TOP FIVE ACTIONS FOR ACCOUNTING & FINANCIAL PROFESSIONALS TO REDUCE THE CYBER THREAT RISK FOR THEIR BUSINESS

By:

Troy McLennan, President & CEO

HUB Technology Solutions Ltd.

www.hub.ca

Definitions

Definitions, according to the Canadian Centre for Cybersecurity (cyber.gc.ca):

Cyber Threat: Is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains. This activity has the potential for causing asset loss.

Cyber Threat Actors: Are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cybersecurity awareness, and technological developments to gain unauthorized access to information systems to access or otherwise affect victims' data, devices, systems, and networks.

Background

Professionals in the accounting and financial fields have access to very sensitive confidential information that belongs to their clients. Accounting and financial professionals have worked very hard at building trust that allows clients to feel confident in providing this information.

It is all this confidential information that makes accounting and financial companies a prime target for cyber threat actors. Once the cyber threat actor gains access to one firm's confidential data, it unlocks numerous other companies' sensitive information.

In the event of a successful attack, the damage to the accounting and financial company's reputation could be enormous, not to mention the loss of profits. Government and regulatory compliance obligate companies to notify clients that their confidential information has been disclosed as a result of a successful cyber threat attack, which virtually guarantees the company's reputation will be damaged.

There are some basic steps that companies can take to reduce their cyber threat risk.

Step #1 - Identify

Know the value of your information! Start by reviewing **ALL** your data and classifying it as high or low value.

High-value data can include, but not limited to:

- Business-critical information that your company needs to operate, for example, line of business applications such as CaseWare.
- Personal information, including names, home addresses, phone numbers, Social Insurance Numbers (SIN).
- Financial data, including bank, credit card information and financial reports.
- Proprietary intellectual property.

Low-value data can include, but not limited to:

- Marketing or advertising material that is readily available to the public.

Know where the high-value data is stored. This can include, on servers, personal computers, laptops, tablets, smartphones, external storage or in the cloud. Identify who has access to the high-value data. By knowing the value, the where and the who of your data, you can more easily identify your vulnerabilities.

Inventory **ALL** your information technology hardware and software. The hardware includes the obvious, such as servers and personal computers, but can also include the obscure, such as internet-connected security cameras and thermostats. Software, just like hardware, includes the obvious, such as Microsoft Windows and line of business applications, but it can also include installed software that you may not be aware of. Employees could have installed some of this software without your knowledge. As well, most hardware manufacturers install software on new servers, computers, and laptops that you may be unaware of, but it still needs to be inventoried. You cannot protect it if you don't know about it.

Step #1 should be in the form of an IT audit. If your company doesn't have the internal expertise or time to perform the audit, hire an information technology consulting company that can do it for you. Perform the audit at regular intervals, minimum every six months. When change happens, you need to know about the risk associated with the change.

Step #2 - Protect

Now that you have completed step #1 and know the what, who and whereabouts of your high-value data, you need to limit access to it. It sounds simple, but it needs to be part of an overall data management policy. Data is constantly changing, and unless you have a policy in place, it will quickly become unruly. Too often, I see companies with one or two shared folders that everyone in the company can access where all it takes is one employee to compromise the high-value data for the whole company. Implementing global security policies found on enterprise server platforms, such as Windows Server, can easily control users' access to folders or have their access entirely restricted.

You need to encrypt high-value data while it is at rest. If the hardware were to be stolen, unless the data is encrypted, it is very easily read and used by the cyber threat actor.

Update **ALL** the software you identified in step #1. Quite often, software manufactures find vulnerabilities in their application, and unless updated, the risk exists that a cyber threat actor will exploit the vulnerability to harm your business.

Don't forget about updating the hardware firmware, which is software that runs internally on almost all hardware devices such as computers, printers, network switches and firewalls. Just like software manufacturers, hardware vendors often release firmware updates that need to be installed to eliminate a vulnerability in the firmware that can be exploited by a cyber threat actor.

Stop threats before they get on your network. The internet is the largest opening cyber threat actors use to get to your high-value data. It makes sense to put the best possible door and locks on that opening. That includes an enterprise-grade firewall, virus and malware detection software, web and email filtering.

Isolate your networks! Most businesses have just one network that all hardware devices connect to, and where all the data resides. Let's call this the Admin Network. The Admin Network needs to be controlled, and only devices that need access to high-value data can connect to it. Other networks need to be created for guests, security devices, telephones and Internet of Things (IoT) devices, such as thermostats. This limits the risk of devices or persons getting access to high-value data on the Admin Network from one of these devices.

Sanitize all media upon destruction. Even after the end of the normal use of IT systems and equipment, residual data can remain and could be of a sensitive nature that you would not want to be disclosed. Take all the necessary steps to protect yourself by sanitizing all media. Media includes not only hard drives, found in everything from computers, photocopies and automobiles to removable media (USB storage and DVDs), smartphones and network devices. The Canadian Centre for Cybersecurity has a publication on IT Media Sanitization that may help you in this process, click this link to view the document: https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006

#3 – Detect

Detection is often forgotten in cybersecurity protection plans. Setting and forgetting your protection systems doesn't work. Anti-virus, anti-malware platforms and firewalls need to be continuously monitored to ensure they are functioning and alerting of threats discovered. Threats are more than likely going to be coming from the internet. Implement an enterprise-grade firewall with intrusion protection that has the capacity for you to monitor activity and audit logs to be aware of threats so the correct action can be taken.

#4 – Respond

Invest in the development of a response plan. If a cyber incident occurs, you will need a plan to have any hope of recovering. Without a plan, it is just PANIC and CHAOS. Trust me, I've seen it. Even a basic response plan helps create policies that address critical elements and processes that should be considered and implemented before a crisis occurs.

Users are frequently exposed to sophisticated social engineering cyber-attacks that get past hardware and software protection, and without training and testing. The users won't be able to recognize these attacks and are vulnerable. Users are typically the weakest link in any cybersecurity plan, and only regular training and testing can improve that.

Know your legal responsibilities. Talk to a lawyer and understand data privacy and protection laws. Let them advise you on the way to protect your business.

#5 – Recover

It isn't a matter of if, but when disaster strikes, you need to be ready. Develop and implement a disaster recovery plan that includes regular testing.

Consider cyber insurance as a way of reducing your risk if a cyber incident occurs. Talk to an insurance professional that specializes in cybersecurity insurance and get advice on how to reduce your risk if a cyber incident occurs.

Conclusion

To reduce your company's cyber threat risk, you need to implement cybersecurity into your day-to-day business processes. Start with these five steps: Identify, Protect, Detect, Respond and Recover. Create a customized action plan that works for your company. If you need help, get assistance from a qualified information technology consulting company.