Trends in Cyber Risk Prevention

In today's climate, cyber risk is top of mind for business leaders. Unfortunately, many still fail to understand the complexities involved and unknowingly leave their businesses vulnerable.

High-profile data breaches grab our attention on a regular basis – like the hack of Under Armour's MyFitnessPal app earlier this year that was called "one of the biggest hacks in history," compromising 150 million accounts. When these incidents occur, businesses should turn the fear of "what if?" into action by evaluating their exposures and ensuring they are properly protected and prepared to deal with a breach should it occur.

Earlier this year, Scott held an educational event in Raleigh featuring a panel discussion on the emerging trends surrounding cyber fraud and techniques for prevention. One of the panelists at our event was Jeremy Gilbert, IT Advisory Manager at Dixon Hughes Goodman LLP. Jeremy's insights regarding this important topic are valuable, and the following Q&A can help your business as you work to build a strategy to combat the cyber risks that face your organization.

What are the main cyber risk threats facing mid-market businesses today?

Gilbert*:* More sophisticated hacking tools continue to become available to lower-level cyber criminals. In some ways, these tools have exceeded the defensive capabilities of typical mid-market businesses; however, they are not often employed because they are expensive and difficult to use. Less sophisticated attacks, usually requiring a user to click a link or open an attachment, are far more common.

Attacks are typically aimed at one of three things:

1. Extortion; typically done with ransomware, a type of software that encrypts files. Following encryption, the criminals offer to sell the decryption key to the business.

2. Stealing valuable PII (personally identifiable information) such as name, date of birth, account numbers, and addresses of your business, your customers, or your employees. This type of attack is often referred to as a data breach and is usually the most financially damaging that a business can suffer.

3. Securing a jumping-off point for attacks against other targets. This typically takes the form of a compromised web server.

What can businesses do to prevent a breach or minimize their exposures?

Gilbert: Mitigating the risk of a breach and the impact if/when a breach occurs requires frequent monitoring and examination of the threat landscape and your IT environment. Establish a breach response team and hold periodic meetings to ensure new threats are mitigated and changes to your IT environment are analyzed from a security perspective. This team should consist of representatives from IT, upper management, public relations and legal. If you don't already have a breach response team in place, this can seem a daunting task. If you carry cyber insurance, and you should, your insurance broker can be a great resource to help you establish and manage this team.

What are some lessons we can learn from previous/recent events?

Gilbert: Common attacks usually require action from an authorized user to become a successful attack. This action could be opening a malicious attachment or link in an e-mail, downloading a malicious file, visiting a compromised web page, or answering a phishing e-mail. Training your employees in good IT security practices is the most effective way to protect your business.

Typical IT security controls like firewalls, intrusion detection systems, encryption and password policies are important and necessary for good IT security, but the users in your IT environment are the weak link that cyber criminals will try to exploit.

Also, if you outsource any IT support, be particularly vigilant about clearly establishing who is responsible for IT security. We have seen multiple companies breached that thought their managed service provider (MSP) was handling security while the MSP thought the company's IT staff were handling security.

What resources are available to help business executives better understand the complexities of cyber risk?

Gilbert: If you have cyber insurance, your first stop for resources to help you should be your insurance broker. They have a vested interest in helping you secure your IT environment and they may have free or low-cost assistance available to you. Also consider having an outside firm perform an independent assessment of your IT environment and systems to identify technical and operational vulnerabilities.

Many companies offer user training for IT security. Dixon Hughes Goodman can offer customized, in-person training. You might also consider the SANS Institute's Security Awareness Training, which can be completed online.

When hiring for IT security positions, pay attention to which IT security certifications the candidate has earned. There are many IT security certifications, so you can't be familiar with all of them, but a quick search online should inform you as to whether a particular certification is valuable to your organization.

At Scott, we understand the importance of developing a strategic approach to cyber risk, including making sure appropriate coverages are in place. If you have questions about protecting your business from cyber risks, contact a Scott Risk Advisor to learn more.

Thanks to Jeremy Gilbert and Dixon Hughes Goodman LLP for their contribution to this blog. Jeremy can be reached at jeremy.gilbert@dhgllp.com.

Written by Chad Duke

Chad is a Risk Advisor in Scott's Nashville office. He joined Scott in 2009 as a Risk Advisor in Scott's Raleigh, North Carolina location and recently moved to Tennessee to assist in the growth of the Nashville branch.

Call Chad at **919-900-0878** if you have any questions or need any additional assistance.