IT Disaster Recovery Planning: Essential to Business Survival

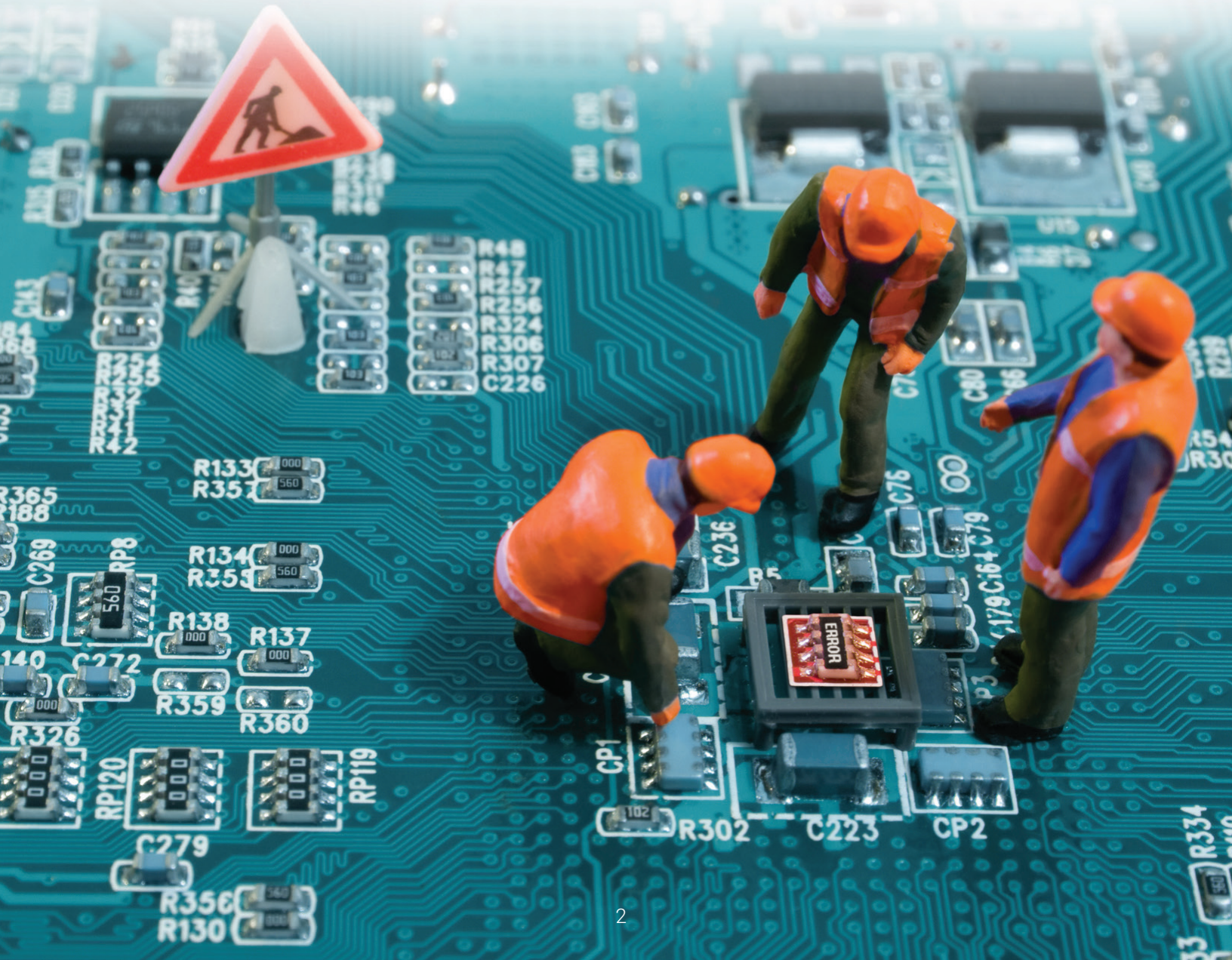
©2018 RCN Telecom Services, LLC. All Rights Reserved. | www.rcn.com/business

Executive Summary

Disasters can happen to companies of every size. Earthquakes, floods, hurricanes, tornadoes; Mother Nature is an equal opportunity destroyer. Manmade disasters like targeted hacking and Distributed Denial of Service (DDoS) attacks, fires and accidental system outages may be more limited in geographic scope but can be equally devastating to affected businesses.

