4imprint®

Blue Papers®

Emergency Planning for Small Business

4imprint.com

Danger, Will Robinson: Emergency planning for small businesses

An emergency is defined as an urgent event—usually unexpected—that requires immediate action. Often when we think of emergencies, we think natural disasters, pandemics, accidents or terrorism and we rarely think of these events in the context of the office.

But this is a grave mistake: Nearly 30 percent of small businesses in the United States experienced a disaster over the past three years and at least one in four of those businesses never reopened.[1]

What's more, these disasters and emergencies were not limited to weather, fire or rare occasions of violence … but the effects were just as crippling. Consider the disasters or emergencies that can occur from an angry former employee, a hacker, the loss of proprietary information or the theft of trade secrets.

The good news is that you can take actions today to prepare your small business for disaster tomorrow. 'Plan for the worst, hope for the best' is the mantra of many emergency preparedness plans for a reason. Emergency planning can help your business address what to do, how to do it and what to communicate to whom in the event that something goes awry. Having plans in place well in advance of potential disaster will not only ensure that your business is protected, but it can give you the confidence to handle a situation with a calm, focused head translating into less time spent freaking out and more time spent effectively addressing the needs at hand.

Rally the troops

Emergency planning should be conducted as a team. Plans are useless if only one or two people know they exist or what is in them. As you begin planning, obtain input from across departments and compile all plans and important contact information in binders or electronic files. These binders should be kept safe in a central location, in a fire-proof room or cabinet, both on and offsite. Should you choose to store this information electronically, don't skip the section on backing up and securing online and electronic data—otherwise, if your internal server gets knocked out so will your entire emergency plan and information.

1 *"BellSouth Emergency Preparedness and Recovery for Small Businesses." AT&T Small Business Bundles Services - AT&T Wireless, AT&T DSL, AT&T Local Services. Web. 03 Nov. 2009. <http://smallbusiness.bellsouth.com/emergency/>.*

Determining the risks

While it's impossible to plan for all possible disasters, a business should plan for all probable disasters. Conduct a risk assessment—with internal staff or with external help from a risk assessment consultancy—that addresses factors such as geographic location, surrounding buildings or sites, weather patterns, security threats, employee screening processes, value and risk of stored data, and any current protection efforts. Also discuss which type of emergency and what kinds of losses would be most damaging to your business: Could you continue to operate without accounts receivable? If you lost customer data? If marketing plans were destroyed?

A story of contingency planning in the real world

Spurred on by the Y2K frenzy that hit just before the turn of the century, a small business located in Mobile, Alabama set out to assess their overall emergency risks. Equity Technologies Corporation first identified workers to serve as key contacts for the 72-employee operation. These key contacts then established safety and security teams which analyzed the entire business's risk and emergency plan.[2]

Through thorough risk assessment, the team realized that the single most important operational factor in an emergency would be communications between the company and the outside world. They developed their plan with this in mind and purchased generators to power the phone systems and computers in situations of power loss.

Ultimately, the risk assessment opened their eyes to very real dangers that had never occurred to them before. "We learned that being prepared means being ready for any kind of emergency, be it hurricane, utility disruption or man-made disaster," said President and CEO Cathy Anderson-Giles.

Just like Equity Technologies Corporation discovered, risk assessment can help focus your emergency planning and can serve to demonstrate areas of strength or weakness in any current plan.

Making sure it's always business as usual

Businesses should also assess day-to-day functions and operations to determine which staff, materials, procedures and equipment are absolutely necessary to keep business operating, no matter what. Then put processes in place

2 *"Small Business Case Study." Ready Business. Web. 10 Nov. 2009. <http://www.ready.gov/business/_downloads/smallbiz.pdf>.*

that determine how these necessities will be facilitated during and after an emergency. This is known as a contingency plan and this part of the overall emergency plan has a very broad scope. Compiling it involves:

- Updating business flow charts and establishing a hierarchy of management responsibility. Make it clear who is in control in an emergency situation, who should be notified or called upon, in what order, and by what means.
- Updating staff files with personal e-mail addresses and phone numbers. If you need to reach employees and e-mail, intranet or phone systems are down, you're going to need this information to successfully communicate.
- Establishing or designating a page within your company's intranet, an e-mail account or hiring an answering service for employees to make contact with during or after an emergency to check in to let management know that they are okay and accounted for.

