arcserve®

Data Protection Trends and IT To-Do's for 2023

Table of Contents

Four Data Protection Red Flags You Should Be Prepared for in 2023

Data is now the lifeblood of every organization. Without access to critical data and systems, your organization can't keep up with your competition. If you're a business or technology leader, you must stay up to date on the latest threats to your data and the tools you can use to protect it.

Here are four red flags to watch for as you address how your organization secures and manages its data in 2023 and beyond.

1. A Massive SaaS Outage Will Serve as a Wake-Up Call

We could see the first significant software-as-a-service (SaaS) outage in 2023. If that happens, every organization will quickly realize that data backup and recovery needs to be front and center. Companies worldwide increasingly rely on SaaS instead of running their own on-premises IT infrastructure. If a SaaS application suffers a major outage—as with Microsoft Teams earlier this year—you need to understand that most vendors guarantee their services but not the availability of your data. That's on you, as outlined in the shared responsibility model.

The 3-2-1-1 data protection strategy says you should have three backup copies of our data on two different media, such as disk and tape, with one of those copies located offsite for disaster recovery. The final one in 3-2-1-1 stands for immutable object storage. Immutable object storage is a next-gen data security tool that continuously safeguards your data by taking a snapshot every 90 seconds. That guarantees you can quickly recover, even if a significant SaaS outage hits you.

2. Cost Cutting Will Do More Harm Than Good

With spiraling energy prices and runaway inflation, your company is likely looking at cost optimization in 2023. One area you can't afford to cut back on is your data protection efforts. Even as you rethink your operational expenditures to address higher costs, you still need to invest in protecting, storing, and backing up your data.

Data protection may look like an easy place to trim your budget. But those savings could quickly be overshadowed by a single data breach. The most recent IBM Cost of a Data Breach Report found that the average cost of a breach is $4.35 million. In 2023, it will be essential to recognize the importance of your data protection efforts and make sure any budget cuts don't impact business operations.

3. Security Budgets Must Be Allocated Wisely

Regardless of the extent of cyber and other threats to your data, some companies will do some belt-tightening in security. If you do, be aware that this is when the bad guys tend to pounce. Cyberthieves are always looking to exploit vulnerabilities, so a smart approach to budget allocation is in order.

If your company is like most, you invest in basics like firewalls, antivirus, and intrusion-detection solutions (IDS). But beware. Cybercriminals inevitably penetrate those defenses—at least once. You need to plan for that eventuality and allocate some of your security budget for solutions that help with data backup and recovery if a successful cyberattack strikes.

4. Scope 3 Reporting: A Cloud Competitive Advantage

In many countries, big companies are asked to report their CO2 emissions and do their part to slow climate change. The problem is that there are no global standards for this reporting—companies are measuring their emissions in various ways, making it hard to track and compare performance. And most only report emissions that they directly produce, such as when offices are heated. These are called scope 1 and scope 2 emissions and are just a fraction of the global total.

Most emissions are in scope 3, produced by the activity of all the participants in a company's supply chain—currently and in the future. Scope 3 emissions are massive, and they mostly go unreported. This blank spot makes it easy for companies to claim they'll be net-zero businesses by 2050 because they don't have to report all the CO2 their supply chains produce.

In 2023, the pressure will be on cloud companies to accurately track their scope 3 emissions or risk greenwashing—being called out for deceiving their customers into believing they are environmentally friendly when they aren't. If your company wants to do its part, it makes sense to seek out partners that accurately report their scope 3 emissions and demonstrate that they are good corporate citizens.

Plan for Better Data Protection in 2023

In today's ever-accelerating and ever-more unpredictable world, business challenges are getting harder to fully comprehend and solve. Data protection is one of these challenges. If your company commits to staying on top of trends while implementing the innovative tools and strategies you need to protect your data, you can move forward into 2023 with confidence.

For help choosing the right data protection solution for your business, choose an expert Arcserve technology partner. And see for yourself what our solutions can do with our demos on demand.

