complete, rapid recovery of data is key to data resilience. Based on this response, nearly all organizations believe they have such capabilities in place.

As shown in Figure 2, only 7.7% of respondents believe their current data resilience efforts are only partially efficient or inefficient. In the main, this would indicate that most organizational leaders believe they have the necessary tools in place to meet their data resiliency needs.

FIGURE 2

Opinion on Data Resiliency Tools



n = 505

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

Key Finding Number 3 — Despite Confidence, Gaps Exist in Data Resilience

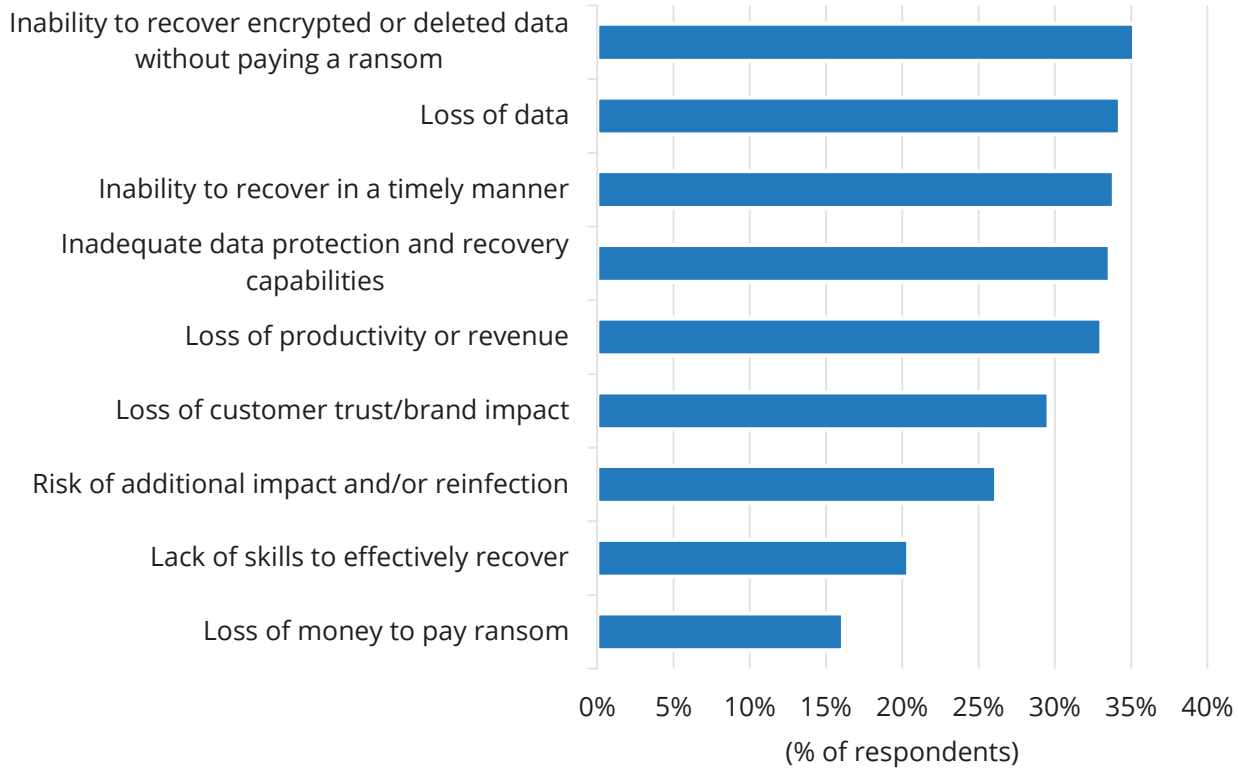
Despite this high confidence in their resiliency toolsets, respondents to our survey expressed concerns about actually recovering data after ransomware attacks (see Figure 3).

It should be noted that the percentages of the first five concerns are so close they are within the margin of error for the survey and therefore can be considered of equal concern. This means, as a

practical matter, all five are equally concerning to the respondents. Of these, four – inability to recover data without paying a ransom, loss of data, inability to recover in a timely manner, and inadequate data protection and recovery capabilities – speak directly to data resilience and recovery solutions. Monetary concerns all fall below these factors.

