Six Steps You Should Take to Secure Your Corporate Data

Sherry Rahbar, Partner, CFO Edge, LLC

It seems that hardly a week goes by without headline news of another major data breach at a large U.S. corporation. A recent online article[1] listing the biggest data breaches so far in 2016 included major cyberattacks at the U.S. Department of Justice and the IRS, Snapchat, Premier Healthcare, Verizon Enterprise Solutions, MedStar Health, Oracle, LinkedIn and Wendy's.

Of course, data breaches at major, well-known corporations get the headlines — and because of this, many owners of small and mid-sized firms think that big businesses are the only ones that have to worry about cyberattacks. In reality, hackers and cyber thieves are looking for businesses of any size that haven't secured their computer networks and sensitive financial information pertaining to both the corporation and its customers, vendors and other stakeholders.

Another mistaken assumption by many owners and entrepreneurs is that the vast majority of cyberattacks and data breaches are originated from outside the organization. However, approximately 40 percent of security breaches are originated via an internal source, such as a company employee.

Critical Data Security Tasks

In recent articles, we have discussed the importance of data security as part of a working relationship between a business and its outside service providers, as well as the different types of cybercrime risk that businesses face today. Here, we will focus on the most critical tasks your business should be performing in order to secure your computer systems and your data.

Following are six data security tasks that businesses of any size should perform right away:

1. **Conduct a data security audit on a periodic basis.** It is imperative to work with a security consultant that is capable of analyzing your entire IT organizational structure, including your network, all company computers and all employees' mobile devices.

2. **Limit employees' access to the network system.** Employee access to the network should be limited to what is required for employees to perform their job functions. Also implement strong internal controls surrounding your IT infrastructure.

3. **Educate your employees about the crucial role they play in securing data.** This includes reminding them about the importance of using strong passwords and not sharing them with others inside or outside the office.

4. **Encrypt all of your data.** This way, if an employee's hard disk or USB flash drive is lost or stolen, whoever has it will not be able to read the data.

5. **Back up all of your data on a daily basis.** This is a simple but often neglected data security practice. Backing up your data is just as important as securing your data. If your systems crash or data is corrupted and you haven't backed it up properly, your business could suffer irreparable harm.

6. **Create security policies and make sure all employees are aware of and understand them.** For example, insist that all devices (such as laptops, mobile phones and tablets) connected to the corporate network have security software. You may also want to consider implementing multiple layers of security technology on all devices. Your security policies should form the foundation of your data security program.

Benefits of Data Security

Your company will realize many benefits by performing these and other data security tasks, including:

1. A minimized or diminished risk of financial loss.

2. A higher level of confidence and greater peace of mind for business owners and the executive team.

3. Safeguarding of your customers' private information, thereby increasing customer confidence and trust in your business.

4. Protection of your computers from physical damage that can be caused by hacking attempts or viruses downloaded from the Internet.

5. Compliance with data security laws, including the Federal and State Unfair and Deceptive Practices Act that requires the use of appropriate security policies and procedures.

Concluding Thoughts

Many owners of small and mid-sized firms think that big businesses are the only ones that have to worry about cyberattacks. In reality, hackers and cyber thieves are looking for businesses of any size that haven't secured their computer networks. This makes it critical that you perform data security tasks to protect your computer systems. An outsourced CFO services provider can evaluate your data security policies and procedures and create an overall strategy designed to protect and safeguard your most valuable asset: your corporate data.

1 The Biggest Data Breaches in 2016, So Far; Judy Leary; IdentityForce; September 6, 2016 www.identityforce.com/blog/2016-data-breaches

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.