CPA
Practice Advisor

Federal Government can be hacked, seemingly at will, what can CPAs and their firms do to mitigate this very real risk?

Jun. 25, 2015

Less than half-way through 2015, business and government entities in the U.S. have been hit with 15 major cyber attacks.

A hacker group identifying themselves as HL4T ushered in the New Year by publishing Microsoft's software development kit, known internally as Xbox One SDK. This proprietary information allows anyone with sufficient expertise to create games for the Xbox console.

Later that same month, in a more serious breach, officials of the U.S. military command overseeing Middle East operations were hacked. Several maps and diagrams were subsequently leaked and posted on the Internet.

In early February, Anthem, Inc. suffered a data breach that compromised the health records of 37.5 million customers of various corporate subsidiaries. This leaked information included not only confidential medical records but also names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, which included income information.

All pale in comparison to the most recent breach occurring in the Office of Personnel Management (OPM). Beyond routine personnel files, which contain the most private of detailed information, including social security numbers, salary information and address information, hackers were able to retrieve information regarding individuals processed for security clearances. Latest government disclosures suggest more than 18 million individuals may ultimately be victims of this cyber attack.

Plainly, when a tech giant the likes of Microsoft, the U. S. Military and agencies of the

look pretty much alike. Hackers get no more information about a computer from an IP address than you would get from reading a social security number. Hackers look for weaknesses and your organization, whether large or small, may be a target solely because of that weakness. Don't place your data at risk by making the assumption that you are too small to be targeted.

Weak or Shared Passwords

This is no revelation but that makes it no less a fact. Simple passwords, sharing passwords with coworkers and failing to change passwords frequently is a risk that you can easily correct. Additionally, IT security experts report frequent instances of passwords being written down and left in plain sight. There were even reports of folders titled "password" being found on the system. Always remember that passwords are intended to be secret!

Phishing and Spear Phishing

Although we are probably familiar with the terms, time and again, data has been compromised when an unwary target opens an email and clicks on a link or attachment opening the door for a hacker to infiltrate the system or infect it with malware. Spear phishing, which targets a person in an organization using information relevant to that individual, is often successful against even the most cautious of recipients. This hazard should be discussed frequently in meetings to ensure it is kept top-of-mind by the entire staff. You cannot rely on email filters to eliminate this risk.

Malware

Backoff, Dyreza, BlackEnergy and Crowti are the names of just a few of the numberless malware programs waiting to infect your computers and systems. This malware can be introduced via phishing or an innocent visit to a website. Many of

these malware programs can be purchased by anyone with the money and intent to

reduced the incidence of security holes, but software applications are often overlooked except by hackers. It is crucial to update software application regularly and reboot systems to ensure that updates take effect. This includes workstations, servers, laptops and routers. In short, all the hardware and software that is used in your day to day operations.

A Word on the "Cloud"

Software as a service (Saas), cloud storage and similar innovations have also heightened the opportunities for hackers to breach your data. Make certain your providers are thoroughly vetted with respect to security.

Concluding Thoughts

While the explosion of software solutions and cloud services has enhanced productivity and profitability, it has also created opportunities for those with malicious and criminal intent. Our profession has a fiduciary responsible that necessarily encompasses the safety and security of client information in our control. An attentive approach to security must be an elemental part of our client relationships.

———————

Andrew Cravenho is the CEO of CBAC, which offers invoice factoring for small businesses. As a serial entrepreneur, Andrew focuses on helping both small and midsize businesses take control of their cash flow.