Commercial Insurance Update

Topics Concerning Buyers of Commercial Insurance

MSP PL -12/2010 "Security and Privacy Liability, aka Cyber Liability December, 2010
Commercial Insurance Update Newsletter

Security and Privacy Liability a.k.a. Cyber Liability

By Jeffrey W. Cavignac, CPCU, ARM, RPLU, CRIS

What is Cyber Liability?

Flash back to 1992 when I started our company and bought my first computer (a Gateway 33 mhz). You couldn't buy a "Cyber Liability" policy. Most people really didn't know what a "web site" was, and "security breaches" created images of Mission Impossible.

Flash forward to 2010, and issues arising out of data security, management of confidential information, and infringement of intellectual property rights are all considered major exposures. We have become so interconnected that the opportunity for catastrophic loss has escalated dramatically. While the early "hackers" seemed to be merely challenging themselves intellectually to see what type of mischief they could cause, today's hackers have serious criminal intent in mind. Terrorists, organized crime, and the random computer geek working alone, are making cyber crime a growth industry. Since 2005, according to Privacy Rights Clearinghouse, over 263 million data records of U.S. residents have been exposed to security breaches.

Risk Analysis

Step one in the Cavignac & Associates Risk Management Process is **Risk Analysis**. Risk Analysis involves identifying assets or circumstances which could give rise to a loss. This is also known as "exposure analysis," and the assets or circumstances are referred to as "loss exposures."

Potential losses include loss of a company's data and the cost to restore it, the cost of defending against or settling a third party claim, the cost of cyber extortion, damage to reputation, the cost to notify individuals

Cyber Liability *(continued on page 2)*

In this issue...

Cyber Liability *(continued from page 1)*

whose personal information may have been compromised, and the cost to pay for credit monitoring for those individuals if required by law. Nearly every state (including California) now requires businesses that have compromised an individual's information to notify that individual. One study of larger companies estimated the cost of a data breach at $204 per compromised record. The same study calculated the average cost of a data breach at $6.75 million!

Risk Control

Understanding what your exposures are is the first step. The second step is to determine how you can manage these exposures. In other words, what can you do to lower the likelihood of a cyber liability claim or the severity of a claim if one happens?

Although an exhaustive discussion of Risk Control relative to cyber liability goes beyond the scope of this article, it should be recognized that a number of companies focus on helping businesses manage and protect both their own data and the data of their customers. In simple terms, the key is to centralize IT management and develop enforceable policies and procedures across your network. These policies and procedures must be periodically checked to see if in fact they are being followed. In the event of a suspected or actual breach, it is important to take action as soon as possible. If necessary the appropriate specialist companies that focus on IT security should be called in.

Is This Risk Insurable?

Although evaluating, selecting, and implementing risk control strategies is critical in order to reduce the frequency and severity of cyber liability exposures, insurance can also play a role. As these exposures have evolved, so has insurance coverage. Although the Insurance Services Office (ISO) created a "standard" policy in November of 2009, most of the

Cyber Liability *(continued on page 3)*

Published by

Cavignac & Associates
INSURANCE BROKERS
License No. 0A99520

450 B Street, Suite 1800 San Diego, CA 92101-8005
Phone 619-234-6848 Fax 619-234-8601
Web Site www.cavignac.com

Risk Management Seminars

2010-11 Series

450 B Tower, 450 B Street, Suite 1800, San Diego, CA 92101-8005

- WC 101 and Post Accident Response Tools (PART)
  Friday, December 17, 2010
  Registration: 7:30 am
  Seminar: 8:00-10:00 a.m.

- OSHA 300 and Safety Issues in the Office
  Friday, January 14, 2011
  Registration: 7:30 am
  Seminar: 8:00-10:00 a.m.

- Measuring Safety Performance for Your Bottom Line
  Friday, February 11, 2011
  Registration: 7:30 am
  Seminar: 8:00-10:00 a.m.

- Sexual Harassment Prevention Training
  Friday, March 4, 2011
  Registration: 7:30 am
  Seminar: 8:00-10:00 a.m.

All training sessions available to our clients
Reserve early / seating is limited! *

For more information about upcoming seminars
Contact **Darcee Nichols** at **dnichols@cavignac.com** or **619-744-0596**.

* **NOTE:** Due to the popularity of our seminars and limited seating, we regret **we cannot provide refunds or credits with less than 72 hours advance notice of cancellation**.