4 Crucial Data Protection IT To-Do's for a Happy 2023

It's time for resolutions. As we send our best wishes to every IT pro around the world, we'll raise a toast in the hope that we can all enjoy a more secure and relaxed 2023. Of course, hopes and wishes will get you nowhere when it comes to avoiding data disasters.

With that in mind, here's a quick recap of some key statistics from 2022 and what you should do about them. They should motivate every IT team to do more to ensure more effective data resilience, data protection, and disaster recovery in 2023.

1. Educate Everyone About Cybersecurity

The Verizon 2022 Data Breach Investigations Report found that 82 percent of breaches involved the human element, including social attacks, errors, and misuse. The report also found that ransomware attacks increased more over the year of the study than in the previous five years combined. And, while a bit out of date, Cisco's 2021 Cybersecurity Threat Trends report found that 70 percent of organizations had users that were served malicious browser ads.

Those statistics illustrate that your people are your first defense in building a more resilient organization. You get a big thumbs up if you already have an ongoing cybersecurity training program. The onset of the new year is the perfect time to ensure it's effective and up to date. If you don't have a training program, now is the time to get one going.

There are plenty of managed service providers and consulting firms that offer these programs. You'll also find a wealth of ransomware prevention and cybersecurity training materials for technical and non-technical audiences, including managers, business leaders, and technical specialists, at the Cybersecurity and Infrastructure Security Agency's (CISA) STOP RANSOMWARE website. No matter how you approach it, make sure your people can spot a scam and know what to do when it happens.

2. Update and Test Your Disaster Recovery Plan

Suppose your disaster recovery plan isn't up to date and hasn't been tested recently. In that case, some—or all—of your data could become irretrievable should a ransomware attack or data breach succeed. So, pull

out your plan and ensure it meets your needs today and in the future. You may find this post, A Step-by-Step Guide to Creating a Disaster Recovery Plan, valuable as you check each box and validate your plan. Once it's updated, test it. Then put a schedule in place to regularly revisit the plan, test it again, and confirm it will still meet your needs.

3. Tighten Your Cybersecurity Defenses

Every day, the AV-TEST Institute registers more than 450,000 new malware programs and potentially unwanted applications (PUAs). SonicWall's 2022 Global Cyberattack Trends found that between January and June of 2022, its customers faced 3 trillion intrusion attempts, 57 million IoT malware attacks, and 4.8 million encrypted threats. That's a lot of threats! At the same time, the (ISC)2 Cybersecurity Workforce Study found a global cybersecurity workforce gap of 3.4 million people.

With that in mind, it's time for every organization to increase its investments in people with cybersecurity expertise and leading-edge prevention technologies. Difficulties in hiring internal IT teams can be overcome by looking to outside partners for help. Many service providers, value-added resellers (VARs), and system integrators can provide expert guidance, ongoing services, and support to ensure your defenses are effective and up to date.

For internal teams, the National Institute of Standards and Technology (NIST) offers courses for executives, managers, and IT staff. These courses follow the NIST Cybersecurity Framework, teaching students how to align and prioritize cybersecurity efforts with business requirements, risk tolerances, and resources.

4. Focus on Data Resilience

The Information Systems Audit and Control Association (ISACA) writes that a "non-vendor-related" definition of data resilience is "a resilient data system [that can] continue to operate when faced with adversity that could otherwise compromise its availability, capacity, interoperability, performance, reliability, robustness, safety, security, and usability." That's quite a list! ISACA boils it down to simpler terms by stating that "data resilience is data risk management."

Achieving data resilience requires investments that, hopefully, eliminate those risks with activities and technologies, as we've noted above. It also demands solutions that provide rock-solid data protection—including immutable backups—and ensure you can quickly recover during a disaster or any unexpected downtime.

This is where Arcserve technology partners can be a game-changer for you and your company. They bring deep expertise in data resilience and can guide you to the right solution for your specific needs. And they can continue to support you as your needs evolve.

