arcserve®

Data Protection and Data Resilience In an Evolving World of Cyber Threats

Table of Contents

How to Ensure Data Resilience in the Age of AI

Generative artificial intelligence (AI) is quickly changing the world and making headlines. And businesses of every stripe are embracing its potential, with IDC forecasting that worldwide spending on AI-centric systems will reach $154 billion in 2023 and rise to more than $300 billion in 2026. We think that's a conservative number.

Unfortunately, there's also a dark side to AI that's making headlines. Cybersecurity firm SlashNext recently confirmed how quickly hackers are adopting AI after discovering WormGPT—ZDNet calls it "ChatGPT's malicious cousin"—a tool being promoted for sale on a hacker forum "designed specifically for malicious activities."

Even more frightening, SlashNext conducted tests focusing on business email compromise (BEC) that produced "unsettling" results. WormGPT created a "not only remarkably persuasive but also strategically cunning" email to pressure an account manager into paying a fraudulent invoice. That tells you that a single malicious email can unlock the door to your data, where hackers can encrypt it and then send you the ransomware note. Because your backups are almost always targeted in an attack, they are equally at risk. And fresh on the heels of WormGPT, a new malicious cybercrime AI tool called FraudGPT has shown up on dark web marketplaces.

The new vulnerabilities that AI has exposed demand that you do more to ensure your data is resilient, even in the face of ever more sophisticated attacks. Here are a few steps you should take:

Employ Advanced Cybersecurity Technologies

The best way to fight back against AI is by using AI. That's why Arcserve Unified Data Protection (UDP) safeguards your data with Sophos Intercept X Advanced for Server, a security platform that protects your cloud, on-premises, or hybrid environments using deep learning AI that proactively prevents attacks. It also includes anti-exploit, anti-ransomware, and control technology that stops threats before they can wreak havoc on your systems.

AI is being employed across the cybersecurity landscape because it can quickly analyze and detect unusual activity that may indicate insider threats. AI is also being used to analyze network traffic, identify possible intrusions, and analyze relationships between threats—malicious files or suspicious IP addresses, for example. From your endpoints to your data center and up to the cloud, invest in cybersecurity solutions that leverage AI so they can adapt as the technology evolves.

Implement Zero Trust Cybersecurity

A zero-trust approach to cybersecurity assumes that no entity should be trusted by default, only granting access to what a user needs and nothing more.

A zero trust posture employs identity and access management (IAM) technologies, including multifactor authentication (MFA) and role-based access controls (RBAC). With MFA, two or more verification methods are used to ensure the people attempting to access your resources are who they say they are, while RBAC limits access only to the resources necessary for an individual to do their job.

Biometrics adds another layer of protection against the malicious use of AI. In a recent Cybermagazine.com article, the CEO of digital identity company Incode says, "AI-powered liveness detection comes into play, which ensures the integrity of a biometric match by distinguishing both ID and liveness via AI. The technology uses facial recognition to determine if a biometric sample is being captured from a living subject who is present at the point of capture; in other words, a real, live person behind the screen." While at this point, it isn't clear if biometrics can solve the problem in the long term, it's another step you can take to protect your data.

While these measures may not directly prevent AI from hacking into networks, they put more obstacles in the hacker's path. Learn about the Cybersecurity and Infrastructure Security Agency (CISA Zero Trust Maturity Model here.

Teach Your Team About Cybersecurity

The Verizon 2023 Data Breach Investigations Report found that 74 percent of all breaches include the human element, whether due to error, privilege misuse, stolen credentials, or social engineering.

That's why the SlashNext BEC test described above is telling. You must train everyone on spotting suspicious or malicious emails and websites and how to avoid helping hackers overcome your defenses. Regular testing keeps everyone on their toes, especially when the results of a successful test attack are shared with the entire team so everyone can learn from the experience. Most importantly, ensure everyone knows where to turn if they are unsure if a threat is present.

Use Immutable Backups

For now, immutable storage is one of your best defenses against AI-driven attacks. For example, the Arcserve OneXafe network-attached storage file system is based on an immutable object store, with every object written only once and never modified.

