Acumen Consulting
connect. create. educate.

https://www.acumen-corp.com/

EVERY BUSINESS MUST HAVE
A DISASTER RECOVERY PLAN (DRP)

Every business must have a disaster recovery plan (DRP)

As a business owner, you might have come across the term “Disaster Recovery” quite often. Whether it is natural calamities like hurricane, floods, wildfires, or terror attacks, a disaster recovery plan can safeguard your business. Leading business consultants stress the importance of having an up to date disaster recovery plan in place and consider it a part of the best practices for running a business. A business without a disaster recovery plan is actually just one mishap away from permanent shutdown.

What is a disaster recovery plan?

A disaster recovery plan is a blueprint to respond and recover from an unforeseen mishap or event. It could be anything--a fire at your place of business, a flood, hurricane, terror attack or even a malware attack. Any of these events could paralyze your business. A disaster recovery plan need not be just about IT. In fact, it shouldn’t be. It should cover all angles of the business including inventory, staff, relocation--basically every element that has a role to play in keeping your business up and running.

Why do you need a disaster recovery plan?

A disaster recovery plan presents step-by-step instructions on what needs to be done in the event of a disruptive event to keep the business operating smoothly. While a DRP cannot instantly eliminate all the negative effects that a disaster may have on your business, it can certainly help you do some damage control. Here are some consequences of a disaster that a DRP can help mitigate.

Client dissatisfaction

If you face a disaster, chances are your clients are impacted by it as it. If your servers are down due to an IT issue or you are unable to deliver due to XYZ reasons, you are inadvertently putting your clients in a spot. Phones or emails go unanswered because telecommunication lines are down, your customers will become frustrated.

Brand image and reputation

Certain disasters like a ransomware or virus attack can shut down your entire IT infrastructure and stop your business from running. To add to the damage, they are often accompanied by the possibility of data leak and customers, and in some case the media, must be notified. The entire scenario gives your brand image and reputation a bad rap.

Revenue loss

A disaster that interrupts your business operations brings along revenue losses.

A DRP is key to minimizing the damage to your clients, brand image, reputation and to limit possible revenue losses caused by disasters. It also prepares your staff better to handle emergencies.

What should your disaster recovery plan contain?

A list of your key contacts

Your DRP should clearly list contact information of all the people who need to be apprised of the disaster. The list should include the names, title in the company, addresses, phone numbers and email IDs of these emergency contacts. When preparing this list, think big. It should not only contain the details of your C-level execs, but also of other key personnel like HR managers, IT head (even your MSP if you have one), client facing managers, etc.

A list of all the software programs, apps and hardware that you use

Your DRP should contain an inventory of all the softwares, apps and hardware used by your business. This list should mention details pertaining to each of them such as

- The name of the app/software
- Version/model number (for software/hardware)
- Vendor name and contact information for each of them
- Warranty/support availability details
- Contact information for customer support pertaining to these hardware/apps

The list should also identify the application or hardware as critical or non-critical. Some companies follow a rating system, wherein you can assign a score to an app or hardware that helps determine how critical it is.

Your list should also mention how often the application is used (weekly, monthly, daily, annually) or if it is used on specific days or dates.

Information about backups

This is one of the core elements of a DRP. Your DRP should contain information about backups. It should mention

- How often are data backups to be conducted
- Which data backups are available (This should ideally be ALL)
- When was the last backup done for each data set
- Where and in which formats are the data backups available

Plan B

Your DRP should contain a Plan B for operations that should come into play when a disaster strikes to interrupt your regular business operations. It can include information about

- Availability of any alternative workspace from where your business can function in the event of a disaster
- Alternative workflows such as options to work remotely or to allow employees to bring their own devices to work (BYOD) until the time regular business premises or systems are ready
- Who (what roles/titles) are to be excused from working during the contingency period and which ones absolutely essential

Floor plans and location

Your DRP should also include floor plans of your offices with the exit and entry points clearly marked up, so they can be used in the event of any emergency. It should also mention the location of data centers, phones, key IT systems and related hardware.

Process definition

This is the key element of a disaster recovery plan. This is what brings the different elements of your DRP discussed above, together. Your DRP should clearly define the process or standard operating procedures to be followed in the event of an emergency. This section should list the to-dos in a clear, actionable manner.

At this time you should also lay down rule for a DRP audit at regular intervals to ensure your DRP is up to date. This is very important as DRPs may not be used at all for years, and may lose relevance by the time an actual emergency occurs.

Implementation of your disaster recovery plan

Putting together a disaster recovery plan for your business is just the beginning. The next step is to create a team for your DRP project. When putting together a team,

1. Decide will take ownership of the whole DRP implementation
2. Break down the DRP into smaller elements and decide who is accountable for each of them

Mock Drills and Dry Runs:

After your DRP is ready, conduct a few mock drills/ dry runs to check how it really works. Such drills will help you identify loose ends, if any, in your DRP and help you be better prepared for implementation of the DRP in the event of a real disaster.

Conduct a debrief of your disaster recovery plan implementation

It is important to conduct an after-disaster analysis to check how useful and effective your disaster recovery plan was during an emergency. This analysis must be recorded and can help improve your DRP in future. The debrief session should

1. Identify the losses you incurred from the disaster
2. Quantify the time taken for implementation of the disaster recovery plan
3. Identify the key positives of your DRP implementation
4. Offer suggestions for improvement in the existing DRP

Disaster recovery planning is an extremely essential element for business success and cannot be ignored. No matter how big or small a business you are, DRP is your lifeline in times of emergencies. Bigger companies often have their own staff (IT as well as non-IT) for disaster recovery planning, but for SMBs to have their own DRP team can be a bit of a strain on their resources. Consider teaming up with a MSP who is experienced in disaster recovery planning, so you don't cut corners now to regret later.

Acumen Consulting, 1735 South Big Bend Blvd, Saint Louis, MO, 63117

CONTACT DETAILS

Deb Wagnon

Acumen Consulting

Email: dwagnon@acumen-corp.com

Phone: 314.333.3330

https://www.acumen-corp.com/