Here's to a More Resilient 2023

While optimism should be part and parcel of every new year celebration, the reality is that securing data in cyberspace can be sobering. So, once the celebration is over, start the new year by working through these four areas and making your organization more resilient in 2023.

Key Takeaways from CISA's 2023-2025 Strategic Plan and How They Apply to Your Business

A recent U.S. News & World Report article listed some of the more notable data breaches in 2022. It includes household names like Microsoft, Uber, and even the Red Cross. Meanwhile, ransomware attacks continue to skyrocket, with 76 percent of respondents to an Illumio study reporting at least one ransomware attack in the last 24 months. Essentially, no matter the size of your organization, you need to be proactive in making your business more resilient.

That's why we read the recently released Cybersecurity and Infrastructure Security (CISA) 2023-2025 Strategic Plan, eager to see how the U.S. government intends to fight back against these threats, helping government and private business entities increase their ability to both prevent and bounce back from attacks. Interestingly, you'll find the word "resilience" appears 30 times in the CISA Strategic Plan.

Important Organizational Attributes and Objectives

In describing the current risk landscape, the plan notes that cyber threat actors use increasingly sophisticated methods to undermine the U.S. economy and democracy, steal intellectual property, and sow discord. CISA also points out that the infrastructures that underpin our National Critical Functions cross multiple increasingly interdependent sectors, with the boundaries between cyber and physical infrastructures becoming blurred. That means a single event can result in losses and degradation of services across multiple industries.

The plan also says that while new and emerging technologies are vital drivers of innovation and opportunity, they can also present unanticipated risks, adding that, in this dynamic risk landscape, CISA must be smart, innovative, and adaptable. CISA also states that its mission is to understand, manage, and reduce risk to our cyber and physical infrastructure. Its vision is to secure a resilient infrastructure for the American people. Each of these attributes and goals should be applied to your business:

Start With Cyber Defenses

CISA lists two primary goals in the plan that you can directly apply to your business. The first states that CISA's role is to "spearhead the national effort to ensure the defense and resilience of cyberspace." Each of the objectives supporting this goal is key to achieving resilience for your business and your data. We'll paraphrase them here so you can apply them to your business.

- Enhance the ability of your systems to withstand cyberattacks and incidents.
- Increase your ability to actively detect cyber threats targeting your infrastructures and critical networks.
- Drive the disclosure and mitigation of critical cyber vulnerabilities.
- Advance your cyberspace ecosystem to drive security by default.

Reduce Risks and Strengthen Resilience

CISA's second primary goal is risk reduction and strengthening the resilience of America's critical infrastructure. Again, we'll paraphrase this goal's supporting objectives as they apply to your business.

- Expand your visibility into risks to your infrastructure, systems, and networks.
- Advance your analytic capabilities and methodologies.
- Enhance your security and risk mitigation.
- Build greater stakeholder capacity in infrastructure and network security and resilience.
- Increase your ability to respond to threats and incidents.
- Support risk management activities.

Unify Your Team

CISA also offers two more goals that apply in a broader sense: operational collaboration and agency unification. While these are aimed at a nationwide audience, they can also be applied to your business. Better collaboration between the executive, IT, and employee teams can significantly improve your ability to prevent and recover from disasters. And executive buy-in ensures IT teams have the budget to put proper prevention and recovery capabilities in place.

Track Known Exploited Vulnerabilities

Moving on from the CISA strategic plan, the agency's "Known Exploited Vulnerabilities Catalog is another essential service. This is where you'll find a complete list of these vulnerabilities, descriptions, and references to advisories, solutions, and tools for each.

Data Resilience: Prevention Plus Recovery

Addressing the onslaught of cyberattacks and ransomware attacks also means preparing for any disaster. Arcserve UDP delivers on both counts, offering unified data protection that safeguards your data with Sophos Intercept X Advanced for Servers that uniquely combines deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity.