Any modification you make to the file system always creates a new object, delivering continuous data protection (CDP) by taking low-overhead snapshots—a view of the file system at the instant the snapshot is taken—every 90 seconds.

Since the underlying objects are immutable and cannot be changed, the snapshots inherit this immutability so that an external source can't change or modify it. Indeed, hackers are very likely working on overcoming immutability using AI, but it's one more weapon you can put in your arsenal today as you fight back.

Talk to a Data Resilience Expert

Arcserve technology partners have the expertise and experience to help you figure out the best way to achieve data resilience within your organization. Find an Arcserve technology partner.

The Seven Stages of Cyber Resilience (and How a Service Provider Can You Survive and Thrive)

Data is the beating heart of every modern-day enterprise, from large corporations to small and medium-sized businesses (SMBs). For many, data is by far the most valuable asset they own, with one survey finding that 99 percent of Fortune 1000 firms are investing in data and AI initiatives. If these companies lose access to their data due to a cyberattack or natural disaster, it can bring their operations to a screeching halt. The results aren't any different for SMBs. That's why data resilience is now a critical necessity for every business.

Resilient organizations implement processes that enable them to quickly bounce back from any situation in which their data is compromised. But only some organizations are resilient. Most SMBs aren't. A recent global survey by Arcserve revealed that only 23 percent of small and midsize organizations have mature data resilience strategies with associated goals they can use to track progress.

That isn't ideal, but it is understandable. As an SMB, you'll likely be laser-focused on your day-to-day operations. Your team may well dedicate almost all its time to running the business, managing marketing and sales, serving customers, and staying on the right side of tax collectors. This focus works great for achieving your business goals but limits your ability to handle additional tasks like cybersecurity.

Keeping Your Business Running In Real-Time Should Always Be Your Top Priority

As an SMB, you already know about cyber threats. But you may think it's just larger businesses in the crosshairs of attackers. The reality is that threat actors are not selective based on industry or company size. They target every potential victim, regardless of how small or large your company may be. No one is immune to the threat of cyberattacks—and the sooner you realize it, the better off you'll be.

The Seven Stages of Cyber Resilience

The "seven stages of grief" refers to the psychological process individuals typically go through when experiencing profound loss or bereavement, including shock, denial, anger, bargaining, and depression. Applying the "seven stages of grief" to SMBs dealing with data protection issues looks something like this:

1. Shock and Denial

This is when an SMB first becomes aware of the potential risks to its data. The organization might be shocked to learn about the extent of the potential damage and the various threats. There might also be some denial, as the SMB may initially find it hard to believe such threats could impact their business so seriously.

2. Pain and Guilt

As SMBs begin to understand the gravity of the situation, they may feel pain from potential losses or damage to their business. They may also feel guilt, particularly if they haven't taken data protection seriously in the past, potentially exposing their business to unnecessary risk.

3. Anger and Bargaining

The SMB might feel anger toward the circumstances that have led to the data threats, such as cybercriminals or past negligence. The SMB may also start bargaining or looking for quick fixes to protect data, which might lead to ineffective strategies.

4. Depression

Realizing how much effort and resources are required to protect their data may lead to feelings of depression. The SMB may feel overwhelmed by the complexities of data protection and the potential impact of data loss on their business.

5. Upward Turn

As SMBs start to take concrete steps to improve their data resilience, things start to look up. They may begin to see that, although the process is complex, it is manageable and within their capabilities. The first step, for instance, is determining the critical operating systems. There are those that, if compromised, will cause a minor disruption. But some will stop the entire business in its tracks, perhaps even put them out of business. SMBs can start by determining where their critical data is stored and which systems are needed for their businesses to function effectively.

6. Reconstruction and Working Through

During this stage, the SMB is actively working on its data protection strategies. It is implementing new measures, improving its systems, training its staff, and generally doing the work needed to improve data resilience. For instance, the SMB can beef up its backup and recovery processes by storing data copies in separate locations to mitigate data loss from events like a cyberattack. Read up on this subject and the 3-2-1-1 backup strategy in this blog post.

