cyber risk in the technologygoldenage

By Woodie Van Horn; Gillis Ellis Baker

Cyber attacks are the hot topic of 2015. Last year saw digital assaults on Home Depot, JPMorgan, and most famously, Sony Pictures Entertainment. But big corporations aren't the sole targets of cyber attacks. According to Property Casualty 360, 85 percent of data breaches occur at the small business level, a threshold occupied by many in the real estate industry.

In today's technology-dependent society, real estate and title agents are especially susceptible to these breaches because they rely on computer and web-based systems to operate. Real estate companies maintain and store the exact types of personal information that cyber criminals want most: social security numbers, credit/ debit card numbers, bank account information, and driver's license numbers. The question most daunting for businesses to consider is no longer if a breach will occur, but when.

The fact that 75 percent of data breaches arise from human error should be of particular concern to real estate professionals, given the personable and hands on nature of the industry and the increasing reliance on smart-phones and tablets. Extra care needs to be taken to limit the damages that can be caused by the theft of an easily lost mobile device. At the very least, and disposal of information. Protocols such as the Fair and Accurate Credit Transaction Act (FACTA) outline specific steps to take to dispose of data-containing records.

The average cost of a data breach is $300,000, yet more than 40 percent of businesses do not have a breach contingency plan to protect them from the costs of recovery. Fortunately, there are a number of tools that businesses can employ in order to limit their exposure to security breaches. The three levels of protection are avoidance, prevention, and transfer of liability insurance.

AVOIDANCE

Everyone should already be cautious enough to not open unknown emails or attachments, but another strategic method to avoid a cyber attack is to minimize the amount of data that is kept and reduce the number of places where data can be found. If a third party keeps or stores your data, review your contract with them to determine if they will indemnify you if a breach occurs.

PREVENTION

All businesses should establish strong IT and malware/antivirus systems within their companies' computer network. There should be firewalls on all business devices and PCI DSS compliance when accepting credit and debit cards. In addition, there should be strong web access and download protection on the server. In the case of stolen or lost laptops, phones or other devices, the ability to remotely remove all data could be a vital tool.

INSURANCE

Cyber insurance policies are becoming a vital piece of the puzzle to protect your assets following a breach. Any policy worth pursuing will have two basic components: coverage for the expenses your business incurs following a loss, and coverage for liability to third parties (e.g. customers) – in this case, those outside your organization affected by a breach.

Coverage for your business' incurred expenses can include: notification costs and credit monitoring costs, cyber business interruption (this covers a business' loss of income if affected by a cyber breach, which is not covered under typical business interruption policies) and denial of service / extortion coverage. Some policies even have coverage to repair or replace computer hardware or software compromised by the breach. Coverage for fines imposed by regulatory agencies may also be covered under your policy.

Liability coverage should also include: liability for breach of personal identifiable information, have a worldwide territory, claims arising from authorized third parties (someone accessing your data with your permission) and reputational damage (libel, slander, or privacy rights).

Many carriers have even begun providing access to their cyber risk management specialists. These specialists will offer pre-loss coaching and advice on infrastructure as well as best practices on breach prevention. Additionally, they can offer post loss event management coordination of responsibilities for which many businesses are unprepared.

Special endorsements can also add coverage for public relations expenses as well as costs related to advertising and media activities following a breach to mitigate any reputational harm. There are even some carriers that will send you tangible hardware for your IT department to incorporate into your IT systems.

Cyber liability policies are evolving products in the world of insurance. Price should be a consideration, but not a sole determining factor. Since not all policies are created equal, best to consult with an experienced agent to select the best one for your business.

As in real estate, the details matter. ■