This White Paper is intended to provide basic guidance mainly to small- and mid-sized businesses (SMBs) and small enterprises that do not currently have a disaster recovery plan for IT systems and data.

An effective IT disaster recovery plan may be the difference between business survival or failure after a catastrophic event. This document reviews the elements of and processes for building an IT-centric disaster recovery plan. Also discussed are simple disaster avoidance and preventative measures any business can take to mitigate damage and recover quickly from an unexpected interruption to the IT side of business operations.



Is Your Business Ready For A Disaster?

Disasters happen. Some with warning, some without. Some emergencies have obvious causes; others take time to diagnose. Outages could last just a few hours or stretch for days, weeks or even months. The only thing we know for certain is that disasters are a not a matter of *if*, but *when*. To paraphrase the US Army, anything can happen, so you've got to be prepared for everything.

Increased Dependence on Technology = Increased Vulnerability

Your business's reliance on technology is a double-edged sword. While computers, data networks and hosted voice systems have allowed companies to exponentially increase productivity, expand operations and enhance communications, these same technologies can grind entire operations to a halt in seconds if they fail. Additionally, the shift from paper to electronic records across all industries, from retail to healthcare, means ensuring stable network and power connectivity, and fast failover is vital to business operations and profitability[1].

Disasters, whether natural or manmade, do not discriminate based on the type of business, its size, age or location. When servers fail the ripple effect on businesses can hurt companies and customers located time zones away from the point of origin.

Many large enterprises, utilities and most government agencies are required by law to have disaster recovery plans in effect. But what about small- to medium-sized businesses? Their order histories and customer databases, inventory, billing and payroll systems, and telecommunications networks are just as critical to the health and well-being of these businesses as they are to Fortune 500 companies. Maybe more so, as SMBs typically do not have ready access to alternative sites for relocation, or the IT/communications system redundancy in place to recover quickly from a catastrophic event.

Some small businesses' disaster recovery plans are as simple as "grab the PC and go." Don't think it can't happen to you. There is no threshold for vulnerability when it comes to disasters. As an SMB, you may not have thought much about disaster recovery, but it can't hurt to take some tips from larger enterprises that have.

What Is Information Technology Disaster Recovery (IT DR)?

Disaster recovery (DR) planning is about preparing for and enabling the appropriate response and recovery to an event that results in a business unable to conduct normal operations[2]. The goal of disaster recovery is to anticipate an interruption in service to minimize impact on revenue through a swift return to normal operations. This white paper limits the scope of disaster recovery to information technology-related issues and steps needed to keep data safe and maintain business continuity in the event of an emergency. **IT DR is therefore defined as creating a plan to minimize potential interruptions to a company's data and/or voice network and restoring full functionality to the information technology infrastructure as quickly as possible**[2].

It doesn't have to be The Big One

Disasters do not have to be natural or monumental in scope to destroy a business. In fact, the larger the event, the rarer they occur. Hurricanes like Katrina and earthquakes along the San Andreas Fault fortunately are few and far between. This gives many businesses the false sense of security that a catastrophe will not affect their business. Rather, smaller disasters that happen much more frequently and strike anywhere without warning can be just as debilitating.

It may be a burst pipe that floods office space and shorts out the network, smoke damage from a fire in the business downstairs that renders the entire building uninhabitable, a power outage from a lightning strike hitting a transformer, a targeted cyberattack, or a simple hardware failure. It's not necessarily a function of duration either. A system breach or outage lasting just a few hours can disrupt a business for days or weeks after the event.

Whatever the cause or extent, the impact of network downtime and/or data loss on a business could mean[3].

