arcserve®

Disaster Recovery Planning, Proactive Cybersecurity, and Immutable Backups: Vital to Ensuring Data Resilience

Table of Contents

The 5-Step Ransomware Disaster Recovery Plan Template

Ransomware attacks continue to impact organizations worldwide—and the costs are staggering. An independent global survey of over 1,100 IT decision-makers at small and midsize companies commissioned by Arcserve found that 50 percent had been targeted by a ransomware attack, with 35 percent of those targeted asked to pay over $100,000 in ransom and 20 percent asked to pay between $1 million and $10 million.

These numbers are not expected to improve anytime soon. The sad truth is that, despite spending billions on cybersecurity tools, businesses still aren't prepared for ransomware attacks. Less than a quarter (23 percent) of all respondents to the survey said they were very confident in their ability to recover lost data in the event of a ransomware attack. Smaller businesses are even less prepared. Under 20 percent are very confident in their ability to recover lost data in the event of a ransomware attack.

Meanwhile, the attack surface continues to expand as organizations using technologies like IoT, artificial intelligence, and 5G generate even more data—data that can be compromised and held captive by ransomware attackers.

That's why you need to take a new approach to data resilience. You need to strengthen your disaster recovery strategies, backup systems, and immutable storage solutions to prevent the loss of mission-critical data.

Many of your peers are already doing just that. The survey found that 92 percent of organizations are making additional investments to protect against ransomware attacks, with the top areas of investment being security software (64 percent), training and certification (50 percent), and managed services (43 percent).

While these investments are encouraging, more should be done. Because, as with most companies, it's not a matter of if your data will be compromised; it's a matter of when. With ransomware attacks continually increasing, data backup and recovery should be at the very top of your organization's priority list.

Here are five steps you can take now to reduce your exposure to ransomware and avoid staggering losses.

1. Educate Employees

It’s essential to invest in training for staff so that they’re aware of how ransomware works. From there, employees will be better prepared to recognize and prevent it. They should know that ransomware can sneak in from anywhere. The training should remind them to scrutinize every link in emails and not open attachments in unsolicited emails.

Employees should be reminded to only download free software from websites they know and trust. When possible, employees should verify the integrity of downloaded software through a digital signature before execution.

2. Focus on Remediation and Prevention

Companies continue to invest loads of money in cybersecurity solutions like next-generation firewalls and extended detection and response (XDR) systems designed to prevent attacks. Yet these same companies are still falling prey to ransomware and being forced to pay a hefty price.

It’s time for you to stop focusing entirely on prevention. You should also invest in remediation measures like backup and disaster recovery and immutable storage. These technologies let you quickly restore your data and avoid paying the ransom when attackers break in.

Regular data backups and encryption play a key role in protecting your organization’s data. A consistent backup schedule will enable you to restore any compromised systems or data seamlessly. Encrypting your sensitive data is also highly recommended. After all, if ransomware attackers gain access to your critical assets, encryption can keep data from being read and further exploited by the bad guys.

3. Place a Premium on Data Resilience

Your data resilience is only as strong as your weakest link. If you monitor your vulnerabilities and fix them when you find them, you can bounce back quickly from disruption and return to normal operation. To do this, you must have the technologies required to back up your data and recover it if necessary, along with the proper mindset. That means a defensive posture is regularly maintained with drills that simulate an intrusion to measure your resiliency and bolster it where necessary.

Many companies develop a strategy and then neglect to test it. That’s like a basketball team devising a sophisticated defense and never bothering to practice it. Your company should regularly test its data backup and recovery plans to ensure it can effectively restore its data and systems if an attack or natural disaster occurs.

4. Know Which Data Is Most Critical

Data varies in value. If you're concerned about costs—as most organizations are these days—you don't have to store or back up all your data in the same place. Look into storage solutions that provide options like data tiering. This enables you to place less-important data in less-expensive levels of storage or "tiers."

Another upside of data tiering is lower energy costs. You'll use less compute power if you're not storing every last byte of your data at the highest security level.

5. Put a Disaster Recovery Plan in Place

Despite all the preventive measures you take, you need to prepare for the possibility of getting hit. So you need a disaster recovery plan. Period. You need to be able to back up data as often as is appropriate. That can range from continuous data protection that takes snapshots of your data every 90 seconds to hourly, daily, or weekly backups, depending on your requirements and the type of data you are backing up. You must also be able to easily verify that your whole environment is backed up, including your remote workers and any SaaS applications you use, such as Microsoft 365.