- Addressing emergency payroll and accounting systems—a way to track money spent and earned during an emergency and a means for ensuring employees still get paid.
- Keeping an updated list of vendors, suppliers, delivery personnel, neighbors and other resources or persons interacted with on a regular or daily basis. These lists should be easily accessible in the event of an emergency—on or offsite.
- Determining alternate locations for conducting business. If an emergency occurs onsite, how will business continue as usual? What should employees expect? Paid leave? Furlough? Continuing work from home? Or, an established alternate work place?
- Ensuring that files with essential client data and contact information are accessible offsite. Basic plans for continuation of services to them in the event of an emergency also need to be outlined.
- Addressing the processes for accessing e-mail, voicemail, backed up data and electronic files in the event of an emergency.

The contingency plan serves as the backbone of the overall plan. Read on to discover the specifics of these points and others in relation to the different aspects of emergency planning and response.

The emergency plan: protecting the people, the data, the investments

The people

As a small business, your team is your company. Take measures to ensure their safety before, during and after an emergency by providing emergency and survival kits, outlining emergency protocol and evacuation processes and identifying areas of shelter or cover. Be sure to hold practice drills throughout the year to reduce chaos or confusion in the event of a real disaster.

The easiest step you can take in protecting your employees in the event of an emergency is making sure that emergency supplies are available onsite. Depending on the size of your office or facilities, make sure these items are available in all departments and on each floor and be sure to consult your state and city requirements for exact number of kits to make available. The American Red Cross[3] and the U.S. Department of Homeland Security[4] recommend that each kit contain:

- Flashlight
- Battery-powered or hand-crank radio (NOAA Weather Radio, if possible)
- Extra batteries
- Matches
- First aid kit and book
- Tool kit—especially containing wrenches and pliers, necessary for turning off utilities
- Buckets
- Plastic sheeting and duct tape (to shield a room if necessary)
- Paper, pens, markers and scissors
- Garbage bags and plastic ties
- Whistle to signal for help
- Dust or filter masks
- Emergency contact information and a copy of your emergency preparedness plan and copies of insurance policies, bank account records, supplier and shipping contact lists and other pertinent documents.
- Maps of the building (with critical utilities marked) and of the surrounding area

3 "Be Red Cross Ready - Get a kit. Make a plan. Be informed." American Red Cross. Web. 19 Nov. 2009. <http://www.redcross.org/portal/site/en/menuitem.d8aaecf214c576bf971e4cfe43181aa0/?vgnextoid=a7c51a53f1c37110VgnVCM1000003481a10aRCRD&vgnextfmt=default>.

4 "Ready.gov: Talk To Your People." Ready.gov - Prepare. Plan. Stay Informed. Web. 10 Nov. 2009. <http://www.ready.gov/business/talk/index.html>.

If your business is at high risk for a natural disaster such as a hurricane, earthquake or tornado, you are more likely to experience disasters that keep you onsite for extended periods of time. For this reason, in addition to the supplies above, make sure there is one gallon of water per person per day for drinking and sanitation and a minimum of a three-day supply of non-perishable food items plus:

- Kitchen supplies such as can openers, knives and utensils, napkins, paper towels
- Hygienic supplies like moist towlettes, hand sanitizer, toilet paper, feminine hygiene products, bleach
- Comfort supplies like blankets, extra clothing and pillows
- An emergency satellite phone, with charger (these are different from cellular phones in that they do not rely on towers, but rather satellites to transmit and receive signals—guaranteeing that you can call for help even if office phone lines are disconnected and cell phone towers are down)

You will want to work with your local fire marshal and property manager to draft evacuation maps for fire escapes and a shelter plan for where employees are to take cover in the event of earthquakes, tornados and hurricanes and creating plans for when to stay and when to evacuate. Also make it clear in your plan who within your company has the authority to make the call for staying or leaving in an emergency situation.

Along with these plans, develop maps and protocol for dealing with an armed person in the building or an intruder—how will the building be locked down while employees are evacuated?

Post all finished maps in common areas in your workplace that also identify an assembly site for all staff to meet once evacuated. These maps and protocol should also be included in your overall plan and binders.

Other necessary measures to protect your employees include requiring all staff to take CPR certification, first aid classes and regular disaster trainings and annual review and reassessment of your overall plan.

