First Line of Defense: YOU!
MCAWW Technology Advisory Committee Report: Data Security

By: Ryan O'Rourke, Holaday-Parks
With help from: Doug Moore, McKinstry Co.; Seth LaRiviere, MacDonald-Miller Facility Solutions; Jennifer Nelson, Hermanson Company; Parker Seaman, Ferguson Enterprises; Tyler Wisenburg, Key Mechanical

It seems like not a week goes by without a warning issued about some sort of data breach occurring. Home Depot recently agreed to pay $27.25 million to affected financial institutions for a breach involving a point-of-sale heist in 2014. Just last year, the Equifax data breach exposed the sensitive personal information of 143 million Americans. Currently, technology's footprint is continuing to grow in our modern society, allowing us to be wired in ways previously not imagined. With our constant connectivity, we are more exposed than ever to the threat of having our personal and professional information compromised. When something as simple as clicking a link in an email can wreak havoc on a network, we must all be vigilant.

In this paper, we will look at ways in which we can be exposed and provide some insight as to how you might be able to protect yourself and your company from being compromised. Most of us have vulnerabilities on several fronts. By taking a look at what is happening behind the scenes to keep our information safe, along with what you can do to prevent information thieves from penetrating your company's sensitive information, we hope to provide the knowledge needed to thwart the next attack on your network.

Let's look at a scenario which could lead to threat and could cost your company big bucks. One of the risks companies face is *phishing*. According to Wikipedia, phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. There are several different forms of phishing that can cause financial harm to institutions, but one of the most prevalent is called *whaling*.

Whaling typically involves hackers targeting C-level executives. According to the Digital Guardian, "a whaling attack is a targeted attempt to steal sensitive information from a company …a whaling attack specifically targets senior management that hold power in companies, such as the CEO, CFO, or other executives who have complete access to sensitive data. Called "whaling" because of the size of the targets relative to those of typical phishing attacks, "whales" are carefully chosen because of their authority and access within the company. The goal of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing."

Imagine the CEO of your company is on vacation, and gets what he thinks is an email from the CFO, when in fact hackers have manipulated one slight thing in an email address they've fabricated (using the number zero instead of letter "O", a "ss" at the end of a name, or possible change a domain name from and "m" to a "rn") in order to hopefully ***not*** raise any red flags to the CEO. The CFO would ask for an expedited transfer to pay off an invoice to one of the vendors. Sitting on a beach relaxing, the CEO might just go ahead and do that and not think twice about it.

Hopefully your CEO has been schooled about wire transfers, and deletes/ignores the email, opting instead to do things the old-fashioned way via direct contact with purchasing or by having a formal telephone conversation. Often these hackers may already know about the executive being away, and the timing is not a coincidence.

These attacks are more common than you think. Here is a true story from an MCAWW member. The company CEO was purchasing a residence. He had corresponded by email with the CFO regarding lender credit checks. Later, the hacker, posing as the CEO and using banter that included recently used familiarity, requested that the CFO wire the large down payment from the firm because the CEO's personal bank had not transferred the money yet. The CFO almost completed the transaction but used good protocol and called the CEO to confirm.

The number one way to stop phishing attacks, including whaling, is ***awareness***. Being aware of this type of attack immediately raises the Executive's chances of noticing the fraud. Having company procedures/policies in place, and being aware of what they are, will also prevent attackers from getting away with this type of scheme.

Aside from phishing and whaling, there are plenty of other methods criminals can utilize to cause trouble. These can include viruses, worms, botnets, ransomware and more. Fortunately, there are lots of things you can do to help keep data safe, both in and out of work, including:

- Create strong passwords and change them often. Never save passwords on your device. Yes, it's convenient. Yes, it saves time. If you need to safely store passwords, look into a secure password manager. Criminals are getting smarter and need just one chink in the armor to get into the system and rob you blind.
- Utilize multi-factor authentication. Having two steps to verify or authenticate your identity can help prevent security breaches.
- Watch out for Bluetooth vulnerabilities. Bluetooth technology offers incredible convenience. It also opens doors for security weaknesses. Make sure you turn off your

Bluetooth when you are not using it. While there are options to place your Bluetooth activity in an invisible or undetectable mode, there are some malicious apps that can change that mode and expose your device to threats.

The impacts of data breaches can be vast for both you and the organization you work for. Your employer likely has a tremendous amount of data on you including your social security number, date of birth, address, and even bank information for auto-deposit…and that could be just the tip of the iceberg. Criminals steal this valuable information because it can be quickly and easily sold on the Dark Web. Potentially it could be sold and used for identity theft or you could get more junk mail because of it. An organizational breach could result in your company's competitor getting their hands on proprietary trade secrets. Maybe you have a custom tool or machine that your shop foreman dreamt up, which was fabricated but never patented? Imagine, malicious or not, if that got into the hands of a manufacturer who then produces and sells this machine to contractor's all around the world. Suddenly your hyper-local competitive advantage could become industry standard, and there's no recourse for intellectual royalties.

Having strong IT security is a must, but that can also become a target. Per cloudmask.com: "Data on IT security is a valuable target in itself because it lets the unauthorized parties gain access to all the other types of information on your system." Once hackers know your security strategies and network structure, gaining additional information becomes easier. Your IT security cannot become complacent. Hackers are constantly revising their strategies and security must do the same to keep up.

In conclusion, it is not a matter of if, but when, a data breech occurs. Make sure you are not next - keep vigilant to prevent it from happening at your company. Putting in place strong IT security and having clearly defines policies and procedures are a must. But the real key is to train employees on what to look for, and what your policies are. Your people, and their knowledge, are the key to keeping things safe, or opening the doors and letting the criminals inside.