

# A new age of disaster recovery planning for SMEs



## Preface

“A new age of disaster recovery planning for SMEs” is an MIT Technology Review Insights report developed in collaboration with OVHcloud. The report is based on interviews with senior executives of data and technology companies conducted in July and August 2022. It examines what disaster recovery planning entails and how small and midsize companies can implement it in today’s fast-evolving cyber landscape. Amanda Simms was the writer, KweeChuan Yeo was the editor, and Nicola Crepaldi and Natasha Conteh were the producers. The research is editorially independent, and the views expressed are those of MIT Technology Review Insights.

We would like to thank the following executives for providing their time and insights:

**Derek Adair**, Cloud Architect, Zerto

**Henry Baltazar**, Research Director of Storage, 451 Research

**Chuck Brooks**, President, Brooks Consulting International

**Duncan Epping**, Chief Technologist (EMEA), VMware

**Theresa Payton**, President and CEO, Fortalice Solutions



# CONTENTS

<b>01 Executive summary</b> .....	<b>4</b>
<b>02 The shape of threats to come</b> .....	<b>5</b>
Attacks from every angle .....	7
The harms to SMEs are existential.....	9
<b>03 What is disaster recovery planning?</b> .....	<b>10</b>
Determining RTO and RPO .....	10
Backup and replication .....	11
Size matters .....	12
<b>04 A holistic view</b> .....	<b>14</b>
Putting it to the test .....	14
<b>05 Conclusion</b> .....	<b>15</b>





## Foreword

Cyberattacks on businesses are soaring, with costs reaching into the trillions. The main targets of these attacks are now small and midsize enterprises (SMEs) that are not prepared to defend themselves and do not have the resources to survive afterward. It is estimated that businesses can lose thousands of dollars per minute, hundreds of thousands per hour, and millions per day due to downtime, not including all the other related costs and damages.

This report, prepared by MIT Technology Review Insights and OVHcloud, based on insights from leading IT cybersecurity experts, looks at how cyber threats have evolved over the last decade, particularly since the post-pandemic catalyzation of cyberattacks. Criminals have become better at employing new technologies, including deepfakes, but most successful attacks still come down to social engineering.

Now more than ever, with SMEs on the firing line, rigorous disaster recovery (DR) plans are essential. More importantly, it's critical to test DR plans regularly, as often as monthly, to ensure the planned failover works successfully. For true business continuity, a DR plan must be designed specifically for an organization's IT enterprise, to ensure it is customized with tools that fit the workloads and environment and guarantee the least downtime possible.

Organizations should take sufficient measures to achieve IT resilience at both the software and infrastructure level. Gaps in the infrastructure not only create security vulnerabilities that expose organizations to malicious attacks, but also increase complexity and incur additional costs in recovery. Distributed data protection, with multiple backups in different locations, enhances recovery and protects businesses from unplanned downtime incidents, including those related to natural disasters.

Rigorous DR solutions ensure critical data and applications are continuously protected, instantly recovered, and readily available, with the lowest recovery point objectives (RPO) and fastest recovery time objectives (RTO). The "3-2-1" rule of keeping three copies, two backups, and at least one different location is now advancing to a safer "3-2-2" strategy, adding a second location for additional redundancy.

For SMEs, it is also important that DR solutions are accessible and affordable, open and flexible – yet world-class in performance. Proprietary tools can ultimately result in unpredictable costs in terms of personnel and data migration and transaction charges. Avoiding these can make disaster recovery planning affordable, manageable, and achievable.

Thank you to all those who have contributed to this informative report.

**Jeffrey Gregor**  
General Manager, OVHcloud US

---

---

---



# 01 Executive summary

Today's cyberthreat landscape has become increasingly complex. Gone are the days when devastation to enterprises' data and IT systems was caused solely by force majeure events and physical terrorist attacks. Rising geopolitical tensions, fast-tracked digital transformation, and remote and hybrid working styles driven by the pandemic have made both public and private organizations across the globe increasingly vulnerable to cyberattacks via ransomware, malware, or hacking.

Today's data is generated and distributed across highly complex ecosystems—multicloud, hybrid cloud, edge, and internet of things. Enterprises' surface exposure to risks has ballooned. It's not just big corporations that are at risk. Smaller, less sophisticated companies are easier targets due to their lack of resources and expertise. According to Accenture, more than one-third of cyberattacks are aimed at small businesses, but only 14% of them are prepared to defend themselves.<sup>1</sup> Cyberattacks could leave many small and midsize enterprises (SMEs) reeling from financial and productivity losses, operation disruptions, extortion payments, settlement costs, and regulatory fines.

Given this backdrop, experts say it's time to plan for when, not if. Clear backup and disaster recovery plans—focusing on IT infrastructure, data, and applications—to execute recovery processes after a disaster are vital in every enterprise's business continuity strategy. This report explores what disaster recovery planning entails and how SMEs can implement it in today's fast-evolving cyber landscape.

The following are the report's key findings:

- **Cyberattacks have grown more frequent and sophisticated, and SMEs are in the firing line.** The data tells a worrying story. With the pandemic, along with geopolitical factors, causing shifts in how we live and work, the case for disaster recovery planning has never been more urgent. According to one cross-industry study, midsize companies were almost 500% more likely to be targeted by the end of 2021 than two years ago.<sup>2</sup> Experts say artificial intelligence–based attacks are rising. Ransomware-as-a-service and, in some cases, deepfakes are also increasing, although most SMEs become victims because of human error.
- **A well-built disaster recovery plan can significantly minimize and even eliminate downtime.** Disaster recovery plans are a key component of business continuity plans. While business continuity focuses on overall strategy, including policies and procedures for recovery following an incident, disaster recovery focuses on IT infrastructure, data, and applications. A well-crafted disaster recovery plan includes clear definitions of recovery time objective (RTO) and recovery point objective (RPO).<sup>3,4</sup> Having such a plan is crucial for protecting data and applications against malware and ransomware attacks and could significantly minimize or even eliminate downtime.
- **Backups and replication of data are essential for disaster recovery.** With cybercriminals spending over 200 days in companies' systems before being noticed<sup>5</sup> and corrupting backups, SMEs need to store their data in multiple formats on different systems or look toward a data replication solution to ensure near-instantaneous recovery. While the longstanding 3-2-1 strategy<sup>6</sup> is endorsed by cybersecurity experts, some organizations are seeking greater security with the 3-3-2 approach<sup>7</sup>, which includes an extra disconnected and inaccessible ("air-gapped") copy.
- **An unexamined disaster recovery plan could bring enterprises back to square one.** Disaster recovery plans are essentially pointless without regular practice runs—and how often this practice should be done depends on how fast an organization is growing or adopting new technologies. Experts say such plans should be updated and tested at least annually, and ideally every quarter.

# 02

## The shape of threats to come



Cybersecurity has never been more critical. Even before the pandemic, cybercrime was on an upward trajectory, with the global cost jumping from \$445 billion in 2014 to \$600 billion in 2017.<sup>8</sup> The last few years have seen a marked acceleration. In 2020, malware attacks swelled 358% while ransomware attacks surged 435%, according to Deep Instinct.<sup>9</sup> Separately, IBM says the average cost of a data breach in 2022 reached "\$4.24 million, up 12.7% from 2020's average. Health care bore the brunt of the burden (see Figure 1).<sup>10</sup>

At their worst, cyberattacks pose an existential threat, but a company's reputation is also on the line. Moreover, studies show that company share prices also suffer, though to what extent depends on the type of company and how its data was compromised.<sup>11,12,13</sup> This can ultimately have knock-on effects on a company's valuation: After three data breaches at Yahoo were exposed, for example, \$350 million was slashed off the original \$4.8 billion price tag for its 2017 sale to Verizon.<sup>16</sup>

### Protection through education

With more people now working from home, security concerns have morphed. Companies' surface exposure has increased due to the cloud, apps, mobile devices, and remote access by employees and customers. As a result, firms are vulnerable to a wide range of attack methods, and all applications used by employees and customers need to be protected.

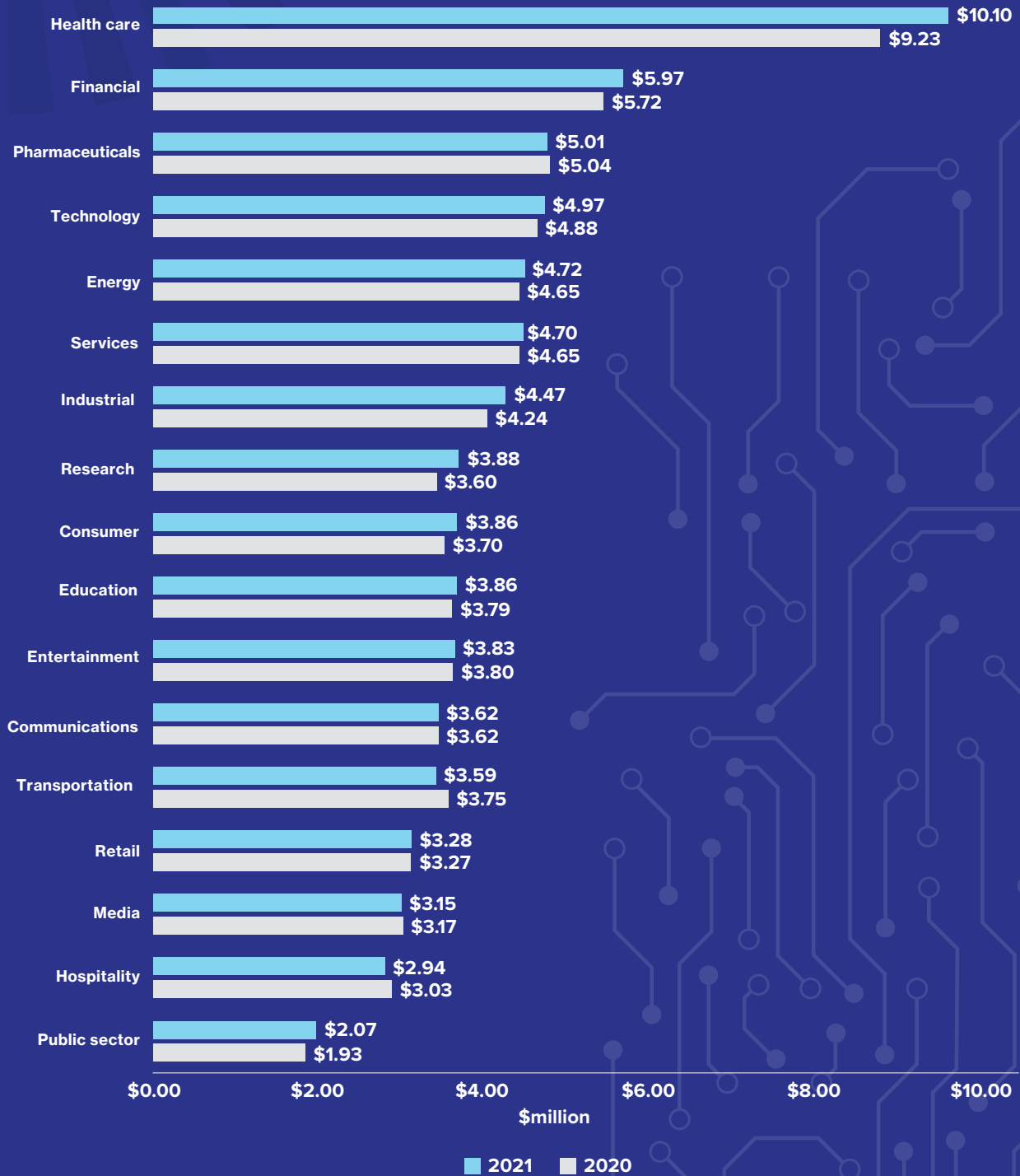
Human error has been found to be at the root of most successful breaches, and 95% of successful breaches come down to employee mistakes.<sup>14</sup> "If there're two fools born every minute, I can guarantee you that they're both going to click on something that exposes

your environment to ransomware," says Derek Adair, cloud architect at Zerto.