Arcserve UDP proactively responds to protect your backups from ransomware and other attack vectors. It includes Assured Recovery to help you comply with SLAs, company regulations, and other requirements and even protects Microsoft 365 workloads on-premises. Arcserve UDP also lets you restore your data faster with instant virtual machine (VM), local and remote virtual standby, and other restore options. Most importantly, Arcserve UDP offers immutable storage for your backups in the cloud via Amazon S3 Object Lock or on-premises with Arcserve OneXafe.

Get Help Getting More Resilient

Arcserve's expert technology partners can help you enhance your overall resilience with data protection, backup, and disaster recovery solutions designed to meet your specific needs. To learn more about Arcserve data resilience solutions, check out our free demos on demand.

How Unified Data Protection Helps Ensure Data Resilience

On its web page titled "Resilience Through Planning," the Cybersecurity and Infrastructure Security Agency (CISA) defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." If you're an IT pro, you probably picture threats to your infrastructure and data when you think about resilience.

That's a good thing because a glance at a recent Bleeping Computer, "The Week in Ransomware," illustrates the impacts of a successful attack. The article notes that Rackspace suffered a massive outage on its hosted Microsoft Exchange environment caused by ransomware, preventing customers from accessing their email. It goes on to list attacks against an MSP in New Zealand, a hospital in Paris, and new ransomware threats.

An astounding 66 percent of respondents to Sophos' "The State of Ransomware 2022" report said they were hit by ransomware last year—65 percent of those attacks resulted in data encryption—while 72 percent experienced an increase in the volume and complexity of cyberattacks.

The point is clear. Every sector, everywhere in the world, is a target. Since you can pretty much count on being attacked, how can you best "withstand and recover" from whatever cybercriminals, well-intentioned or malicious users, or Mother Nature throws your way?

Unified Data Protection: On- and Off-Premises Protection

Data resilience starts with prevention and continues through recovery. Arcserve Unified Data Protection (UDP) combines every data protection capability you need without adding complexity. It delivers all-in-one data and ransomware protection to neutralize ransomware attacks, restore data, and simplify disaster recovery (DR).

Arcserve UDP leverages available Sophos Intercept X Advanced for Server cybersecurity to prevent ransomware attacks on critical disaster recovery infrastructure. And your data backups can be stored in an immutable format with Amazon S3 Object Lock support.

Protections against data loss and extended downtime—the keys to data resilience—from Arcserve UDP extend across cloud, local, virtual, hyperconverged, and SaaS-based workloads. Arcserve UDP protects Microsoft 365 workloads—Exchange Online, Teams, SharePoint Online, and OneDrive for Business—on-premises. And, because Arcserve UDP was designed to be simple to use, you can accelerate your time-to-value by eliminating the need for extensive training or professional services.

Orchestrated Recovery Reduces Downtime

With orchestrated recovery, Arcserve UDP reduces your downtime from days to minutes. It also validates your recovery time objectives (RTOs) and recovery point objectives (RPOs), and service-level agreements (SLAs) with automated testing and granular reporting.

You can even restore faster with instant virtual machine (VM) and bare metal recovery (BMR), local and remote virtual standby, application-consistent backup and granular restore, hardware snapshot support, and extensions that deliver high availability and tape support.

Easy Scaling, More Flexibility

Arcserve UDP lets you quickly scale hybrid business continuity topologies—locally or over long distances—including service and cloud providers. You can easily create data stores on your recovery point server, add the nodes you want to protect, a storage destination, and a plan.

It's also easy to perform jobs like backup, virtual standby, and replicate. You can back up to a local machine or a central recovery point server (RPS) with global, source-side deduplication to reduce your storage footprint. And Arcserve UDP protects a wide range of platforms.

See for Yourself Why Experts Agree About UDP

Phil Goodwin, research director for IDC, says, "Arcserve UDP is designed to bring technologies together in a way that simplifies the infrastructure running a combination of on-premises, virtual, and SaaS-based applications and systems. Organizations may be susceptible to downtime and data loss without a comprehensive solution spanning these different application environments."

Check out our Arcserve UDP 30-day free trial to see how the software can help you ensure data resilience. For expert help, talk to an Arcserve technology partner.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com