Is Cybercrime a Threat to Your Business?

Howard Goldman, Partner, CFO Edge, LLC

Most Los Angeles and Southern California business owners and entrepreneurs are familiar with recent headline-grabbing cyber attacks on large organizations like the ones that have occurred at Target, Home Depot, Anthem Blue Cross and Sony Corporation. It is easy to think that cybercrime is only a threat to large corporations and not something that smaller businesses need to think about or plan for.

However, the fact is that most cyber thieves are not zeroing in on businesses based on size. Rather, they are looking for businesses of any size, in any industry, that have not implemented adequate data security safeguards to protect sensitive corporate, employee and customer information. In fact, some cybercriminals are specifically targeting small and mid-sized firms that are less well protected. These companies are large enough to have significant financial resources, but small enough that they do not employ the latest and most sophisticated cybercrime defenses.

Frightening Cybercrime Stats

According to a study performed by Norton Symantec, 18 cybercrimes now occur every second, and an average of 1.6 million people are victimized by cybercrime every day. In addition, 77 percent of respondents to the *2014 U.S. State of Cybercrime Survey* said they had experienced at least one cyber-security event in the past year. Cyber crime has become such a concern that the Director of National Intelligence has listed it as today's top national security threat, even ahead of terrorism.

Statistics like these make it clear that no business, regardless of its size, can afford to take the cybercrime threat lightly. This makes it critical to devise strategies for protecting your business from the potentially devastating effects of a cyber attack. There are several different types of cybercrime risk your business might face, including:

- The theft of customer and employee data like credit card and Social Security numbers that can be used to make illegal purchases.
- The theft of intellectual property, corporate trade secrets and sensitive internal communications, including emails between employees and with customers and vendors.
- The introduction of malware into corporate networks that can be used steal employees' bank account and wire transfer login credentials (such as user names and passwords) and launch denial of service website attacks.
- The introduction of ransomware into corporate networks to encrypt and deny access to company files unless a ransom is paid to the cyber thief.

The Sony Pictures cyber attack provides a case study of the second risk noted above. In this instance, cyber thieves stole and released internal emails that proved to be both embarrassing and damaging to key executives and some other employees. In addition, they stole and released on the Internet movies that had yet to be released, costing Sony untold thousands (or possibly even millions) of dollars in revenue.

 © 2015 CFO Edge, LLC

A Cybercrime Prevention Plan

To protect your business from a potential cyber attack, you and your key managers should create a comprehensive cybercrime prevention plan. This plan should start by identifying the areas where your company is most vulnerable to a cyber attack. Then you can devise specific strategies that are designed to guard against these vulnerabilities. Some of the most effective cybercrime prevention strategies include the following:

1. Make password strength and security a high priority. Your employees should be using strong passwords and changing them on a regular basis. Whenever the feature is available and appropriate, implement two-factor authentication at login.

2. Use the most recent versions of anti-virus and anti-malware software on all of your company's computers and servers and keep the software updated.

3. Make sure your email servers and wireless networks are secure. If you offer Wi-Fi to your customers, provide them with a separate wireless network from the one used by your business.

4. Closely regulate and monitor employee Internet activity.

5. Severely limit the kinds of software your employees can download from the Internet.

6. Devise and implement firm policies for how employees can use mobile devices such as smart phones, laptop computers and flash drives and how these are kept secure. Also, protect laptops and mobile devices with the ability to remotely wipe clean any device that is lost or stolen.

7. Educate employees about the most common schemes used by cyber thieves to try to steal sensitive corporate information, including phishing and spear phishing email scams.

8. Look into obtaining a cyber liability insurance policy to help limit the financial damage that could occur as the result of a cyber attack on your business.

Concluding Thoughts

While owners might not realize it, small and mid-sized businesses are at just as much risk of cybercrime as are large corporations. The effects can be far more damaging since these businesses might not have the resources to recover from such attacks. This makes it critical to devise strategies for protecting your business from a cyber attack. An outsourced CFO services provider can help assess your company's specific cybercrime vulnerabilities and risks and work with your IT staff, third-party providers and others to protect your company from the potentially devastating effects of a cyber attack.

About CFO Edge

CFO Edge, LLC delivers enterprise-class financial and operational performance solutions to executives throughout Southern California. Based in Los Angeles, our formerly-seated chief financial officers engage on demand as part-time CFOs, single-project CFOs, and interim CFOs to help business leaders successfully resolve pressing challenges and realize their financial and operational goals. At CFO Edge, we are passionate about helping our clients create, grow and sustain value. For more information, visit www.cfoedge.com or call 800.276.1750 Ext 101.

This publication has been prepared for general information on matters of interest only, and does not constitute professional advice on facts and circumstances specific to any person or entity. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication. The information contained in this material was not intended or written to be used, and cannot be used, for purposes of avoiding penalties or sanctions imposed by any government or other regulatory body. CFO Edge, LLC, its members, employees and agents shall not be responsible for any loss sustained by any person or entity who relies on this publication.