But education can be transformative. Duncan Epping, VMware's chief technologist for Europe, Middle East, and Africa, explains that many technology-based companies skip education, because they focus on the product rather than people. Cybercriminals "don't go through a machine first, they go through a person," he says. "Make sure you educate every single person within your organization, not just the people within the IT team. Everyone needs to understand what these types of attacks will look like and what the impact could be."

### Figure 1: Average cost of a data breach by industry in the U.S.

The health-care industry incurred the highest average cost in 2021 and 2022 and saw one of the largest year-on-year absolute increases.



Source: IBM Security, 2021<sup>15</sup>

It's often assumed that larger companies are the most appealing targets, but criminals are not discriminating anymore. "In the past, the focus would be on mainly large companies," says Duncan Epping, VMware's chief technologist for Europe, Middle East, and Africa (EMEA). "What we're also starting to see is that it doesn't really matter whether it's 15 people that work for the company or whether it's 25,000." According to the U.S. National Cyber Security Alliance, 47% of all SMEs were hit by a successful cyberattack in 2021 alone, and 60% of those never fully recovered.<sup>17</sup>

### Attacks from every angle

Social engineering, whereby people are manipulated into giving up information or bypassing security protocols, is an increasingly common tactic used by cybercriminals to trick people into compromising their organizations' data. This reflects the fact that people are often a company's

main weakness (see sidebar "Protection through education"). According to 2021 research by Barracuda Networks, companies with less than 100 employees were 350% more likely to be victims of social engineering attacks.<sup>18</sup>

Ransomware is the threat du jour. It's what every company seems to be preparing for, with media reports on devastating attacks compounding this fear. Ransomware attacks have surged since the pandemic (see Figure 2), doubling year on year in 2021, although they comprise only 10% of overall cyberattacks.<sup>19</sup> Even if companies pay up, most hackers take the money and run, with 92% of paid ransoms resulting in the company losing their data.<sup>20</sup>

Meanwhile, the emergence of ransomware-as-a-service (RaaS) has "resulted in almost a landslide of attacks happening all over the world," says Epping. "The people

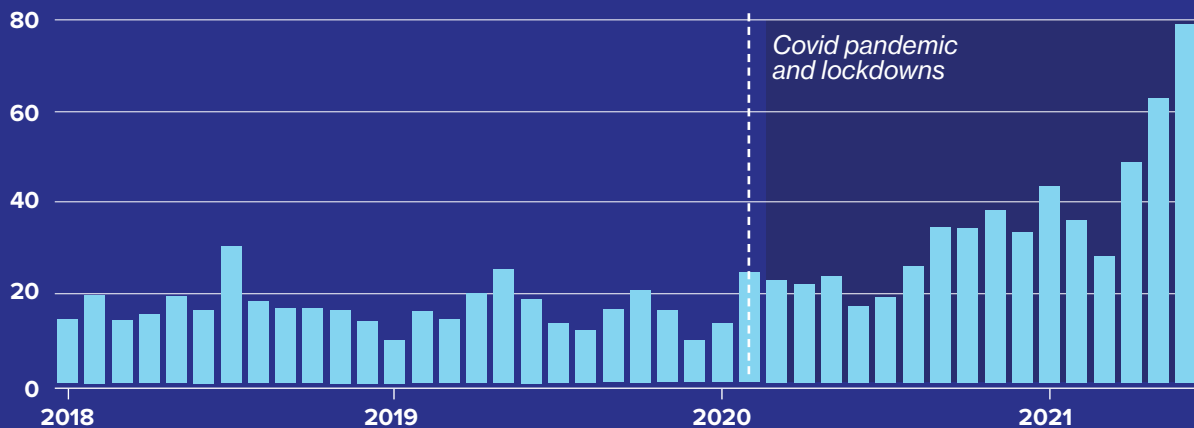
**"Make sure you educate every single person within your organization, not just the people within the IT team. Everyone needs to understand what these types of attacks will look like and what the impact could be."**

Duncan Epping, VMware's chief technologist for Europe, Middle East, and Africa

**Figure 2: Ransomware attacks from 2018 to 2021**

Attempts to hold data hostage have reached record levels, with a distinct uptick since the pandemic started.

Global ransomware attempts (million)



Source: Financial Times, 2021<sup>21</sup>



actually doing the attack itself don't necessarily need to have all the knowledge that would be required for those types of attacks. They just rent a service."

Some hackers leak stolen data or sell it on the dark web, potentially posing regulatory issues for their victims.