The data: storage, security and back up

The information a business stores on customers and employees, along with trade secrets, documents and financial information, is the lifeblood of day-to-day

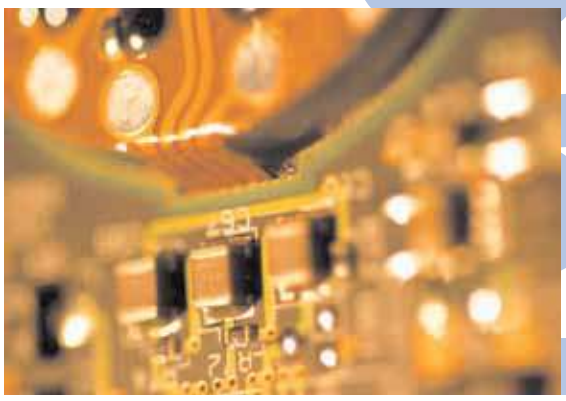
survival and success. Unfortunately, it's also the meal ticket for hackers worldwide. As such, unsecure data is a ticking time bomb—it's like locking your most precious and expensive belongings in a safe, but leaving the combination on top. What's more, by taking measures to protect your data and store it in more than one capacity, your business will be more likely to recover data after disasters like fires, floods, hurricanes or power surges.

When you first set up your office, it's likely you addressed the question of where or how to store files, data and software in a central, secure location. Onsite servers are the popular response. Hopefully, when you set up your server your business took appropriate measure to start your data protection and storage on the right foot. When setting up a server, Tara Wisdorf, risk advisory services consultant with Jefferson Wells, recommends changing all default IDs and passwords and removing or disabling services that are not needed or will not be used. She adds that restricting access and accessibility is key.

"If you store nonpublic data, use common sense," says Wisdorf. "Don't, as one client did, have the server next to a regular external glass window on ground level where it was seen by anyone walking past the window."

It's quite common to find servers in locked, interior, climate-controlled rooms at larger companies and for good reason. As a small business and depending on the data you store, you may not have a need to store servers this securely. Your overall risk assessment when preparing your emergency plan should help you determine the level of security needed, but you may have chosen to forgo external help in conducting this assessment. In this case, it is strongly recommended to still bring in an external consultant or firm, like Jefferson Wells, to specifically conduct a risk assessment based solely on data storage ad computer and Internet usage.

Once you address the initial question of where and how to store files and data within your offices, consider next how to back up this data in the event of an emergency.



So, what should your business back up and how?

Back up the following:[5]

- Bank records and financial information and databases
- Mailing and contact lists and databases
- Customer or client information

5 *"Backing up: What, how, where - Microsoft Protect." Microsoft Corporation. Web. 10 Nov. 2009. <http://www.microsoft.com/protect/data/backup/about.aspx>.*

- Software purchased on and downloaded from the internet
- Outlook or other e-mail and calendaring systems, plus corresponding archives
- Files, photos and documents necessary to conduct and continue work

As far as your options for backing up, Wisdorf says there are many options depending on the size needed to accommodate files and your budget. "Daily tape or disc backup with rotation to secure offsite storage is the most common backup process for small businesses," says Wisdorf. "There are also many online backup services available."

Backup options to consider include:

- Discs and tapes
- External hard drives
- Backup servers
- Online backup and storage services, some of whom also provide e-mail archiving and encryption, IT security audits and services like continuity management and data loss prevention consulting

Wisdorf stresses that whatever type of backup is utilized, it is very important to test restoration of backups and to do so regularly. She also notes the all data that is backed up to tapes, discs or portable external hard drives should be encrypted—just in case these are lost or stolen.

Security of the files and data stored is the next issue to be addressed. The Payment Card Industry Data Security Standards (PCI DSS) has outlined the following standards for storing and securing credit cardholder information, but these standards really apply to all electronic data and files:[6]

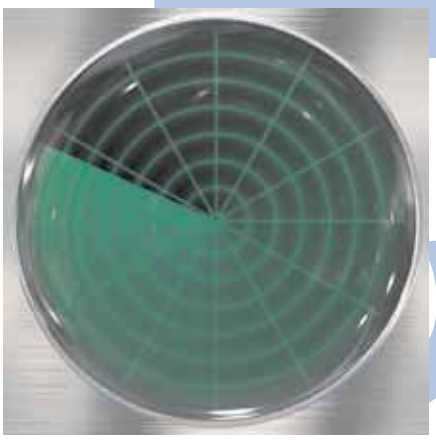
1. Build and maintain a secure network—install and maintain a firewall configuration to protect data and do not use vendor-supplied defaults for passwords or IDs.
2. Eliminate prohibited data—check with your POS systems or payment software to confirm that your software does not store magnetic strip data, CVV2, Pins or encrypted pin blocks. Also confirm that the data your systems and software are storing is only data that is absolutely necessary and appropriate for the transaction type. Typically, it is permissible to store cardholder name, primary account number, expiration date and service code, but to reduce risk to small businesses, it is recommended that none

6 *Visa USA | More People Go with Visa. Web. 03 Nov. 2009. <http://usa.visa.com>.*

of this information is stored but rather processed per transaction and deleted.

