arcserve®

Tips and Resources for Business Continuity, Disaster Recovery, and Ransomware Protection in 2022

Table of Contents

Business Continuity in 2022: How to Prepare for Any Disaster

There are plenty of business continuity threats that bring a frown to the faces of those of us in IT. 2021 brought us cold, heat, fires, hurricanes, and tornadoes. It is projected to cost U.S. businesses a collective $13.5 billion in 2022 just from damages associated with flooding. Companies bear many of those costs—insurance and other resources may help—but that doesn't even take the added expenses of downtime into account. Then there's ransomware. The third quarter of 2021 saw the average duration of downtime after a ransomware attack increase to 22 days. Add in potential business interruptions due to cyberattacks, hardware failures, network issues, and who knows what else—and business continuity should be at the top of your list of IT concerns. That point is driven further home when you consider that any break in business continuity can be incredibly costly, with 44 percent of enterprises in a recent survey saying downtime costs them more than $1 million an hour.

Data Is Essential to Your Business

Today's businesses run on data. Whatever the cause, IT teams are tasked with ensuring that downtime is minimized and data is protected. That includes an effective backup strategy and moves beyond application recovery times to application and system availability. Arcserve Continuous Availability ensures business continuity with proven technologies that have one common purpose: keep your business up and running. That includes giving you confidence that you can meet the most stringent service-level agreements (SLAs) by continuously replicating data at the file system level of files or folders, applications, and full physical or virtual systems, with heartbeat-powered automatic failover to ensure the systems stay operational.

High Availability Made Simpler

Arcserve Continuous Availability makes it simple to deploy a robust high availability strategy by eliminating the need for a collection of expensive replication tools focused on specific applications and systems. Designed to work in dissimilar hardware and environments, it prevents downtime across your entire infrastructure with high availability and continuous data protection for Windows and Linux applications and systems on-premises, remote, and in the cloud. Now you can deliver true application and system availability without worrying about recovery time or data loss while validating SLAs and keeping business stakeholders informed with built-in testing.

Business Continuity: Powered by Continuous Availability Software

Powered by asynchronous replication technology, Arcserve Continuous Availability delivers enterprise-grade features that help you eliminate business downtime, including:Maintaining up-to-date replicas of mission-critical systems: Windows and Linux systems, VMware, Hyper-V, Amazon EC2, Microsoft Azure, KVM, XenServer.Keeping applications available and accessible through real-time replication on physical servers, VMware, Hyper-V, Amazon EC2, or Microsoft Azure.Managing data replication for Exchange, SQL, IIS, SharePoint, Oracle, Hyper-V, and custom applications in one program.Rollback of applications to a point in time before a system crash, natural disaster, data corruption, or ransomware attack.Transferring data with AES-128, AES-256, or custom-level encryption between local and remote locations without the need for a VPN.

Try It and See for Yourself

Now you can take advantage of our Arcserve Continuous Availability free trial and see for yourself the difference it can make. Or contact us to talk to one of our business continuity experts. It really is possible to be prepared for any data disaster, no matter what comes your way in 2022.

How to Ensure You Can Always Meet Your RPO and RTO

Two metrics matter most regarding disaster recovery solutions: your recovery point objective (RPO) and recovery time objective (RTO). The reason these two parameters are critical is directly related to the cost of downtime. Ninety-one percent of respondents to ITIC's 2021 Hourly Cost of Downtime Survey said a single hour of downtime that takes mission-critical server hardware and applications offline averages more than $1 million to $5 million due to lost business, productivity disruptions, and remediation efforts. The same survey found that 44 percent of enterprises surveyed said hourly downtime costs exceed $1 million to more than $5 million. And that's excluding any legal fees, fines, or penalties.

What is RPO?

