A publication of

ImpTrax

Solutions that make a difference

How to create a Disaster Recovery Plan that Works

The Biggest risk to your business is being unprepared

Because of fast and expansive technological developments, no business can function without incorporating IT (Information Technology) anymore. Speed is an essential component of business practices which makes rapid and efficient processing of information a requirement. It's required to communicate with suppliers, clients and your marketing audience—making IT essential to business success.

However, the IT department is not immune to disasters. Despite advances in technology there are still many threats that can create problems—ranging from a disruption of a single IT function to the destruction of an entire system or whole software infrastructure.

IT's importance requires a comprehensive disaster recovery plan. When disaster strikes there must be a way to continue operations and IT functions at a sustainable level. It's important for businesses to understand the impact of looming IT disasters to encourage them to implement adequate plans.

How Necessary is an IT Disaster Recovery Plan?

It's easy to live in denial of the necessity of a disaster recovery plan (DRP). Business owners may think modern technology has enough built-in fail-safes to guard IT systems. Unfortunately, this couldn't be further from the truth. As technology gets more advanced, attacks and imminent dangers expand. Apart from natural disasters that you can never predict you must plan for the human component as well.

What Statistics Tell us

According to Redspin's seventh annual cybersecurity report, 2016 has seen a significant increase in cyber attacks[1]. This increase is reported to be 320 percent higher than previous measurements taken. No industry can ignore this threat since a huge focus of hacking is about accessing members of the public's information. This puts any business that stores client or personnel information at incredible risk.

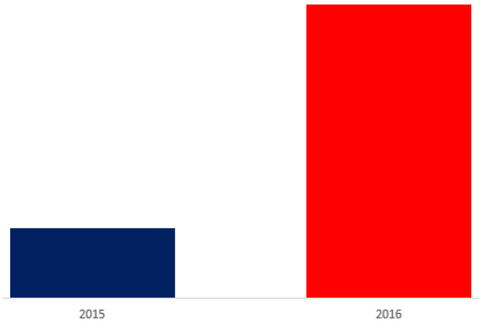

Figure 1: 320% increase in cyber-attacks for healthcare organizations

In addition, 2017 saw an uncommon rise in natural disasters such as hurricanes, fires and other climate change events[2]. Some storms affected areas that had never experienced such a disaster before. Keeping this trend in mind it would be foolhardy to assume that any area is completely safe. With global warming on the rise, your business' future is more at risk than ever.

What do You Put at Risk?

> *"75 percent of businesses fail within three years after a major disaster"*

IT risks can influence many aspects of your business:

- Loss of data prevents you from functioning
- Hacked data can ruin your business' reputation
- Your bottom line will suffer when operations fail to function

This makes a DRP essential to business success. Here we discuss various aspects you must consider in drawing up your plans.

[1]Health IT Outcomes "Cybersecurity Report Shows 320% Increase In Hacking Attacks In 2016" https://www.healthitoutcomes.com/doc/cybersecurity-report-shows-increase-hacking-attacks-0001 Accessed 23 Oct 2017

[2]The Economist "Weather-related disasters are increasing" https://www.economist.com/blogs/graphicdetail/2017/08/daily-chart-19 Accessed 23 Oct 2017

It's About Continuity not only Recovery

It's bad practice to only put a recovery plan in place. The importance of a continuity plan has made people use the two terms—DRP and Business Continuity Plan (BCP)—almost interchangeably.

When businesses don't consider both these perspectives, they put themselves at higher risk.

"A BCP enables you to continue with essential business functions when a disaster takes place, while your DRP repairs your IT system"

If your business experiences a complete breakdown in IT services, you haven't planned well enough. The DRP forms part of your continuity process to function optimally once again, but until you reach that state of activity you must be able to handle minimal tasks at least.