They could even destroy the data as a means of derailing operations. And sometimes, the threat is internal. In one case, a disgruntled former employee deleted a company's data from two database servers and two application servers, leading to a restoration cost of about \$30,000.<sup>23</sup>

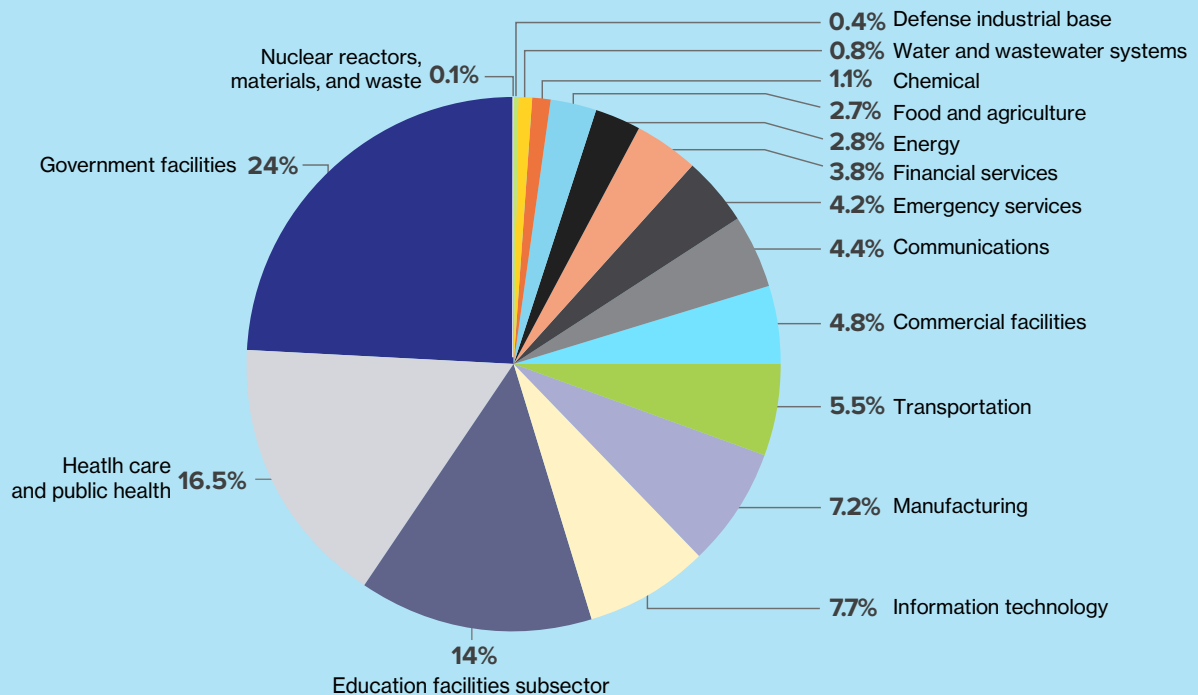
## Most targeted industries

Internet companies like Yahoo were the primary focus of past attacks because of their big surface exposure to cyberattacks. However, Duncan Epping, VMware's chief technologist for Europe, Middle East, and Africa, says "companies with masses of end-users are more at risk, as the impact of a breach for them is much higher" (see Figure 3). The health-care industry is one of the biggest targets for hackers, owing to the abundance of personal data it collects and the pandemic.

Education and financial services providers are also frequently targeted, although the financial services sector has invested heavily in cybersecurity defenses, keeping it relatively secure. Government agencies appeal to cybercriminals because the repercussions of breaches can be particularly disastrous. Essentially, in picking their victims, criminals are looking for easy targets, rich data, or reputational damage.

### Figure 3: Ransomware attacks by industry

Based on data on 1,137 incidents from November 2013 to January 2022, government, health care, and education facilities were the biggest targets of ransomware attacks.



Source: Fitch Ratings, 2022<sup>22</sup>

Data poisoning, whereby a hacker injects corrupted information into a set of machine learning data to steer subsequent actions toward the hacker's desired outcome, is another risk. This could, for example, lead to phishing emails sailing through spam filters or even tricking facial recognition systems.

Added to this is outdated technology, both hardware and software, which can increase a company's susceptibility to malware. The pandemic has made tackling these shortfalls even more urgent. Theresa Payton, president and CEO of Fortalice Solutions, cites McKinsey research showing that the pandemic caused companies to accelerate their digital transformation plans by seven years.<sup>24</sup> "Despite this, I haven't heard a lot about retiring old technology," Payton says. With digitalization strategies advancing rapidly, companies need to examine vulnerabilities in legacy systems and outdated hardware.

### The harms to SMEs are existential

Cybercriminals target SMEs because they believe such businesses have fewer resources and less expertise to deal with attacks.<sup>25</sup> And when breaches are successful, they are almost always disastrous. "If they get taken down, they go out of business pretty quickly," says Chuck Brooks, president of Brooks Consulting International. According to a study by the U.S. Securities and Exchange Commission (SEC), more than half of SMEs shut down within six months of an attack.<sup>26</sup>

Some business leaders might operate under the false assumption that their SMEs are flying under the radar, but every type of firm is targeted. Efficient Services Escrow of California was forced to shut down in 2017, following a loss of \$1.5 million after cybercriminals gained access to the company's bank data through Trojan horse malware.<sup>27</sup> A Kansas car dealership, Green Ford Sales, lost \$23,000 after hackers infiltrated its network, stole bank account details, and added fake employees to its payroll. Maine-based Patco Construction lost \$588,000 in 2009 from a Trojan horse attack.<sup>28</sup>

As these examples show, disaster recovery planning is imperative for SMEs. But not everyone has caught on. Brooks says that although he is seeing many more disaster-focused recovery plans than in the past, "this really permeates mostly [across] very large companies, but not so much [among] the smaller and medium companies." In the face of constant, existential threats, it seems obvious that all organizations—big and small—should be doing everything they can to protect themselves. Still, one survey found that just over half of companies have a disaster recovery plan in place.<sup>29</sup> And even if companies have firm plans for how they could recover when disaster strikes, many go untested. This is not because businesses don't care, however; it's that "they don't know where to start," says Payton.

In the face of constant, existential threats, it seems obvious that all organizations—big and small—should be doing everything they can to protect themselves. Still, one survey found that just over half of companies have a disaster recovery plan in place.



# 03 What is disaster recovery planning?



Constituting one element of business continuity, a disaster recovery plan formally outlines how a company will resume normal operations after an unplanned incident, focusing on IT architecture, data, and applications. Like an instruction book, a disaster recovery plan clarifies each employee's role and the steps to return to business as usual.