3. Protect cardholder data—if it is absolutely necessary to store credit card information or magnetic strip data, account information should be encrypted.
4. Maintain a vulnerability management program—use and regularly update anti-virus software and develop and maintain secure systems and applications. Be sure to replace missing or outdated security patches and establish software upgrade policies and procedures to ensure patches are reviewed and installed in a timely manner.
5. Implement strong access control measures—restrict access to data based on necessity and assign a unique ID to each person with computer access. Also restrict physical access to credit cardholder data.
6. Regularly monitor and test networks—track and monitor all access to network resources and cardholder data and regularly test systems and processes.

While we're hitting on the topic of credit card information, allow us to point out that Visa recommends that small businesses do not store any credit card information to reduce liability. Small businesses are at increased risk of falling victim to hackers. [7]



Bill Shore, manager of security at Carnegie Mellon University and former supervisor of the FBI's Computer Crimes Squad in Pittsburgh, said that hackers have moved beyond simply seeking fame and glory to more sinister motivations.[8]

"Now they are trying to keep under the radar," Shore said. "They are much more profit motivated. They're trying to find ways to get access to money."

Keep your money out of their pockets—protect your data!

The investments

We're not talking about your stocks and financials here, we're talking about your assets—your building, office supplies and equipment. If you haven't already, get insurance that will not only cover your premises in the event of a fire or theft, but will protect the people in your building and any accidents or disasters that could occur. If your risk assessment deems appropriate, seek additional coverage

7 Visa USA | More People Go with Visa. Web. 03 Nov. 2009. <http://usa.visa.com>.

8 Lyons, Kim. "Protecting data from danger." Pittsburgh News | Pittsburgh Business Times. 16 May 2008. Web. 02 Nov. 2009. <http://pittsburgh.bizjournals.com/pittsburgh/stories/2008/05/19/focus1.html>.

for flood, earthquakes or other business interruptions; many businesses make the expensive mistake of assuming this kind of coverage is included in basic insurance policies when they usually are not.

Also take the time to plan for utility disruption and consider the purchase of a back-up generator to provide power to your building and computers in the event of power failure. This is especially crucial if your business chooses to defer offsite backup of data.
Copies of insurance information, along with inventory lists of all high-valued office items and electronics with serial numbers, and utility contact information should be easily found in your plan binder or electronic plan files.

Take care to keep expensive equipment, cash, financial information, confidential files (hiring files or proprietary information or data like trade secrets) locked up and install security systems, especially if your risk assessment identified an increased risk of crime or theft based on your location or the nature of your work. If your business operates primarily on paper files, consider making electronic scans of especially crucial documents.

Who's going to answer that 3 a.m. phone call?

In the event of an emergency or crisis, perhaps the most important part of handling the situation at hand is communication. Whether your business's emergency is a natural disaster, a data loss by a disgruntled employee, or the theft of customer data, you need to be prepared to disclose emergencies and crises and address questions of staff, investors, the public and the media.

Essentially, there are two kinds of crisis or emergency plans: Those that address internal audiences (your employees) and those that address external audiences (everyone else).

Ideally, in your emergency planning, a preliminary crisis or emergency communications plan will be created—outlining possible scenarios and a plan for communicating to all audiences for each.

As your communications plan develops, know that there is always a hierarchy of concern—one that for many is natural but will reinforce credibility with audiences: Be concerned for victims first, employees second and customers and investors third. Of course, sometimes the victims are employees, customers or investors.

A solid crisis or emergency communications plan is built on the following ten action steps and points:

1. Contact senior level staff and communications personnel immediately.

2. Secure the site of the crisis and gather facts, working cooperatively with authorities.

3. Work with communications staff to create a communications command center and designate a spokesperson. If your business lacks an experienced communications team, now is the time to consider consulting a public or crisis communications consultant or agency. Outside help may not be necessary for things like natural disasters, but topics with broader public interest like scandal and data loss require professionals. Create talking points and key messages, anticipating the questions that will be asked and practicing the response. Repeatedly. Develop messaging knowing that in interviews, your spokesperson will need to speak calmly in a conversational tone and stop talking once they have made their point and expressed and recapped all key messages.

