CAMMACK RETIREMENT

Securing Your Organization's Data

Earle W. Allen, MBA, CEBS
Parnter, Cammack Retirement Group

Data security is a major concern for all organizations. Regardless of the industry in which a business operates, if it is using the Internet and electronically transmitting data to external sources, it is subject to potential data security threats and breaches. In light of this, it is important to be aware of different threats and defenses in order to protect your organization's network and data.

As part of a 2017 cybersecurity sweep initiative, the SEC reported that more than one-half of all cyber-attacks come from employee negligence or intentional malicious efforts from current and former employees[1]. With respect to negligence, the concern is that employees may click on emails without thinking. Whether it be from an unfamiliar source, or from a familiar source (which has been hacked), it is not uncommon for an employee to open an email and then click on an embedded link, thereby releasing the virus or other spyware/malware, which infects both the employee's computer and others on the network. According to a 2017 Verizon report on data breaches, one in fourteen users were tricked into following a link or opening an attachment; and one-quarter of those were duped more than once[2]. These attacks are known as "phishing."

Successful phishing emails are not always quick incidents. Often, the link installs malware to enable the phisher to identify the information it seeks. This may last for a period of months before it becomes obvious that there is a problem. Sometimes phishing is strictly to identify people who are likely to open malicious emails. The phisher records the email address of the person opening the email, and then sells the list of email addresses to a third party, who uses that list for future malicious attacks.

There is also the threat of having your organization's data hacked and held hostage. In 2017, ransomware was the fifth most common malware, up from twenty-first just three years before. With Bitcoin as the currency for ransom payments, hackers have been successful in anonymously implementing and collecting on their cyber attacks.

Financial organizations are common targets for hacking attempts. Criminals seek out an individual's personal financial data and then use that stolen data to make illegal transactions. Because of the value of these records, financial companies spend significant resources building strong defense systems to protect their data. But it is not only financial companies that have come under attack by hackers. Healthcare institutions are also very popular. Hackers seek health records to aid in identity theft. According to some reports, health records are worth more on the black market than financial records.

It is important to recognize that breach attempts are not solely focused on large companies. In its 2017 report, Verizon noted that 61% of breaches were perpetrated against companies with fewer than 1,000 employees[3]. Smaller firms are coveted targets because they can be conduits to

reach larger entities. In attempting to access the network systems of larger organizations, hackers may try to find entry points through smaller entities that do business with these larger companies. Smaller businesses are more likely to have less sophisticated cyber threat protection mechanisms, thereby potentially enabling easier access to larger organizations' data.

DEFENSIVE ACTIONS

How can organizations take action to protect themselves and their networks? Some steps include:

- **Develop a Written Information Security Program (WISP) —** A WISP provides employees with a procedural roadmap to follow in order to maintain security and describes the actions to take when an event, such as a breach, occurs. With respect to the WISP, the descriptions must be accurate. In establishing these policies, an organization is setting an expectation about processes that it will follow. It is important that the internal operations match the written documentation and specific details should be used whenever possible.
- **Conduct Periodic Risk Assessments —** Review systems annually to identify any vulnerabilities. Outside providers completing this assessment may be able to provide more insight, since they will likely look at your organization's situation from a different perspective than an internal IT Department or current IT consultants.
- **Analyze Cyber Security Incidents from the Past —** It is worth re-visiting any previous cyber incidents to recognize the path through which the incident occurred. Could it happen that way again? What changes have been made since then to prevent future similar incidents?
- **Identify the Information Sharing Networks —** Understanding your company's internal network and how information is shared and available to users is a helpful step in identifying vulnerabilities. It is also important to periodically review the users on the network to confirm there is no one who should be removed (e.g., former employees).
- **Conduct Third-Party Vendor Reviews —** Organizations need to conduct due diligence on their own defenses, as well as those of providers that may have access to their network. It is important to understand what data security protocols your vendors follow and to confirm that their systems are sufficiently robust to protect their network, and potentially yours, from cyber threats.
- **Establish Data Encryption Protocols —** All critical and sensitive data should be encrypted to prevent viewing by unauthorized users. This will typically be described in the WISP, so that all employees follow the same encryption processes and understand your company's requirements.