- Loss of revenues from the inability to deliver products or services and conduct transactions during the actual outage period.
- Loss of future business from customers who defect to competitors to fulfill immediate needs and never return.
- Reduced credibility/customer trust in conducting ongoing business with your organization.
- Increased expenses to re-capture lost customers.
- Months to rebuild lost customer databases, order histories or supply chain information.
- Lower profits and/or the threat of business failure through the inability to communicate with customers, suppliers and employees to restore operations quickly.
- Exposure to legal fees and federal fines from possible compliance violations.

Many businesses cannot survive an extended outage. Even small events that cause businesses to suspend operations for three days or more can trigger an exodus of customers that can be fatal. Research by the University of Texas has shown that **only 6% of companies suffering from a catastrophic data loss survive**; 43% never reopen and 51% fail within the ensuing two years[3].

The smart business will therefore have an IT disaster recovery plan in place to minimize financial impact, reduce downtime and speed the return to normal operations. Having an IT DR plan in place also helps eliminate panic. It provides a roadmap of actionable steps written with a calm hand in the event of an unexpected outage or data loss, and becomes even more critical when management is absent or incapacitated for any reason. **But where to begin?**

Disaster Preparedness Steps

There are some simple ***disaster avoidance*** and ***preventative measures*** any business can implement:

- ✔ **Backup! Backup! Backup!** The number one best practice for IT DR is data backup. Companies should perform periodic back up of critical files in an easy to access off-site storage medium to maintain current records. A full backup may be very time and space consuming depending upon the database size. Many businesses perform *incremental* or *differential* backups in which only files created or modified since the last backup are saved.

  How often should backups be performed? That depends. How long can the business escape harm without access to emails and data transactions? The answer is the minimum backup frequency.

- ✔ **Distribute an updated list of key management business and personal contact information** to select employees in the event of an emergency.

- ✔ **Assemble a list of emergency contacts** for all IT vendors, utility and telecommunication partners.

- ✔ **Maintain secure employee access privileges** to the data center at all times.

- ✔ **Install an Uninterruptable Power Supply (UPS) generator. Install a second generator** or a battery backup system in the event the first UPS fails.

- ✔ **Contract with multiple ISPs.** Have a secondary network connection and internet service provider ready to take over for the primary carrier if disaster strikes *their* network.

- ✔ **Position fire suppression equipment appropriately throughput the premises.** Check and test periodically and make sure employees know how to use the equipment.

- ✔ **Install elevated flooring in IT rooms** if located on ground level to guard against water damage.

- ✔ **Enter into a reciprocal agreement with a similar business or organization** to share space and access to IT and telecommunications in the event of a disaster.

Ancillary Benefits of IT DR Planning[4]

In addition to having plans in place to quickly restore data networks, accounting/order entry systems and telecommunications, companies with an effective IT DR plan also realize:

- **Improved business processes.** Because all facets of the IT infrastructure undergo detailed analysis, companies almost can't help but find areas for improvement.

- **Improved technology.** Many companies find they need to update current IT systems to achieve disaster recovery objectives. This often leads to better performance across the entire IT infrastructure as well as energy savings and a reduced carbon footprint.

- **Fewer disruptions.** As a result of improved technology, events that used to cause minor outages like server crashes or viruses don't happen as often.

- **Higher quality services.** Because of improved processes and technologies, the business delivers better service to its customers and supply chain partners and enjoys better communication among employees and internal business units.

- **Competitive advantages.** Promoting the existence of a solid IT DR plan allows a company to claim higher availability and reliability of service, which in turn makes the company more valuable to prospective customers over competitors that do not have a plan.

- ✔ **Consider outsourcing Disaster Recovery as a Service (DRaaS) to off-site third party providers.** SMBs typically are not in the data center management business. It may make sense, therefore, for companies to find a strategic partner to help manage IT infrastructure and data center disaster recovery services. Renting or co-locating these services may be more cost efficient for SMBs and small enterprises rather than building, housing and staffing a redundant IT infrastructure in another facility. When outages strike for any reason, IT services failover to the secondary site almost instantaneously, preserving business continuity.

