The Cyber War Against Small and Medium-Sized Businesses

As published by the Inland Empire Business Journal, September 2013

Many small and medium-sized businesses are not aware that they are at high risk for a cyber attack. As the economy improves in the Inland Empire, it is critical businesses under- stand and plan for cyber liability issues. John Sileo, a professional identity theft consultant and speaker, shares on his Solutions Blog, "Approximately 80 percent of small businesses that experience a data breach go bankrupt or suffer severe financial losses within two years of a security breach."

Unfortunately, a common misconception is that hackers will not waste their time on a small business. This belief means organizations are unprepared for a risk that could destroy their business. In fact, according to the Symantec 2012 Internet Security Threat Report, "In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them."

Why your business is at risk

When it comes to cyber liability, there are four types of companies: Those already breached; those unaware of a breach; those about to be breached; and, those no longer in business due to a breach. Why are small and medium-sized businesses at risk for a breach?

Legally, regulatory burdens for data protection and breach notification are significant in both California and at the federal level. Regulations may allow individuals to pursue private action or require millions in potential fines for a breach.

This means any businesses with a computer system that contains personnel and client information is at risk of a multi- million dollar lawsuit or fines. The vast majority of small and medium-sized businesses hold data classified by the government regulations as personally identifiable information (PII) and protected health information (PHI). PII and PHI are regulated under a variety of state and federal data privacy and breach notification laws.

The Ponemon Institute's 2011 notes in their seventh annual study concerning the cost of data breach incidents for U.S.-based companies that the average cost of a breach was 5.5 million dollars. The report also states, "Negligent insiders are the top cause of data breaches while malicious attacks are 25 percent more costly than other types."

At an average breach cost of $5.5 million, the risk is high, especially because data classified as PII or PHI is more far-reaching than ever. Threats now extend beyond basic malware. Hackers are able to gather information on nearly every aspect of an employee's life from browsing and banking activity to keystrokes. Actual views of a computer screen, user names and passwords, or images can be captured. Today's technology even allows a hacker to turn on and control a computer remotely, activate microphones and cameras and become an employee or employer in chats, emails and social networks. Intellectual property is also a key target for hackers. Information such as campaign concepts, recipes or new products on a computer system may be taken in a breach. With a few keystrokes, an adept hacker is able to steal ideas critical to a company's growth.

Protecting Against Cyber Liability: A comprehensive risk management plan

Clearly, cyber liability is a serious threat to small and medium- sized businesses. Fortunately, a comprehensive risk management plan can help an organization guard against a catastrophic breach.

A comprehensive risk management plan includes leadership's strong understanding of new notification laws, a post-breach plan, a competent spokesperson, and cyber liability insurance. Information for new notification laws can be found at www.perkinscoie.com/sc_california. A post-breach plan will detail company-wide directives for employee actions in the case of a breach, and a spokesperson will deliver key messages to the media.

© Edgewood Partners Insurance Center

Cyber Liability Insurance

Key to an effective risk management plan is cyber liability insurance. For a small or medium-sized business, it can be the life or death difference in a cyber attack. About 80 percent of the claims in a breach are of a first party nature. First party losses are damages to the business itself and third party losses are damages to any person or entity other than the breached business. Cyber insurance coverage that protects against first and third party damage falls into two main categories: casualty/liability and property.

Casualty/liability coverage protects against a cyber-breach event related to network security, privacy liability, employee privacy liability, and electronic media liability. An example would a hacker gaining access to a past customer's social security number or data from an employee health insurance census.

The property category addresses the restoration of data, costs of business interruptions, crisis management costs such as forensics, fulfilling legal obligations, and cyber-extortion. It also includes things such as the cost to comply with the new notifications laws, credit monitoring, the loss of digital assets, cyber terrorism, security and other expenses. Choosing the correct cyber-insurance is a challenge. Policies vary widely on coverage, sub-limits and terms. Fortunately, there has been a dramatic drop in pricing in the last few years as more insurers see the importance and jump on the cyber bandwagon. A knowledgeable insurance broker to negotiate the correct terms of coverage based on a company's individual risk is critical. Excellent coverage paired with an understanding of cyber liability and a thorough risk management plan can help avoid or prepare for the significant damages resulting from intrusions of an organization's confidential data. As the Inland Empire's economy continues to improve, small and medium-sized businesses that prepare for a breach are setting the stage for economic success.

Byline information

David J. McNeil, Associate in Risk Management (ARM) is a vice president at EPIC. David has 25 years of experience specializing in cyber-exposures for technology, manufacturing and water infrastructure segments. Contact David at 714.856.4221 or dmcneil@edgewoodins.com.

Kevin B. McDonald, CHPSE is president of Noloki HealthCare Information Technology and Compliance and EVP at Alvaka Networks. Alvaka is a recognized market leader and pioneering information technology managed services provider. He can be reached at 714.793.3191 or by email at kevin@noloki.com.

Dan Ryan, Certified Insurance Counselor (CIC), is the managing principal for EPIC's new Inland Empire office. Dan Ryan has more than 30 years of insurance experience. Dan can be reached at 909.456.8933 or by email at dryan@edgewoodins.com

About EPIC

EPIC is the 7th largest broker based in the U.S. West, EPIC has more than 300 team members operating from 10 offices across California. With more than $80 million in revenues, EPIC ranks among the top 40 retail insurance brokers in the United States. For additional information, please visit www.edgewoodins.com.

© Edgewood Partners Insurance Center CA License 0B29370