Cybercrime: A Growing Risk for Businesses & CFOs

John W. Braine, Partner, CFO Edge, LLC

In recent years, cyber security has become one of the top concerns for businesses of all sizes. We addressed cybercrime risk in our 2015 article – *Is Cybercrime a Threat to Your Business?* – and the risk has become even greater since then.

Given the traditional role of the CFO as a safe-keeper of corporate assets and overseer of risk management, the rise of cybercrime has had a disproportionate impact on the finance departments of many organizations. Although other executives and C-suite officers are parties to the decision-making processes included in risk management, CFOs are unique in their expertise within a risk-based, internally controlled environment. This environment is responsible for identifying threats and assessing the cost of cyber security tools to prevent such threats from becoming a reality.

All Industries Are Affected

Protecting data from cyber security threats means different things for different industries. For example, financial institutions and healthcare organizations have long been required to secure client and patient information under regulatory guidelines such as the Health Insurance Portability and Accountability Act, or HIPAA. With the significant increase in cybercrime in recent years, virtually all industries must be cognizant of the potential for cybercrime to severely interrupt their operations.

In the past, many small and medium-sized enterprises (SMEs) didn't believe they needed to take steps to guard against cybercrime. But this is clearly no longer the case — in fact, cyber criminals frequently target SMEs because they are often less likely to have robust cybercrime defenses. Also, many SMEs have entered into cloud-based operating systems that could further expose them to cyber security risks. Such external cybercrime risks can be difficult or impossible to control.

The fact is, most businesses have prepared disaster recovery plans in the event the business needs to respond to interruptions caused by disasters like storms, floods, fires or even terrorist attacks. However, many haven't planned for the destruction and disruptions that could be caused by a cyber attack — disruptions that could be even longer in duration. Therefore, contingency plans should be made now for any types of interruptions that could result from a cyber attack so you can be prepared to get your operations back up and running again as quickly as possible after the attack.

Creating an Effective Cybercrime Defense System

Your challenge is to create an effective cybercrime defense system within an acceptable budget that will safeguard your company's operating environment and assets. A managed security service provider can help you accomplish this by performing an overall cyber risk assessment and conducting comprehensive cyber security planning.

One of the first steps in your cyber security planning should be to rank all the data assets your company employs based on their value to the company. This ranking should be based on the importance of the information and the

applications used in the business operations, including the generation of revenue. Another planning step is to assess the following:

- How extensive is the risk of cyber attack to the company?
- How could a criminal use the stolen information?
- What techniques might criminals use to commit cybercrime?
- Should you purchase cyber insurance?

Cyber insurance has been a particularly hot topic among business owners and CFOs. There is, of course, the question of how much insurance is needed and how much money to spend on cyber insurance. Most experts agree that cybercrime risk will continue to rise — therefore, your coverage and spend should consider the unique needs of your company, the likelihood and magnitude of a loss due to cybercrime, and the significance of your downside cybercrime risk.

Here are a few other steps that can help you guard your company's operating assets against cybercrime:

- Monitor your employees' Internet activity and password strength as well as your authentication procedures.
- Keep your company's antivirus/malware software up to date.
- Find and hire a managed security service company with highly trained personnel to assist with your cyber risk assessment and cyber security planning.
- Review your company's audit procedures and security and internal controls.

Concluding Thoughts

In recent years, cyber security has become one of the top concerns for businesses of all sizes. And cyber criminals frequently target SMEs because they are often less likely to have robust cybercrime defenses. Your challenge is to create an effective cybercrime defense system within an acceptable budget that will safeguard your company's operating environment and assets. Working together, a managed security service provider and an outsourced CFO services provider can help you accomplish this by performing an overall cyber risk assessment and conducting comprehensive cyber security planning.

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.