Is Cyber-Coverage Part of Your Business Insurance Program?

Everyone is aware of the problem of computer virus and computer hacking issues that have caused considerable havoc and unrest in corporate America. News of malicious intrusions by hackers stealing millions of personally identifiable information from businesses has grabbed the headlines, and rightfully-so, but it's the less publicized claims that insurers see in far greater numbers that can be just as involved and costly. These claims involve privacy-related breaches that require strict compliance within numerous state and federal laws; incidents arising out of human error, lost equipment with unencrypted data, insider threat, and more.

Due to both increased claim activity and the increased threat for claim activity, most within the insurance industry agree that we can expect a continued trend increase in rate, i.e. premium. Not necessarily specific to food products, or any one industry necessarily, but most potential insureds should expect increased scrutiny surrounding network security. In other words, how is your data protected?

Fortunately, 2016 didn't see the large, news worthy cyber losses of years past. That can be viewed as good news that data protection is advancing. It could also be that the public has become desensitized to it. The truth is that privacy and security issues have never been more

prevalent. What might consider traditional buyers – retail, financial, and healthcare – still make up approximately half of known data breaches. However, this still leaves a large segment of industry outside the traditional buyers with exposure to cyber loss. No industry is immune. Any company, large or small, can be targeted. It's not just the Home Depots and Target Stores that we've heard about in the news.

Misuse of Privilege

Data breaches are often thought of as the result of specific, targeted, criminal actions. However, more data shows miscellaneous errors as a leading factor in data security events in almost a quarter of all incidents. Misuse of privilege wasn't far behind. Misuse of privilege is particularly interesting. Almost 80% of the attacks on company data are actually executed by employees or ex-employees. And, it's a totally different ballgame if someone abuses privileges they have legitimately. Abuse of legitimate privileges can be considered a database vulnerability if the malicious user misuses their database access privileges. For example, an IT person at your company looks into data that he/she has no business knowing, such as individual employee compensation. And, from there, leaks that information causing harm to the company. It is true that this could also be an application problem, but typically that is not the case.

Keep in mind that it's not just the outside threat, i.e. a former disgruntled employee, that poses a problem to your sensitive data. Over 60% involved abuses of privileged access. Privileged access meaning personnel with approval for access to certain data. However, data mishandling and/or unapproved hardware and software applications all involved claims activity. In addition, possession abuse, email misuse, knowledge abuse, illicit content, to name a few, also come into play.

The majority of perpetrated acts have come through malicious email attachments, drive-by downloads on websites, or a hybrid-type approach, where a malicious email contains a link to a website with harmful downloads. The golden rule here is, if you are not sure the email is safe to open, don't. This doesn't mean that every email that sits in your email spam-bin is a bad email. However, practice caution here.

Credit cards

Vendors continue to be a leading source of incidents. There are numerous types of malware that may be used in an attack. Fortunately, Europay MasterCard Visa (EMV) standards required as of Fall 2015 have helped curb this area of malware attack, but for those not to EMV standards, the exposure if very real.

So, with everything said to this point, what exactly is Cyber-insurance? The short version is that cyber-insurance is an insurance product used to protect businesses and individual users from internet-based risks. Risks of this type are typically not addressed in general liability policies, or excluded from what we might consider a traditional business policy. With a cyber-specific insurance policy, coverage will typically include first-party coverage against losses that can include data destruction, extortion, theft, and hacking. In addition, a cyber-liability policy will typically indemnify a company for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation. Other coverage benefits may include post-incident public relations, investigative expenses, and criminal reward funds. Each insurer will have a policy that varies, but this gives you an idea of coverage provided.

Bottom Line

Cyber insurance premiums are expected to grow from the neighborhood of $2 billion in 2015 to an estimated $20 billion or more by 2025. Insurers and reinsurers are continuing to refine underwriting requirements based on type of loss, frequency of loss, and quite frankly, the misguided intelligence that continues to develop and perpetuate this activity. And, how does an insurer price cyber coverage? Rating is still a fluid proposition.

The underwriting of cyber products today makes it an interesting place to be in the insurance world. Interesting and insurance…two words you probably would not align! But, think about it…not only do you have an insurance marketplace that's trying to reach a standard to accommodate the needs of today's insured across a broad spectrum of industry, but you also have, as mentioned, a rapidly developing exposure. The bottom line is to make sure you have cyber-coverage as part of your business insurance program. Talk to your insurance representative about the specifics of the policy (not all policies are created equal) and examine what you are doing within your own organization to minimize your exposure to this growing concern.