RPO sets the maximum amount of data your organization is willing to lose in the case of a data disaster. It is a core component of your business continuity and disaster recovery plan because it defines your minimum backup frequency schedule, limiting your data loss to the amount of time between backups. For example, if a ransomware attack strikes and you are backing up once a day, you'll have to go back at least one day to restore your data. Frequent backups enable shorter RPOs. Here are some basic RPO questions you need to answer as you develop your disaster recovery plan:

- How much data will we lose over a specific period of time if operations are disrupted?
- What is the cost of lost data, and what is the maximum amount of data our business can tolerate?

What is RTO?

RTO sets the maximum amount of time your organization can tolerate without access to your applications and systems after an outage. Also, a critical part of your disaster recovery plan, your RTO determines the

length of time it will take to recover these vital resources. Here are some basic RTO questions to answer as you develop your disaster recovery plan:

- How much revenue are we projecting we'll lose if a system is unavailable?
- Does the system handle customer data? If yes, what service-level agreements (SLAs) are in place that we must meet?
- What are each system's dependencies? Would other systems be impacted? If so, are we able to meet the RTOs for those systems?
- What would the impacts be for lost and dissatisfied customers and employee productivity if customer-facing systems or applications are unavailable?

Business Continuity Cloud: Meeting Cloud and On-Premises RPOs and RTOs

Meeting your RPO and RTO can be critical to your business's survival. That's why Arcserve has developed a new approach to backup and disaster recovery that makes it possible for you to instantly recover and meet your RPO and RTO and, of equal importance, your SLAs. Arcserve Business Continuity Cloud protects against IT outages across x86, cloud, physical, and virtual environments. It also works with whatever type of storage you use—public or private cloud, disk, or tape—and the applications you count on like Microsoft Exchange, SQL Server, SharePoint, Office 365, Oracle Database, and more. Arcserve offers several options to meet your specific needs.

Arcserve Continuous Availability: Simple and Easy

Arcserve Continuous Availability eliminates the need for expensive replication tools and technologies for specific applications and systems. You can easily create systems and replicate data without making changes to your existing environment. And you can ensure high availability by continuously protecting applications and data on-premises, remote, or in the cloud, preventing downtime. Arcserve Continuous Availabilty continuously replicates data at the file system level of files/folders and applications and entire physical/virtual systems, with automatic failover to ensure your applications and systems remain operational without having to worry about RPO and RTO. You can simply roll back to the point immediately before a system crash, data corruption, or successful ransomware attack.

Arcserve UDP

Arcserve Unified Data Protection (UDP) software gives you all-in-one data and ransomware protection, neutralizing ransomware attacks and letting you restore your data with effective, efficient disaster recovery. Safeguarded by Sophos Intercept X Advanced cybersecurity, Arcserve UDP combines deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity. The result is a multi-layered approach that gives you complete IT resiliency for your virtual, physical, and cloud infrastructures so you can rest assured you can meet your RPO and RTO.

Arcserve UDP Cloud Hybrid: Cloud Economies for Backup and Disaster Recovery

With Arcserve Unified Data Protection (UDP) Cloud Hybrid, you add cohesive data security, protection, and retention strategy. As the only direct-to-cloud backup as a service (BaaS) and disaster recovery as a service (DRaaS), you get comprehensive data protection with consumer-friendly usability. Arcserve UDP is scalable and flexible for always-on continuity while letting you quickly adapt to changing business needs by delivering industry-best RPOs and RTOs.

Take a Free Test Drive

If you're facing challenging RPOs and RTOs, it's time to take a closer look at Arcserve data protection solutions. Start your free trial today and see for yourself the difference Arcserve can make for your business.

CISA Cybersecurity Public–Private Partnerships: A Model for Disaster Recovery

A glance at the "Significant Cyber Incidents" posted on the Center for Strategic & International Studies (CSIS) website says it all. There were seven of these "incidents" in December 2021 alone. They ranged from a cyberattack on the Belgium Ministry of Defence that exploited the Log4j vulnerability—forcing part of its computer network to shut down for several days—to a breach of four U.S. defense and technology firms by Chinese hackers. To help fight back, the Cybersecurity & Infrastructure Security Agency (CISA) is developing critical infrastructure partnerships to test emergency response plans. CISA's Partnership and Engagement branch serves as CISA's focal point for strategic and customer engagement with state, local, tribal, and territorial governments, and private sector customers.

