Network & Privacy Liability

Winters-Oliver Insurance **3/1/2014** Author: Ben Winters, CIC

Privacy & Data Breach

The unseen risk faced by every business.

It may sound odd, but cyber hackers conduct their "business" much in the same manner as you and me. Of course they'd like to achieve the "big hack" just as you would like to land the big account for your business. While it's important to focus on acquiring big customers, it's crucial you focus on volume by adding smaller customers to maintain your pipeline. Smaller customers require a shorter sales cycle and have lower acquisition costs, and provide a more predictable revenue stream.

Hackers look at your small business as their "small customer." Small business is crucial to maintaining their scam. While organizations like Target, Zappos, and Sony make attractive targets (all of which have suffered a data breach), they are much more difficult to penetrate. While cyber events like these make big headlines, they are actually in the minority when it comes to data breaches. Most data breaches occur because of stolen laptops, USB flash drives, followed by systems failure, loss of paper records, and hacker attacks. Your business has a greater chance of being breached because an employee loses a laptop than being hacked!

Experts say that between 50% to 75% of small businesses suffer a data breach each

> *"…just because a merchant outsources all payment processing does not mean that the merchant won't be held responsible by their acquirer or payment brand in the event of an account data compromise."-www.pcisecuritystandards.org/faq*

Ben Winters is a Certified Insurance Counselor (CIC) and insurance professional who works extensively in the management liability space. He advises businesses on insurance and risk management solutions to protect their assets and operations. He can be reached at 804-746-5178 ext. 112 or bwinters@woinsure.com

WINTERS-OLIVER
INSURANCE AGENCY, INC.

year. If this number sounds high to you it's because most of these businesses never know they suffered a breach and therefore did not report the breach as required by law.

Most states have laws for data and privacy breach. Common regulations require the business that suffered the breach to notify effected customers by phone, mail, or email and provide credit monitoring for 12 months. Some states require the breached business to pay for credit cards to be reissued to their customers and levy regulatory fines that can reach six digits.

Small businesses sometimes believe they are not subject to a data breach because they use a third party credit card processor. While this lowers exposure it certainly does not eliminate the exposure. First, unauthorized collection of customer payment information is only one cyber exposure faced by a business. Second, it is likely that your business will be named in a suit if a data breach occurs meaning you will need to defend yourself. The general liability policy does not provide coverage for a data breach nor defense of a data breach. Third, most credit card processors will not accept liability for a breach if your systems are not not PCI compliant shifting responsibility back to your business.

The cost of responding to a data breach can be staggering. *Time* is a major cost contributor. Most businesses do not discover a breach right away. Target's breach occurred on Black Friday (11/27/2013) but it was not discovered until December 15, 2013 – almost three full weeks after the breach occurred. In 2007, TJX (T.J. Maxx, Marshalls) suffered a data breach where 45.7 million customer credit cards were stolen. Eleven months elapsed from breach to discovery. The breach becomes more severe with the passage of time.

Let's look at the consequences to a business if only 200 customer records are breached. According to the Ponemon Institute, the average cost of a data breach is $188 per customer record.[1]

200 records X $188 for customer notification, credit monitoring, crisis management = $37,600

This number *does not* include regulatory fines or judgements awarded. For the most part it includes the cost of responding to the breach and it's effect on revenue. In 2010, the top three causes of a data breach were:[2]

Causes	Examples
Unintentional Employee Action	Libelous post on social media
Lost or Stolen Computing Devices	PDA's, Smartphones, USB Flashdrives, etc.
Third Party Error	Cloud server provider suffers a breach

The top two *reasons* cited for data breach; inadequate budget and lack of trained staff or end users.

The health care industry should be especially careful when choosing a cyber liability policy. Hospitals and doctors' offices are the most at risk for a data breach because they store so much personal health information (PHI) and personally identifiable information (PII). As medical facilities continue the conversion to Electronic Health Records (EHR) privacy protection and data risk

management will be crucial. Perhaps more than any other industry, health care is subject to the most regulation (and highest penalties) with regard to data and privacy protection. HIPAA, HITECH, and now HHS mandated audits just to name a few.

As the threat of hacking and cyber risk becomes more prevalant, many businesses are looking for ways to transfer this risk with many looking to an insurance policy. Cyber Liability Insurance is gaining popularity and becoming better priced as underwriting data and knowledge of the risk develops. Business owners and consumers should know that unlike a general liability or commercial property form, cyber liability forms differ from carrier to carrier. Some have as few as three claims triggers while some have has many as eight. Some policies respond to regulatory fines while others exclude this coverage.

Cyber Liability Insurance has been available since the late nineties but is becoming more relevant as technology plays a larger role in our businesses and our lives. One carrier reported an 18% increase in Cyber Liability Insurance applications following the December 2013 Target breach. When purchasing a cyber liability policy, one should be sure to may careful attention to the nuances in these policies and work with an insurance agent who is knowledgeable of the coverage.