FIGURE 3

Concerns About Data Recovery After Ransomware Attack



n = 505

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

Interestingly, when we asked respondents about their confidence in their data resilience, only 14% were extremely confident. Of the rest, 36% had high confidence, 38% had good confidence, 9% had low confidence, and 3% rate themselves as poor. Thus, despite confidence in their tools, these IT leaders recognized potential gaps in their data resilience capabilities.

Key Finding Number 4 — Attacks Are Common

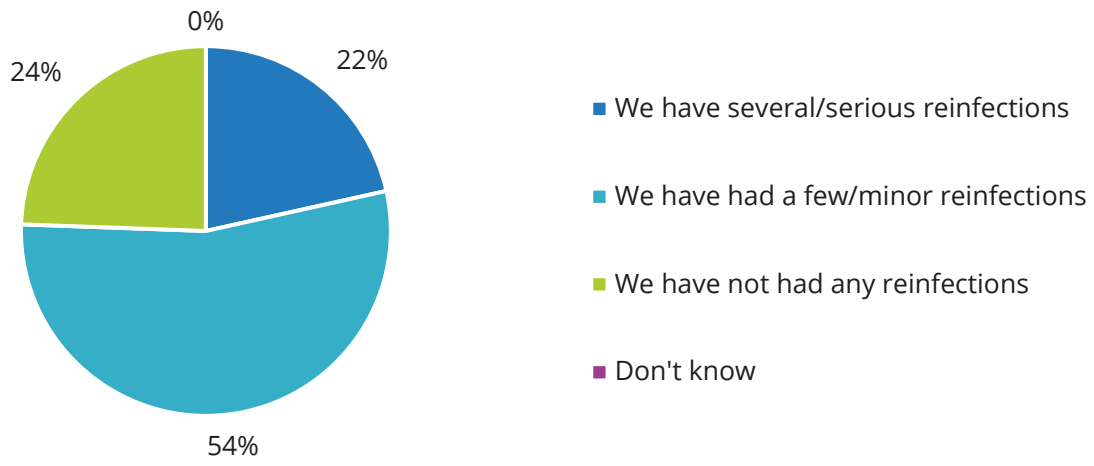
It's easy to believe one organization is among the millions of potential targets of cybercriminals and therefore safe through the anonymity of numbers. Unfortunately, that is not true — it's not always "the other guy." In our survey, nearly half (46%) of the respondents have been *successfully* attacked by ransomware in the past three years. Unfortunately, it is not a question of "if" or even "when" but rather "how often" and "how seriously." To wit, during the early days of ransom attacks, victims could be stigmatized in the marketplace. Today, attacks are so commonplace that, while hardly a badge of honor, attacks do not result in the previous stigma.

When we delved into the consequences of attacks in our survey, we learned that 33% of respondents had both primary and secondary data impacted (secondary data being data copies and backup sets). Unfortunately, attackers have learned that compromising the backup raises the odds that companies will be forced to pay the ransom to recover the data. We also learned that the scale of attacks is significant. In our survey, 55% of respondents had 25–50% of their data impacted by the breach.

To add insult to injury, 76% of respondents experienced reinfection (22% serious plus 54% minor) following the initial attack and recovery. This is most likely caused by the malware being backed up and restored with the data and highlights the need for detection tools that can find malware in backup data and prevent its reintroduction. Figure 4 highlights the research findings.

