arcserve®

Cybersecurity, Data Protection, and Disaster Recovery: Ensuring Business Continuity for Your Organization

Table of Contents

Employing Effective Cybersecurity Solutions for Data Protection Against AI-Assisted Attacks

Cyber risk provider IT Governance says over 6 billion records were compromised through November 2023. IBM's 2023 Data Breach Investigations Report found that 83 percent of breaches involved external actors. The immediate future doesn't look bright either because those statistics mostly predate the arrival of new artificial intelligence (AI) applications like ChatGPT.

Hackers are now using AI to increase the frequency and severity of their attacks. Empowered by easy-to-use AI tools, even many newbies are even jumping in to try their hand at cybercrime. Black hat wannabes with zero coding experience can now grab off-the-shelf AI tools and create and deploy malicious software relatively easily.

All it takes is one individual with bad intentions to quickly develop and unleash malware that can wreak havoc on your company. These readily available AI tools empower even unsophisticated actors to execute denial-of-service attacks, create phishing emails, and launch ransomware. These attacks can be run simultaneously from systems spread worldwide, making it nearly impossible for human operators to manually detect all the attacking systems accessing their websites and portals.

Fight Back With AI-Driven Cybersecurity Solutions

There is good news. AI and deep-learning technologies give you potent weapons in the fight against cybercrime. AI-driven security solutions with self-learning capabilities can proactively respond to emerging threats and protect against a wide range of threats like ransomware and malware, effectively empowering you to fight back.

These solutions, such as Sophos Intercept X Advanced, can detect anomalies and patterns indicative of malicious behavior and stop attacks before they can cause harm. This intelligent approach to data protection reduces your reliance on reactive measures and allows you to stay a step ahead of cybercriminals.

AI and deep-learning systems can adapt and evolve to counter emerging threats, learn from previous incidents, and continuously improve defense mechanisms. By leveraging techniques like transfer learning, these systems can update their knowledge bases with the latest threat intelligence and ensure greater data resiliency against future attacks.

These systems can also take proactive, automated actions based on predefined rules or learned behavior. For example, when a security breach or anomaly is detected, the system can automatically trigger measures like isolating affected systems or blocking suspicious traffic.

This automated response cuts the time between detection and remediation, minimizing the potential impacts of a cyberattack.

AI In the Real World

One example of AI in action is the well-known threat in the cybersecurity world called remote access Trojan (RAT). A RAT can be embedded into a simple email attachment, such as a JPEG image, allowing cyber attackers to gain unauthorized access to your systems. Since the IBM report also found that 74 percent of breaches involved the human element, this is a common scenario.

Antivirus engines typically detect RATs based on their signatures and then distribute an alert to all endpoints to identify and remove the RATs. However, attackers can easily modify RATs—even slightly—to generate a different signature and evade traditional signature-based detection.

AI and deep learning technologies are crucial to fighting back. Instead of relying solely on static signature matching, modern cybersecurity tools powered by AI can analyze the behaviors of files and processes. They can observe whether a file is executing specific actions or installing software. They can flag suspicious behavior and prevent potentially malicious actions by learning and recognizing patterns in these activities.

Ensuring your data protection solutions employ this approach gives you more effective defenses against emerging threats. Attackers are constantly developing new methods to evade conventional cybersecurity measures, so you must keep pace with these changes by taking a proactive approach.

AI's Evolution Continues

When you implement AI and deep learning tools, it's essential to consider the challenges they may bring. While the benefits of AI are clear, mistakes can still occur because it is quickly evolving. Sometimes, AI may misinterpret what is happening, disrupting data or system availability.

These disruptions could occur if AI detects what it thinks are illegal activities. For example, AI tools often work with a reliability score, triggering a response from your organization if the score falls below a preset threshold. If that happens in error, the result is costly unplanned downtime. As an evolving technology, AI can't guarantee perfection, and the threat of errors will always exist. Regardless, AI will continue to improve its ability to distinguish real threats from other events.

Getting Started With AI

While many companies are excited by AI's potential, most don't know where to start. The easiest way to leverage the benefits of AI is by working with a reliable security solution provider well-versed in deep learning and AI. Your vendor of choice should already incorporate AI into its products, as is the case with Arcserve Unified Data Protection (UDP) software. That way, you can realize the benefits of AI immediately.

