McGowanPRO

Professional Liability Insurance

Managing IT Disasters with Written Information Security and Data Recovery Plans

IT disasters may seem like unexpected, isolated incidents, but the reality is that they can happen at any time to companies of any size. A 2022 Cost of Data Breach Report from IBM found that the global average cost of a data breach is $4.35 million, with ransomware, in particular, seeing a 41% increase in the share of breaches happening across the globe.

Data is one of an organization's most valuable assets, requiring a high level of care to prevent data security incidents.

In this uncertain landscape, businesses need to think of how to mitigate disasters, regardless of whether they are artificial or natural. They must have a backup plan to rapidly restore services and manage risk. Preparation is vital, with enterprises needing to research, fund, and develop a disaster data recovery plan.

What is a Disaster Data Recovery Plan?

Businesses are likely already familiar with a business continuity plan outlining how companies will maintain operations during disasters. While the business continuity plan is focused on keeping operations running, a disaster data recovery plan is instead a subset of this plan that zeroes in on recovering from an interruption.

It details how a business will return at pace to its IT operations following the disaster, with specific threat management tactics that can prevent the disaster from occurring in the first place. With a strong disaster data recovery plan, businesses benefit from the following:

- **Reduced costs**: Businesses can save hundreds of thousands of dollars by planning for disruptions of all kinds, and it can even be the difference between weathering a disaster and closing doors permanently.
- **Agile recovery**: Businesses that can get up and running quickly following a disaster can sometimes continue operations as if nothing has happened.

What Should the Plan Contain?

As disasters disrupt IT workflows and interrupt access to data, the data recovery plan focuses on minimizing any server downtime while bringing critical systems quickly back online.

The best disaster data recovery plans are put together with the business environment in mind, with companies conducting a thorough evaluation of potential threats, vulnerabilities, and origins of disasters. It should define the company's goals if a disaster happens: what should be prioritized, who is in charge of ensuring recovery timelines are adhered to, where and how will backed-up data resources be recovered, and when should an IT inventory be made and refreshed?

Staff should be fully aware of their responsibilities, know where disaster recovery sites are located, which procedures must be immediately implemented, and how often the plan should be tested. In short, the plan should contain the following:

- The procedure team members should follow during data recovery.
- A list of essential databases, copy storages, active-data pools, and the IT solutions needed to read them.
- Copies of files that detail server options, device configuration, and volume history.
- A complete inventory of all IT hardware and software.
- Any commands needed to complete database recovery, register licenses, and more.

The result will be an in-depth, cost-saving recovery plan that strengthens a company's business continuity plan.

The Written Information Security Plan (WISP)

Increasingly, governments and regulatory bodies are requiring formalized security plans. In the U.S., some states require financial institutions, such as CPAs, accounting firms, mortgage brokers, universities, and nonbank lenders, to establish a Written Information Security Plan (WISP). This formal plan outlines the roles of staff in data security protections, steps to follow in the event of a data breach, and risk assessments. The chief difference between a WISP and a data recovery plan is that the former focuses on information security and data breaches, while the latter covers natural disasters and other catastrophic events. The two documents should work hand in hand.

Even if it is not a requirement in your state, generating a WISP demonstrates that your organization is serious about protecting sensitive data for your clients. Additionally, a WISP may limit your liability in the event of a data breach.

For more on generating a WISP for your organization, visit the IRS' guidance on the subject here.

Putting the Data Recovery Team Together

Companies must assign a disaster recovery team to develop, implement, and manage the data recovery plan. The identity of these members will differ depending on the organization, but there are some key roles to assign, including:

- **Crisis management**: This team member kicks off any recovery plans, coordinates efforts between different departments, and resolves challenges as they occur.
- **Impact assessment and recovery**: Requiring expertise in IT infrastructure, this team member assesses the effect of the disaster on servers, storage, databases, and networks.
- **IT applications**: The team member in charge of IT applications will need to monitor which IT processes are implemented in which order according to the plan. Applications settings, configuration, data consistency, and more will be under their purview.
- **Business continuity**: One team member should ensure the disaster data recovery plan aligns with the company's overall business continuity goals and needs.
- **Additional roles**: While not essential to the plan's efficacy, executive management will need to approve the plan, while critical business units should provide feedback on disaster recovery planning to address any concerns.

