READY FOR DISASTER?

READY TO RECOVER?

Disasters don't just happen during hurricane and tornado season. And hackers don't care what your business does; they just want to exploit vulnerabilities for profit. Be sure to take steps to protect your data and your business from man-made and natural disasters and ransomware before the worst-case scenario occurs.

ARE YOU READY?

When IT professionals were asked about the actual disasters they reported experiencing over the last year, man-made disasters topped the list (**65%**), followed by technology incidents (**29%**), and IT security incidents (**22%**). *(Carbonite)*

THE THREAT OF DOWNTIME IS REAL

The single biggest driver for business continuity planning for many organizations is the threat of downtime. IDC indicates **80% of small businesses have experienced downtime at some point**, with costs ranging from $82,000 to $256,000 for a single event. For larger enterprises, downtime costs can reach $9,000 to $17,000 per minute.

Here are recommendations from the Cybersecurity Infrastructure Security Agency (CISA) to consider:

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Change passwords regularly in network systems and accounts.
- Use multi-factor authentication where possible.
- Identify critical assets and create backups of these systems; house the backups offline from the network.
- Implement network segmentation; sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

PROTECT YOUR DATA USING 3-2-1

IT best practices say you should leverage **3-2-1** to properly protect the critical data that runs your organization. This means:

3 copies of data: primary, plus 2 copies for safekeeping

2 copies on two different types of storage: prevent a single source of failure

1 copy offsite for ransomware recovery and disaster recovery

Iron Mountain offers a variety of data protection solutions that can help you satisfy **3-2-1**, including multi tier data storage solutions that can help you archive inactive data, backup active data, and isolate data required to recover from a disaster or ransomware.

TESTING 1,2,3

You never know when a man-made or natural disaster will strike – or when a ransomware attack might occur – meaning it's time to update your business continuity plan and test if you can fail over and recover whenever necessary.

Fail Over to a Disaster Recovery Environment Built on Trust

Iron Mountain has been a leader in information management services for over 70 years and has an extensive background in disaster recovery services. Use Iron Mountain's Iron Cloud infrastructure-as-a-service and our geo-resilient, climate-controlled data centers to create a failover environment – that you can test regularly – so you are ready to keep your business running if your primary site becomes infected or is unavailable due to ransomware or a man-made or natural disaster.

Verify Threats Are Gone Before You Restore

Iron Mountain can also offer an isolated, unhackable, virtual clean room environment where you can restore your systems and check to ensure that your data is not corrupted or infected with ransomware before you attempt to restore.

HOW IRON MOUNTAIN CAN HELP

IT'S A FULL-TIME JOB TO PROTECT YOUR DATA, AND IRON MOUNTAIN CAN HELP

Iron Cloud Data Protection

Our cloud-based backup and recovery services can help you get back online after a crisis event, such as a system failure, a man-made or natural disaster, or a ransomware attack. These services use secure, high-speed, reliable connectivity to an Iron Mountain data center. This means your data is backed up, protected, and recoverable 24/7, helping you establish recovery point objectives (RPOs) and recovery time objectives (RTOs) that will minimize the impact of possible business disruptions at a low cost while keeping costs in check. Within Iron Cloud Data Protection, you can choose to back up servers, endpoint devices, and Microsoft 365, so you can deploy the right form of protection for all data types across your organization's information ecosystem.

Iron Cloud Secure Offline Storage (SOS) with Vault Lock

Since ransomware can happen to any organization at any time, you need a cost-effective long-term storage solution to protect your data that has built-in safeguards for ransomware recovery. With Iron Mountain's Iron Cloud Secure Offline Storage (SOS) with Vault Lock, you can create an air-gapped, gold copy of your valuable data that is stored offline and retrievable using multi-factor authentication to ensure secure recovery. With our virtual compute option, you have the ability to fail over to Iron Mountain to keep day-to-day business operations going if the worst-case scenario occurs. Virtual clean room capabilities are also available, so you can verify your data is not corrupted before you restore.

CUSTOMER SUCCESS

A local government suffered a cybersecurity attack, with hackers demanding **$400,000** in ransomware payments. Three servers protected by Iron Cloud Data Protection remained safe from the attack, and the IT team was able to restore the data without giving in to the hackers' ransom demands. To optimize backup and disaster recovery services, Iron Cloud Data Protection was deployed to all servers and devices in all government office locations afterwards.

PREPARE TO RECOVER TODAY. CONTACT IRON MOUNTAIN TODAY.

1.888.386.3916
IRONMOUNTAIN.COM/ SOS

USDR-INFO-072321A