As the technology evolves, watch for more advances in data protection solutions that leverage AI and deep learning. In the meantime, strengthen your defenses by working with a solution provider with readily available AI-powered tools you can use to neutralize cyberattacks and protect against data loss.

For expert guidance in implementing AI-driven data protections, choose an Arcserve technology partner.

Request a demo to learn more about the AI and deep-learning data protections included with Arcserve UDP.

Why Management Buy-In to Cybersecurity Solutions and Strategies Is Essential

Cybercriminals are threatening every business. The average cost of a data breach is now $4.45 million, according to the IBM Cost of a Data Breach Report 2023. And Statista found that 6.41 million data records were leaked in worldwide data breaches in the first quarter of 2023.

These statistics should make any business leader take notice and act. Unfortunately, many still don't take a practical, hands-on approach to cybersecurity solutions and data breach protection. Many aren't even aware of their business's data disaster recovery strategies and plans.

Vulnerabilities Directly Threaten Business Continuity

That may surprise business leaders who are directly involved, given that threats like ransomware continue to increase. As attacks increase in sophistication and frequency, leaders must recognize their central role in ensuring data and business resiliency. Without active involvement, the risk of a reactive rather than proactive approach to cybersecurity grows. That increases the business's vulnerability and directly threatens its ability to continue to operate if faced with data loss and the associated financial impacts of a data breach.

Why does this knowledge gap exist? Historically, many managers preferred to stay clear of the technical aspects of their business. Data disaster recovery was viewed as an IT responsibility rather than an essential pillar for ensuring the business's prosperity. But ignoring data backup and disaster recovery isn't an option anymore. Leaders who fail to get involved in the planning and executing of business continuity plans risk the very existence of their business.

Why Management Buy-In Matters

Getting your CEO involved in business continuity planning is crucial for several reasons. First, leaders set the tone for their company's priorities and values. They clearly communicate its importance by actively participating in discussions and decisions relating to data protection strategy. That kind of leadership promotes a culture of responsibility and accountability throughout the organization.

CEO buy-in is also vital for securing the resources required to implement data protection strategies. Data protection and disaster recovery demand investment in technologies, staff training, and infrastructure. When management actively supports these initiatives, it helps ensure that cybersecurity is a priority throughout the company.

CEO and management buy-in is also essential because these leaders bring in-depth knowledge of the company's core functions, critical data, and key stakeholders. That knowledge is necessary for identifying potential risks and vulnerabilities. And it is crucial for creating an effective, robust disaster recovery plan that addresses overall business objectives within a framework that monitors evolving threats and adapts as needed.

Regulatory compliance is another critical consideration. Many sectors are subject to strict data protection regulations, such as the EU's General Data Protection Regulation (GDPR). These regulations impose specific requirements for protecting sensitive information and deliver severe penalties for non-compliance. By actively participating in developing and testing disaster recovery plans, business leaders can ensure their business stays compliant.

Get Business Leaders Engaged

So, how do you ensure your business leaders and senior managers are involved in these endeavors?

One way is to promote awareness by holding regular training sessions to keep everyone updated on evolving threats and the importance of data backup and disaster recovery planning. These sessions should emphasize the potential impacts on operations and the essential nature of planning and data protection strategy to minimize risks. These sessions also provide senior leaders with the information they need to make informed decisions based on a clear understanding of the risks they face.

A dedicated cybersecurity committee or working group—driven by management—can also facilitate active participation and the continued development of effective policies. This committee ensures that security measures are integrated into the organization and aligned with the company's overall objectives. Incorporating disaster recovery and cybersecurity considerations into strategy planning sessions and regular board meetings further highlights the importance of cybersecurity, data protection, and business continuity at the highest decision-making level.

Access External Expertise

Collaborating with external experts and participating in strategic events can give management valuable insights and establish benchmarks for measuring progress. Bringing in external perspectives keeps everyone informed about emerging threats and industry best practices. Consistently executing exercises and simulations ensures you are actively testing your organization's threat-resistance capabilities and identifying areas that need improvement.

Active participation in disaster recovery planning fosters an authentic culture of data resilience. By emphasizing the importance of data protection and preparedness, leaders can ensure their business thrives, even in the face of disaster.

For expert help with all your data protection, backup, and disaster recovery needs, choose an Arcserve Technology Partner.

