Disaster Preparedness - How Ready Are You?

The Systems Thinking Approach® to

Creating a Business Disaster/Continuity Plan

By Jeri Denniston and Gary Rossi

It was a beautiful day in North San Diego County where Softec has their headquarters. Nancy Mandell, the IT and Operations Manager was reviewing the firm's strategic plan and making edits to her section in preparation for the Executive Team's retreat next week. Feeling the sun streaming in through her office window, she gazed out and saw something a little concerning. In the distance was a plume of smoke. She quickly checked the internet for local news and learned there was a fire burning out of control about 10 miles north. Winds were kicking up and blowing in a southwesterly direction, and Softec was right in the path.

Time to put Level I of our disaster plan into action, thought Nancy. She e-mailed Bob, her direct report responsible for company-wide IT communications. "Put Level I of our disaster plan into action. There's a fire burning north of us and it may beheaded this way. I want all staff on alert."

Steve Wilder, the Marketing Director, was having a staff meeting in his office when the alarm rang on his computer and his Blackberry simultaneously. His two managers felt their Blackberries buzz at the same time. They checked their PDA's and each had received a text message: "Possible fire headed this way. Level 1 of Disaster Plan activated." Steve quickly wrapped up their staff meeting and called in the rest of the department.
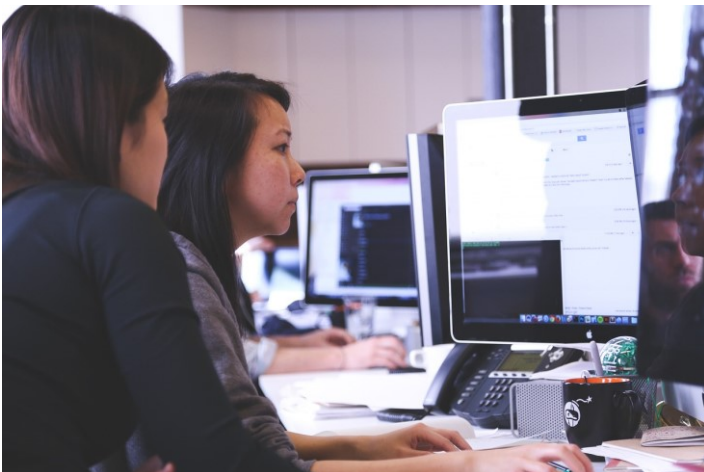
"Level 1 of our disaster plan has been activated. Pull out your disaster plans and begin making the appropriate preparations," he instructed everyone.

Similar activity was taking place throughout the company. Messages went out to all computers and blackberries. An announcement was posted on the company intranet. Human Resources Manager, Carol Standers had her Employee Relations Representative post announcements on all bulletin boards, and the Telecom department issued a companywide voicemail announcement. Additionally, an announcement was made over the public address system. An alert went up on the company website to inform customers and suppliers of the current situation and how to contact Softec if necessary.

President Joe Baum called his Executive Team into his office for a quick meeting. "Ok, what's the status?" he asked. "We're monitoring all news channels to track the path of the fire," said Nancy. It's still 10 miles away, but the wind's kicking up. Security's been in touch with the Fire Department and they will alert us if it looks like we need to evacuate. Level 1 has been activated and we're in a watch and wait mode, she added."

"Good work," said Joe. "Let's hope it doesn't go beyond this."

Jeri Denniston: 858-357-9600 x5 • jdenniston@dennergroup.com • Gary Rossi: 858-538-7988 • Baldrigecoach@yahoo.com

They filed back to their departments and teams to continue with preparations. Within the next two hours, things had changed dramatically. The fires had spread and were headed in their direction....fast. Nancy activated Level 2. Again messages went out via intranet, email, and text messages. Alerts were posted on the company's websites and emails went out to customers to alert them to the company's possible evacuation. Personnel were instructed to pack up critical documents, laptops, and important personal possessions. Everyone was on high alert. Employees whose homes were in the path of the fires were told to go home and take care of their families. Once they and their families were safe, employees were instructed to call into the out of state 800 number that had been previously set up for just such an event.

Level 3, emergency evacuation, was activated an hour later after a call from the Fire Department .All employees were instructed to evacuate to safe locations except those who were part of the disaster preparedness team. After checking in with their own families, the president and his disaster team headed for their prearranged disaster headquarters. Their disaster plan included three different locations within the county depending on the location of the impending disaster. Again messages were sent via internet, intranet, text messages and voicemails to all cell phones, and e-mails to employees, customers and suppliers. The company had also made arrangements for backup network operations at two different remote locations, both outside the County. The first one was activated, and the network operations were switched to that location. This meant no disruption of email, or document file access, enabling employees to connect remotely to the network and continue working. Within an hour, the building and parking lot were empty.

the fire's progress, coordinating calls and information updates both to and from employees, suppliers, customers and government and emergency personnel. 12 hours later, they were informed that their building complex had been spared and they were cleared to return. Notices went out to all employees that they could return to the office the next day. Customers and suppliers were notified via email the next day that they were back in their offices and open for business. A similar message was posted on the company website. Thanks to the advance preparation and quick action of the disaster team, there was no business interruption. Three employees had lost their homes and five had suffered damage, but fortunately no one was hurt.