FIGURE 4

Incidence of Reinfection



n = 250

Base = respondents who indicated data was unrecoverable as a result of ransomware attack

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

Key Finding Number 5 — Many Plans Apparently Failed

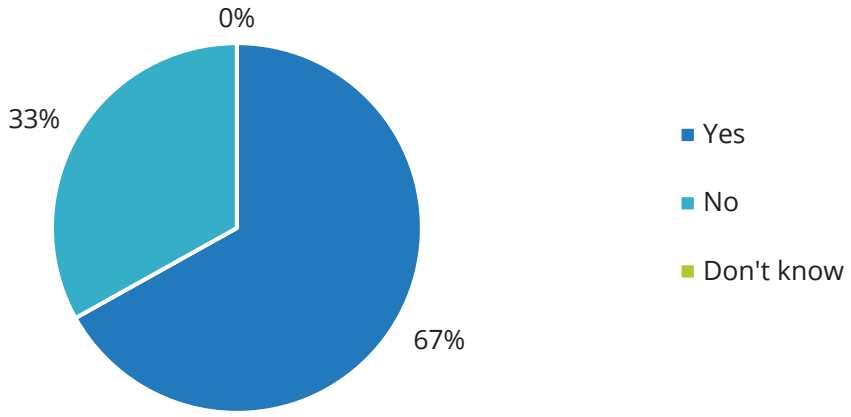
As noted previously, there are three KPIs for evaluating success against ransomware attacks. In this regard, here is the scorecard from this survey:

1. **Necessity of paying a ransom:** Ideal KPI is 0%; actual results = 67%.
2. **Data loss:** Ideal KPI is zero loss; actual results = 50% of organizations had unrecoverable data.
3. **Rapid recovery:** Ideal KPI is within 48 hours; actual results were 69% within three days and 36% within a week, less than 3% recovered within a day.

These findings indicate that many plans failed, at least to the extent of achieving the ideal. It is interesting to note that these results were consistent across regions in the world and across company sizes. One might think that large-scale organizations would be better prepared to deal with attacks because they have greater resources and larger staff. However, this survey did not show a significant advantage for larger companies versus smaller companies. When it came to paying a ransom, 62% of large organizations paid compared with 72% for midsize organizations and 65% of small organizations (see Figures 5 and 6).

FIGURE 5

Organizations Compelled to Pay a Ransom (Total)



n = 250

Base = respondents who indicated organization was successfully attacked by ransomware within the past three years

Notes:

Data is managed by IDC's Quantitative Research Group.

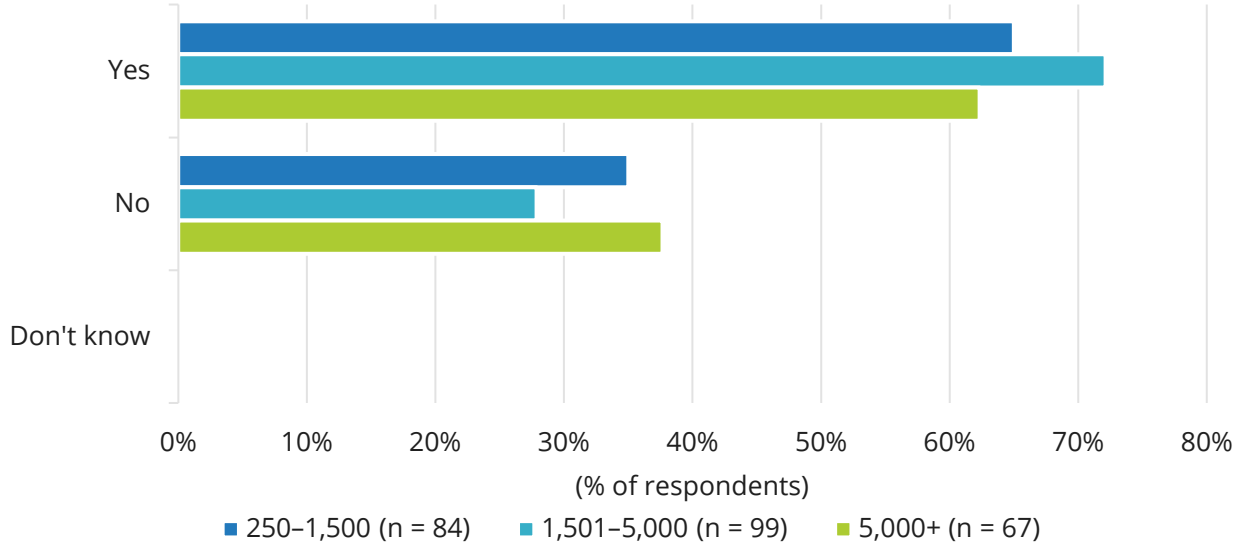
Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

