KROST
CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS SINCE 1939

PrimeGlobal | An Association of Independent Accounting Firms

What You Need to Know About Cybersecurity

All too often we read headlines about major companies that have some sort of breach, Equifax, Target, Sony, Home Depot, just to mention a few. Most people think, "wow, how could they be that careless and then go about their day?" Recently, the Equifax hack hit home for most Americans because it virtually affected all of us. Most people should be wondering if it can happen to them, it can happen to me and my company. We should all be thinking what have I done to prepare myself. One of the easiest ways for a hacker to disrupt a business today is with ransomware.

There are 6 ways for ransomware to penetrate your network:

Inside attacks from phishing emails – Emails appear legitimate, but require your username and password via three distinct methods.

1. Request to respond to email with the personal information requested, which not only allows them access to your computer as you, but grants unrestricted access to your company network.
2. Request to click a link that will automatically download the ransomware to your computer and any immediate network.
3. Downloading attachments from unknown email sender, after downloading, the ransomware will immediately take over all files and connected network drives.

Outside attacks – These are attacks that do not require a hacker to deploy malware from within the physical network of a company.

4. Internet access port – Backdoor program looking for access points to spread malware during a seemingly daily internet routine.
5. USB drives – USB drive hacks have crippled companies for days and some even include location tracking so that hackers can know when someone has brought one into a company. This does not only include USB sticks, but can also be done through any USB cords that have been manipulated.
6. Outside service professionals – These are done through a third-party vendor contracted to work on site who may have access to servers, network ports, or desktop terminals.

In May 2017, AICPA released the Cybersecurity Risk Management Reporting Framework Guide. With the overwhelming threats of cyberattacks, the AICPA recognized a need to arm CPAs with the latest cybersecurity audit guidelines to assist the practitioner and client. The cybersecurity risk management examination is part of the AICPA's SOC reporting, which means that CPAs can provide an opinion on a service of the organization's system controls. The new framework calls

management to take actions and prepare certain information about the entity's cybersecurity risk management program.

There are two sets of criteria proposed by AICPA to be used on this new framework guide, description criteria and control criteria. Description criteria is used when preparing a narrative description of the entity's cybersecurity risk management program. Control Criteria is used when evaluating the effectiveness of the controls within the program. We see these two criteria as (1) Can you document what you can do to safeguard your network and data? And (2) What can you do to prevent a cyberattack?

This new audit service will result in a cybersecurity report that includes management's description of the entity's cybersecurity risk management program, management's assertion on whether the description is presented in accordance with the description criteria, and a CPA's opinion on the description and on the effectiveness of controls within the program.

We see the cyber threat increasing every day. The new AICPA Cybersecurity Risk Management Reporting Framework Guide provides CPAs with an organized way to help identify significant risks with the tools to correct them. We at KROST CPAs & Consultants are prepared to assist businesses with these types of engagements to help prevent successful cyberattacks by helping to document the systems and identifying potential weaknesses that could be exploited by a hacker. It's worth taking the necessary actions now to prevent rather than to resolve issues created by cyberattacks such as ransomware. The time to act is now.

Author: Jason C. Melillo, CPA