While this is an example of a fictional company, it could happen to any of us. What did this company do that made the difference? Is your company equally prepared? Here's a simple plan you can follow to ensure your organization weathers a disaster as well as Softec did.
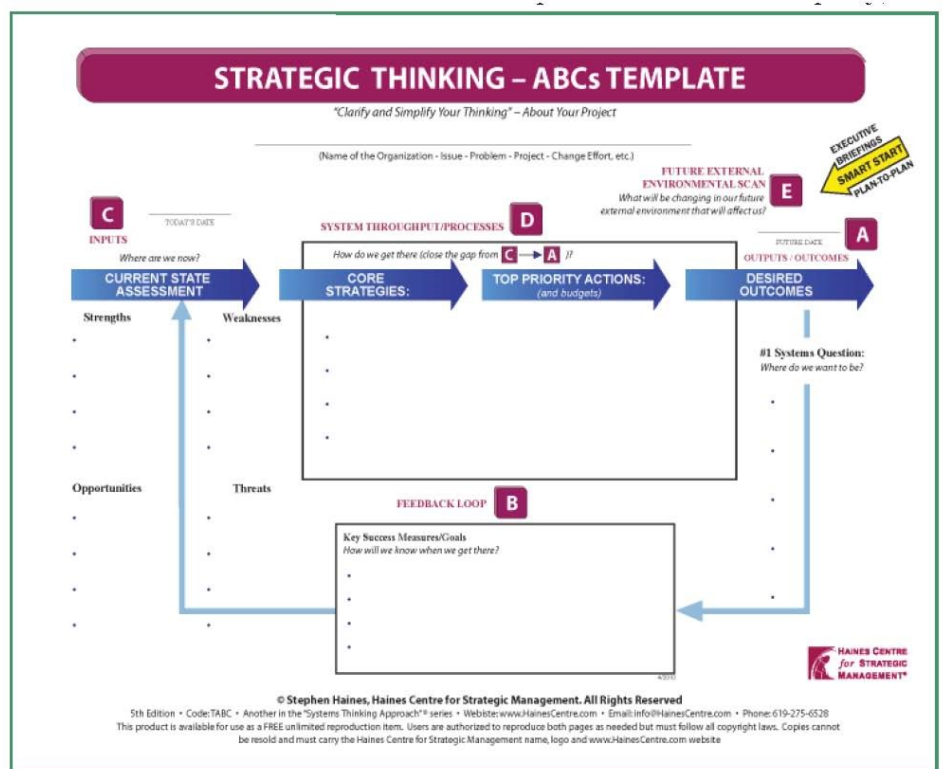
Create a Business Disaster/Continuity Plan.
Where do we want to be in an emergency?

Put the systems, structures and procedures in place to ensure you can stay open for business or get back in business within 24 hours. How did Softec do this? They had a vision for how they would continue to operate in the event of an emergency. This included pre-established remote locations so they could switch their network to a remote facility and keep the critical computer operations humming.

They put communications plans in place for two-way communications between the company and staff and clients so everyone knew the status of the company and the employees. And they made it possible for key employees to work remotely, accessing their files and staying in communication with company personnel and clients. Once you have created your disaster plan, it is important to review it at least annually when you do a review and update of your strategic plan.

Establish key success metrics. How will we know everything's working successfully?

If you don't have a strategic plan, create one, and be sure that disaster preparedness/business continuity is part of it. When preparing your disaster plan it's a good idea to identify metrics for tracking how well you are implementing the plan. These might include the different ways to communicate both with employees and clients - your company intranet, your website, email, text messages, etc. They should include an update of the number of employees that have been trained in what to do, where to go and where and how to call or email in the event of a disaster. A regular communications plan also should be included that identifies how frequently you will be training, informing and reviewing the disaster plan with employees, as well as how frequently and in what way you will keep your customers informed in the event of an emergency.

Do a current state assessment. Do we have the right structures/teams in place?

Evaluate your current situation and assess how prepared (or not) you are in the face of an emergency. Use the following Quick Assessment to determine your level of preparedness in the critical areas:

- Employee contact list
- Key supplier/vendor information
- Key contacts
- Critical business functions
- Recovery location
- Shelter in place procedures
- Vital records
- Critical telephone numbers
- Supplies
- Equipment/machinery/vehicles
- Computer equipment and software
- Voice/data communications
- Identification of risks: fire, flood, earthquake, tornadoes, power outage, etc.