FIGURE 6

Organizations Compelled to Pay a Ransom by Company Size



Base = respondents who indicated organization was attacked by ransomware within the past three years

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

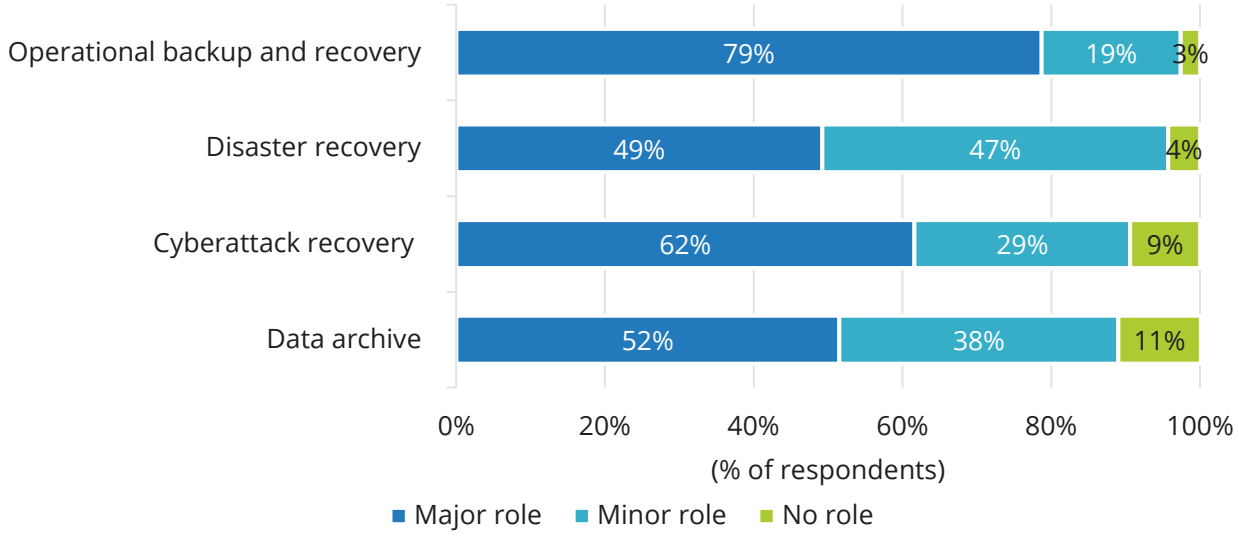
Clearly, even though more than 80% had a plan, that plan failed to yield a fully positive outcome in most cases.

Key Finding Number 6 — As Organizations Modernize Data Resilience, Cloud Will Play a Central Role

Digital transformation is an ongoing effort for most organizations as separate IDC research shows 60% of organizations with such efforts underway. In this survey, 50% of respondents indicated cloud is set to play a major role in backup/recovery strategies, DR, cyber-recovery, and data archive (see Figure 7).

FIGURE 7

Role of Cloud in Organizations Compelled to Pay a Ransom



n = 505

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

We asked organizations for their top desires when modernizing their data resilience systems. The number 1 desire for change was fully automated and nondisruptive infrastructure updates. While automation may be something that evolves over time, managed infrastructure for data protection operations can be achieved through BaaS and DRaaS solutions where updates and patches are the responsibility of the provider.

What Organizations Want

The number 1 desire among respondents for data protection modernization is fully automated/nondisruptive infrastructure updates.