A Four-Pronged Data Classification Strategy for Effective Data Protection, Retention, and Storage Optimization

Statista predicts that the data created, consumed, and stored globally will reach 180 zettabytes by 2025. Handling the growing amounts of data your business generates—and avoiding pitfalls and problems scaling to meet that demand—requires a well-defined data classification strategy so you can make informed decisions regarding data storage, access, and sharing.

Not all data is equally valuable. By classifying data based on attributes such as sensitivity, value, and whether it is subject to governance, risk, and compliance (GRC) requirements, you can establish clear, efficient guidelines for how long each data category should be stored and retained.

For example, sensitive customer information may require extended retention periods due to regulatory requirements, while non-critical operational data might require shorter retention periods. Ultimately, sound data classification enables you to reduce storage costs, minimize clutter, and ensure compliance. For your reference, the ASEAN Data Management Framework stipulates in its guidelines that data management policies should clarify to internal and external stakeholders how your organization handles data to internal and external stakeholders.

The Consequences of Ineffective Data Classification

You could expose your business to significant risks if you don't have a solid data classification system. Here are some examples:

- Inability to differentiate between critical and non-critical data means your storage resources could be overloaded with redundant or outdated information, wasting precious IT budget.

- Without proper classification, your business may struggle to identify data subject to retention requirements, leading to noncompliance and potential legal repercussions.

- Poor data classification often translates to poor data security management. Without clear guidelines on handling data, your employees and partners may inadvertently mishandle sensitive information, ignore encryption protocols, share it with unauthorized users, and store it on devices that aren't well secured.

One major obstacle to establishing effective data classification policies is the sheer volume and diversity of data generated across your business operations. Data may also be stored in different formats, file types, and locations. That makes the process more complicated and can lead to misclassification. Finally, a lack of employee awareness and training regarding the importance of data classification can also slow adoption.

Four Steps to Effective Data Classification

With that in mind, here is a data classification guide that can help you ensure easier access, enhanced security, and improved decision-making:

1. Establish a Cross-Functional Team

Assemble a task force involving IT, data management, legal, and compliance experts to define clear data classification criteria that ensure your classification system meets regulatory requirements and supports business goals.

2. Invest in Automation

Data management and classification tools and solutions that automate the process can scan and analyze data to assign appropriate labels and tags based on predefined rules. Automation offers many advantages, including dramatically reducing the potential for human error—a common problem in manual classification efforts.

The result will be higher accuracy in data classification and a reduced likelihood of sensitive information being mislabeled or improperly handled. Finally, automation ensures a consistent classification standard across diverse data sources and types, eliminating discrepancies arising from human interpretation or judgment variations.

3. Invest in Training and Awareness

Educating your employees regarding the importance of data classification, the potential risks of mishandling data, and proper procedures for accurately classifying data is vital. Doing so enables you to foster a culture focused on responsibly handling data throughout your organization.

4. Adopt a Dynamic Strategy

Data classification isn't a one-and-done deal. It's an ongoing task that demands continuous monitoring and adjustment. Your business—and the world—doesn't remain static, nor does your data. Proper classification requires periodic reviews and updates to accommodate changes in data types, regulatory requirements, and business needs. Regular audits and assessments can identify areas where classification may have deviated from standards or when new data categories have emerged.

An effective data classification strategy empowers your organization to harness the true potential of its disparate data and replace chaos with clarity.

Protect Your Data Properly

Because Arcserve offers the broadest set of best-in-class solutions to manage, protect, and recover all data workloads, from SMB to enterprise, regardless of location or complexity, you can count on finding a solution that cost-effectively covers every data classification type.

To learn more about Arcserve data protection solutions, choose an Arcserve technology partner.

Business Continuity Matters Most: 7 Crucial Questions to Ask Your Disaster Recovery as a Service Provider

An ITIC study found that downtime costs exceed $300,000 per hour for small, medium, and large enterprises. The same report noted that 44 percent of responding mid-sized and large enterprises said that a single hour of downtime can cost upward of $1 million. If your business hasn't paid this price yet, it likely will at some point. The Uptime Institute's Annual Outages Analysis 2023 found that 78 percent of respondents had an outage (i.e., downtime) in the past three years.

With the odds stacked against you, preventing downtime is a paramount concern for IT pros. That explains why Markets and Markets projects the disaster recovery as a service (DRaaS) market will grow from $10.7 billion in 2023 to $26.5 billion by 2028.

