# Insurance Buyers' News

MOC Insurance Services
Maroevich, O'Shea & Coghlan Insurance

Divisions of MOC Insurance Services
Farallon Associates Insurance Brokers
San Francisco Insurance Center

44 Montgomery Street, 17th Floor, San Francisco, CA 94104
Toll Free (800) 951-0600 | Main (415) 957-0600 | License # 0589960

WWW.MOCINS.COM

Risk Management | Insurance Buyers' News • March/April 2016 | Volume 27 • Number 2

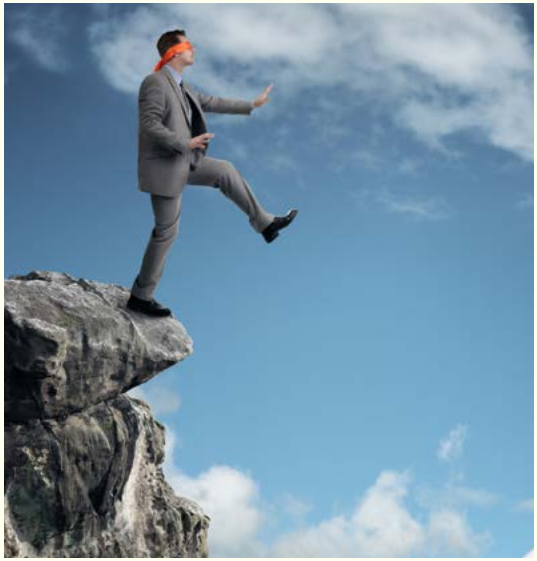
## How to Develop a Business Continuity Plan

**When your business must close or suffers a disruption due to any kind of natural or man-made cause, a good business continuity plan can ensure it can survive until repairs are made and operations return to normal.**

If a facility is damaged, production machinery breaks down, a supplier fails to deliver or information technology is disrupted, it could affect your business. The business impact analysis identifies possible effects from disruption of business functions and processes. It also helps you make decisions about recovery priorities and strategies to help you minimize the loss of income and customers.

To perform an impact analysis for your organization, have all business function and process managers complete an operation and financial impacts worksheet. Impacts to consider include:

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)



*continued on next page*

## This Just In

**The number of data breaches reported in the U.S. in 2015 dropped slightly from 2014, with a total of 781 versus 783 in 2014. The figures come from a report released by the Identity Theft Resource Center and sponsored by IDT911™.**

**The business sector topped the list of industry types reporting data breaches in 2015, accounting for nearly 40 percent of the publicly reported data breaches. Health/medical organizations ranked second, with 71 breaches for 35.5 percent of total breaches reported. The banking/credit/financial industries reported 38 breaches, nearly double the number reported in 2014, for 9.1 percent of all breaches**

*continued on next page*

- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative.

Once all worksheets are completed, tabulate worksheets to summarize:

- the operational and financial impacts resulting from the loss of individual business functions and process, and
- the point in time when loss of a function or process would result in the identified business impacts.

Functions or processes with the highest potential operational and financial impacts become priorities for restoration. The point in time when a function or process must be recovered, before unacceptable consequences could occur, is often referred to as the "Recovery Time Objective."

Recovery of a critical or time-sensitive process requires resources. Business function and process managers should also complete a business continuity resource requirements worksheet, which will help you determine the resource requirements for recovery. These resources may include:

- Employees
- Office space, furniture and equipment
- Technology (computers, peripherals, communication equipment, software and data)
- Vital records (electronic and hard copy)
- Production facilities, machinery and equipment
- Inventory, including raw materials, finished goods and goods in production
- Utilities (power, natural gas, water, sewer, telephone, Internet, wireless)
- Third-party services.

Recovery strategies may involve contracting with third parties, entering into partnership or reciprocal agreements or displacing other activities within the company. Staff with in-depth knowledge of business functions and processes are in the best position to determine what will work. Explore possible alternatives and present them to management for approval and spending authorization. Depending upon the size of the company and resources available, you can explore many recovery strategies.

After a disruption, you might relocate operations to an alternate site — assuming it hasn't been affected by the same incident. This strategy also assumes that the surviving site has the resources and capacity to assume the work of the impacted site. Prioritization of production or service levels, providing additional staff and resources and other action would be needed if capacity at the second site is inadequate.

Telecommuting can reduce alternate site requirements. This strategy requires ensuring telecommuters have a suitable home work environment and are equipped with or have access to a computer with required applications and data, peripherals, and a secure broadband connection.

In an emergency, organizations can convert other spaces into workspace, such as cafeterias, conference rooms and training rooms. These spaces will require furnishings, equipment, power, connectivity and other resources to meet workers' needs.

