Tackling Cybersecurity

Protect Assets to Keep Your Competitive Edge

In May of this year, sophisticated cyber-thieves launched the "WannaCry" ransomware attack on Microsoft operating systems across the globe. Described as the largest ransomware attack in history, the thieves demanded ransom from targeted individuals and companies to regain access to their own data files.

In the past, nearly 70 percent of companies affected by similar schemes opted to pay the expensive ransom. If a similar attack happened to your company, what would you do?

Criminals = Entrepreneurs

It's important to acknowledge the mindset of criminal hackers. As shocking as it may seem, like many business owners, they are entrepreneurs. They are quick, clever and committed to doing what they do best. Unfortunately, they do so to the detriment of others.

Knowing what makes them tick — money and intellectual challenge, to name a few motivators — allows you to create a plan that meets the serious nature of their "work." Sometimes they are working for themselves, hoping to sell what they find to the highest bidder. Other times, they are hired by third parties to seek and deliver specific data of value.

IT security experts suggest a number of strategies manufacturers and distributors can take to protect corporate assets. Here are three steps you can take:

- **Realize that you are a target.** While most organizations in the financial services and healthcare industries are aware of their vulnerabilities, many manufacturers and distributors do not always consider themselves to be attractive targets.

  But know this: Cyber criminals would love to get inside your company's network, seeking whatever can be exploited and monetized. Their schemes range from social engineering designed to lure employees to reveal personal information to ransom or outright theft and sale of intellectual property.

- **Acknowledge what's valuable.** Survey your company to discern what might be valuable to others. Consider every area, from human resources to finance and operations.

  Among the potential targets are customer payment information; employees' personally identifiable information; manufacturing processes and procedures; product designs, patterns and schematics; and current research initiatives. All of these assets can be sold to criminals, foreign agents or competitors.

- **Be serious about protection.** Once you have detailed the critical assets at risk, create a plan to protect them. Best practices suggest assigning one person to lead and manage security efforts rather than dissipating responsibility among many individuals. With one person in charge, you are ensured focus and accountability.

IT security experts recommend a multidisciplinary approach. One easy-to-implement measure is prohibiting cameras in the warehouse or on the manufacturing floor. Other tactics include conventional measures such as permissions and access controls and more sophisticated firewalls and encryption.

Threats Are Evolving. Remember that cyber criminals are always one step ahead, plotting and scheming future attacks. Many industry trade groups are trying to stay abreast of the latest threats, and there are outside data security companies available to help you create a security plan. You've worked hard to develop your business and its intellectual property. Don't wait until a data breach occurs to take action.

We are dedicated to your company's success. Our tax team is ready to assist you with any Cybersecurity concerns. Contact us to discuss your questions.

John E. Oeltjen, CPA, CMP
Partner | Director of Manufacturing and Distribution Services
joeltjen@muellerprost.com
314.862.2070
Click here to view previous articles