Benefits of Dynamic BCPs and DRPs

The results of dynamic plans speak for themselves:

- A detailed plan describes what must happen in the case of an emergency. When personnel know what is supposed to happen less decision making and guidance is necessary. This minimizes downtime until the business is back up and running.
- A BCP puts backup systems in place. You need these to function even before the DRP has an effect. When your backup system allows for basic activities to continue, you won't lose respect from consumers and you can still operate to fulfill some of your duties and reach your goals.
- Because many disasters can include people's information, a proper plan is essential to limit legal implications you may face. If you can protect Personally Identifiable Information (PII) and prove you can be trusted there's less chance of legal repercussions.
- The benefits of a DRP even have effects before disaster strikes. Employees feel secure when they know proper plans are in place. It creates a more relaxed working environment and leads to improved productivity.

Business owners and CEO who are serious about long-term success will include all manner of contingency plans in their long-term planning. Dynamic long term planning isn't only about economic factors but possible disasters too. As stated above disasters can't be predicted. All types of problems must be anticipated and planned for.

Understand Which IT Areas are Influenced by Disasters

Business owners and their management teams must understand what encompasses IT infrastructure. When one part of this system is missed in the planning phase, an entire system can be prevented from getting back online.

IT Components to Consider

You must have contingency plans for each of the following components:

- **Networks:** You must know the quickest way to establish a secure network after a disaster strikes. The focus here is on secure. If natural disasters result in network problems, it's the ideal time hackers will try to infiltrate businesses. Do you know how to create a network in the shortest amount of time so your business can get back online? This is essential for team members to get access to your information once again.

- **Servers:** Where your data is stored can be one area that presents you with a problem. When servers are destroyed or breached new ones must be acquired. Servers can be your own or the service providers who host your IT network. The latter creates an additional threat since you don't have control over how they manage or secure their servers. It's essential your BCP includes sourcing the most secure service providers and finding out how to access others if the originals are compromised.

- **Computers and laptops:** Each computer device used on the network helps you perform your duties. Unfortunately, they also serve as points of access to your network that hackers can use to access your network. To recover after a hacking disaster, you must ensure each computer provides secure access once again.

- **Wireless devices:** Each member of your team who accesses the IT system wirelessly—or through Smartphones—need to ensure it happens in a secure way.

- **Data:** Where is your data kept? Firstly you must ensure that a backup of your data is always accessible. As part of your BCP, you must ensure access to this data can be established quickly, even if access is limited to certain parties only. Your DRP will aim to establish normal functioning once again so users can access and use data. This requires collecting and storing data before disasters take place.

Expert knowledge of each system is essential when orchestrating a plan. When putting together a DRP, IT technicians should form part of the planning process. They will understand the importance of each of these units and how they impact each other. A system will recover its original function only through managing each connection point. And this is your ultimate goal.

Know what Types of Disasters to Prepare for

A DRP requires detailed steps on how to achieve optimum functioning. But each type of disaster calls for different steps.

Here are a few possibilities:

Hardware failure: You have no guarantee that an IT network's hardware will work consistently. Having insurance on the parts does not constitute a DRP. You must plan how the hardware will be replaced in the shortest amount of time so employees can continue work. These may be temporary units while you source new permanent versions. Suppliers and costing information must be available to the DRP team.

- **Human error:** Anyone working for your business can accidentally cause an IT system to malfunction. While you have security features in place, no one can prevent someone dropping hardware or entering faulty information. It's important to know how you can limit the impact of human error and get the system back to normal.

- **Common natural disasters:** The list of natural disasters is endless. The common ones are listed below and should be included in anyone's contingency plans. The question is what you do when each of these takes place. While some may require fighting the event—such as a fire—others call for shutting down the system and evacuating the area.
    - Fire
    - Fallen trees
    - Storms
    - Earthquakes
    - Lightning
- **Uncommon natural disasters:** These are uncommon and are usually limited to certain natural features:
    - Volcanic eruptions when you're near volcanoes
    - Tsunamis if located near an ocean
    - Landslides in hilly areas
    - Limnic eruptions if located near lakes

- **Hacking/Malware:** This is a manmade threat where hackers—or their malware—infiltrate your software and IT systems. Expert hackers can shut down your entire system or extract private information from it.

Which of these do you need plans for?

Your Plan

It's important to understand that a DRP must be a comprehensive yet simple and user-friendly plan employees and partners can follow.

After determining which of the threats above are probable and how the events will influence each part of your IT network you need step by step plans to counter the event's effects.