Keeping Tabs on Your Hardware

To plan for recovery, companies must first perform an audit of their IT resources. Understanding which resources are essential to the regular operation of a business will allow teams to assess their impact if they become unavailable.

This audit will require businesses to assemble an inventory of the entire network infrastructure, including hardware. Understanding what data each resource holds will help locate them quickly in the case of a disaster and help identify data sets that are no longer critical to operations and would only create unnecessary extra work during the recovery.

Companies should take the time to sort through all data during the audit, reducing the size of any backup files, freeing up storage space and saving costs even before a disaster occurs. Businesses can also consider investing in streamlining or otherwise consolidating their IT resources to be simpler to recover, saving valuable time and resources.

A good data recovery plan can resume critical services as quickly as possible by identifying business-critical assets essential for business continuity and detailed, outlined steps for data recovery.

Why is Backing up Data so Important?

IBM has found that identifying and containing a breach within 200 days can save $1.12 million per data breach. Quickly recovering from a data disaster is one of the best ways to reduce associated costs, yet 2022 saw an average recovery timeline of 277 days.

At the same time, the rate of disasters such as cyber-attacks is increasing while also becoming more costly. One of the key targets is the cloud, which accounted for 45% of all data breaches in 2022. What this means for businesses is that having data backed up helps address the concerns of cloud vulnerabilities and allows companies to get up and running again within those critical 200 days. Testing your data recovery plan is vital, as companies that test their plans save an average of $2.66 million per data breach versus those that do not.

Beyond backing up data, companies can also implement a variety of other strategies to help keep operations running in the case of a disaster, such as:

- **Cold sites**: A basic network infrastructure that can be set up in seconds, providing a place for employees to work in the event of a disaster.
- **Hot sites**: Containing up-to-date copies of a company's data at all times, hot sites are costly to set up but drastically reduce company downtime during a disaster.
- **Point-in-time copies**: These are snapshots of a company's entire database at a given time, allowing data to be restored that may be slightly out of date but will enable companies to move on and rebuild quickly.

Other methods exist, such as disaster recovery as a service (DRaaS), in which a provider moves an organization's computer processes to its cloud network in the case of a disaster. This allows companies to continue working even if their servers are down. Companies should evaluate their options and assess their viability as part of their data recovery plan.

Timelines for Recovery

How quickly a company should be able to recover from a disaster and how much data is acceptable to lose are both critical factors of a data recovery plan. These are known as the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), with their calculations used to set limits within the recovery plan that team members can use to test its efficacy.

By setting the RTO as the maximum number of minutes, hours, or days that an organization can survive an IT service outage, companies know what timeline they must work to for continued operations. This hard deadline is crucial to the recovery plans protocols, while the RPO helps outline how much data the organization can afford to lose during the outage. Together, they provide a strong indicator of the plan's performance.

Ultimately, testing is critical. Recovery teams must continually test the limits of the recovery plan and update it to ensure it can address new threats as they emerge. The beauty of data recovery plans is that they require companies to consistently evaluate the needs of their data systems and their contents, eliminating bloat from servers and finding new ways to apply this data. This means that continual testing will only benefit companies.

Beyond Recovery Plans

Planning for the inevitable will help companies weather any disaster, but they can take a further step to secure continued operations. Investing in insurance will protect against the emerging data security and privacy exposures companies face today.

Companies are increasingly at risk of having client information such as social security numbers and credit card details stolen by cyber-criminals. For 83% of companies, it's not a question of if a cybersecurity breach will happen, but when. Securing a business against the potential litigation following the loss of sensitive client information could make the difference between keeping doors open or closing them permanently.

McGowan PRO provides Information Security & Data Privacy Liability Insurance, offering coverage for the costs associated with a data breach. Policies cover legal liabilities, expenses related to providing notification of the breach, the cost to defend a regulatory proceeding, and more.

Contact us today.

McGowanPRO
Professional Liability Insurance

Contact us:

McGowanPRO
150 Speen St., Suite 102, Framingham, MA 01701
Phone: +1 866 262 7542 | Fax: +1 508 656 1399

Rob Ferrini | Program Manager | McGowanPRO
Phone: 508 656 1327 | Fax: 508 656 1399 | Mobile: 508 330 0454
RFerrini@mcgowanprofessional.com

https://mcgowanprofessional.com/