While disaster recovery plans will look different for each organization, two key parameters guide such plans—recovery time objective (RTO) and recovery point objective (RPO). RTO is the amount of time it will take an organization to recover lost data and resume operations.<sup>30</sup> RPO is also measured in terms of time: it refers to the duration that might pass during a disruption before the quantity of data lost reaches a level that will completely disrupt operations.<sup>31</sup> Both parameters help organizations decide how often data needs to be backed up and how it can be stored.

## Determining RTO and RPO

To define their RTO and RPO, companies need to rank their data by importance. Different types of data can fall into three categories: mission critical, which is essential to

immediate operations; business critical, which is integral to a company's long-term success; and noncritical, which can come back online last.<sup>32</sup> This then dictates the organization's recovery plan: business-critical data that is important to an organization's daily operations, for example, can wait a few hours to get back up, but mission-critical data that could be devastating if it's not restored immediately must be back up and running instantly.

Key stakeholders need to be involved in determining RTO and RPO. "The business is going to say everything has to be back running in the same business day," says Payton. "We can show them the dollars and cents of how expensive that is. And it's nearly impossible to find something like that." In order to prioritize, Payton says, the business should consider customer experience—essentially, ranking what applications are the most integral to serving clients. As an exercise to determine this, Payton recommends disconnecting systems to see how long the organization can go without using them or restoring from backup.

Once RTO and RPO have been established, they can help organizations choose their infrastructure assets, deciding what to back up and replicate (see Figure 4), which are

**"The business is going to say everything has to be back running in the same business day. We can show them the dollars and cents of how expensive that is. And it's nearly impossible to find something like that."**

Theresa Payton, President and CEO of Fortalice Solutions

“Customer expectations and client expectations have gone up, and because of that daily backups are not enough, so we’re starting to see more and more granularity in terms of data protection.”

Henry Baltazar, Research Director of Storage, 451 Research

essential steps in building a disaster recovery plan.<sup>33</sup> For example, if a company identifies one mission-critical application that needs to come online first, it may choose to explore data replication via a cloud-based service for that application. If an organization has slower data turnover, however, due to its industry or size, it may decide that daily backups are sufficient and, therefore, it does not require more costly disaster recovery solutions.

### Backup and replication

Data backup involves making copies of data. It relies on taking historical data “snapshots” at predetermined points in time, which can then be revisited. The process is time consuming, but it is more affordable than replication. Replication, meanwhile, is more focused on business continuity. Data is transferred in real time to multiple servers, which may replicate a company’s entire system or just parts of it. Replication allows for a near-instantaneous recovery and resumption of operations.

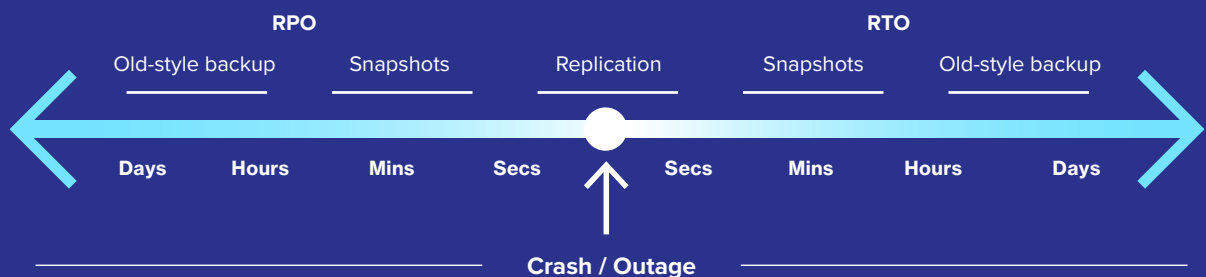
Each option has its pitfalls. If systems were to go down

just before a scheduled backup, days’ worth of data could be lost, which would be disastrous for some industries. These snapshots are also incredibly draining on servers; hence they are scheduled infrequently or overnight. It’s also far more time consuming to resume operations from backups when disaster strikes. Replication, on the other hand, is expensive and potentially allows malware to be transferred along with the rest of the data. Unlike backups, replication doesn’t provide a historical account of data, which is sometimes needed for compliance reasons.

Although some firms opt for a combination of these two strategies to offset their respective vulnerabilities, Henry Baltazar, research director of storage at 451 Research, a part of S&P Global Market Intelligence, says companies are largely shifting away from the daily backup approach. “Customer expectations and client expectations have gone up, and because of that daily backups are not enough, so we’re starting to see more and more granularity in terms of data protection,” he says. “We need to have

**Figure 4: Data backup and replication**

Recovery point objective (RPO) and recovery time objective (RTO) are key parameters that guide organizations in picking the best data backup and replication options for their disaster recovery plans. Snapshots can be a critical part of the backup process.



Source: OVHcloud, 2019<sup>34</sup>

snapshots and replication capabilities so that, at most, we lose only a couple of minutes or maybe even a couple of hours of data.”

Strength in diversity is another important theme. The 3-2-1 strategy (see Figure 5) has been a stalwart of backup plans for decades. It entails creating three copies of data, keeping two on different backup mediums, and moving one offsite. However, in the face of ever-increasing threats, particularly ransomware, organizations looking for extra padding can opt to use a second cloud storage location (3-2-2 strategy) or network-attached storage, tape, and cloud (3-3-2 strategy) for added redundancy.<sup>36</sup> In addition, Baltazar points out that immutable data is equally important. “You can’t delete, can’t modify; you can’t write on top of it once it’s there,” he explains. “So, you basically capture it like a backup. And then you have a retention period, in which case nobody can do anything to that.”

