Insurance Institute for Business & Home Safety®

MAKE TELECOMMUTING PART OF YOUR BUSINESS CONTINUITY PLAN

What is telecommuting? Telecommuting is a growing workplace strategy that allows employees to work from home or any location away from the office, while staying connected through various I/T networks. Today, telecommuters make up a small but growing segment of the everyday workforce—growing nearly 80 percent from 2005 to 2012, and now representing about 3 percent of non-self-employed workers. However, beyond its routine function in the workforce, telecommuting can also be a vital option during a weather emergency or other workplace disruption.

This article looks at telecommuting as a key business continuity tool—one that enables businesses to maintain operations even if the workplace itself is shut down. While disruptions such as widespread power outages could still cause problems for some employees, telecommuting could help a business avoid a total shutdown by relying on remote employees to perform vital job functions. Highlighted here are some ideas about how business owners can include telecommuting in their business continuity plans, and what other considerations should be made before implementing this type of strategy.

BLIZZARDS, ILLNESS AND ROAD CLOSURES, OH MY!

The winter of 2014–2015 has brought record snowfalls in the Northeast and early snowfalls as far south as South Carolina. While the snow will eventually melt, telecommuting is a useful way to keep employees off dangerous roads, and also keeps employees from being stranded at work. In the case of a severe outbreak of influenza or other illness, telecommuting can separate healthy from potentially contagious employees to help maintain productivity and reduce anxiety. Similarly, telecommuting in response to a localized infrastructure problem, such as a bridge or major road closure, allows employees to stay focused on work and not on the difficulty of getting there. These are just a few examples of ways in which telecommuting can help businesses respond to emergencies.

IMPLEMENTING TELECOMMUTING AS A RECOVERY STRATEGY

For telecommuting to be a successful business continuity tool, businesses need to plan ahead by deciding which jobs are suitable for telecommuting, training staff, putting the right technology in place, addressing administrative challenges, and testing the new system.

Listed here are a few considerations that should be well-thought-out in advance.

IDENTIFY THE TELECOMMUTING FORCE

Telecommuting is an option only for employees whose jobs can be performed from a remote location, and only for employees whose work styles require minimal direct supervision. Generally, jobs that require significant onsite resources and equipment, hands-on service, or face-to-face interaction are not well-suited for telecommuting, while those that focus on reading, writing and analyzing, or are phone-intensive, are more suitable for telecommuting.

MANAGE EMPLOYEE CONCERNS

When identifying only some employees for the telecommuting force, it is important to manage perceptions of unfairness—either for employees who think they would otherwise get a "free day" if the workplace were closed, or those who are required to physically report to work, even during adverse weather or other circumstances, while others are not.

DOCUMENT THE TELECOMMUTE POLICY

When the office is closed because of a disruption, the business continuity plan should specify who is expected to work remotely and how the activation will take place, including the following considerations:

- Determine when and how employees will be advised not to come into the office and to begin working remotely.
- Determine how employees' time and attendance will be tracked, verified and controlled.
- Establish guidelines for employees for required communication by phone and email with their supervisor/manager.
- Decide whether to create a signed agreement stating what is expected of employees who telecommute during a disruption or emergency.
- Make sure telecommuting employees have an appropriate work environment in order to perform their job. The location needs to have safe working conditions and the employee must maintain protection of proprietary information, records, documents and equipment.

INFORMATION AND COMMUNICATIONS TECHNOLOGY REQUIREMENTS

As part of the planning process, appropriate technology for each job function must be put in place, including equipment, communications systems and security. Additionally, employees should document what is in place at their remote locations in order to provide and maintain I/T capabilities and support.

EQUIPMENT

- If equipment is required, what will be provided by the business and what is the employee expected to possess?
- What expenses will be covered by the business (Internet, a second phone line for business calls, etc.)?
- What hardware is needed (e.g., desktop PC, laptop, tablet)?
- If the business issues supplies such as a laptop or tablet, what triggers when the employee must take it home to make sure it is available if needed?
- What software, applications, firewalls, antivirus and anti-spyware will be needed?
- Are there any other components necessary to do the job (e.g., printer, scanner, a particular operating system, UPS, etc.)?

I/T INFRASTRUCTURE

- What type of Internet connection and/or bandwidth is required (broadband, DSL, cable)?
- What WIFI systems will be in place, and how can they be secured?
- What type of communication equipment is needed (phones, teleconferencing capabilities, tools like instant messenger, video conferencing and other online collaboration tools, etc.)?
    - Determine how voice communications will be handled. Will the capability of rerouting the calls to employees' home or cell phones be available?
    - Provide a list of contact information as a handy reference for telecommuting staff.
- Will access to remote help desk support be available to assist telecommuters with I/T issues?
- What type of training is necessary? Employees will need to be comfortable with the use of I/T systems (e.g., login process into VPN, etc.).