These growing investments in DRaaS make sense when balancing risks against costs because they help your organization recover its IT systems and data quickly. Calculating what downtime and data loss would cost your organization easily makes the financial case for DRaaS.

The best DRaaS cloud solutions provide data backup and protect on-premises business systems and data. They also ensure recovery even if you experience a sitewide disaster that destroys your on-premises and offsite backups. Many choices are available today, so what should you look for in a DRaaS solution? Here are a few questions you can ask cloud solution providers to help you make the right choice for your business.

1. Does your solution support my recovery point and recovery time (RPO/RTO) objectives?

Your RPOs and RTOs are vital metrics that define how much data your business can afford to lose and how much downtime it can handle before the damage becomes too great. Arcserve Cloud Services, our cloud-based DRaaS solution, delivers total business continuity and ensures you can get critical business systems back online quickly and easily.

With Cloud Services, you can meet your unique recovery requirements while enjoying access to data anywhere, anytime, with instant failover to a secure, fault-tolerant business continuity cloud. It also offers the resilience and elastic scalability to adapt to continuously changing business continuity requirements in real time.

2. Can I customize the solution to fit my needs and budget?

Arcserve Cloud Services offers three service levels that provide preconfigured retention settings or allow you to customize your setup to meet your RPOs and RTOs. While default settings are three daily and two weekly retention points, 20 more retention points are available at no additional cost. So, you can customize your backup strategy by adding more daily, weekly, or monthly recovery points. Choose the service level based on your needs and enjoy low costs, control over cloud settings, and predictable monthly pricing.

With Cloud Basic, you get secure offsite storage of critical business backups with a complete system restore via a bare metal restore (BMR) drive. With Cloud Plus, you get everything in Cloud Basic, adding immediate file and folder recovery from the cloud. And with Cloud Premium, you also add fast virtualization of your systems and data in the cloud.

3. Is protection from data loss, hackers, ransomware, and other threats included?

Arcserve Cloud Services is built over an enterprise-grade, secure, and redundant cloud infrastructure. The solution is housed in one of the world's most secure and energy-efficient facilities, with layered security, built-in redundancy and fault tolerance, and controls that strictly limit access to your data.

When paired with Arcserve's backup and recovery solutions, Cloud Services ensures complete and reliable business continuity, even if you're hit by ransomware or other attack vectors. You can replicate backup images from Arcserve OneXafe appliances, ShadowXafe, or ShadowProtect software to Cloud Services to keep your business running no matter what because your data is always fully recoverable.

4. Do I have to pay additional fees to recover my data?

Many DRaaS providers charge for data recovery. Not Arcserve. Cloud Services includes 30 days (720 hours) of free virtualization per machine per year. That means you can frequently test your business continuity plan to ensure you are always prepared and recover when needed without worrying about a hit to your budget.

5. Is it easy to manage data protection and disaster recovery?

The Arcserve self-service cloud portal lets you centrally manage your cloud backup and recovery solution anytime, anywhere. The portal dashboard shows the status of all accounts, machines, seed drives, BMR drives, virtual machines (VMs), and account space used.

Cloud Services lets you set individual account alerts to notify you when uploads become inactive or data growth exceeds established thresholds. You can also set alerts to notify you when new machines are added or deleted, VMs are running, and seed and BMR drives request updates. And if disaster strikes, you can fail over without third-party intervention.

6. Does the solution offer one-click failover and orchestrated recovery?

Use Virtual Machine Policy, available with Cloud Premium, to configure your mission-critical systems' recovery sequence, order, and timing. Cloud Services also offers the unique—and patented—ability to test or start site-wide failover processes by pressing a single button.

7. Do you offer advanced networking support?

With Cloud Services, you can customize your recovery network firewalls and update your recovery networks through Open VPN or IPsec to enable site-to-site, single-user, or virtual private network (VPN) connections.

Advanced networking features include:

- Port forwarding
- Port blocking
- Network control options such as DHCP
- Independent and isolated recovery networks
- Static public and private IP address reservations
- Dynamic private IP address available at the time of a disaster
- Flexible and custom VPN configurations

Arcserve Technology Partners: The DRaaS Experts

Arcserve's partners are data protection experts who can help you put the optimal DRaaS solution in place for your business.

Choose an Arcserve Technology Partner.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com