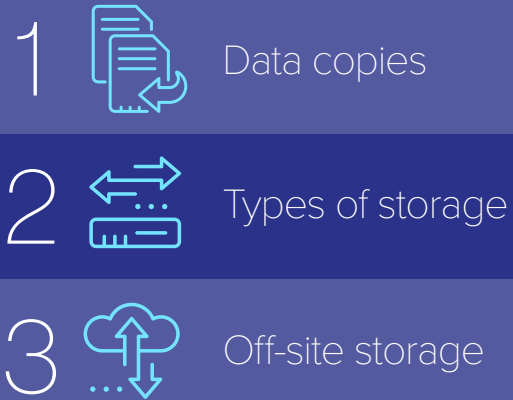
## Size matters

How organizations protect themselves and set up their disaster recovery plans will differ based on company size and each company’s unique traits. Larger companies may have more resources to protect themselves against cybercrime, but their surface exposure to attacks is significantly bigger and harder to manage. “Most big companies don’t even realize what assets they have from 20 years ago,” says Brooks. SMEs, however, can be more agile and come up with a disaster recovery plan faster. “It doesn’t have to be a sophisticated plan like a big company,” says Brooks. “And also, they’re dealing with fewer people and probably a lot less data.”

When planning for a failover, which requires switching to a backup operational system, SMEs typically tend to focus more on buying a service because they have limited staff. “So, they acquire servers from a cloud company,” Epping

## Figure 5: The 3-2-1 backup strategy

Three copies of data—one original and two backups—are created; both backups are stored separately in different types of media; and the original is stored offsite or in a remote location.



Source: Techtarget, 2019<sup>35</sup>

says. “They store the data in the cloud and then they work with that company to ensure that they can recover into the cloud as well.”

Another benefit to cloud-based managed services is that SMEs can choose to pay for only what they need—and only when a disaster occurs. That is attractive, explains Adair, because “I can have enterprise-level protection for exactly what my business runs on, and not break the bank to be able to do that.”

While SMEs may find some parts of disaster recovery planning simpler, however, their stakes are much higher. Larger organizations might find planning and implementation more of an administrative headache, but they also typically have the financial reserves to withstand a successful attack.

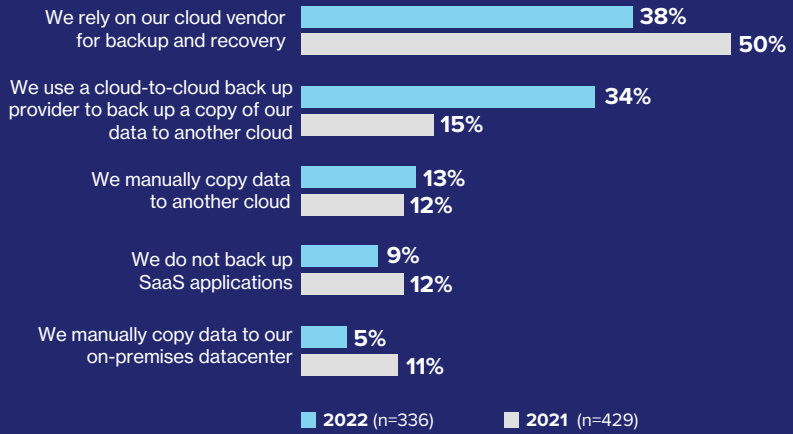
## Different types of data backup

When it comes to backing up data, companies are looking more toward hybrid and cloud solutions, and away from on-premises storage (see Figure 6). “A lot of people are realizing that they can’t just stick to their guns and just say okay, we’re all going to keep it

on-premises and all in our sight,” says Henry Baltazar, research director of storage at 451 Research, a part of S&P Global Market Intelligence. Storing data in the cloud helps ease organizations’ concern about physical viability and allows them to offload some storage responsibility.






**Figure 6: Data protection preferences**

A significant number of organizations are still in the process of upgrading their data protection for software-as-a-service applications. Manual copying of data to on-premises storage has fallen in 2022, but manual copying to the cloud remains almost unchanged.



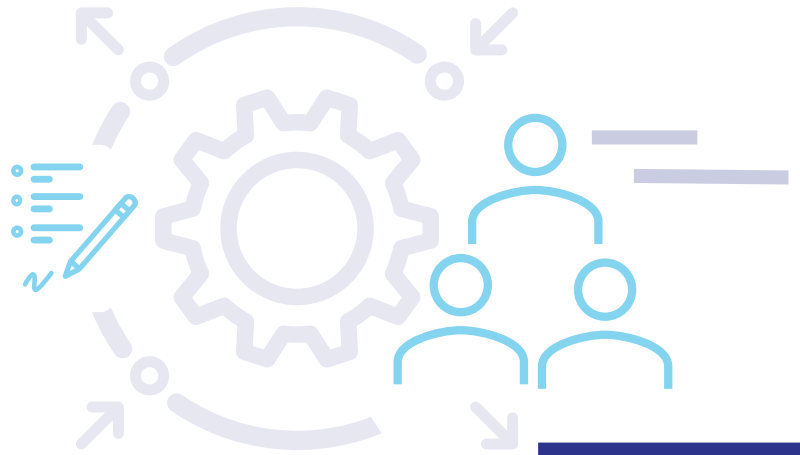
Source: S&P Global Market Intelligence, 2022<sup>37</sup>

## Strategies for backing up and recovering data

	WHAT	HOW
<b>Cloud</b> 	Resources and data are stored on a cloud-based service. Management of data is done in-house or by a third party.	During a failover, which is the process of moving from the damaged system to the backup, the organization simply reverts to the backed-up cloud version, as if switching to a spare tire.
<b>Off-site</b> 	This essentially means storing one version or multiple versions of data off-site.	Some organizations opt for the 3-2-1 strategy—creating three copies of data, keeping two backups on different mediums, and moving one copy offsite. Alternatively, they can separate one copy of their data via an “air gap,” meaning that it’s offline and physically locked up.
<b>Hybrid</b> 	Employing both private and public cloud backups is an effective way to diversify your data protection, as it combines in-house and offsite backups. Data can be made available at any time for backup.	This is an expensive and resource-intensive undertaking, as it involves creating and maintaining a private cloud, which requires skilled staff, physical hardware, and constant maintenance. <sup>38</sup>
<b>Disaster-recovery-as-a-service</b> 	This form of cloud-based disaster recovery allows organizations lacking in-house capacity or with more complicated needs to outsource.	This works like any other software-as-a-service solution—with the added benefit of expert help and the fact that many providers only require payment when a disaster occurs.
<b>Virtualized</b> 	Rather than creating a physical backup, a company’s entire working system or just parts of it are split and housed virtually.	This typically involves replication, which means the organization can simply move over to the virtualized version of its data when an incident occurs.