Determine what Happens Beforehand

A DRP can't be a hypothetical plan you outline and place in your safe. You must have proof it will work or it's useless.

Put a Team Together

For a plan to take effect each activity and responsibility must be taken care of by a team member. Part of your DRP is allocating actions to certain personnel. You may even have to contract people from outside your company if you realize your team needs help.

Budget

Nothing in business can take place without calculating the financial effect on the business. Each expense in your plan must be calculated so you know your financial risks when disaster strikes. When something happens, you can quickly prioritize expenses without wasting time on sourcing prices.

Remember, A DRP is about reinstating business operations as soon as possible. Anything you waste time on after the disaster translates into lost income. You can prevent this from happening by doing adequate research even before there's a problem.

Test the plan

How realistic was your team's prediction of the impact of a disaster? You won't know until it's tested. Make sure the plan doesn't show its problems when disaster strikes. Have a dry run when the plan is finalized. This will show you the areas of improvement in your plan and also help the team practice their role.

Your plan will contain different stages. Here's what you must include.

Determine what Happens Immediately

Your goal straight after disaster strikes is to limit damage and re-establish basic functionality. This forms part of your BCP. Here are questions to help you think this through:

How can you minimize damage to equipment?
Where will you operate from if your buildings are compromised?
How can you gain access to your data?
Which hardware can you set up fast?
Who will handle the duties of setting up and continuing business activities?

Determine what Happens Later

While some staff members can handle the interim period activities, others need to re-establish your long-term plans:

- Prepare your premises if you can return to it
- Establish a secure network
- Install new hardware items if they were damaged
- Establish access to data again

Allocate Timelines

In all of these, you need to allocate timelines. Persons handling the tasks must know what is expected of them. Your research and testing beforehand will help them handle this in the shortest possible time.

Handle Challenges

It's important to note that the unforeseen nature of disasters will cause challenges to pop up. It's a business owner's responsibility to ensure these don't prevent the execution of the plan:

- **Staff shortage**: After a disaster responsibilities increase while staff numbers stay the same. One way of circumventing this is to hire temporary staff.
- **Buy in factor:** When everyone in a business—employees and management—don't all commit to the plan it can cause great losses when time is wasted. Ensure everyone takes part in testing the plan so you know there aren't any loose ends. Instil faith in the plan so people follow it without question.

No business should operate without such a proven plan in place. The challenges of sacrificing time and effort to create your plan is an investment for the future. The possible losses you can incur because of a poorly-written plan far outweigh the time and money you need to invest in one now.

Checklist

Here's a quick checklist to help you keep track of your DRP and BCP:

The components you need to plan for: ☑
- Network/Servers
- Devices
- Data

The disasters you need to plan for: ☑
- Human error
- Hardware problems
- Natural disasters

Stages of your DRP: ☑
- What is necessary before?
- What happens immediately after the disaster?
- What is your long-term plan?

Did you test your plan? ☑

Did you strategize to circumvent all possible challenges after testing the plan? ☑

Focus on your core business and leave IT to us

ImpTrax provides an entire IT department–from CTO to support and engineering–to help you solve your IT challenges.

- **Our reputation**– We've been in business for more than 20 years and have earned the trust of numerous, long-term clients that continue to call us year after year.
- **Our people**– Our people are industry veterans with years of experience under their belts. We never stop learning either. We ensure our techs continue their education and training to stay up to date with the latest trends in technology.
- **We have everything you need –** You don't need to go shopping for your IT needs. No need to get a specialist for this or that. We take care of everything. Whether its process automation, software development, technology support, network and technology stack deployment or maintenance we'll have you covered.
- **We're human (and we talk that way)** – We speak in plain English just like you. No time or need for complicated tech acronyms and hard to follow jargon.
- **Client satisfaction guaranteed** – Your growth and satisfaction is the cornerstone of our success. We want you to be completely satisfied with our services and we will do whatever it takes to make sure this happens.

Contact Us | Our Services

Healthcare Revenue Optimization Solution

Software Development

Technology Consulting

Cybersecurity

Disaster Preparedness & Response