arcserve®

Data Protection, Resilience, and Disaster Recovery: Fighting Back Against Ransomware and Data Loss

Table of Contents

8 Ways Employees Can Help Reduce the Risk of Ransomware

Businesses are at great risk for ransomware attacks because they often don't have a sound cybersecurity posture. That's why they need to educate their people about basic cybersecurity and cyber hygiene, according to the Australian Cyber Security Cooperative Research Centre.

So, it's little wonder that the question, "How do I make sure my company never pays a ransom for our data?" is moving up on business owners' agendas.

The first step in preventing a ransomware attack is properly educating your employees about ransomware and how it infects systems. The most iron-clad software and hardware is of no help if an employee is careless. Part of your strategy should include a plan for helping your users spot and avoid ransomware. Many businesses hold mandatory quarterly security seminars where admins help employees understand various types of cyberattacks. Your plan should cover everything from ransomware to phishing to the growing threats from social engineering scams.

The following are eight simple security practices for employees to ensure they do their part in keeping these increasingly common attacks at bay.

1. Use Email Filtering

This reduces the number of potentially malicious emails coming your way. Businesses should invest in enterprise-grade solutions. These will use techniques such as blacklisting, whitelisting, and user-based email analytics to balance spam and legitimate mail filtering.

2. Scan Attachments

If email is the vehicle that drives it, then the attachment is the cargo you open to unload the malware on your system unknowingly. Many enterprise spam filters have scanning functions that allow you to check your messages for potential threats. Whether they're built into your spam filter or anti-malware software, put those scanning capabilities to use before opening any email attachments.

3. Block Attachments

Blocking select attachments is one of the most effective ways to stop ransomware at the gate. The system may prevent users from opening .exe, .com, .bat, .js, .docx, and other file types commonly associated with malware. Because this method could also restrict access to legit files you need, it might be a good idea to designate a separate server, such as one in the cloud, for exclusively handling blocked file types.

4. Preach Safe Surfing

Like malware in general, ransomware distribution is not limited to email. This type of infection can be spread by visiting rogue websites, downloading free software, and even connecting infected USB drives to your system. A computer security training program that covers all the basics of responsible web browsing can make a world of difference when it comes to staying protected.

5. Promote Good Data Backup Habits

With so many employees working remotely, it's harder for businesses to manage backups and store data on the corporate network. Encourage employees to be responsible and back up their data regularly. If an employee stores data on a local flash drive inserted into a laptop, that employee should back it up to the cloud or another hard drive. If employees store their data primarily in the cloud, they should be sure to have copies somewhere offline.

6. Encourage Stringent Cyber Hygiene

All employees, especially those working at home, need to be regularly reminded to update the software on their devices and enable all available security features, such as firewalls and anti-malware. Failing to install updated software and security patches is a well-known employee misstep that creates the gap for malware and ransomware to seize on.

7. Limit the Number of Files Employees Can Access

Employees should only be able to access data and folders based on the principle of “least privilege.” This is the concept of only giving employees enough access to perform their required jobs. Least privilege can prevent workers from accidentally deleting or corrupting files they should never have had access to in the first place. Enforcing least privilege can significantly reduce the risk caused by human error.

