Cyber Liability – Not Just for the Big Guys

By Dillon Behr
Producer
RPS Executive Lines

"I am convinced that there are only two types of companies: those that have been hacked and those that will be." - Robert S. Mueller, III - Director, FBI

It seems every day we read about a new company being hacked and clients' personal information released. After more than a decade in the military, government and commercial security industry, I keep my cyber security pretty tight, yet my personally identifiable information (PII) has still been compromised in the Target®, Home Depot®, and the federal government's Office of Personnel Management (OPM) breaches. One might think that by now there is nothing left to steal. On the contrary, foreign governments, international crime organizations, hacktivists, rogue and for-hire hackers, and even the "script kiddie" next door all want your clients' information.

The companies listed above are all large, household names, but the fact remains that companies of all shapes and sizes are targeted by hackers. If Anthem, Home Depot, and Ashley Madison each have millions of dollars to spend on their information technology (IT) security, and they still can't get it right, then the smaller companies stand almost no chance of preventing a determined attacker from getting to the information they want.

Sound a bit gloom and doom? It is. Fortunately, a well-designed cyber liability and breach response insurance policy can help your clients weather the storm should they become a victim (or a Target®). This article is designed to give you some ammunition for selling to those small-to-medium sized companies that just don't think they are going to be attacked. Here are some of the questions I hear quite regularly:

Why Would They Attack Me?

Consider this: a company does not have to actually be targeted in order to be breached. Acunetix (and many others like it) is a freely available commercial software tool that allows any ill-intentioned hacker to remotely scan computer networks for vulnerabilities. It wasn't designed for that. It was designed to help a company scan its own networks and look for vulnerabilities so it could patch them. But the bad guys got ahold of it and it is used to identify vulnerable businesses, all day every day. The software will tell an attacker where targets of opportunities are, and which specific vulnerabilities they have. He can then remotely attack that network without

even knowing or caring who it belongs to.

According to the Symantec 2014 Internet Security Threat Report, small businesses accounted for 30% of targeted spear-phishing attacks in 2013. Verizon reported that approximately 40% of all data breaches occur among companies with fewer than 100 employees. Even more alarming is the fact that 60% of these companies are out of business within six months. That last statistic should be enough to convince anyone with a business and a computer to purchase a policy.

How Would They Attack Me, And How Would I Be Covered?

What follows is a variety of attacks that can be launched at your clients' networks. You do not need to understand the technical aspects of these attacks as well as I do, but you should be able to explain to your clients why they need specific coverages, and have examples of what might trigger them. The relevant coverage areas are noted in **bold**.

Phishing, Whaling, and Spear Phishing: digital forms of social engineering to deceive individuals into providing sensitive information. Phishing emails are often laden with malicious links and attached documents that can run unknown scripts that can turn the host computer into a slave for the attacker, or worse, give them a deep entry point into the organization's network. Despite the best efforts of the mandatory 1-hour a year automated training course, a recent study by the security firm PhishMe found that 23% of recipients open phishing emails and 11% open attachments. Phishing attacks that result in corruption, deletion of or damage to electronic data to the insured can be covered under the **security breach response** coverage, while damages to a third-party can be covered by the **security liability** coverage as a "Security Wrongful Act".

Malware: software that compromises the operation of a system by performing an unauthorized function or process. An invasive malware attack can be devastating to your client. Data can be deleted, corrupted, changed, or just rendered inaccessible. To clean up this mess it may be necessary to bring in outside expertise. These cyber security experts will conduct digital forensics, identify the malware and point of entry, provide mitigation services, and hopefully restore the network to its pre-infected state. These security experts can become quite costly. **Security breach response** coverage provides pre-negotiated rates with trusted security firms, and **digital asset restoration** coverage helps cover the cost of getting your clients' digital assets back to their pre-loss state.

Insider: a person or group of persons within an organization who pose a potential risk through violating security policies. An insider attack can be crushing for an organization. Insiders may have privileged access to private information that the organization has an obligation to safeguard. A malicious insider can steal and release that data, or even leave a bit of code designed to encrypt or delete the information if fired from his job.

Physical Theft/Loss: 15.3% of all attacks come from this category. Many think the term "Cyber" implies coverage only for incidents that involve electronic hacking or online activities, when in fact it can and should be much broader, covering private data and communications in many different formats—paper, digital or otherwise. Even having your briefcase stolen from your car could activate a solid policy.

Denial of Service (DoS and DDoS): an attack that prevents or impairs the authorized use of information system resources or services. I have seen this in action. Earlier this year there was a group that was sending a high volume of data to targets, hoping to overload networks and effectively block the targeted company from conducting business as usual. This group concurrently sent an email to the company stating that the attack will continue unless they pay the attackers 70 BitCoin ($16,000 USD). In another attack, instead of blocking business networks, the attackers encrypted the workstations of employees, rendering them useless unless the victim organization payed a BitCoin ransom by a specified deadline. These attacks are known as **cyber extortion**, and can leave the business open to **business interruption**.

How Much Would A Breach Really Cost Anyway?

The Ponemon Institute has estimated that the average cost per electronic record lost is $201 without insurance. That cost can be reduced to as low as $20-$24 with a good cyber policy because the insured now has access to a 24-hour breach response firm and pre-negotiated rates for forensics, remediation, legal, and notification firms. Handling a cyber breach is not a do-it-yourself project.

Another element that many people do not consider when calculating the costs of a data breach is the potential for lost income while the business is recovering from an attack. For instance, **cyber extortion** coverage will cover the costs of preventing encryption of data or a DDoS attack, while **business interruption** coverage can help the organization recoup the cost of lost business if the attack is successful and keeps the company from conducting its daily business for an extended period of time.

Isn't This Covered By My BOP Or GL Plan?

In short, NO. Some General Liability, Commercial Crime and D&O policies do contain limited data breach and privacy claims language, but these forms are not intended to respond to the attacks outlined above. Carriers are going to great lengths to include exclusions that make clear their intentions of not covering these threats. Additionally, even in the rare instances coverage does exist, these policies lack the expert resources and critical first-party coverages that help mitigate the financial, operational and reputational damages a data

breach can inflict on an organization.

Your clients trust you to help them prepare for worst case scenarios, for the risks that they cannot mitigate themselves. There is no such thing as a 100% secure network and no industry is immune to security failures. Don't let your client get away with "that won't happen to me because I'm too small". Your clients need broad coverage and they need it now, but it might take a bit of convincing for them to realize that they can be affected just like the big guys – in fact, smaller companies need this coverage more because they don't have the balance sheet to sustain the costs associated with a breach. The cyber insurance industry is just now starting to really take off, and you need to understand the threats in order to sell it effectively.

About RPS Cyber

With regard to the purchase of insurance, at RPS we understand that the complexity and length of the application process was a significant impediment to the procurement of cyber insurance. RPS has built a platform at **RPSCyber.com** that will allow a retail broker to procure a bindable quote for their clients under $100M in revenue within 60 seconds. The policy comes with full first and third party limits as well as access to an industry leading breach response team. To learn more please visit **RPSins.com/cyber**.

Get a Cyber Liability quote in seconds at www.NFIBCyber.com

Call us toll-free at (855) 200-5313

or email us at
nfibcyber@selectsolutionsins.com