



Sirtawn Systems

Start Fighting Cyber Crime with Knowledge and Action.

Our Newsletter for Issue #171 is dedicated to Disaster Preparedness.

**Why you need a Disaster Preparedness Program**

## What is Disaster Preparedness?

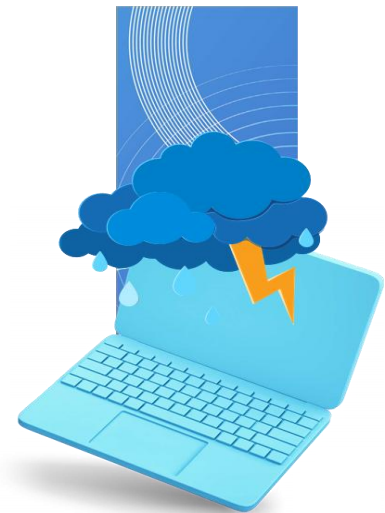
*For any business to survive a disaster, having a comprehensive disaster preparedness program in place before calamity strikes is key.*

Disaster preparedness refers to a set of proactive measures that predict, prevent and mitigate the impact of a disaster. It should be viewed as an action plan that prepares your business to withstand potential disasters or emergencies that may affect your business operations.

It involves identifying potential risks, vulnerabilities and threats to help businesses like yours effectively prevent, mitigate and respond to unexpected hazards.

A disaster preparedness plan enhances your readiness against disasters, both man-made and natural. It helps you minimize financial losses and ensures business continuity by implementing preparedness plans and strategies.

As a business owner, you want to secure your business against various threats affecting normal business operations. A disaster preparedness plan gives you the edge you need to protect your business and stay ahead of competitors.



## Why Would You Need a Disaster Preparedness Program?

*A disaster can quickly spiral into a business-ending event if you don't have a disaster preparedness program.*

For business owners like you, a disaster preparedness plan is an investment that ensures business continuity, protects employees and assets, safeguards your reputation and ensures your business complies with regulatory requirements.

However, as a business leader, there's a lot that needs to be done to prepare your organization for disasters. Since every disaster is different, a disaster preparedness program helps you gauge its impact on your business.

Let's discuss how various disasters can hurt your business:

### *Natural disasters*



Hurricanes, floods, tornadoes, earthquakes and wildfires are all disasters that damage your IT infrastructure and disrupt communications and power supplies, leading to data loss, downtime and revenue loss. Natural disasters can also cause injuries and fatalities if employees are present at the workplace during a disaster.

*Health threats*



Health hazards, such as the flu and other severe illnesses that can spread fast, can significantly impact your employees, customers, business partners and suppliers.

*Cyber-attacks*



Phishing, malware and ransomware are cyber-attacks that can hurt your business in multiple ways. Cyberattacks compromise your IT systems and data, leading to downtime and financial loss. You lose customer trust and may face compliance woes, including heavy fines for failing to detect and stop a breach.

*Power outages*



Businesses may face power outages due to a grid or equipment failure. Natural disasters can also cause power outages. This disrupts IT operations, leading to downtime, data loss and revenue loss.

*Equipment failures*

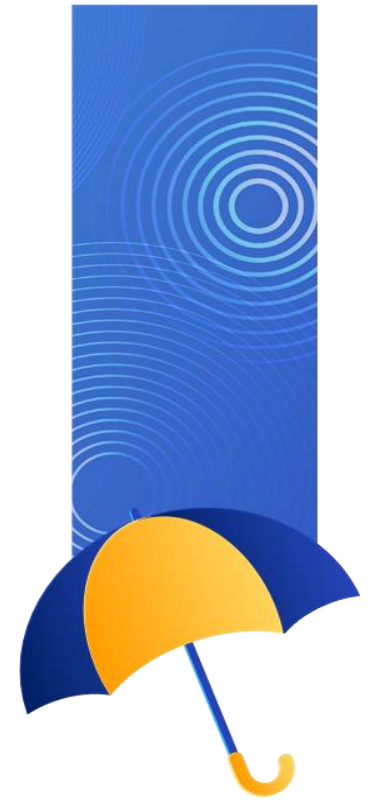


Equipment failures are a common occurrence. Server crashes, network and hardware malfunctions are equipment failures that cause IT disruptions, leading to data loss, downtime and revenue loss.

*Human-caused hazards*



Human-caused hazards like conflict and violence, accidental fires and spills, epidemics and biological hazards have wide-ranging consequences for business operations



## Potential Business Impacts of Unexpected Incidents & Disasters

**Unexpected incidents and disasters can have severe consequences for your business. They can disrupt operations, damage assets, harm employees and cause reputational damage. Let's dive into how disasters, both natural and man-made, have the potential to impact your business.**

*Risk to employee safety*

Unexpected incidents and disasters can compromise the safety of your employees. Natural calamities and even man-made incidents cause injuries, health issues and even loss of life.

*Physical damage to buildings, equipment, inventory and infrastructure*

Disasters can destroy your business premises, equipment, inventory and vital infrastructure, necessitating extensive repairs or replacements for business continuity.

*Data loss or breach*

Data loss or breaches caused by a cyberattack can compromise sensitive customer information and lead to legal and financial consequences.

*Business interruptions, downtime and closures*

Disasters disrupt business operations, causing significant downtime, interruptions and potential closures. This, in turn, can impact your revenue generation and customer satisfaction.