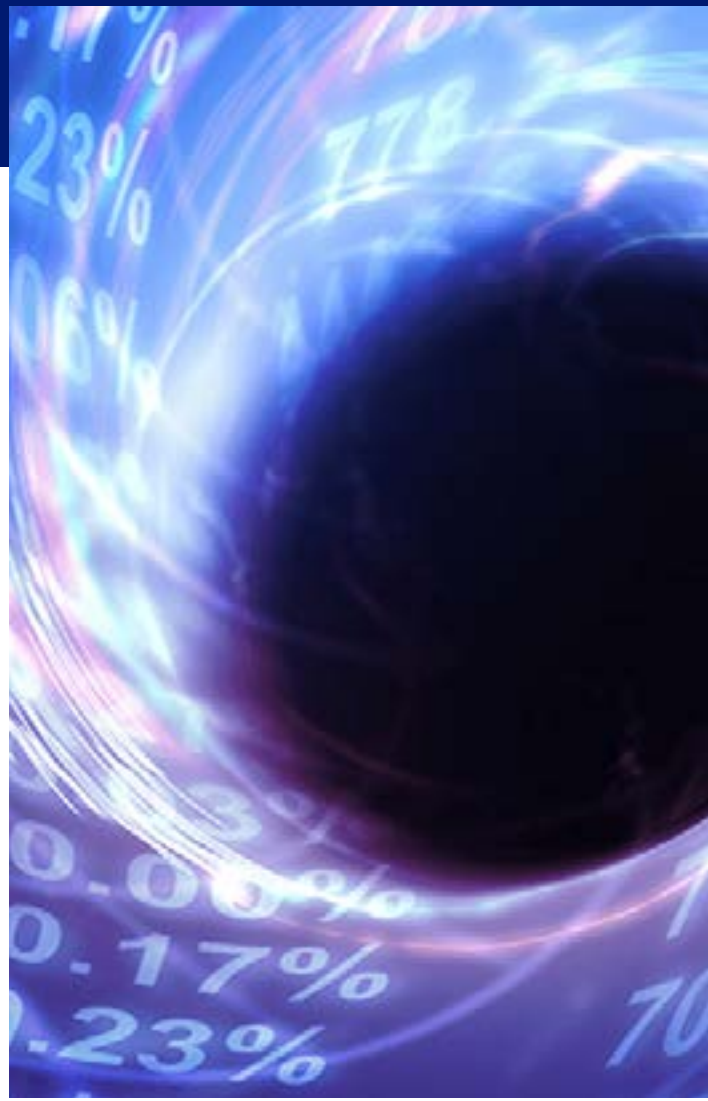
8. Test Your People and Systems

It is wise to consider regular testing once your network is in tip-top shape. This includes network vulnerability testing, testing backups, and testing employees—people are often the weak link in the security chain. That’s why some businesses formulate strategies for testing employees. That could include sending fake phishing emails or even hiring companies to conduct mock social engineering scams. Whatever the case, testing should be a regular part of your security strategy.

Talk to a Data Protection Expert

Arcserve has the broadest portfolio of data protection solutions available under one roof. To learn more, contact us.

4 Critical Steps You Should Take to Prevent Data Loss



There are so many potential pitfalls that can befall your company's data and cause significant damage to your business. A good case in point—and one of the most high-profile data loss stories in recent memory—is when one of Pixar's animators accidentally entered the wrong command and instantly deleted about 90 percent of the Toy Story 2 production files. Pretty bad, no? It gets worse. The data backup system malfunctioned due to inadequate disk space. For a brief, bloodcurdling moment, it looked like almost the entire production would be lost. Thankfully, after much blood, sweat, and tears, the crew recovered the data and restored the film files.

But not every data horror story ends well, and we have all witnessed our share of data disasters. For example, one small company backed up all its data on tape drives. The managing director would bring the current drive back to his home for safekeeping at the end of each day. One evening, he put the tape on the top of his car and drove away without noticing. The company immediately lost all its data for the previous day.

Sadly, data loss stories are an ever more common occurrence as millions of people worldwide continue to work remotely. Moving employees, devices, and data from a secure office setting to a less secure remote environment introduces many data loss risks, from human errors to technical glitches and cyberattacks.

Here are four critical steps you can take to ward off potential disasters and ensure your corporate data stays safe.

1. Never Stop Testing

Arcserve conducted a survey of IT decision-makers and found that nearly a quarter of all organizations don't even test their data recovery plans or don't have them in the first place. It's vital to regularly test backups so you can be certain you can recover in the case of data loss. The last thing you want is to rely on

a backup that fails during an emergency— whether it's a cyberattack, natural disaster, or system failure.

While having a backup is essential, recovering all data completely and quickly is just as crucial for business continuity. Your organization should make it a habit to periodically test your backup copies to ensure you can reliably restore your data.

2. Embrace Multifactor Authentication

Multifactor authentication (MFA) is one of the most critical security features for protecting corporate data. With millions of passwords constantly being stolen and becoming available to attackers, many businesses are now implementing MFA to provide an extra layer of security. Adding a second authentication factor is vital for protecting your accounts and locking down your data. According to the latest Verizon Data Breach Investigations Report, MFA is especially crucial given that 61% of all breaches involve stolen or compromised credentials.

By requiring employees to enter more than just a password to gain access to their data, you make it harder for a criminal to impersonate that employee. With MFA, a stolen password alone is not enough to gain access, so you're putting a big hurdle in the path of cybercriminals. And cybercriminals don't like hurdles—they want the low-hanging fruit.