Lastly, it is important to establish practice and testing schedules. If employees do not work from home on a regular basis, the first few times may be confusing and difficult. Practicing and testing are key factors in having a successful telecommuting recovery strategy program available when needed.

Appropriate technology for each job function must be put in place, including necessary equipment such as a laptop.

TELECOMMUTING: NOT THE SOLE SOLUTION

When a disruption occurs, telecommuting can be critical to getting key employees productively working, but it is not a cure-all for all business recovery challenges. A severe natural disaster could damage many employees' homes or result in widespread power or communications outages. In these situations, business owners may want to consider the following more comprehensive approaches to relocation of employees.

- ✓ "Hot sites" are commercial workplace recovery facilities that have equipment readily available to address the business' critical needs. This may involve high monthly standby fees, and space may be limited as these types of providers do not have just one customer.
- ✓ "Warm/cold sites" are equipped with some of the business' needed equipment and may only be capable of providing backup after additional provisioning, software or customization is performed, generally at a lower standby cost.
- ✓ Memoranda of understanding (MOUs) or reciprocal agreements with a business ally that is accessible but not in the same risk zone may provide for shared office space or equipment if one company's workplace is inaccessible or inoperable.

After considering all of the advantages and disadvantages, choose a combination of the above alternatives to best meet the specific needs of the business.

INCORPORATING TELECOMMUTING INTO A BUSINESS CONTINUITY PLAN

The Insurance Institute for Business & Home Safety (IBHS) has created OFB-EZ®, a free business continuity planning toolkit to help businesses translate professional continuity concepts into an easy-to-use guide. By using OFB-EZ, a small business can take advantage of many disaster planning and recovery best practices without the need for a large company budget. To download OFB-EZ, go to www.disastersafety.org/open-for-business. Though the toolkit does not specifically include steps to incorporate telecommuting into the plan, the "Know Your Operations" and "Know Your Information Technology" sections can assist businesses with the necessary decisions for considering telecommuting as a possible solution. With the knowledge gained from completing an OFB-EZ plan, businesses can make an educated decision about whether telecommuting is a workable recovery strategy for them.

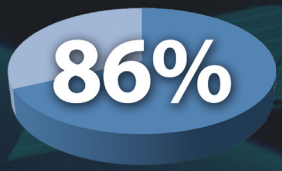
VIRTUAL PRIVATE NETWORKS (VPNs)

Providing secure access to the company's network is crucial for employees who telecommute during a disruption. A Virtual Private Network (VPN) is essentially a channel between the telecommuter and the office's local area network (LAN). When a telecommuter logs on through a VPN, he or she is routed to the company's internal network. From there, they can access drives and resources that are usually only accessible from inside the office. VPN access secures the Internet connection to guarantee all of the data being sent and received is encrypted and secured from unwanted eyes.

Keep in mind:

- Public WIFI networks are completely open and are not secure. If employees are permitted to use public WIFIs, have them use a VPN to guarantee security. Using a VPN encrypts communications no matter how or where they are connecting.
- If the VPN capacity is limited, implement a VPN login schedule (stagger access to eliminate sluggishness in speed). Staggering times during a workplace disruption—asking an employee to work late, start early or move their workdays around—to accommodate a VPN schedule is conceivable because employees are able to work from home.
- Not all VPNs are created equal. It is important to do research on the various options before selecting a VPN service/provider.

TELECOMMUTING BY THE NUMBERS

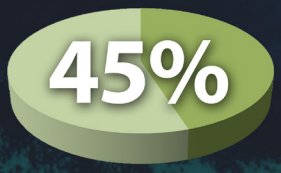


In 2009, a leading research and advisory firm conducted a survey which asked 285 business continuity/disaster recovery decision makers if their company had strategies for workforce recovery in their business continuity plans. 68% said yes. Of that 68%, 86% indicated they use remote access procedures as part of their strategy.

blogs.forrester.com/stephanie_balaouras/09-04-29-swine_flu_what_it_means_it_professionals

Three out of four teleworkers say they could continue to work in the event of a disaster compared to just 28% of non-teleworkers, according to a study conducted by an independent research firm that consults on emerging workplace issues and opportunities.

globalworkplaceanalytics.com/resources/costs-benefits



In late 2014, a company that offers software for remote access solutions conducted a survey of 916 employed people from five U.S. cities: Houston, Los Angeles, Miami, New York City and San Francisco. They found that despite the importance of information to most businesses and the push toward flexible work environments and mobile workforces, 45% of all respondents lack the ability to access company information from offsite locations.

www.hobsoft.com/solutions/HOB_Business_Continuity_Survey.jsp

IBHS is a non-profit applied research and communications organization dedicated to reducing property losses due to natural and man-made disasters by building stronger, more resilient communities.

Insurance Institute for Business & Home Safety
4775 East Fowler Ave.
Tampa, FL 33617
(813) 286-3400
DisasterSafety.org