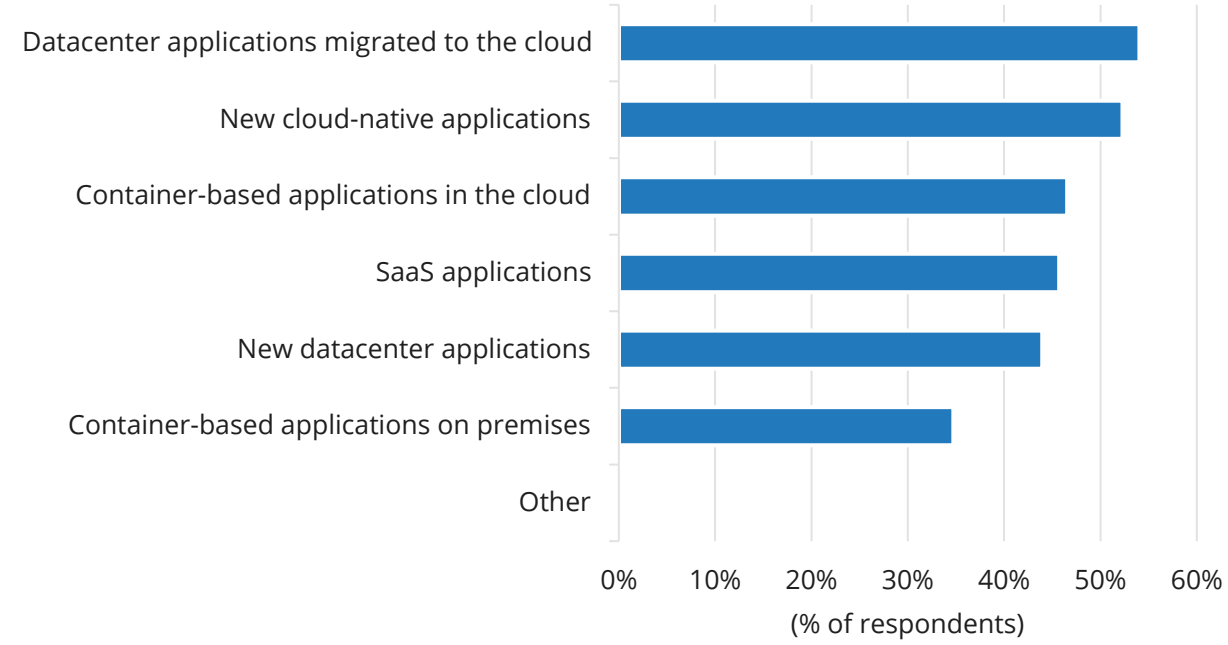
The number 2 desire is greater automation and recovery orchestration from ransomware, specifically automation to find the most recent recovery point. This is known as automated curated recovery. Because ransomware can take days, weeks, or months to fully detonate, the correct recovery point for different objects will be at different points in time. Currently, most organizations are forced to curate the recovery manually by searching backups, snapshots, and other copies for the latest clean version of an object. (By "object," we mean a specific file in the file system, database, or table.) Indeed, this is often the longest, most difficult part of cyber-recovery. Automated or orchestrated curation assists organizations in finding the most recent clean version of any data object even when some objects were clean yesterday and other objects corrupted months

ago. Automated curation reduces the manual effort of determining recovery points and can significantly reduce recovery time.

As these organizations modernize their data resilience, greater emphasis will be on cloud-based applications. Indeed, from this research, the top 4 workload categories anticipated by respondents were cloud related: datacenter applications migrated to the cloud, new cloud-native applications, containerized applications, and SaaS applications (see Figure 8). This emphasis on cloud applications indicates a need to adopt a more cloud-centric data resilience platform.

FIGURE 8

Most Important Future Workloads in 12 Months



n = 505

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *Druva Data Resilience Awareness Survey,* May 2022

FUTURE OUTLOOK

Considering Druva

Druva is an organization with a strong history of providing data protection solutions architected for cloud as-a-service delivery. Druva solutions address the broad spectrum of data recovery scenarios from day-to-day backup/recovery up to disaster recovery and ransomware recovery. Druva's platform architecture is cloud centric, but it protects workloads across the enterprise, from on premises to the cloud to edge, endpoint, hybrid cloud, and multicloud. Built on AWS, the Druva Data Resiliency Cloud platform is designed to provide a true cloud experience, including scalable resources, subscription pricing, and on-demand provisioning. The platform is fully managed and maintained by Druva.

