NO BUSINESS IS TOO SMALL FOR A CYBER-ATTACK

Large companies like Sony, Home Depot and Target are well-known today for more than just their popular brand names; they've been the well-publicized victims of vicious cyber-attacks. Once relegated to the IT or security department, cybersecurity now has the attention of senior executives worldwide. The impact of cyber intrusions can run deep into an organization and bring about devastating loss of business, reputation and create liability on an unheard of scale.

And it's not only large organizations that are at risk; in the past few years, cyber criminals have focused their efforts on small and medium-sized companies in a big way. The 2012 Data Breach Investigations Study by Verizon shows that 71% of data breaches happened in businesses with less than 100 employees. And according to security expert Symantec, cyber-attacks on smaller businesses are on the increase: over 40% of the cyber-attacks the company prevented in early 2012 targeted companies with less than 500 employees.

All sizes and types of business are fair game for cyber criminals today, with smaller organizations often viewed as a much easier target. Small and medium-sized enterprises (SMEs) don't usually have the in-house expertise or resources to deal with cybercrime, and most are too focused on the day-to-day of growing and running their business to deal with the risk. But smaller businesses are often ripe opportunities in the eyes of a criminal, loaded with valuable intellectual property, customer payment info and cash in the bank.

Other reasons smaller businesses are so attractive to cyber criminals? In spite of recent highly-publicized hacks, large companies have invested heavily in sophisticated security strategies and teams and are now harder to penetrate. Cyber criminals have become increasingly sophisticated too; they often see the smaller vendors and partners of large companies as an easier way in, a stepping stone to the databases, networks and customer information of major corporations.

WHAT IS CYBERCRIME AND WHO'S AT RISK?

Cybercrime refers to any criminal activity that's conducted using the internet. Attacks of this sort can include stealing bank accounts, intellectual property and trade secrets, confiscating and distributing confidential business or financial information, disrupting everyday business operations, planting and spreading malicious computer viruses and more.

Any business that uses computers, smartphones, email, websites, social media or cloud-based services provides a point of entry for hackers and thieves. And, if your business creates, collects, stores or processes payment info, client names or records, intellectual property, has access to a business partner's website, personal information or other sensitive financial or proprietary information, you are a potential target with much to lose.

HOW CYBERCRIME CAN IMPACT A BUSINESS

Cyber-attacks are a serious matter for company of any size, but their impact can devastate a smaller organization. A cyber-attack can:

- Damage or destroy your company's brand image and reputation
- Result in the loss of sensitive and proprietary information and intellectual property
- Immediately and negatively impact sales volumes and market competitiveness
- Perpetrate fraudulent activity in the name of your company, leaving you open to lawsuits, fines and penalties
- Cause employee, client, vendor and business partner identity theft

- Leave company owners/directors vulnerable to lawsuits and personally liable for damages and fees
- Be the cause of class action lawsuits by customers
- Expose a company to the tremendous financial burden of litigation costs, compensatory actions and awards, business interruption and brand name restoration, to name a few.

According to a 2012 nationwide study by digital security company Symantec and the National Cyber Security Alliance (NCSA), cyber-attacks cost small and medium-size businesses an average of $188,242. Not surprisingly, many of these companies are forced out of business within months of being attacked.

And while the number and frequency of major data breaches continues to increase overall awareness of the cybercrime threat, the study reports that the majority of small and medium-sized businesses have a false sense of security about their own chances of being victimized. While 77% of businesses studied say that strong cyber security is critical to their operations and brand success, nearly 60% have no plan for dealing with an attack if it were to occur.

SIMPLE THINGS EVERY BUSINESS CAN DO RIGHT NOW

Here are steps that any business can take to shore up defenses and lessen the probability of a cyber-attack:

1. *Take an Inventory* of data, intellectual property and other assets that your firm has. Know just what you possess and where it's located. You can't defend what you can't identify and locate. Then, back up everything – consistently and frequently.

2. *Train employees on the basics* – Employees are often the unknowing cause of breaches. Educate them about internet safety, deleting suspicious emails, as well as offline best practices like shredding or properly disposing of sensitive documents, and not providing proprietary information over the phone.

3. *Control and review* – Disable user accounts when employees leave the company, regularly audit accounts, monitor access to sensitive files and let employees know that there are consequences for misusing company assets - all ways to help mitigate the chances that assets are leaked internally. The key is regularly reviewing, which will aid in early detection and damage mitigation.

4. *Practice good password management* – A policy that enforces minimum password length, complexity, expiration and other basic best practices goes a long way to deterring brute force password violations.

5. *Isolate business-critical functions and information* – Do not browse the web, use email or social media, play games or other potentially vulnerable activities on systems that house your product software, sensitive financial information, Point-of-Sale system or other business-critical functions or data.

6. *Strongly consider a Cyber Liability insurance policy.* Many companies assume that their General Liability (GL) coverage includes cyber risks, but that's most often ***not*** the case. Insurance carriers provide Cyber Liability coverage through their Professional Liability lines, so be cautious when assessing exposure. Given the devastating business and financial fallout from a cyber-attack, strongly consider coverage specifically written for these events.

RESOURCES THAT CAN HELP

While cybercrime is an ever-present threat, there are some excellent resources that can help you stay a step ahead. Here are a few:

PropertyCasualty360's article full of links to useful articles on the subject

TechNet's article on setting strong password policies

An excellent 'primer' from a cyber-security consultant that's easy to read and understand.

StaySafeOnline.org's list of cyber resources, including links to the National Cyber Security Alliance/Symantec study

The 6 most dangerous cyber-attack types that can plague a small business

EXPERTISE TO MANAGE CYBER LIABILITY CLAIMS

In the event your company is the victim of cybercrime, it's critical to have professionals who are experienced in handling the multitude of complex business and legal issues that result, including:

- Assessing the scope of the breach and damages
- Complying with all federal and state notification and credit monitoring regulations
- Advising on a response plan to mitigate business interruption and brand damage
- Interceding with credit/debit card processors
- If necessary, bringing in forensic and public relations experts to assist in investigations and brand damage control
- Manage and litigate any professional or management liability claims

YorkPro, a dedicated team within the York Risk Services Group family of companies, specializes in professional and management liability claims and has experienced adjustors/litigators well-versed in handling the complex management liability claims that can arise from a cyber-attack.

Cybercrime is one of the most devastating events that can happen to a small business; having knowledgeable professionals to guide, advise and defend can give an organization the best possible chance to minimize the damage and get back to business as usual.