September 2016 • Vol. XXIX • Number 9

PLUS Journal *Reprint*
5353 Wayzata Blvd., Suite 600
Minneapolis, MN 55416-4758
phone 800.845.0778 or 952.746.2580

The mission of the Professional Liability Underwriting Society is to be the global community for the professional liability insurance industry by providing essential knowledge, thought leadership and career development opportunities.

PLUS
PROFESSIONAL LIABILITY UNDERWRITING SOCIETY
Journal
YOUR SOURCE FOR PROFESSIONAL LIABILITY EDUCATION AND NETWORKING

Dan Vecchio's *career spans more than 29 years, all of which has focused on management liability and professional liability. He began his insurance career underwriting management liability for some of the most financially challenged banks and savings and loans in the mid-1980s. He then became a retail broker, and for 22 years placed management liability and cyber liability for large companies, many in the Fortune 500. Today, as a wholesale broker at Founders Professional, Dan helps retail agents place the same specialty coverages for any size risk.*

Small Company Cyber Hazards Hiding in Plain Sight

by Dan Vecchio

Today, companies would never think of operating without property and casualty insurance. Yet, everyday companies are ignoring a risk that has the potential to cause just as much financial damage and even impact future viability.

An Overlooked Risk

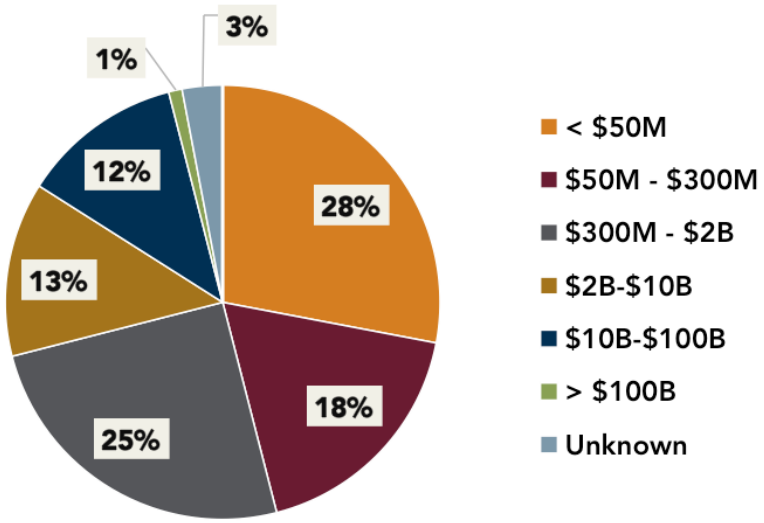
In the last 20 years, small companies, like large companies, have become hyper-dependent on technology. Technology is the lifeblood of every company today. Whether simply storing employee and customer information, or conducting e-commerce; technology has become a significant risk that companies can't afford to overlook. As reliant on technology as small companies have become, there are still only a small percentage that have invested in cyber liability insurance.

Small Company Exposure

Many small companies are unaware of the high risk that data breaches can have to their financial viability. The misconception is that hackers only attack high-profile, high-revenue firms. The fact is, small businesses are statistically more likely to be hacked. The reason is that they are easier and more attractive targets. Many small firms are unaware of the potential exposures, and some don't have the financial resources to adequately protect their data.

FIGURE 1

Percentage of Claims by Revenue Size



Source: NetDilligence 2015 Cyber Claims Study

According to the NetDilligence 2015 Cyber Claims Study, only 13% of all cyber claims filed were from companies with revenues in excess of $10 billion. Amazingly, 28% of all cyber claims are against companies with revenues under $50 million, and almost half of all cyber claims filed were from companies with revenues under $300 million (Figure 1).

Five Financial Exposures

When a company has a breach, restoring data is not the only expense that will occur. Below are five common exposures that can occur after a breach:

1. Notification Costs: There are 46 U.S. states that have adopted a breach notification law. The laws generally apply to all companies that own, license, store or maintain certain sensitive personally identifiable information ("PII").
2. System Recovery: Recovering data can be expensive. Recovery strategies should be developed for information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity.

3. Regulatory: If a data breach results from your business' lack of compliance with regulatory guidelines, the government will levy substantial fines. In many cases, small companies may not have known they've violated a law or statute.

4. Liability: Small companies will be responsible for costs incurred by customers and vendors as a result of a cyber breach.

5. Class Actions: Class action lawsuits are less prevalent against small companies, but they do exist. There are class action cases on record of stolen customer data.

Inadequacy of Traditional Policies

Many small companies believe that their Business Owners Policy (BOP) provides coverage for cyber breaches. Unfortunately, the coverage can be limited to replacement and recovery cost of equipment, but not lost data. A standalone cyber liability policy can cover the following:

- Identity theft
- Loss or corruption of data
- Computer and legal forensic costs
- Credit monitoring costs
- Business interruption
- Website media liability
- Cyber extortion

Risk Management and Prevention

Unlike large corporations, many small companies do not have a risk management department. Insurance companies that write cyber liability contract with third party risk management firms, which can provide guidance and suggest risk management policies and procedures. Below are examples of risk management services provided to better secure data systems:

- Installing security software and hardware
- Using cloud computing services
- Developing and using a data privacy policy
- Backing up data at offsite locations
- Contracting with a security services vendor

Regardless of size or industry, companies should consider implementing additional risk management practices to protect their data. Doing so on the front end can help to secure your and your customers' valuable data against the possibility of a cyber-attack.

For most companies, data exposure is in the number of records kept. Hackers are usually after social security numbers, credit card numbers, addresses, bank account numbers and other personal identifying data. There is a correlation between the number of records kept and the amount of loss incurred after a breach. (Figure 2).

FIGURE 2

Records Kept	Expected Loss	Average Loss	Predicted Loss
100	$25,450	$35,730	$555,660
1,000	$67,480	$87,140	$1,461,730
10,000	$178,960	$223,400	$3,866,400
100,000	$474,600	$614,600	$10,283,200
1 million	$1,258,670	$1,775,350	$27,500,090
10 million	$3,338,020	$5,241,300	$73,943,950
100 million	$8,852,540	$15,622,700	$199,895,10

The average loss should contain the mean loss (if there were multiple incidents). The predicted loss shows the (rather large) estimated range we should expect from any single event.

Source: Verizon 2015 Data Breach Investigations report

The High Cost of a Breach

In many instances, when small companies' data systems are hacked, customer and employee data is lost or stolen. The cost of an investigation and reconstruction can be significant. Customer and vendor notification expenses alone can be enough to financially impair a small company.

Once a breach is detected, the process of getting everything back to "normal" can be very expensive.

The affected company will need to hire experts to determine if lost data can be retrieved, or if new hardware and software needs to be purchased. Another cost associated with internet-based attacks and breaches include losses in productivity. Additionally, hired experts will need to assess what it will cost the company to protect its data systems and websites from future breaches.

A small company's level of preparedness is often insufficient for a cyber breach. After a breach, companies without insurance can expect to pay significantly more, primarily because they generally don't have instant access to resources and experts needed to mitigate the breach in a timely manner. Insurance companies have third-party specialty firms on call that are deployed at the time of the claim.

The Solution

Today, business owners can protect themselves by purchasing cyber liability insurance. Cyber liability insurance can provide peace of mind for any company, in any industry. In recent years, the cyber liability insurance market has expanded greatly and there are policies available for any size company. The coverage provided is broad and tailored to each company's needs.

For business owners to operate their company with peace of mind, cyber liability insurance should be considered an essential part of their firm's insurance portfolio and risk management strategy.