A good disaster recovery solution will back up your data to the locations of your choice and on a schedule that fits your needs. It will also be easy to test, which is crucial because testing is the only way to validate that your recovery time objectives and recovery point objectives (RTOs/RPOs) can be met. It may seem obvious, but this is where many solutions fall short. Your disaster recovery solution must be able to recover your data every time and on time. When ransomware hits, you want to be confident you can recover your data and get on with business as soon as possible.

Check out this step-by-step guide to creating a disaster recovery plan as a good starting point.

Final Thoughts

There is no perfect defense against ransomware. The best approach is a multilayered one that includes educating your staff and investing in data resilience, including reliable data backup, disaster recovery, and immutable storage solutions. And it includes having a robust disaster recovery plan. That's how you can stay ahead of this growing threat and protect your data and bottom line.

To learn how Arcserve can help you prevent the consequences of ransomware, talk to an expert Arcserve technology partner.

Why Your Organization's Cybersecurity Strategy Should Be Built on Backups, High Availability, and Immutable Storage

You may be asking yourself what data backup, high availability, and immutability have to do with cybersecurity strategies. In a word, everything. These data protection components give you a rock-solid foundation for a comprehensive cybersecurity strategy that protects you from a wide range of cyber threats. They also reduce the impact of security incidents and ensure business continuity.

Backups Are the Foundation for Data Disaster Recovery

Data backup solutions create copies of critical data and store them separately from your primary data, preferably offline or disconnected from the primary system, using virtual or physical air-gapping.

That ensures you have a clean copy of your data that you can use for restoration and recovery in case of a ransomware attack, data breach, accidental deletion, or other data disaster. Backups give you a safety net by providing a means to restore lost data and minimize downtime.

Business Continuity Depends on High Availability

Keeping your operations continuously going demands that your data is highly available. That ensures critical systems and services stay up and running, reducing your risk of business disruption and financial loss. But immutability matters most. More on that later.

Massive Data Growth Means More Vulnerabilities

Statista reports that the amount of data created, captured, copied, and consumed globally will reach 120 zettabytes this year. That's why incorporating these technologies and processes into your cybersecurity strategies is essential to safeguarding your ever-growing amounts of data and your systems and operations.

But there are many types of data, including financial records, private customer data, and emails. Statista predicts that 347.3 billion emails will be sent in 2023. That translates into a ton of targets for hackers' favorite entry strategy: infiltrating networks using phishing, malicious attachments, and other social engineering schemes. But that's just the entry point. Once inside your systems, hackers move through servers and critical databases across your network, encrypting files. This is where immutable backups make all the difference.

Immutability Starts With 3-2-1-1

Did you know that when you keep your backups in immutable storage, they are immune to cyberattacks? Immutable backups are copies of data saved in a write-once-read-many-times (WORM) format that unauthorized users can't alter, tamper with, or delete—even if they gain access to your primary and backup systems.

That's why we urge you to follow the 3-2-1-1 backup strategy. The first three digits haven't changed from the traditional meaning: Keep three copies of your data (production data and two backups) on two different media (disk or tape, for example), with one copy kept offsite for disaster recovery.

The last "1" refers to keeping one copy of data in immutable storage where it's safeguarded from malicious attacks, accidental deletions, and any other type of data loss. That makes it a core component of any data resiliency strategy.

Your Last Line of Defense

What about the ever-present threat of malicious insiders? Employees with access to critical information can create a data disaster with a single click. Immutable backups give you a last line of defense by ensuring a usable copy of your data is always available for recovery.

Immutable network-attached storage can deliver continuous data protection by taking low-overhead snapshots every 90 seconds, with each snapshot creating a new object. Each object preserves the image of the file system at the instant the snapshot is taken. Since the underlying objects are immutable, the snapshots inherit that immutability.

Snapshots Simplify Data Backup and Disaster Recovery

Immutability keeps your backups secure, ensuring data integrity by enabling you to compare backups to the original data to validate that it is intact. Using snapshots also makes it simple to go back to specific points in time and recover entire file systems in minutes.

The only way to ensure you can recover from a data disaster is by implementing a sound data resiliency strategy. That includes choosing business continuity solutions that automate disaster recovery testing of business-critical systems, applications, and data on replica servers to ensure data integrity.