Managing a Security Breach

If you become aware of an actual or potential security breach, you should investigate it immediately. If, in fact, personal information has been compromised, at a minimum you should do the following:

- Depending on the circumstances, contact local law enforcement, and if appropriate the FBI and possibly the U.S. Postal Inspection Service (if the fraud involves mail theft).
- Put any businesses that could be impacted on notice of the breach.
- Put on notice any individuals whose personal information may have been compromised. Make sure you have designated a contact person to coordinate the notification process.
- If the incident involves Social Security numbers, credit card information, or other sensitive personal information, contact the major credit bureaus.
- Any inappropriately posted information on your Web site should be removed **immediately**.
- Consult with legal counsel to make certain you comply with any applicable laws, specifically those pertaining to notification and credit monitoring.
- Notify your insurance advisor to determine if insurance may apply to the incident.
- If necessary, consider contacting your public relations consultant to help manage the process and protect your firm's reputation.

Cyber Liability *(Continued from page 2)*

policies on the market today are unique to the company offering the coverage. Because of this, each policy needs to be evaluated to make certain it addresses the exposures that your company may have.

These policies include both first party and third party coverages. First party coverage indemnifies you for the costs you incur to repair or replace damage caused by a covered peril; third party coverage includes the cost to defend against and settle a third party claim, including regulatory actions.

These policies commonly include coverage for some or all of the following exposures:

- Web Site Publishing Liability – Nearly everyone has a Web site these days. This coverage protects you from liability arising out of information posted on your Web site, which might include actual or alleged misstatements; infringement of another's copyright; trademark, etc., or violation of a person's right to privacy.
- Security Breach Liability – Provides coverage for your liability arising out of a security breach or transmission of a computer virus to a third party. A security breach occurs if someone who is not authorized to do so accesses the personal information of another, or if someone who is authorized to access such information uses the information inappropriately.
- Programming Errors and Omissions Liability – Protects you for your legal liability arising out of actual or alleged programming errors that results in the disclosure of a client's personal information.
- Replacement or Restoration of Electronic Data – This is a first party coverage which indemnifies you for the cost to replace or restore your data or programs that are damaged or destroyed as a direct result of a computer virus or similar bug designed to damage, destroy or corrupt your computer system.
- Extortion Threats – Reimburses the insured for extortion expenses and ransom payments incurred as a direct result of an extortion threat. Typically these threats focus on introducing a virus, malicious code, or publishing of clients' personal information.

- Business Income and Extra Expense – This provides coverage for the actual loss of business income and the extraordinary operating expenses incurred as a result of a cyber incident or extortion threat.
- Public Relations Expense – Cyber liability incidents can create bad press. This covers the costs of a public relations firm to help the insured protect or restore their reputation subsequent to a cyber liability incident.
- Security Breach Expense – Expenses incurred to notify others that their personal

Cyber Liability *(Continued on page 4)*

Cyber Liability *(Continued from page 3)*

information has been compromised can be significant. This coverage would reimburse the insured for those costs, including overtime salaries paid to employees dealing with the issue, fees and costs of a company hired to operate a call center, post-event credit monitoring services, and other reasonable expenses.

What Does It Cost?

Cost can vary dramatically depending on the type of business, type and volume of information on file, and other factors. Since this is a relatively new coverage, there is not an adequate data base on which to calculate rates. Most companies offering the coverage are really pricing their programs based on what they believe the exposure to be and what they think they can charge.

Prices for smaller firms (<50 employees) will probably be in the $1,000 to $10,000 range. Larger firms might expect to pay $15,000 to $25,000. In order to get an indication of cost, you can complete the attached questionnaire and return it to us.

Best Practices

Every firm, regardless of size, should evaluate their exposure to this type of loss. It should also be determined what steps can be taken to manage this type of potential claim. Finally, you should obtain a quotation for coverage. Even if you elect not to purchase the coverage, you should know the cost and make the conscious decision not to buy it as opposed to assuming you don't want to afford it.

Disclaimer: This article is written from an insurance perspective and is meant to be used for informational purposes only. It is not the intent of this article to provide legal advice, or advice for any specific fact, situation or circumstance. Contact legal counsel for specific advice.

"New" Organ and Bone Marrow

Donation Leave

By Sandra W. Rugg, SPHR-CA

Director of Human Resources, Cavignac & Associates

As an encouragement to help save lives, the California legislature has added a new leave entitlement which will be effective January 1, 2011.

Employers in California who have 15 or more employees must provide **paid** leave (up to 30 days per year for those donating organs and up to 5 days for bone marrow donations), including guaranteed reinstatement rights and continuation of benefits while on leave.

The employer may require the use of up to two weeks of accrued paid time off for organ donations, and five days for bone marrow donations.

This leave does NOT count toward FMLA or CFRA, and the employer must guard against discrimination or retaliation against the person requesting the leave.

Don Phin of ***HR That Works*** (a Web-based HR resource site) has written an employee handbook policy which addresses the requirements of this new law. We provide the following link to it for your use:

Organ Donation Policy

This is just one of over 225 forms / policies found in ***HR That Works***, and it demonstrates Don Phin's commitment to keeping the materials available in ***HR That Works*** current and useful.

If you are interested in learning more about ***HR That Works***, a "must have" HR resource, please contact Sandee Rugg at srugg@cavignac.com.