CISA Incident Response Exercise: A Model for Public and Private Sectors

Last fall, CISA, in coordination with public and private sector partners, held an exercise in Tulsa, Oklahoma, to test emergency response plans. The exercise brought together multiple agencies and stakeholders to gauge prevention, response, recovery, and overall business continuity capabilities. If you're an IT pro working in the private sector, state or local government, education, or nearly any other industry, CISA's approach is a great model for ensuring your organization is prepared to respond and recover from any disaster, whether it's a hurricane, data breach, or ransomware attack. Here are some key takeaways and resources we want to highlight:

Develop Your Disaster Recovery Plan

Obviously, the stakeholders had to develop those emergency response plans before they could be tested. It would be best if you did the same. Bring together the key stakeholders and partners within

your organization to identify mission-critical systems, applications, and data. Develop a comprehensive business continuity plan that includes a business impacts analysis and recovery strategies, then test your plan to make sure it meets your objectives. The U.S. government's Ready.gov website offers a great starting point for developing your plan.

Build In Effective IT Disaster Recovery Strategies

Your business continuity plan must include an IT disaster recovery plan. Here, another Ready.gov IT web page can help you kickstart your planning process. Your recovery strategies are the most crucial elements of your plan, so they should address all of your IT systems, applications, and data. That includes networks, servers, desktops, laptops, wireless devices, data, applications, and connectivity. You need to prepare for the loss of any of these system components and make sure the recovery strategy you develop can meet your RPOs and RTOs. Some organizations that can't tolerate any downtime choose to use two data centers—each capable of handling all their data processing needs—running in parallel, with data mirrored or synchronized between the two centers. That's a very complex, expensive strategy. A better approach is to choose a disaster recovery solution that can meet your needs without breaking your IT budget. Backup and disaster recovery as a service (BaaS/DRaaS) should be part of that discussion.

Test Your Plan and Train Your People

As we noted above, the key to successful disaster recovery is preparation. Sponsored by the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST) offers a tremendous resource for this purpose, the "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities." This in-depth guide covers every aspect of IT disaster recovery plan testing and training, including tabletop exercises, functional exercises, and test scope.

Leverage CISA Service Offerings

CISA's Cybersecurity Quality Services Management Office (Cyber QSMO) Marketplace is another excellent resource. This online platform offers high-quality, cost-efficient cybersecurity services from CISA, the Department of Health & Human Services, the Department of Justice, and the Department of Transportation. Cyber QSMO's initial list of offerings ranges from anomaly and event detection service to supply chain risk management tools and services. CISA also provides a catalog of known exploited vulnerabilities to reduce these significant risks to organizations further.