*Financial losses and increased expenses*

Natural calamities and man-made threats cause heavy financial strain on businesses. Businesses affected by disasters face financial losses due to revenue decline, increased repair expenses and raw materials costs. Sometimes the cost of disaster recovery is too much for small businesses to bear, forcing some of them to close shop.

*Reputational damage*

Mishandling incidents and disasters can lead to reputational damage, loss of customer trust and negative public perception. Businesses that have effective crisis management and transparent communication gain customer trust even during a disaster.

## Some Benefits of Disaster Preparedness in IT Security

Disaster preparedness in IT security is crucial for businesses. Here are some of the key benefits for businesses:



### *Ensures business continuity*

Disaster preparedness for IT security helps ensure an organization's critical systems and data are available and secure during and after a disaster.

Businesses can minimize downtime and swiftly recover from unexpected incidents.

### *Protects against data loss*

By creating regular backups and securing them in a safe location, you can protect your business against data loss from a disaster or cyberattack.

### *Reduces recovery time*

A strong disaster preparedness program reduces the recovery time after a disaster or cyberattack.

### *Limits unexpected expenses*

By implementing a robust disaster preparedness plan, you can avoid financial losses associated with recovery efforts, legal liabilities, reputational damage and potential regulatory fines.

### *Avoids reputational damage*

A disaster preparedness plan can help you avoid the reputational damage

that often leads to lost customers and revenue loss resulting from an unexpected incident.

### *Improves compliance*

Disaster preparedness measures can help an organization comply with industry and regulatory standards for IT security.

## 5 Components of a Comprehensive Disaster Preparedness Program

A comprehensive disaster preparedness program is vital for businesses like yours to mitigate risks, ensure business continuity, prioritize employee safety and maintain their reputation. However, many organizations don't have the knowledge or expertise to build a solid disaster preparedness plan. These simple steps can quickly get you started. You can additionally consider taking the help of an experienced IT service provider to develop a robust plan without burning a hole in your pocket.

### **1 | Build a team**

- Build a dedicated team led by a program coordinator. While the program coordinator will lead the overall disaster management program, you can assign additional roles and responsibilities to other team members.
- Define clear, achievable objectives for the program, including policies, regulations, budget, schedule, resources and evaluation.

### **2 | Planning**

- Identify threats, hazards and potential disruptions to business operations and IT infrastructure by conducting a thorough risk assessment process.
- Conduct a business impact analysis to help identify critical processes and impacts from disruptions.
- Identify ways to prevent, reduce and mitigate risks to your business.

### **3 | Develop an implementation strategy**

- Identify business-critical resources and assets.
- Develop a plan of action to respond to disruptions, resume business operations and manage communications.
- Develop an emergency response plan that ensures employee safety and protects your business property.
- Develop a detailed business continuity plan that can identify, counter and minimize risk from potential threats and ensure business process continuity.

- Create an IT disaster recovery plan with a clear strategy to quickly restore hardware (servers, desktops, laptops, etc.), software and data.
- Develop a crisis communication plan that lays down procedures with clear objectives, processes and strategies to communicate to your employees, customers and suppliers.
- Build an incident management system with clear protocols to restore regular operations and resolve incidents during unplanned interruptions.
- Conduct regular training to improve disaster preparedness among your employees.

4 | Testing and exercises

- Evaluate your business’s preparedness plan to test its effectiveness and find gaps.
- Carry out routine exercises to assess employee disaster readiness.

5 | Improve preparedness program

- Test and review your preparedness program.
- Identify and fix the gaps.

IS YOUR BUSINESS  
**PREPARED?**

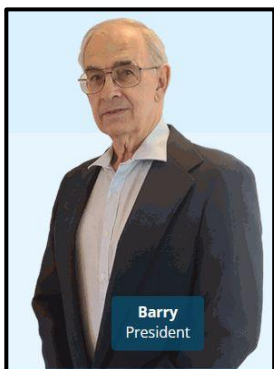
**Don’t let a disaster stop your  
business from growing.**

Contact us today to develop a disaster preparedness  
program that helps you weather the storm.

**Remember, your cyber security strategy is also a crucial part of your disaster preparedness plan.**

Best practices must include:

- **Protect your IT infrastructure and data.** Your data is a gold mine for cybercriminals.
- **Back up critical data.** Recovery can be costly, time-consuming and seemingly impossible.
- **Improve employee awareness.** Your employees are your weakest link without training.
- **Review insurance policies.** It’s a good idea to have property insurance, business interruption insurance and cybersecurity insurance to cover all bases.
- **Evaluate vendor and supplier preparedness.** Any weak link will only increase your vulnerability.
- **Review and revise your preparedness strategies.** Test for weaknesses and shortcomings regularly.



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

**FIGHTING CYBERCRIMINALS ON YOUR OWN CAN  
BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.**

**CONTACT US TODAY**

**FIND OUT WHAT IT’S LIKE TO HAVE  
OUR CYBERSECURITY EXPERTS IN YOUR CORNER.**

We are offering a FREE Network Security Audit with no obligation. You will receive a “Cyber Security Audit” outlining our findings following the audit. Again ... **NO Obligation....**

**Sirtawn Systems**  
Your Cyber Security Experts

Phone: (905) 947-1636  
Website: [www.sirtawn.com](http://www.sirtawn.com)