It's also worth considering solutions that let you spin up virtual machines (VMs) from backup data that can serve as standbys should a source node fail. Finally, immutable backups can be crucial for compliance with regulatory requirements ranging from POPIA to GDPR.

Get Expert Support

Arcserve technology partners can help you put a sound data resiliency strategy in place that ensures your company can recover from any data disaster—no matter what. You can find an Arcserve technology partner here.

How Immutable Storage Ensures Data Resilience

Virtually every company today depends heavily on data. Data drives decision-making, improves efficiency, and helps you stay one step ahead of competitors. However, you must carefully manage the vast amount of data you collect and store.

Countless regulations and requirements applying to the collection and storage of data must be followed if you are to stay in legal compliance. That can be difficult and often requires specialized knowledge. That's important because the legal and financial consequences of noncompliance can be steep.

Companies worldwide must constantly deal with data protection and security regulations, even as these regulations constantly evolve. You must stay informed and adapt your policies and practices to avoid hefty fines and damage to your reputation.

The European Union's (EU) Digital Operational Resilience ACT (DORA) is one example. This regulation applies to financial institutions, including banks, insurance companies, investment companies, and cryptocurrency service providers. The regulation ensures that these organizations have solid data protection solutions in place.

The challenge is that DORA doesn't only apply to financial institutions. It also applies to all other companies with whom they outsource their technology services, whether inside or outside the EU. That means many companies are subject to the DORA regulation—but don't know it.

Immutable Storage and Compliance

There are a variety of technology solutions you can use to comply with data security regulations. Immutable data storage is one of the most valuable of those technologies. According to TechTarget, one of the critical benefits of immutable storage is its ability to protect against ransomware. Immutability also helps you comply with regulations by giving you a storage system where your data, once written, can't be altered, modified, or deleted.

Solutions like Arcserve OneXafe deliver continuous data protection by automatically creating and storing snapshots. If your primary systems are compromised by ransomware, hardware failure, or other disasters, you can quickly and completely restore your data and return to normal operations. Immutable storage is particularly useful in industries with strict compliance and data regulations, like healthcare, finance, and government.

The immutability of stored data ensures compliance because it ensures the security of your data. Immutability makes it virtually impossible for hackers to damage your operations, even if they gain access to your network. That's because the data snapshots can't be changed, overwritten, or deleted. It also ensures you comply with data retention regulations.

Immutability in the Real World

One example of a company successfully meeting data compliance requirements is Concorde Motorhomes, a manufacturer of luxury motorhomes. The company must retain the historical data of all vehicles it has sold since 1985. Concorde also must ensure that all data relating to a specific vehicle is retained, such as the components used throughout, as motorhomes have an extremely long lifespan and feature extensive customization.

Any data loss would be critical for Concorde and have severe consequences from production to customer satisfaction. That's why the company uses Arcserve OneXafe as an immutable network-attached storage solution that creates snapshots every 90 seconds. This ensures Concorde meets the highest security, scalability, and data compliance levels. And the company can recover quickly from a data disaster.

Cloud Services Simplify Compliance

Another simple and effective way to ensure compliance with data security regulations is to work with a cloud-based data backup and disaster recovery provider. Cloud-based solutions—such as Arcserve Cloud Services—offer scalability and flexibility that traditional backup and recovery solutions often lack. These solutions let your organization quickly expand backup and recovery capabilities without investing in additional hardware or infrastructure.

You should work closely with your cloud provider to stay informed about updates and changes to compliance requirements. A good cloud provider will also help you regularly review and update your backup and recovery strategies to ensure compliance.

Many cloud providers, like Arcserve, offer geographic redundancy, so your data is stored in more than one data center within any given region. Arcserve and other cloud providers also ensure that you can meet data sovereignty or residency requirements—meaning user data is stored in the region where it is generated—as required by the EU's General Data Protection Regulation (GDPR).

You must also understand the shared responsibility model many cloud providers employ. While cloud providers usually take responsibility for the security of their cloud infrastructure, you are responsible for securing your data and applications. But cloud providers also simplify data management, taking care of maintenance and updates so your IT team can focus on strategic tasks, making them valuable partners.

Secure Data Storage Is Crucial to Business Success

Every organization deals with an accelerating feedback loop, where the amount of data generated increases in size and value. That's why hackers are targeting your data with increasing sophistication—think AI—and regulators are imposing ever-tighter rules to protect it.