  Mobile devices create another level of security concern. By their nature, laptops and hand-held devices such as phones are portable and out in public, so they are easier targets than computers in an office. In an analysis of data breaches from September 2009 through May 2017, laptops and other portable storage devices accounted for 26% of large breaches[4]. Organizations need to have a set of policies for the handling of sensitive data on mobile devices. If sensitive data, such as name, social security number, credit card numbers, date of birth, date of hire, address, compensation (referred to as personally identifiable information or PII), is necessary to be accessed or stored on mobile devices, it must be encrypted. While this seems self-evident, it is easy

for it not to occur. And if somehow the device gets lost or stolen, now that PII is out in public.

- **Appoint an Information Security Officer Tasked with Keeping Your Data Protected —** Having one individual tasked with the overall responsibility for maintaining data security helps keep that person focused on the important duties and working with internal and external teams to maintain the protection of the network.

CHANGING ACCESS

The nature of access to data has been changing over the past few years. Historically, passwords have been the primary method for access to websites and computer networks. However, because there is heightened awareness of the problems associated with password entry (81% of hacking-related breaches leveraged stolen and/or weak passwords[5]), more sites are now requiring multiple-factor authentication. Typically, this means a person logs into a site, enters his/her password, and then a text message is sent to his/her phone with an authentication code. The person needs to then enter the randomly generated code into the site to satisfy the second authentication method and gain access to the information. This certainly helps with security, since anyone trying to access a site without authorization must have both the authorized person's password and his/her phone.

Biometrics are another growing area for authentication. This may include fingerprint and/or retinal scans. Other systems use facial and voice recognition modules to enhance security. Behavioral authentication is another sophisticated system of access that uses algorithms to assess the tempo and pattern of the keystrokes on the keyboard to authenticate the user. The algorithm assigns risk scores to the person seeking access and grants levels of access based on matching the baseline authentication profile.

Establishing access zones can also help better protect data. Rather than having all of a particular site or network available upon confirmation of access data, some sites open small portions of the total site with each protocol that is successfully authenticated. If somewhere in the process the input does not match the profile, the person's access can be restricted from further entry. These types of systems often analyze the keystroke patterns to complete the authentication.

As more and more of these options become available, the use of passwords for data access will likely decline. Passwords are often very simplistic, and people use the same ones for multiple data sites. This means that if the hacker gains access to one facet of a person's protected information, they are likely to gain access to more, or all, of a person's protected information.

CONCLUSION

Training is critical. Employees must be taught how to identify potential red flags in the emails that they receive. It is also a good practice to test your employees. Some organizations hire outside firms to send their employees phishing emails to see what portion of their population click on those messages. This is a way to confirm the success of the training exercises, as well as to identify individuals who may require more training than others.

Keeping all hardware and software up to date can also aid in protecting your company's network. Manufacturers are regularly improving their products to respond to the latest cyber threats. Patching should be completed quickly. Once a weak spot has been identified and the software provider has reached out with the solution, it should be implemented as soon as possible.

Physical security is also important. Confirming that file cabinets and other sources of sensitive data are appropriately locked and placed in locations with limited access can help guard data.

There are many elements involved in protecting your own employees' and your clients' PII. And it is an ongoing game between the criminal element bent on stealing such information, and the cyber security industry trying to combat the latest theft techniques. Conducting a self-assessment and developing your organization's internal policies are a good starting point. But it is important to recognize that the job of data protection will never be complete; there will always be new items to add to your security to-do list.

References:

[1]*NCS Regulatory Compliance Cybersecurity Summit, 9/21/2017; "SEC Alert Overview and Background" presentation*

[2]*Verizon's 2017 Data Breach Investigation Report*

[3] *Verizon's 2017 Data Breach Investigation Report*

[4] *Retrieved from United States Department of Health Services, Office of Civil Rights, HIPAA Breach Highlights*

[5]*Verizon's 2017 Data Breach Investigation Report*

ABOUT CAMMACK RETIREMENT GROUP

Cammack Retirement Group has been helping retirement plan sponsors meet their goals for half a century. Solely focused on serving retirement plan sponsors, we provide a tailored approach to investment advisory and consulting services. We work with some of the nation's leading academic and research institutions, healthcare providers, corporations, non-profit organizations and public sector employers to help them manage fiduciary risk.

For more information on our services, please contact **Earle Allen,** Partner, at **646.839.8206** or **eallen@cammackretirement.com**.

Note: *This feature is to provide general information only, does not constitute legal advice, and cannot be used or substituted for legal or tax advice.*

Investment products available through Cammack LaRhette Brokerage, Inc. Investment advisory services available through Cammack LaRhette Advisors, LLC. 100 William Street, Suite 215, Wellesley, MA 02481 | p 781-237-2291