3. Teach Employees to Back Up Their Data

When employees work remotely, they probably won't be as vigilant as they would be in the office. They're using their home PCs and clicking on links that, perhaps, they should not be clicking on. That puts their data at greater risk. Even worse, that puts your corporate data directly at risk, too. That's why it's so important to encourage employees to be responsible and back up their data regularly.

You should also adopt the 3-2-1-1 data-protection strategy. The 3-2-1-1 strategy says you should have three backup copies of your data on two different media, such as disk and tape, with one of those copies located off-site for disaster recovery. The final one in this equation is immutable object storage.

4. Make Data Protection a Priority

Consider implementing a data storage solution that can protect your data from human error wherever it lives—on-premises, off-site, or in the cloud. The most effective solutions can quickly recover individual files and systems—or an entire data center—in minutes while ensuring that the data is always available, no matter what happens.

This sounds almost too good to be true, but it's easily achievable with next-generation solutions. These solutions provide immutable object storage, providing safeguards to protect your data from human error by taking snapshots of that data every few seconds. And, because the object store is immutable, it can be restored in a snap, even if someone tampers with the data.

When it comes to your business, you already have plenty of things to worry about. With the right strategies and systems in place, data protection can be one less item on that list. Contact us to talk to a data protection expert and learn more about Arcserve's effective solutions.

Backup Strategy: Prevention, Protection, and Recovery

Businesses saw a 50 percent increase in cyberattacks per week in 2021, due, in part, to the Log4j vulnerability, which helped push cyberattack attempts to an all-time high. A recent ZDNet headline proclaimed, "Ransomware in 2022: We're all screwed." Every small, medium and large business needs to take these threats seriously—especially companies that don't have security experts on their internal team. That's why backing up your data is the single most important "last line of defense" you should implement. Today, backing up your data is much more than just copying it to another storage medium. So, what should companies consider when planning and setting up a backup process to protect themselves against ransomware and cyberattacks?

Prevention, Protection, and Recovery Basics

Three stages need to be carefully considered and included in your disaster recovery plan: prevention, protection, and recovery. Addressing and coordinating these stages gives your company the best chance of recovering from a cyberattack or ransomware infiltration.

Cyberattack Prevention

Prevention includes backup and recovery but also takes security into account. Ideally, security should not be set up independently from your backups. Instead, it should be integrated into your overall data protection strategy. That's why we have tightly integrated an artificial intelligence- (AI) supported security ecosystem into our Arcserve UDP appliances. Regardless of the security solution you use for your endpoints, with Sophos Intercept X integrated with Arcserve UDP, you get additional, dedicated protection for your backups.

Data Protection

Protection describes the structure and architecture you choose for your backups. That could include snapshots, local storage, disk, tape, remote sites, or cloud instances. Immutable storage is another critical consideration. Ideally, your solution—or combination of solutions—should allow for any backup model while efficiently scaling as the company grows.

When disaster strikes, recovery is your highest priority. You need to ensure that your systems and data can be recovered with a clearly defined RTO and RPO. One of the fastest ways to recover is the capability to power up your critical systems in virtual instances in the cloud until your systems are recovered in your core infrastructure. This is your last line of defense.

Planning and Coordination Come First

The most important step in your backup strategy is making sure the backup and disaster recovery solution you choose meets your company's specific requirements. That requires expert analysis. For many companies—especially medium-sized companies—one of Arcserve's specialized partners can provide that support.

Of course, your disaster recovery plan is just as important as the planning and implementation of your solution. When disaster strikes, everyone involved must know what they need to do and the order in which they need to do it. Prioritizing critical data and systems is essential for shortening or even preventing failures. You also need to address many other planning details, including having alternate communication channels, as your normal channels may be interrupted in the event of a cyberattack. And it is imperative to test your backup and recovery plan regularly. That way, you can ensure that your recovery process works as expected and that your emergency team is well prepared.

Flexible Immutable Storage Options

While there are a variety of Immutable storage systems available, at Arcserve, we believe that immutable storage must adapt to your specific infrastructure. That's why we offer a wide variety of solutions, including OneXafe, which features scalable object-based immutable storage, as well as solutions that seamlessly integrate tape or cloud storage into your overall backup and recovery solution. Arcserve's immutable storage can be integrated into any existing infrastructure as an add-on, so even if you are using other backup software, Arcserve provides an added level of security.

Keeping Ransomware Out

Typical disk storage is available as a shared network resource to ensure fast backups and restoration. Because OneXafe is object-based, when the immutable snapshots are written to storage, they cannot be modified by ransomware. That limits your maximum data loss to the time interval between each snapshot. With Arcserve, those intervals between snapshots can be extremely short, so your data loss is kept to a minimum.