The good news is that modern data protection technologies can keep up with this cycle, ensure your data is safe, and keep your operations moving.

To help you determine the optimal immutable storage and data resilience solutions for your requirements, choose an Arcserve technology partner. To learn more about Arcserve OneXafe, request a demo.

Enhancing Data Resilience With Deep-Learning Cybersecurity Solutions, Immutable Storage, and Scalable Business Continuity

Data is the pulse of every organization's operations today. If data stops flowing, everything comes to a screeching halt. Downtime is incredibly expensive, too. Recently, MGM Resorts was hit by a cyberattack that one analyst estimates cost the company $8.4 million in daily revenue. Just days before, casino operator Caesars reportedly paid a ransom worth $15 million to a cybercrime group.

But it isn't just large enterprises that are getting hit. Grant Thornton's International Business Report, a survey of midmarket companies, found that nearly half of business leaders cited cyberattacks as a threat to their business in 2023. And research from Techaisle found that 71 percent of midmarket firms experienced ransomware attacks last year.

Deep pockets make a difference, and large enterprises usually can put the resources in place to recover from a cyberattack. But midmarket companies don't have to overspend to have confidence that their data is protected and that they can recover from a cyberattack, ransomware incident, or other data loss. Here's how Arcserve can help your organization get there.

The Unified Data Resilience Platform

Arcserve Unified Data Protection (UDP) software is built on the same three pillars that underpin the Arcserve Unified Data Resilience Platform. Arcserve UDP ensures your midmarket business can count on business continuity. Let's look at these pillars to see how UDP delivers on multilayered data protection.

Prevent

Arcserve UDP is safeguarded by integrated Sophos Intercept X Advanced for Server cybersecurity. That's the first line of defense for defending your backups. Intercept X for Server uses deep learning, an advanced machine learning form that detects known and unknown malware without relying on signatures.

Deep learning makes Intercept X for Server smarter, more scalable, and more effective against never-before-seen threats. And it outperforms security solutions that use traditional machine learning or signature-based detection alone.

Learn more about Arcserve's partnership with Sophos.

Protect

There are plenty of computing and data storage technology options for midmarket companies for computing and data storage. That's why Arcserve UDP protects against data loss and extended downtime across cloud, local, virtual, hyperconverged, and SaaS-based workloads.

You can count on another layer of data protection because Arcserve UDP assures the immutable storage of your data backups with support for Amazon S3 Object Lock in the cloud. Arcserve UDP also delivers off-premises and on-premises data protection when paired with Arcserve OneXafe immutable network-attached storage appliances.

When your backups are saved in immutable storage, they are converted to a write-once-read-many-times format that unauthorized users can't alter or delete. Even if hackers get past your defenses, you can be confident that your immutable backups will be there, ready for recovery when needed.

Recover

Nothing matters more to a business than getting up and running again if your systems are taken down by ransomware, hardware failure, or any other data disaster. That's why the third pillar of the Arcserve Unified Data Resilience Platform is all about recovery.

With Arcserve UDP, you can reduce your downtime from days to minutes. That includes restoring faster with instant virtual machine (VM), bare metal recovery (BMR), and local and remote virtual standby. You can also validate your recovery time and recovery point objectives (RTOs/RPOs) and service-level agreements with automated testing and granular reporting. Add it all up, and it means that Arcserve UDP is the all-in-one solution you can count on for business continuity.

Data Resilience With the Lowest TCO: Built for Midmarket Companies

Like many midmarket companies, you rely on SaaS solutions like Microsoft 365 to keep your business running. Arcserve UDP protects Microsoft 365 workloads, including Exchange Online, SharePoint Online, and OneDrive for Business on-premises. The software also offers deep data reduction, granular recovery, and more.

With IT budgets always a concern, it's important to note that Arcserve is the industry's lowest total cost of ownership (TCO) unified data resilience provider.

By working with an Arcserve technology partner, you can identify your business's best data protection solutions. They'll also work with you to control costs today and into the future and ensure you're ready as threats evolve and technologies advance.

Find an Arcserve technology partner here. And be sure to check out our 30-day free trial offer on Arcserve UDP.

Need Answers?

Arcserve is always here–
standing by and ready to help.

arcserve®

+1 844 639-6792
arcserve.com