  When investigating DRaaS providers, ideally the host should be located in a separate geographic region with a low risk of natural disasters and have access to dual power and network feeds for redundancy. It should be far enough away from the primary business site so there is little chance of it being impacted by the same disaster. Finally, ensure the selected DRaaS data center provider is fully compliant under SSAE-16, SOC 2, Privacy Shield, HIPAA and PCI standards, as well as any other regulations relevant to your industry[2].

- ✔ **Know the proper authorities to call after an event** to report security breaches, alert consumers/media, or if there are any legal ramifications stemming from the outage.

Stay In Control When Things are Out of Control

An IT disaster recovery plan is designed to restore critical IT operations at the same or alternate site after a disruption. The ultimate goal is to enable temporary operations while the primary system is brought back online as soon as possible[2]. When an IT outage occurs for any reason:

Step 1: Determine the cause. Is the event a widespread natural disaster, localized fire, human error or hardware failure?

Step 2: Assess damage. What systems are affected? Are other areas of the business still operational? Will data be permanently lost? Are people and property at risk?

Step 3: Estimate length of potential outage. Will the network be down for minutes, hours or days?

Step 4: Disaster declaration? Determine if the severity of the event, its impact and estimated downtime warrants the initiation of disaster recovery procedures. If so, assemble key management and emergency response team members and implement the IT DR plan.

Step 5: Communication. Ensure all internal stakeholders are aware of the incident and are constantly updated as to progress toward recovery. Alert customers, partners and vendors if possible, with a potential timeframe for return to normal operations.

3 Types of IT Disaster Recovery

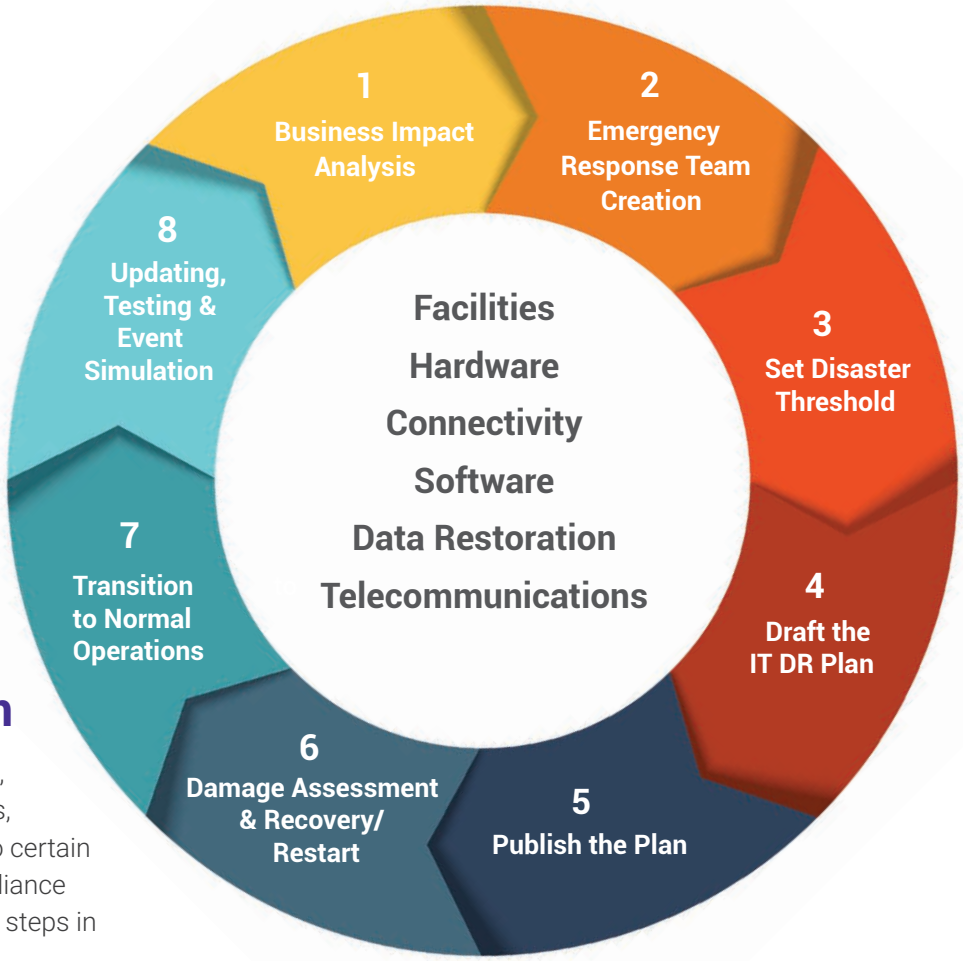
Before discussing the elements of and process for building an effective IT DR plan, it is important to note the differences in the types of IT environments and some considerations for effective disaster recovery strategies in each.