# 04

## A holistic view



There is a lot more to disaster recovery planning than just technology. It can also be an important exercise to investigate vital issues that are overlooked when it's business as usual—such as where data is collected, how it is stored, and who is responsible for it. “This is something I want people to have hope and optimism [about],” says Payton. “To recognize this is actually a great business practice and it has more benefits than just recovering from a cyber incident.”

As such, disaster recovery plans should be multifaceted. They should include a statement of intent and essential information ranging from insurance, financial, and legal details to which authentication tools are used. Communication is a frequently overlooked aspect: the plan should detail not only who is responsible internally for its various parts, but also how public relations will be managed and how to deal with affected customers and the media.

Constant revision is another necessity. Disaster recovery plans should be updated once a year, and that may not even be enough for some organizations.<sup>39</sup> If a company is rapidly scaling up, taking on new employees, or integrating all kinds of new hardware and software, quarterly or even monthly updates of disaster recovery plans make more sense.

### Putting it to the test

A disaster recovery plan is effective only if it's tested. Not doing so can render disaster recovery plans pointless. “In that case, no one knows what's going to happen if there is a failure—it's basically a guessing game,” says Adair. But testing your plan is an opportunity to check that the recovery portion—which is under your control—runs as smoothly as possible.

There is more than one way to test, with each providing a different benefit. One is a live failover, where operations are completely shut down and then restored, which “allows you to validate your resilience strategy and ensure recovery will be successful in the event of a real disaster or disruption,” Adair explains. Another type of test is conducted in the background via a production copy. In that case, “you don't have to take any applications offline. You don't have to lose an entire weekend trying to see if you're prepared for any outage or data loss,” says Adair. “It's invisible to the end user, too, so a complete failover test can run without either slowing down the network or hindering any other IT functions.”

Payton recommends testing different disaster scenarios once every quarter, and at a minimum once a year. “You don't have to spend a lot of money and bring in outside consultants to facilitate it,” she explains. “If you take a staff meeting once a quarter and say somebody steals our data, somebody's leaking all of our client information, somebody's wired money to the wrong place because of fraud, what would we do? You can talk through that disaster and come up with a rough emergency response plan. That's going to take you very far down the road of knowing what your gaps are.”

There's another reason for regular testing, says Baltazar. “If you have a lot of major changes that happened after that test, how do you know that the recovery will still work?” That's why, he says, automation is so critical, not only for testing, but to incorporate new applications into the disaster recovery ecosystem. “I think one of the big gaps and areas we need to focus on as an industry is making sure that automation happens more and makes it so it's integrated from the start,” he says. “So, when somebody creates an application, the automation is in there to have the data protection already bundled.”



# 05

## Conclusion



The time to start a disaster recovery plan was yesterday. Data tells a worrying story about the state of cybercrime since the covid-19 pandemic struck—breaches are inevitable. “I think most companies have been attacked, whether they know it or not,” says Brooks. “It’s just a numbers game.” This is true of all organizations, but should be a particular concern for SMEs, who are now targeted more often and do not have the resources larger enterprises do to recover from successful attacks.

The uptick in ransomware is another significant development—particularly because paying the ransom often doesn’t get organizations their data back. In addition, ransomware-as-a-service means that more criminals have access to this technology and are sometimes spending months exploring organizations’ data undetected and even infecting backups.

But disaster recovery planning goes a long way in tempering these challenges, and disaster recovery plans are critical for organizations, particularly SMEs, to have in place. A holistic data recovery plan can give an enterprise a vital overview of its data, where it is stored, and who is responsible for it. And that, in turn, will help them prepare to respond to security breaches.

Although organizations should customize response plans to their own needs and traits, they should adhere to several key principles. One is diversity. Storing data, some of it immutable, in various locations via the 3-2-1 or 3-3-2 strategies should provide a failsafe backup. Cloud should also be at the core of recovery strategies. “The best part about the cloud is the elasticity,” says Baltazar. “You’re

only paying for the resources when you’re actually using them.” Disaster recovery-as-a-service is another option for SMEs, with expert advice provided on how best to curate the available options according to an organization’s needs.

“The best part about the cloud is the elasticity. You’re only paying for the resources when you’re actually using them.”

Henry Baltazar, Research Director of Storage, 451 Research

Testing should not be ignored either. This doesn’t just tell organizations if their plans work in practice, but it can also highlight how they should adapt. As Brooks emphasizes, “the whole thing about cybersecurity [is that it is] morphing. It’s never a stagnant thing. And the threats are morphing too, and you have to morph with them.”

All of this does not have to be viewed as “an onerous, financial resource [draining], burdensome exercise,” Payton says. “You can do it in such a way that you put the business mission and focus and user stories first, and then the technology, the security, the redundancy, and the reliability will follow.”