*This Just In*

**reported. Government/military agencies came in fourth, with 8.1 percent of all data breaches, followed by education, with 7.4 percent.**

**Data breaches can create serious liability and other problems for all types of organizations. For more information, please see the article on P. 4 or contact us for assistance in mitigating your data security risks.**


You can also arrange partnership or reciprocal agreements with other businesses or organizations that can support each other in the event of a disaster. Assuming space is available, you must address issues such as the capacity and connectivity of telecommunications and information technology, protection of privacy and intellectual property, the impacts to each other's operation and allocating. Agreements should be negotiated in writing and documented in the business continuity plan. Periodically review the agreement to determine if there is a change in the ability of each party to support the other.

*continued on next page*

Many strategies exist to help in the recovery of manufacturing operations. Manufacturing strategies include:

- Shifting production from one facility to another
- Increasing manufacturing output at operational facilities
- Retooling production from one item to another
- Prioritization of production—by profit margin or customer relationship
- Maintaining higher raw materials or finished goods inventory
- Reallocating existing inventory, repurchase or buyback of inventory
- Limiting orders (e.g., maximum order size or unit quantity)
- Contracting with third parties
- Purchasing business interruption insurance.

You can find worksheets for the business impact analysis and business continuity resource requirements and other useful information on business continuity at the website of the Federal Emergency Management Agency (FEMA), www.ready.gov.

For more information on business interruption insurance, which can replace income lost due to an insured disaster and provide the cash needed to help your business remain in operation during recovery, please contact us.

# Email, Phone and Social Media Monitoring in the Workplace — Know Your Rights as an Employer

**Do you know how much privacy your employees are entitled to? For example, if you feel employees are abusing their work privileges, is it legal to intercept emails or phone conversations to find out what they're up to and confirm your suspicions? Can you ask potential job candidates for their Facebook profile log-on information? Here are some general guidelines that can help.**

## Screening Job Candidates' Social Media Profiles

Most businesses investigate a prospective hire on Facebook and other social media. Some go so far as to ask job candidates for their Facebook passwords as part of the screening process. Although there is no federal law prohibiting this, the Department of Justice considers it a crime to violate social media terms of service and enter these sites illegally. Asking an employee or candidate for their log-on information means you and that individual are both in direct violation of Facebook's Terms of Service, which state the following: "You will not solicit login information or access an account belonging to someone else" and "You will not share your password... let anyone else access your account, or do anything else that might jeopardize the security of your account." Many states are also now looking to make this practice illegal.


The bottom line: Simply asking for access to personal passwords is a clear privacy violation and is both offensive to the candidate and unethical. Employers and managers should also be careful they're not accessing profile information to determine an employee's religious, sexual or political views. If it's determined that you used this information to discriminate against an employee, you may be found in violation of equal employment opportunity and privacy rules.

*continued on next page*

## Monitoring Employee Social Media Activity in the Workplace

A report by Gartner suggests that by 2016, up to 60 percent of employers are expected to watch workers' social media use for security breaches. Employers are on the lookout for unauthorized posting of company content — videos, documents, photos, etc. Currently, no specific laws govern the monitoring of an employee's social media activity on a company's computer. However, the U.S. National Labor Relations Act does address employee rights in regard to the use of social media and acceptable social media policy. There has also been a ruling against employers who fired workers for complaining on social media sites about their workplace conditions.

The bottom line: Provide employees with a social media policy and be sure to include information about what you consider confidential and proprietary company information that should not be shared. For more tips on social media monitoring do's and don'ts, check out this article from Small Business CEO: Considerations for Social Media Use in the Workplace, www.smbceo.com/2012/05/24/social-media-in-the-workplace/

## Intercepting Email or Phone Conversations

Increasingly sophisticated ways of storing and accessing email have made it easier than ever for employers to monitor email accounts. But is this an invasion of privacy? The law is fuzzy.

The Electronic Communications Privacy Act (ECPA) of 1986 prohibits the intentional interception of "any wire, oral or electronic communication," but it does include a business use exemption that permits email and phone call monitoring.

This exemption often comes under close scrutiny by courts, and includes several elements. Generally, if an employee is using a company-owned computer or phone system, and an employer can show a valid business reason for monitoring that employee's email or phone conversations, then the employer is well within his or her rights to do so. Likewise, if employees have consented to email or phone monitoring (in their contract of employment, for example), then you may monitor their calls or emails.

But here's the rub: the ECPA draws a line between business and personal email content you can monitor — business content is ok, but personal emails are private.

Tip: If in doubt, consult your legal counsel. Develop and share a monitoring policy with employees (for example, in your employee handbook). If possible, get them to agree to it. Courts often look at whether employees were informed that their calls or emails might be monitored in the workplace, whether there was a valid business justification for the monitoring, and whether the employer complied with established policy. Source: U.S. Small Business Administration

For more information on protecting your business from liability claims by employees, please contact us.