- **Data Center Disaster Recovery.** This refers to the traditional on-premises IT department with servers, switches and hard drives physically located in the same facility as the primary business operation. Internal IT personnel must be prepared to handle any event that disrupts business. They have total control over their IT infrastructure, but also must have the manpower, equipment and expertise on site to restore power, replace hardware and troubleshoot telecommunications and ERP systems to keep the business running.

- **Cloud-Based Disaster Recovery.** As computing technologies shift to the cloud, many SMBs and small enterprises are switching to cloud-based service providers for their data storage and real-time data management needs. Businesses employing this strategy need only to maintain a secure, stable connection to the service provider. In the event of a disaster at the business site, all vital records are safely stored in the cloud. The trade-off is that the business has no control over cloud performance or disaster recovery capabilities of the provider should the cloud fail. There is still only one IT entity serving the business. Companies considering this alternative should investigate the cloud-based data center provider's own disaster recovery procedures and redundant power and network connectivity capabilities before committing.

  One possible solution for SMBs is to use their on-premises data center as the primary IT infrastructure and enter into a contract with a cloud-based DRaaS provider for disaster recovery/backup purposes.

- **Virtualization Disaster Recovery.** The issues facing companies employing a virtual computer network environment are akin to cloud-based disaster recovery. In this IT model, the entire network including the operating system, applications, patches, updates and all data are stored and run on a software-based server. This means there are fewer physical devices to track and repair, but companies must have a plan in place to backup data and replicate the virtual server to access the network from an off-site location in the event the primary location becomes inaccessible. Then, all that is required in the event of a disaster or network outage is a process to flip the failover switch to a new virtual host.



Building An IT Disaster Recovery Plan

The type of business and IT environment, the volume and kinds of data it generates, the physical location and susceptibility to certain types of natural disasters, and any compliance issues will dictate the specific actionable steps in an IT disaster recovery plan.

Ready Business

Business Impact Analysis Worksheet

Department / Function / Process _____

Operational & Financial Impacts

Delay / Duration	Operation Impacts	Financial Impact

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- < 8 hrs. < 24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Considerations (estimates for your business)

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact

Quantify operational impacts in financial terms.

ready.gov/business

However, every plan should include the following elements at a minimum[4,5,6]:

1. **Begin with a Business Impact Analysis (BIA).** This is a risk assessment exercise that identifies all time-sensitive and mission critical functions and processes in each business unit and the resources required to support them. Develop a questionnaire or go to Ready.gov/business to download a BIA worksheet (pictured) from FEMA for managers to document and quantify the operational and financial impact of a disaster on their department and any interdependencies with other business units. This will create an inventory of documents, files and hardware to help identify the most valuable data, drives, libraries and systems that should receive priority in the event of a disaster.

2. **Create an emergency response team (ERT).** Develop a contact list of the most critical employees who will be called in to work first during a crisis. ERT members should have the expertise to implement the processes to restart/restore operations in their respective department, and should be assigned any cross-over IT DR roles and responsibilities beforehand to avoid confusion, such as addressing the media. Then designate and train a back-up employee for each ERT member, as every primary ERT member may not be available when the time comes.