4. Your messaging should also communicate your action plan—what are the next steps? What is your business doing to resolve the situation and ensuring that it does not happen again? Remember that actions speak louder than words—you will be expected to follow through with this action plan and you can expect to be called out if you don't.

5. Avoid jargon in your messages; this can work against your messages and key points by creating further confusion.

6. Don't speculate in your messages—stick to the facts!

7. Be accountable—don't blame others. It is possible to be accountable without admitting guilt or wrongdoing by simply acknowledging that an event has occurred.

8. Tell the truth. Always. There isn't a crisis communications lie on this planet that wasn't ousted eventually and you can bet your bottom dollar that the fallout of lies far exceeds the fallout of the crisis to begin with.

9. Remember that the media is not the bad guy—they can and often will help you get your message out during a crisis or emergency. Just remember that they are doing their job; there is no such thing as "off the record" and don't argue with reporters or go on the defensive. Perhaps most importantly, when dealing with the media know that silence is not golden. Nor is a statement of "no comment." In fact, that's not a statement. That's the media relations kiss of death. Not commenting opens the floor to the public filling the void with rumor and speculation and in many cases, doing so appears to be admission of wrongdoing, apathy or negligence. There are of course situations in which you will be legally prohibited from providing a direct comment to a crisis such as a pending lawsuit or legal action—but usually in these situations although you cannot go into specifics, you should still be able to draft a canned response.

10. Use multiple channels to get your messaging out. Media are often the first to come knocking when word of your emergency or crisis gets out, but keep the message in your control by consistently communicating with multiple channels. Utilize social media such as Twitter™, Facebook℠ and blogs and update your Web site as the crisis or emergency is dealt with. Many companies have found great success in temporarily turning their home page or adding a specific landing page into an online communications command center. Larger companies also often implement hotlines for those affected by the crisis or emergency to call for information or assistance. As a small business, this may be an unnecessary gesture. In your case, don't discount the power of personal phone calls or e-mails.

A story of crisis communications and data loss[9]

Heartland Payment Systems®, one of the United State's largest payments processors experienced a massive security breach in early 2009 when hackers gained access to computers it uses to process 100 million payment card transactions per month for 175,000 merchants.

Unlike many who find themselves at the helm of the embarrassment and outcry caused by data breaches, CEO Robert O. Carr acted quickly and accountably to address the

9 *"The Quintessential Data Loss Response." BulletProof. Web. 11 Nov. 2009. <http://www.bulletproofblog.com/2009/11/02/the-quintessential-data-loss-response/>.*

issue. Within a few days of receiving investigators' clearance to disclose the hack, Heartland had reached out to all of the merchants involved and countless consumers with the same consistent message of concern for, commitment to, and action on behalf of those affected.

After the company announced that it would be accelerating development of an encryption system to protect credit cardholder data throughout the payment process, most stakeholders would have considered Heartland's response adequate. But Carr understood that true leadership in crisis often requires going above and beyond what's expected. So, he cofounded the Payments Processing Information Sharing Council, an organization that disseminates information on the latest threats to data security. In doing so, Heartland is now leading an effort to see that no company ever experiences such a large data breach again and demonstrating its commitment not only solving its own problem, but a problem that could potentially impact any business, in any industry, at any time in the process. Heartland not only responded ideally to the situation, they turned it into an opportunity to learn from their mistakes and become industry thought leaders.

Practice makes perfect

You've likely noticed that practically every section of this Blue Paper mentions practicing and testing. That's because the only way to make sure that emergency preparedness plans will be effective in real-life situations is to practice and prepare others. With a solid plan in place that addresses contingency planning, people, data, investments and communications in a variety of emergencies, and lots of practice, your business will feel confident in being prepared for the worst so employees and other stakeholders only know your best.

Resources and templates

Additional resources and templates for contingency and emergency planning and checklists, visit the following Web sites:

- U.S. Department of Homeland Security's Ready Business: www.ready.gov
- The Canadian Centre for Emergency Preparedness: www.ccep.ca
- Government of Canada/Gouvernment de Canada Get Prepared: www.getprepared.gc.ca
- American Red Cross: www.redcross.org