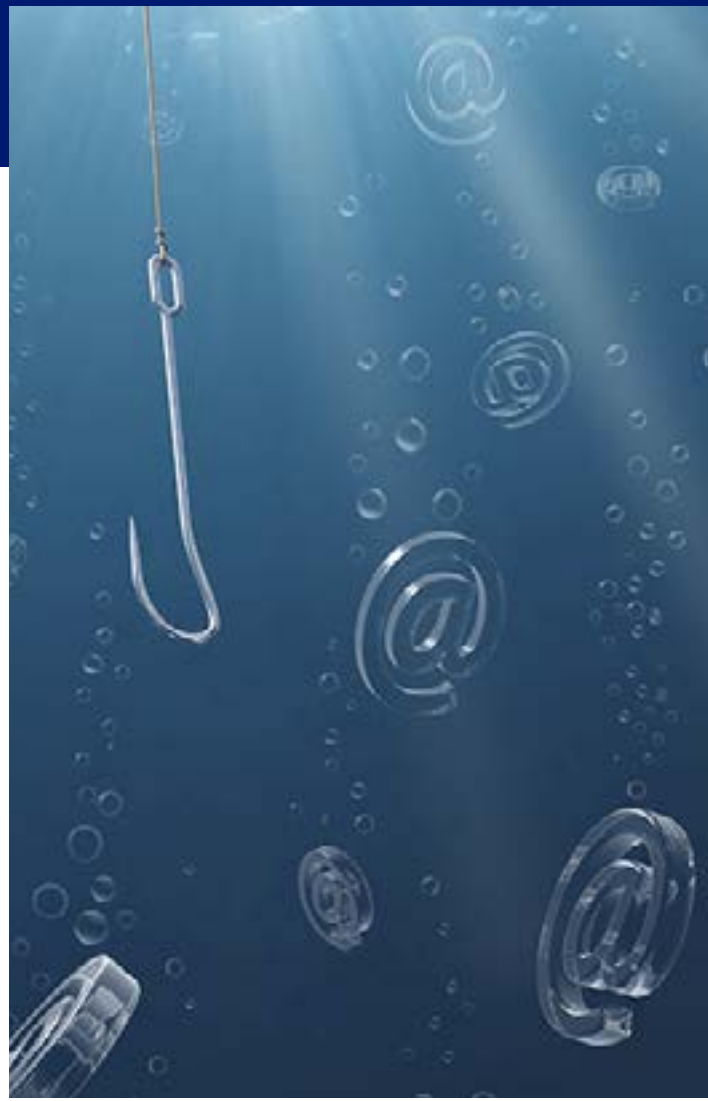
Fight Back Against Ransomware

We want to share one last resource: CISA's Stop Ransomware website. The site offers resources, news, alerts, and how to report a ransomware attack so others can benefit from your experience, good or bad. On the subject of ransomware protection, we recommend a proactive, multi-layered approach that prevents, protects, and immunizes your backup data from cyberattacks using immutable backup storage. You can learn more here.

Be Ready to Recover

While these resources are valuable, the ultimate key to IT disaster recovery is choosing the right solution for your organization. That's why we suggest you talk to an Arcserve backup and disaster recovery expert to find out which options may work best for you. You may also want to consider our Arcserve Continuous Availability software free trial for Windows, Linux, and UNIX environments.

Microsoft Uncovers Evolved Phishing Campaign: Targets Those Without MFA



The Microsoft 365 Defender Threat Intelligence Team has recently uncovered a new phishing trick that should make anyone without multi-factor authentication sit up and take notice. Microsoft notes that this latest attack form builds on traditional phishing tactics by joining a device that the hackers have taken control of to an organization's network to spread the campaign.

Multi-Factor Authentication Is the Key Vulnerability

Microsoft says the campaign started with hackers accessing stolen credentials from target organizations via a phishing campaign. These credentials were then used for the second, more damaging phase. Hackers used compromised accounts to spread the attack within the network via lateral phishing—and outside the network via outbound spam.

The common thread in successful breaches during the second stage of the campaign was that victims didn't have multi-factor authentication (MFA) in place. MFA is a crucial element for securing devices and networks because, without this extra layer of cybersecurity, hackers can hijack, register, and operate a device using recently stolen credentials.

The Microsoft post includes the phishing email spoofing examples—remarkably authentic-looking email and dialog boxes using the DocuSign and Microsoft Outlook brands. It's understandable why anyone would be fooled and click on the link.

Defense and Remediation

But here's your key takeaway: For organizations that did have MFA in place, the attack was contained for most targets. For organizations that didn't have MFA in place, the attack spread. If you aren't using MFA throughout your organization, it's time you do.

Microsoft also offers guidance and links for remediating device persistence, noting that resetting passwords isn't enough. The post says that good credential hygiene, network segmentation, and similar best practices are also vital defense tactics, along with advanced security solutions that provide visibility across domains and coordinate threat data across protection components.

On a side note, Arcserve UDP features MFA to ensure your backups are always protected. Stay tuned for updates.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com