SMBs can also implement immutable data storage, which safeguards information by taking snapshots every 90 seconds. So even if ransomware does sneak through and data is overwritten, the information will still be easily recoverable to a recent point in time.

7. Acceptance and Hope

Finally, the SMB accepts the importance of data resilience and the effort required to achieve it. When the proper controls and alerts are in place, the SMB is in a much better position to prevent unauthorized access and remedy unexpected incidents. The SMB also has hope for the future, knowing it is better prepared to handle data threats and recover from potential data loss.

The Value of a Service Provider

If you're like many SMBs, your focus is almost entirely on your day-to-day operations. That's frequently an absolute necessity. That's why it makes sense for you to consider collaborating with a specialized service provider with expertise in data backup, cybersecurity, and data resilience.

Partnering with a service provider that knows best practices and works with best-in-class vendors will complement your internal IT knowledge and ensure a solid and effective data resilience plan. This proactive approach is crucial, as you may only know some regulations you must follow.

Engaging a Service Provider Ensures That You'll Be Informed and Compliant

Cost and affordability are, of course, among your most significant concerns. While Fortune 1000 organizations may be able to dedicate personnel or entire departments to cybersecurity and data backup roles, that may be out of the question for your company.

But by working with a service provider, your SMB can cost-effectively access the best practices and expertise you need. And you can focus on your core operations and growth while entrusting resilience and recovery strategies to a knowledgeable professional.

Considering the stakes involved, allocating a budget to data resiliency is crucial, even if it's a modest amount. That's precisely what Fortune 1000 companies are doing. Service providers and specialized vendors now offer solutions that let you start small and scale as your business grows. You don't necessarily need a massive upfront investment. With the right tools and practices, you can establish a solid and updated data resilience plan with a smaller footprint, ensuring you're well-prepared for potential incidents at a price you can afford.

Arcserve Partners: Expert Service Providers Ready to Help

Arcserve technology partners can remove the burden of ensuring cyber resilience from your internal teams and let you focus on success. You can find an Arcserve partner here. To learn more about Arcserve products, contact us.

Ensuring Data Resilience: The Importance of Orchestrated Recovery, Preparedness, and Testing

In a recent independent global study commissioned by Arcserve, 41 percent of respondents said their organization's disaster recovery plans weren't updated.

A recent article from SolarWinds says the cost of downtime these days runs from $427 per minute for small businesses and $9,000 per minute for larger enterprises.

But the same article says that your industry has a considerable impact on downtime cost, ranging from $90,000 per hour for media to a whopping $6.48 million per hour for the brokerage service industry. Regardless of where your business falls on that spectrum, ensuring your data is resilient and recoverable matters most. Because the costs of not doing so are high.

Data Resilience Depends on Orchestrated Recovery

You need a well-defined disaster recovery (DR) plan and the right tools to minimize downtime due to a disaster or cyberattack.

The most effective approach to mitigating the cost of downtime due to a disaster or a cyberattack is investing in an orchestrated backup and recovery architecture that ensures data resilience and keeps your operations running.

That's why the same Arcserve study noted above found that 77 percent of IT decision-makers are now investing in orchestrated recovery architectures. And that's good news because backup and recovery are fundamental to any data resilience strategy.

Testing, Orchestration, and Preparedness: Three Vital Elements of Data Resilience

All kinds of variables and unknowns can come up during an incident. Sound backup and DR policies will ensure you are prepared—but only if you include a regular testing program in your policies.

With DR testing, you can identify and document the procedures necessary to restore your operations and systems if an incident occurs. Once documented, you can validate your processes and fix potential gaps from policy and personnel perspectives. Testing is the only way to make sure that gets done.

Another component of data resilience is orchestration, where automation accelerates end-to-end recovery. With orchestration, your interconnected systems are recovered in the optimal sequence for meeting your requirements. Orchestration also identifies any intermediate steps you must take for validation at each stage, ensuring a smooth and orderly restoration.

Although we bring it up last, preparedness should be your highest priority. With 74 percent of breaches involving the human element, you need to train your employees so they can spot suspicious emails and attachments and avoid malicious websites. Testing should also be part of this process so employees can learn from others' experiences.