3. **Set a disaster threshold.** Define the level of event severity that qualifies as a disaster to trigger implementation of the plan. This is not about the *cause* of the outage, but rather pinpointing a **recovery time objective (RTO)** – the maximum length of time a system or application can be unavailable before the business is negatively impacted by downtime or data loss.

4. **Draft the plan.** Use the information from the BIA to document the processes, milestones and/or manual workarounds needed to recover data and restore IT operations in order of the identified system priority. [For an on-premises data center this could involve all the steps needed to rebuild the IT side of the business from the ground up. For businesses using a cloud-based or virtual network, it could be setting the disaster threshold to contact the DRaaS provider.]

5. **Publish the plan**. Each ERT member should have at least two hardcopies of the finished plan, one at the office and another at home. Make sure mid-level employees know where to find the plan in case ERT members are not available. Put a copy of the plan online – on a separate digital platform – that will be accessible through alternative means if the hardcopies are inaccessible.

6. **Establish damage assessment and recovery/restart roles and responsibilities.** Know who is going to analyze what. Ensure that each individual has the managerial and/or financial authority to initiate restart processes as outlined in the IT DR plan or allocate funds to replace/repair damaged equipment as quickly as possible.

7. **Transition back to normal operations.** Know when it's time to "go home." Remember, the goal of IT DR is to maintain normal business operations on a secondary network or location while the primary system is being restored. Outline the minimum requirements needed to function before transferring operations back to the primary business site.

8. **Updating and periodic testing.** Every IT DR plan should be regularly reviewed and updated to reflect any changes to software applications, operating system versions, hardware and personnel. Further, the plan should be tested periodically through drills and event simulations. It's not enough to have the IT DR binder on a cubicle shelf. People need to practice emergency procedures to keep them top of mind when a crisis happens. Testing will also identify and help correct any gaps or weak spots in the plan.

Parts of the IT DR Plan[5,6,7]

An effective disaster recovery plan should account for the following IT infrastructure components:

- **Facilities** – the physical data center environment such as climate control, backup power supply, fire suppression, protection from water damage, and maintaining secure access to prevent sabotage.
- **Hardware** – networks, routers and switches, server racks and hard drives, desktop workstations and laptops, mobile devices and peripherals.
- **Connectivity** – maintaining stable communications with an internet service provider via fiber optic, cable or wireless connection.
- **Software** – email, ERP and HR applications, office productivity and project management packages, licenses and contracts.
- **Data restoration** – emails, transaction histories, patient records, customer accounts and internal financial records.
- **Telecommunications** – hosted voice (VoIP) and voicemail systems tied into the IT network.

In sum, the biggest mistake most companies make is waiting until after a disaster strikes to figure out what to do next. Statistically, that can be a death sentence for a business. No one has ever gotten into trouble for being overly prepared, but many businesses have failed because they weren't able to recover from a catastrophic event. The best advice is *don't wait*.

Developing a comprehensive IT DR plan is a huge undertaking that could take several months to coordinate and require buy-in from multiple stakeholders. Don't let that stop you. If you must, start with an interim plan that covers just the basics like maintaining connectivity to the ISP and power supplies, restoring telecommunications ASAP, and grow from there.

Need more information? Talk to your **RCN** representative to learn how we can help with your data redundancy plan for the unexpected.

Sources & Acknowledgements

1. *The State of Business Continuity Preparedness,* Forrester Research and Disaster Recovery Journal, 2011
2. *Disaster Recovery White Paper,* posted by Online Tech, 2013
3. *Top 5 Reasons Why Your IT Disaster Recovery Plan Should Be A Top Priority,* onlinetech.com
4. *IT Disaster Recovery Planning for Dummies* by Peter Gregory, Wiley Publishing, Inc., 2008
5. *Ready.gov/Business Continuity Plan,* Office of Department of Homeland Security
6. *7 things your IT disaster recovery plan should cover,* posted by James Martin, csoonline.com, 7/2017
7. *Business continuity and disaster recovery planning: The basics,* posted by Derek Slater, csoonline.com, 5/2015

RCN BUSINESS

©2018 RCN Telecom Services, LLC. All Rights Reserved. | www.rcn.com/business