# Employee Theft and Fraud: Could it Happen to You?

**It could, and if your business is a cash business, it probably is. The typical organization loses five percent of revenues each year to employee fraud, according to estimates by participants in the Association of Certified Fraud Examiner's 2014 Global Fraud Study.**

The study also found that the median sum lost was $145,000; however, 22 percent of cases involved losses of at least $1 million.

Another study found that 64 percent of small businesses have experienced employee theft, most of which were of money. *(Jay Kennedy, University of Cincinnati criminal justice student, "From Apathy to Disdain: Why Small Businesses Refuse to Call the Police When Employee Theft Occurs").* Interestingly, only 16 percent of organizations that had experienced a theft had reported it to police. Reasons vary, but can include embarrassment, avoidance of negative publicity and the fact that in a small business, the owners and employees often know each other well.

So what's an employer to do? The typical commercial property policy covers your business for theft committed by outsiders, but specifically excludes employee theft. You can buy commercial crime coverage, a type of fidelity bond, to protect the organization from employee theft.

Fidelity bonds indemnify employers for the loss of money or other property sustained through the dishonest acts of bonded individuals. Often called "honesty insurance," bonds provide coverage for intentional acts of

*continued on next page*

fraud, larceny, misappropriation, forgery, embezzlement and other dishonest acts committed by a bonded employee. The acts must also be intended to cause a loss to the employer and financially benefit the bonded person. The bonds are technically a form of surety, but are similar to an insurance policy in format and terminology.

## Types of Crime Coverage

There are four major crime coverage forms available:

- Form A, employee dishonesty
- Form B, forgery or alteration of documents
- Form C, theft, disappearance and destruction, and
- Form D, robbery and safe burglary.

Most businesses buying crime coverage will need one or more of these forms. Forms to cover more specialized exposures, such as items in hotel/innkeepers' safe deposit boxes, also exist. The Insurance Services Office has packaged these forms into crime packages for specific types of businesses. You can buy them as separate crime policies or attach them to your commercial package policy. Whatever you need coverage for, whether it's money and securities, the contents of safes, the property of guests and lodgers, there's probably a program that meets your needs.

Most crime programs exclude coverage for crime or dishonest acts committed by the insured or any partner, seizure or destruction of property by order of governmental authority, indirect or consequential loss, and legal expenses. Most plans cover only workers employed in the U.S., its territories and Canada.


## What About Data Theft?

To be sure your crime coverage will protect you for data theft, read your policy carefully. A broadly drafted policy might provide coverage for electronic data, including data stolen by employees. Some insurance forms also extend coverage to certain computer contractors. We can help you review your operations and coverage to help you minimize exposures to employee theft. Please contact us for more information.

*more on next page*

# What to Do in a Policy Review

Scheduling regular policy reviews can ensure your business has enough insurance to survive a disaster. Here are a few action items to consider when filling out the insurance portion of your business continuity plan:

- Review your current coverage with your insurance agent. The policy should be tailored to your business and take into consideration not only property damage but loss of revenue and extra expenses that occur when a disaster causes a temporary shut-down.
- Ask a lot of questions. Make sure you understand the policy limits, the deductible, and what is actually covered.
- Consider business owner's insurance. The business owner's policy (BOP) is a standard insurance package of coverages that a typical small or medium-sized business would need. In addition to covering your property, it includes general liability protection and business interruption insurance, which provides money to offset lost profits or pay operating expenses the business could have covered if the disaster had not occurred.
- What about flood insurance? According to the U.S. Geological Survey, floods are the leading cause of natural disaster property losses. Small business owners, particularly those running home-based businesses, should consider getting coverage from the National Flood Insurance Program (NFIP). Most homeowners' insurance policies don't cover flood losses. The NFIP also covers business property.
- Know what you own. Inventory your personal and business assets before the disaster occurs. Record the price and estimated replacement cost of furniture, computers, machinery—everything of value at your business. Keep receipts, take photos and video of your property, and store that information at a secure location.

Having the right insurance policies and the right amount of coverage will make a difference when it comes time to deal with the aftermath of any kind of disaster, whether it's a massive hurricane, or the water-main break in the alley behind your business. For more information, please contact us. ■

Insurance Buyers' News

THE INSURANCE 411
What you need to know about insurance

SmartsPro MARKETING

The information presented and conclusions within are based upon our best judgment and analysis. It is not guaranteed information and does not necessarily reflect all available data. Web addresses are current at time of publication but subject to change. This material may not be quoted or reproduced in any form without publisher's permission. All rights reserved. ©2016 The Insurance 411. Tel. 877-762-7877. http://theinsurance411.com.