The Digital Threat

By Mano Mahadeva, CPA, MBA | Column Editor

Read recent news headlines and one is easily reminded how vulnerable even the most cautious of organizations can be to cyberattacks. Even when companies invest in technologies and implement safety policies, cyberattacks can happen and they have lasting impacts on organizational security and the bottom line.

"The attack hobbled hospital customers within the British National Health System turning away ambulances and canceling surgeries." ... "The internet company, being bought by Verizon, says a state-sponsored actor stole email addresses, passwords and birth dates." ... "The data breach was significantly broader than originally reported – the company reported that 70 million customers had information such as name, address, phone numbers and email addresses hacked." ... "Millions of health insurance customers woke up Thursday morning to an email from the company telling them hackers had gained access to its computers and that demographic information might have been stolen" ... "This malicious code is capable of directly controlling electricity substation switches."

Attacks such as these are increasing in numbers even as companies invest in technologies, improve their capabilities and tighten their policies. Why? It's because more companies are stashing their valuables, such as intellectual property, customer data, financial data and other critical assets, online. And we are more open and connected now on the internet in transacting business than we have been compared to years past. These valuables have become a treasure trove for many bad actors – cybercriminals engaging in fraudulent transactions, politically charged hacktivists trying to change political outcomes and even state-sponsored hackers looking to steal critical information.

Not all of these attacks are external in type – internal attacks do occur, where some are intentional and some unintentional. I have been "spear phished" a few times – once I received a very innocent email from our CEO to wire funds to a specific company, not a large amount, where the contents looked legitimate. I called my CEO and asked him about the wire and he was quite surprised. The sender email was perfect, but when I hit "reply," I was looking at a strange looking return address! Another example is that of the Target hack, which was external in that a vendor employee fell for a malicious email where the hacker sent malware-laced emails to take over the victim's computers, and upon gaining control of a laptop via remote access, stole the retailer's payment card data.

Now think about one of your employees looking up a website of a sandwich shop that delivers food. Most likely, this sandwich shop does not have the resources to fortify its web practices and as a result, gets easily infected by malware. Your employee, who is not educated or trained about cyber issues, looks for a lunch option using the office network and gets infected. Or another employee receives an email that looks very legitimate or enticing, but contains malware and opens the email. A frequent problem is that of sharing, or using, another person's password (think Snowden) or keeping one's laptop logged on with the owner nowhere to be seen. These are examples of internal attacks, none of which were malicious, but occurred due to a lack of training and/or non-compliant behavior.

Building a fortified defense to protect a business against such attacks is not cost efficient. Complying with a security framework is nice, but not enough to fend off sophisticated hacks. Having employees merely sign off paperwork annually to say they "read and will comply" is not being compliant! Being in denial by saying that "nothing will happen" is playing the odds. And playing it "safe," is NOT a goal!

So here are some proactive measures to think about:

- comprehensive education for all on cybersecurity;
- frequent training for all employees, with a focus on office tools being used for personal use such as Facebook and Twitter;
- educating the board on the risks – some may not be aware of the dangers;
- using an outside company to complete a formal assessment of cybersecurity efforts;
- conducting periodic audits on IT security;
- assessing the security of outside vendors and customers – ask them for a pertinent date to confirm that their risk culture is similar to yours;
- very careful hiring practices that maintain robust ethics and compliance policies;
- within legal bounds, possibly monitor employee activity in specific cases;
- raising awareness; and
- making EVERYONE accountable for sound, safe and compliant practices.

No cyber system will ever be impenetrable. But one must do what should be done as the costs to remediate can crush a company. The loss of proprietary data, blackmail, regulatory costs, public relations fallout, company reputation, ransom demands, the timing of audit disclosures and associated lawsuits – all of these costs can easily outstrip what was paid in Bitcoins on the WannaCry attack. So spend the time and invest wisely by defining and deploying the right technology along with the appropriate policies and operations, which become a strategic asset of your company. ■

Mano Mahadeva, CPA serves on the Editorial Board for TSCPA. He can be reached at manomahadeva@gmail.com.