Learn More About Your Backup and Recovery Options

Contact us to talk to an Arcserve data protection, backup, and recovery expert.

Ransomware and Cybersecurity Resources: How to Create a More Resilient Organization

The Oxford Dictionary defines resilience as “the capacity to recover quickly from difficulties; toughness.” That definition should speak volumes to you if you’re an IT pro, given that you’re likely responsible for making sure your organization can recover quickly from a data disaster like ransomware or any other cybersecurity breach. Resilience is a two-part equation. The first part is toughening your organization’s cyber defenses as much as possible. The second part is to make sure you can spring back if disaster strikes. And more than likely, it will strike. The Q3 update to the SonicWall Cyber Threat Report offers up some heart-stopping numbers:

- Global ransomware attacks surged 148 percent in 2021
- Ransomware attacks were projected to total 714 million in 2021
- Ransomware attempts through Q3 rose to 1,748 per customer!

The pressure is on to make your organization ever more resilient. Here are some tips and resources to help you get there.

Start With a Cyber Resilience Review

The Cybersecurity and Infrastructure Agency (CISA) offers several valuable resources for conducting a Cyber Resilience Review (CRR). This no-cost, voluntary, non-technical assessment that you can conduct yourself or have facilitated onsite by Department of Homeland Security (DHS) cybersecurity pros measures your current organizational resilience and provides a gap analysis for improvements based on best practices.

The CRR assesses your enterprise's programs and practices across 10 domains:

- Asset management
- Controls management
- Configuration and change management
- Vulnerability management
- Incident management
- Service continuity management
- Risk management
- External dependency management
- Training and awareness
- Situational awareness

The result of the review process is a CRR final report that documents your organization's current status and offers relevant options for improvements based on best practices. The report also maps your organization's relative maturity in resilience processes in each of the 10 domains listed above.

Cybersecurity Resources for Business

CISA has put your tax dollars to work, building a deep repository of cybersecurity resources for businesses. Here, CISA breaks down its resources into the five Cybersecurity Framework Function Areas from the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce. The five functions of the Framework Core are:

- Identify
- Protect
- Detect
- Respond
- Recover

The NIST website provides detailed descriptions for each of these functions, noting that these five primary pillars form the foundation for a successful and holistic cybersecurity

program. CISA offers resources specifically for small and midsize businesses (SMBs), including a Cyber Essentials guide for small businesses and local government agencies to help kickstart implementing improved cybersecurity practices. The CISA site also includes links to a Cybersecurity Resources Road Map to help you put cybersecurity best practices in place and deploy the resources you need.

Ransomware Resources and Alerts

CISA offers more ways for your organization to become more resilient with its StopRansomware.gov website. The site includes resources, guides, and services to support your efforts. These services include free scanning and testing and the Cyber Security Evaluation Tool (CSET), a standalone desktop application that guides you through a systematic process of evaluating operational technology (OT) and information technology (IT). CSET was updated last year to include a Ransomware Readiness Assessment (RRA), a self-assessment based on a tiered set of practices to help you understand your current defense posture and ability to recover from a ransomware attack. You can also stay aware of the latest alerts from CISA, the FBI, and the Department of Treasury on the site.

Cybersecurity Awareness Tools

Another excellent resource for increasing cybersecurity awareness in your organization is the CISA Cybersecurity Awareness Program Toolkit. Here you'll find materials ranging from social media cybersecurity tips to how to report a cybersecurity complaint.

Ensuring Business Continuity

In a recent post, we shared five tips for a critical component of resilience: closing gaps in your business continuity plan. The post covers five areas to focus your efforts: data and technology; internal communication; communication channels, essential personnel, equipment, and hardware. Arcserve UPD Cloud Direct is worth including in any conversation around resilience, data backup, and disaster recovery. This direct-to-cloud backup and disaster recovery as a service (BaaS/DRaaS) give you comprehensive data protection with consumer-grade usability—and without any hardware required on-premises.

Contact us to talk to an Arcserve data protection expert to learn more about your options for improving your organization's resilience.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com

Copyright © 2022 Arcserve (USA), LLC and its affiliates and subsidiaries. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective owners. This document is for your informational purposes only. Arcserve assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, Arcserve provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will Arcserve be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if Arcserve is expressly advised in advance of the possibility of such damage. AD2100XX