**Footnotes**

1. Accenture's "[Steps small businesses can take to mount an effective defense against cyberattacks](#)," The Business Journals February 15, 2022
2. "[Report: Mid-sized businesses are 490% more likely to experience security breach since 2019](#)," VentureBeat, November 22, 2021
3. The amount of time it will take an organization to recover lost data and resume operations.
4. The amount of time that might pass during a disruption before the quantity of data lost reaches a level that will completely disrupt operations.
5. IBM's "[IBM Report: Cost of a Data Breach Hits Record High During Pandemic](#)," IBM, July 28, 2021
6. Creating three copies, keeping two backups in different types of media, and storing the primary copy offsite.
7. Creating three restorable copies in three different places on two different types of media.
8. Robert McCullen, "[Cyberthreats: A 10-Year Perspective](#)," Forbes, May 15, 2018
9. Chuck Brooks, "[Alarming Cybersecurity Stats: What You Need to Know for 2021](#)," Forbes, March 2, 2021
10. IBM's "[How much does a data breach cost in 2022?](#)" IBM, 2022
11. Keman Huang, Rebecca Ye, and Stuart Madnick, "[Both Sides of the Coin: The Impact of Cyber Attacks on Business Value](#)," Working Paper CISL# 2019-25, MIT Management Sloan School and Cybersecurity at MIT Sloan, December 2019
12. Samuel Tweneboah-Koduah, William J. Buchanan, and Francis Atsu, "[Impact of Cyberattacks on Stock Performance: A Comparative Study](#)," Information and Computer Security, July 2018
13. Kelly Sheridan, "[Do Cyberattacks Affect Stock Prices? It Depends on the Breach](#)," Dark Reading, April 27, 2021
14. Edward Tuorinsky, "[Compliance Score Alone Won't Keep Your Company Safe From Data Breaches](#)," Forbes, October 8, 2021
15. "[The Average Cost of a Healthcare Data Breach Is Now \\$9.42 Million](#)," HIPAA Journal, July 29, 2021
16. Jeremy Kirk, "[Yahoo Takes \\$350 Million Hit in Verizon Deal](#)," Bank Info Security, February 22, 2017
17. Zinnov's "[Why SMB Cybersecurity Is a Non-negotiable Today](#)," Zinnov, August 24, 2022
18. Edward Segal, "[Small Businesses Are More Frequent Targets of Cyberattacks Than Larger Companies: New Report](#)," Forbes, March 16, 2022
19. Chuck Brooks, "[Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know](#)," Forbes, June 3, 2022
20. Davey Winder, "[Ransomware Reality Shock: 92% Who Pay Don't Get Their Data Back](#)," Forbes, May 2, 2021
21. Hannah Murphy, Patrick Mathurin, and Chris Campbell, "[Ransomware attacks rise despite US call for clampdown on cybercriminals](#)," Financial Times, July 30, 2021
22. Fitch Ratings' "[Russia/Ukraine War Increases Spillover Risks of Global Cyberattacks](#)," Fitch Ratings, March 4, 2022
23. Bill Toulas, "[Angry IT admin wipes employer's databases, gets 7 years in prison](#)," Bleeping Computer, May 14, 2022
24. McKinsey's "[How COVID-19 has pushed companies over the technology tipping point—and transformed business forever](#)," McKinsey, October 5, 2020
25. Nicholas Fearn, "[Why SMEs are at a higher risk to cyber crime](#)," IDG Connect, October 1, 2019
26. My Business's "[More Than Half of Small Businesses Close After a Cyber Attack](#)," My Business, February 24, 2022
27. Syscon's "[Stories From Small Businesses That Were Attacked](#)," Syscon, 2018
28. Calyptix Security's "[Small Business Cyber Attacks That Stole Thousands](#)," Calyptix Security, September 22, 2015
29. "[Only 54% of organizations have a company-wide disaster recovery plan in place](#)," Security Magazine, June 29, 2021
30. OVHcloud's "[Now Is the Time to Take a Close Look at Your Disaster Recovery Plan](#)," OVHcloud, 2020, page 6
31. Ibid., page 5
32. Ibid., page 7
33. Ibid., page 6
34. Ibid., page 5
35. Rich Castagna, "[3-2-1 Backup Strategy](#)," Techtarget, July 2019
36. Surya Varanasi and JG Heithcock, "[2021 Reflections and 2022 Predictions](#)," DRJournal, December 28, 2021
37. Henry Baltazar, "Ransomware and Cloud Services Failures Force Organizations to Rethink Data Protection Strategies," 451 Research, S&P Global Market Intelligence, May 2022
38. Clients First's "[5 Essential Benefits of Hybrid Cloud Disaster Recovery](#)," Client First Business Solutions, August 4, 2020
39. University of Michigan's "[Maintain Your Disaster Recovery Plan](#)," Safe Computing, University of Michigan

## About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution—producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review [Global Insights Panel](#), Insights has unparalleled access to senior-level executives, innovators, and entrepreneurs worldwide for surveys and in-depth interviews.

## From the sponsor

OVHcloud US is a subsidiary of OVHcloud, a global player and Europe's leading cloud provider operating more than 400,000 servers within 33 data centers across four continents. For 20 years, the Group has relied on an integrated model that provides complete control of its value chain from the design of its servers to the construction and management of its data centers, including the orchestration of its fiber-optic network. This unique approach allows it to independently cover all the uses of its 1.6 million customers in more than 140 countries. OVHcloud now offers latest generation solutions combining performance, price predictability, and total sovereignty over their data to support their growth in complete freedom.



---

### Illustrations

All illustrations assembled by Shultz Design Collaborative, with art from Shutterstock: Cover: building, Studio Caramel; circuit board, mydegage; icons, Blan-k and Motorama, sunburst, Topilskaya. Internal pages icons by Thanakit Jitkasem, Limeart, Motorama, Topilskaya.

*While every effort has been taken to verify the accuracy of this information, MIT Technology Review Insights cannot accept any responsibility or liability for reliance by any person in this report or any of the information, opinions, or conclusions set out in this report.*


© Copyright MIT Technology Review Insights, 2022. All rights reserved.



## MIT Technology Review Insights

 [www.technologyreview.com](http://www.technologyreview.com)

 @techreview @mit\_insights

 [insights@technologyreview.com](mailto:insights@technologyreview.com)