Privacy Quick Quote Application

1. **Name of Parent Company** _____
   Address _____
   Number *Street*
   _____
   City *State* *Zip Code*

2. **Standard Industrial Classification Code (SIC)** _____

3. **Nature of Operation** _____
   _____

4. **Please provide the following information:**

   a. Approximate number of clients, customers, and employees whose personal information records the Company collected, stored, maintained, or transmitted during the last 12 months.

   ☐ 0 to 5,000 ☐ 5,001 to 10,000 ☐ 10,001 to 25,000 ☐ 25,001 to 50,000 ☐ 50,001 to 100,000 ☐ Above 100,000
   Number above 100,000 _____

   b. Revenues of the Company for the last 12 months $ _____

   c. Are the revenues of the Company anticipated to increase more than 25% in the next 12 months? If "Yes," please provide details on a separate sheet of paper. ☐ Yes ☐ No

5. **Within the past 5 years, has the Company been subject to or suffered any losses or litigation from any:**

   a. Breaches of security? ☐ Yes ☐ No

   b. Unauthorized acquisition, access, use, identity theft, mysterious disappearance, or disclosure of personal information? ☐ Yes ☐ No

   c. Violation of any privacy law, rule, or regulation? ☐ Yes ☐ No

   d. Technology or extortion threats? ☐ Yes ☐ No

   If "Yes" to a. through d. above, please provide details (use a separate sheet of paper if necessary):

   Details:
   _____
   _____
   _____

6. **Signature** _____ **Title** _____ **Date** _____

Articles courtesy of Cavignac & Associates Employee Benefits Department

LIVE WELL, WORK WELL

Stress-Free Holiday Budgeting

With proper budgeting and a few smart shopping ideas, it is possible to find the perfect gift for everyone on your list and stay within your budget. These tips will help you stick to your spending plan and minimize your holiday financial stress:

- **Make a list and check it twice —** Does everyone on your list need to be there this year? A simple phone call, holiday card or homemade treat can feel just as special as a store-bought gift.
- **Set limits —** Write down a maximum dollar amount for each person on your list and stick to this limit.
- **Be creative —** Do you enjoy baking or crafts? Giving homemade gifts can add a personal touch and creating them can be a fun holiday activity for the whole family.

- **Be realistic —** A good rule of thumb is to leave your credit cards at home. If you don't have the cash for the gift, don't buy it.
- **Shop online —** With high gas prices and many stores offering online-specific sales, shopping online can be a very cost-effective option. Find sites that offer free shipping.
- **Consider a holiday job —** Many places look for part-time, seasonal help during the holidays and can help you pick up a little extra cash.

Get a Head Start on Your New Year's Resolution

Yes, it's only December, but that doesn't mean you can't get an early start on your New Year's resolution. If you start implementing some good habits now, it will be much easier for you to maintain them when January rolls around.

Here are some good starting points for resolutions:

- **Remove one bad item from your diet —** For example, if you drink a lot of soda, try to give it up for one month. Eliminating two 12-ounce cans of soda per day from your diet cuts about 300 calories from your diet each day.
- **Get more active —** Start by trying to exercise for 30 minutes, at least three times a week. Crunched for time? Even walking or cleaning your house for 30 minutes can have a positive impact on your health.
- **Get more sleep —** Most people do not get the recommended amount of sleep. Shoot for at least seven, preferably nine, hours of sleep a night.

Community Bulletin Board

"Neighbors helping neighbors in San Diego"

Monarch Schools

- Web Site

Senior Community Centers

Mission:

To provide quality and compassionate services for the survival, health and independence of seniors living in poverty

- Web Site

San Diego Humane Society and SPCA

- Web Site

SAN DIEGO POLICE FOUNDATION

The San Diego Police Foundation supports the men and women who "protect and serve" by raising community awareness of important unbudgeted or "discretionary" needs that will improve crime-prevention and law enforcement efficiency. The Foundation puts your tax-deductible contributions to measureable work in local communities.

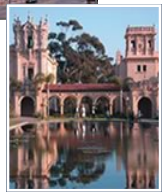
- Web site
- SafetyNet
- For more information, contact **info@sdpolicefoundation.org**

DOWNTOWN YMCA

500 West Broadway, Ste. B, San Diego 92101 619-232-7451

- Web Site
- Questions? Contact **Alicia Gettys** by phone at **619-232-7451** or e-mail at **agettys@ymca.org**

SDAF SAN DIEGO ARCHITECTURAL FOUNDATION



- Web Site
- Questions? E-mail **info@SDArchitecture.org**

Society for Design Administration

An Affiliate of the American Institute of Architects

Mission:

The Society for Design Administration advances management and administrative professionals in the A/E/C industry through education, networking and resources.

- Membership
- Web Site
- For more information, e-mail **vicepresident@sdasandiego.org**