Key components of the Druva Data Resiliency Cloud platform include:

- **Data protection.** Data protection is the "blocking and tackling" of data resilience. The Druva platform provides backup and recovery and disaster recovery with user-definable service levels (recovery point object [RPO] and recovery time objective [RTO]) that are manageable across the enterprise.
- **Cyber-resilience.** Based on key pillars of the NIST framework (protect, detect, respond, and recover), the Druva platform offers a multilayer cyberdefense. This platform includes automated curated recovery to speed recovery and minimize data loss.
- **SaaS app protection**. From its central console and using the global policy engine, Druva protects key SaaS applications including Microsoft 365, Google Workspace, and salesforce.com. This protection goes well beyond the default capabilities of the application provider to assist organizations in proper data retention and governance.
- **Public cloud support.** The Druva platform supports data protection for applications deployed on key public clouds including AWS, Azure, and GCP. This includes AWS EC2 and Kubernetes on AWS.
- **Datacenter software.** Druva fully supports key datacenter environments, including VMware and Nutanix, along with Oracle and Microsoft SQL server databases.
- **Edge — Android, iOS, Windows, and Linux.** As an enterprise platform, Druva's capabilities extend to edge devices, including Android, iOS, Windows, and Linux. As such, the platform is truly across the core, cloud, and edge. This enables data governance activities such data archival, compliance, and ediscovery and legal holds.
- **Cloud economics.** With the flexibility and on-demand nature of the public cloud, organizations can manage and optimize their costs for the lowest TCO.

CHALLENGES/OPPORTUNITIES

Future ransomware attack methods are difficult to predict and constantly evolving as new systems and vulnerabilities open and as attackers learn to circumvent defenses. Ransomware defense is inherently reactive — we are at best defending against known attacks but vulnerable to never-before-seen methods. IT and business leaders have learned that reacting is not enough; they are increasingly looking for integrated data security and data protection products, and Druva will need to stay in front of these requirements.

We believe that artificial intelligence and machine learning (AI/ML) is a key technology in the future battle against ransomware as it is the only way to detect new attack methods. AI/ML is sophisticated

software that can take time to develop and, if done incorrectly, will not be up to the task of countering ransomware. While AI/ML in cyberdefense and recovery is only now emerging, it will be an important differentiator between products, and Druva must be aggressive in this area to stay ahead of the competition. AI/ML also takes time to "learn" and requires greater transparency for developers, cloud ops, and end users to understand its capabilities. Druva expects to leverage the collective data points from its many cloud deployments to enable this learning.

There is also a common misperception that data protection is a mature, steady market. Quite to the contrary, data protection software is a highly dynamic and competitive environment. Druva currently has more than 40 direct software competitors and thousands of cloud service provider competitors. Druva must innovate in the right areas, partner as needed, and build an ecosystem around its products to stay ahead of so many competitors.

CONCLUSION

Organizational leaders think they are ready for a ransomware attack, but the research from this study illustrates that most are not. Too many organizations were forced to pay the ransom, lost data, or took excessively long to recover. Unfortunately, no one knows what they don't know until it's too late. Attacks come in unexpected ways, and cybercriminals have extensive experience in finding vulnerabilities. IT and business leaders need to make a frank, honest assessment regarding their data resilience and cyber-recovery capabilities.

We believe that "go it alone" efforts are likely to be insufficient, as they are too insular in perspective, lack the necessary breadth of experience, and require ongoing updates and maintenance based on new threats. Cyberdetection and cyber-recovery are complex tasks, and piecemeal efforts across the enterprise add even more complexity and can be costly to implement and maintain. We recommend that organizations leverage the experience and capabilities of providers that have a greater breadth of experience and knowledge in cyberprotection and cyber-recovery.

Cloud solutions can prove to be essential tools to modernize data resilience systems. Cloud offers financial flexibility, native protection of cloud apps, simplified operations, and a higher degree of automation than is typical for on-premises deployments. Utilizing data resilience solutions from cloud providers also frees up IT staff to focus on higher-value activities. Although cyberattacks are top of mind for IT and business leaders, they must not forget the day-to-day need for data resilience and disaster recovery. Comprehensive, enterprisewide cloud solutions can save time, optimize cost, and provide the fastest possible recovery when the inevitable happens.

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