RPO, RTO, and Acceptable Downtime

You already have plenty on your plate. That can sometimes mean backup and recovery aren't given the priority they should. That's why you must conduct regular backup tests—quarterly, annually, concurrent with changes in systems or the organization, or more frequently, depending on your situation. Best practices dictate that setting a calendar for disaster recovery testing is crucial so you're ready for a disaster anytime.

Your comprehensive data resilience strategy must address two vital thresholds: recovery time and recovery point objectives (RTOs and RPOs).

Your RPO determines the amount of data loss your organization can tolerate in an incident. It is the primary driver of your backup frequency, whether every hour, once a day or week, or as often as every 90 seconds, as Arcserve OneXafe network-attached storage offers with its snapshot feature.

Your RTO determines how long your organization can tolerate being down before your systems are recovered, and your operation is fully functional following an incident.

An Arcserve-commissioned independent study found that 83 percent of respondents said that 12 hours or less is an acceptable level of downtime for critical systems before there is a measurable negative business impact. But only 52 percent said they could actually meet their recovery time objective (RTO). So nearly half will experience a measurable negative business impact from downtime.

The Arcserve study results highlight the gap between expectations and actual capabilities. That's why you must improve your data recovery capabilities to meet your RTOs and RPOs. Closing this gap will help you mitigate the impacts of data loss and minimize downtime.

Preparation Is the Priority

With more businesses being targeted by cyber threats and ransomware, being prepared means being proactive. That includes understanding potential threats, mitigating risks, and developing strategies for recovery.

A proactive stance can help you withstand any disaster.

Get expert help to put an effective data resilience strategy and backup and disaster recovery plan in place by talking to an Arcserve technology partner. Find a partner here.

How to Protect Against Ransomware With a 3-2-1-1 Strategy

A quick Google News search on the term "ransomware" today brought up headline after headline about new ransomware strains, ransomware gangs, and companies that had recently been attacked. That aligns perfectly with the Sophos State of Ransomware 2023 report finding that 66 percent of surveyed organizations say they were hit by ransomware in the last year. And the costs are high, with the IBM Cost of a Data Breach Report 2023 finding that the global average cost of a data breach is $4.45 million.

It doesn't matter whether your company is large or small—or what industry you're in. It's only a matter of when, not if, you'll be facing an attack. Fighting back demands a data resilience strategy that ensures you can recover your data, even if you fall victim to a ransomware attack.

Backups Are a Target

A recent article in CIO and Leader explains that hackers target backups because they recognize that doing so makes it challenging, if not impossible, for you to recover. Once hackers breach your primary data or backups, they could have free rein to broaden their attack across your systems. That's why the 3-2-1 backup rule, coined initially by photographer Peter Krogh in his book about digital asset management, is no longer enough.

The rule says you should keep three copies of your data—one original and at least two copies—on two different types of media (network-attached storage, tape, or a local drive, for example)—with one copy stored offsite in the cloud or secure storage. That strategy won't fly anymore because if hackers get to your primary data, they'll likely try to get to your backups. And if your backups aren't available to you, the costs of downtime, damage to your reputation, and recovery can destroy a business.

Complete Ransomware Protection Demands Immutable Backups

For those reasons, Arcserve advises following the updated rule: 3-2-1-1. The meaning behind the first three digits hasn't changed. But that added "1" makes all the difference, and it means one backup copy of your data must be immutable. Immutable backups are saved in a write-once-read-many-times (WORM) format that can't be altered or deleted, even by hackers or admins.

For example, Arcserve OneXafe employs a file system based on an immutable object store, with every object written only once. Any modifications you make to your file system result in new immutable objects being created. There isn't any way to reverse this immutability.

Even if hackers get their hands on compromised admin credentials and gain full access to your network, immutability makes it harder for them to delete your copies or alter the data's state. The bottom line is that you won't have to pay a ransom to recover your data and get your business back up and running if you're attacked.

Expert Help is a Click Away

Arcserve technology partners can help you put an effective 3-2-1-1 strategy in place that fits your business. You can find an Arcserve technology partner here. To learn more about Arcserve products, check out free demos.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com