Some steps to take for little or no cost

No Cost:
- Meet with your insurance provider to review current coverage. Create procedures to quickly evacuate and set up shelter-in-place.
- Talk to your people about the company's disaster plans. Two-way communication is key before, during and after a disaster.
- Create an emergency contact list that includes employee emergency contact information.
- Create a list of critical business contractors and others you will use in an emergency.
- Talk to utility service providers about potential alternatives and identify back-up options.

Under $500:
- Buy fire extinguishers and smoke alarms.
- Decide which emergency supplies the company can feasibly provide, and talk to your workers about supplies individuals might want to consider keeping in personal and portable supply kits.
- Set up a telephone call tree, password-protected page on the company website, an e-mail alert, or a call-invoice recording to communicate with employees in an emergency,
- Use and keep up-to-date computer anti-virus software and firewalls.
- Elevate valuable inventory and electrical machinery off the floor in case of flooding.

More than $500:
- Consider additional insurance such as business interruption, flood or earthquake protection.
- Purchase, install and pre-wire a portable generator to the building's essential electrical circuits.
- Upgrade your building's HVAC system to secure outdoor air intakes and increase filter efficiency.
- Hire a security professional to evaluate and/or create your disaster preparedness and business continuity.
- Send safety and key emergency response employees to trainings or conferences on disaster preparedness.

Develop key initiatives or strategies. To ensure a successful execution plan

Once you've identified your current state of preparedness, list the key initiatives you need to take to bridge the gap of where you want to be in terms of preparedness and where you are today. This should include departmental action plans in critical areas that need to support the plan. Create a matrix that identifies each key initiative and the actions supporting those initiatives. For each key initiative, identify the champion and who else to involve, as well as the date by when the initiative will be completed. For each action task, identify the person responsible and who

SKEPTIC WORKSHEET
Future External Environmental Scanning/Trends

List the 5-10 Future External Environmental Trends - Projections facing you over the life of your plan:
(Implications for your organization today - i.e, Opportunities and Threats come next: Backwards Thinking)

S Socio-Demographics (People/Society):

K Competition/Substitutes:

E Economics: **E** Ecology:

P Political/Regulatory:

T Technology:

I Industry/Suppliers:

C Customer/Citizens:

© Stephen Haines, Haines Centre for Strategic Management. All Rights Reserved

5th Edition • Code: TABC • Another in the "Systems Thinking Approach"® series • Website: www.HainesCentre.com • Email: info@HainesCentre.com • Phone: 619-275-6528
This product is available for use as a FREE unlimited reproduction item. Users are authorized to reproduce both pages as needed but must follow all copyright laws. Copies cannot be resold and must carry the Haines Centre for Strategic Management name, logo and www.HainesCentre.com website

---

Business Disaster Preparedness & Survival Quick Assessment

Is your business prepared in the event disaster strikes? Below are some guidelines to help you determine your level of readiness. Your company is in a good state of readiness if you can answer yes to most of these. For the complete Quick Assessment tool, visit www.dennergroup.com or call Eric Denniston: 858-603-2047.

- We ensure our employees know what emergency supplies the company provides and which ones the staff should consider keeping on hand.
- We have a detailed evacuation plan for our business.
- We have a prioritized list of our company's critical operations, staff and procedures for recovery.
- We have a Cyber Security plan which includes computer software and hardware.
- We have established grab and go boxes throughout the company and employees know where they are.
- We have a detailed training regime that we exercise at least annually.
- We conduct an annual disaster plan review.
- We have a 3-year strategic plan which includes an emergency disaster plan.
- We have a 1- to 3-year business plan.

else he or she needs to involve to get the job done, as well as the date by when each action will be completed. Establish the appropriate procedures to follow up monthly and ensure that the actions and initiatives are being addressed.

Scan the external environment often to determine might trigger an emergency

Conduct an environmental scan at least annually, and even more frequently depending on the conditions under which you're operating. If you operate in a high risk environment, then a monthly scan may be necessary to check the external factors that could precipitate a disaster. If you operate in an area prevalent with tornadoes during certain times of the year, then a frequent external scan is necessary only during tornado season. Set up the appropriate structures and procedures so these scans are completed and reported to your disaster planning team as frequently as indicated in your plan.

If you follow each of these steps, you should be as prepared as our mythical Softec was in the face of an emergency. At some point in the life of a business, there will be a critical emergency that tests the organization's preparedness and ability to continue operating. Don't wait until then to discover your level of preparedness. Take the steps now to ensure your company's and your employees' safety.

Jeri Denniston 858-603-3425
Jeri@Dennergroup.com
www.dennergroup.com

Gary Rossi 858-533-7988
Baldrigecoach@yahoo.com
www.thebaldridecoach.com

DO NOT DUPLICATE WITHOUT EXPRESSED WRITTEN CONSENT

For additional copies please contact jeri@dennergroup.com