Cyber Attack Prevention Strategies

By Brian Johnson

You don't have to look far to find a company that's experienced a cyberattack. The healthcare industry has certainly seen their fair share of attacks throughout 2021. Large hospitals, small clinics, and cloud based electronic medical record (EMR) solutions are included in the growing list of organizations falling victim to cybercriminals. [1] Ransomware attacks against large hospitals, especially ones that cause surgeries to be cancelled and patients to be turned away, certainly make the headline news, but most cyberattacks aren’t juicy enough to reach that status. Many of you reading this article represent an organization that wouldn't make the headline news following a cyberattack, however, you would certainly feel the impact. Consider a ransomware attack that left you unable to care for your patients or a HIPAA related data breach that required you to report to the Department of Health and Human Services. Thankfully, it's not all doom and gloom as there are fundamental security controls that you can implement to help protect your organization. In this article, we will discuss the threats and the proper security controls to mitigate the risk.

It is common for organizations to release an official announcement following a cyberattack

that reads, “advanced adversaries using sophisticated hacking techniques have breached the organization’s network.” Some attacks are sophisticated; however, investigations of security breaches show that many cybercriminals are not using sophisticated attacks to gain entry. Instead, they are taking advantage of easy to exploit vulnerabilities caused by poor security hygiene. [2] Security hygiene is a term used to describe basic and fundamental security practices that must be in place to properly secure your environment. A healthy security hygiene environment will provide protection against many of the techniques used by cybercriminals.

Cybercriminals are very good at obtaining passwords. They do this through various means that include guessing, purchasing, and asking. The act of guessing a password might seem unlikely as most organizations have complex password requirements that require upper case, lower case, and numbers to be included in a password. Those who set these standards expect people to create passwords that look like “St3ps2scre” but in reality, they create passwords like “Summer2021” that pass security requirements. Furthermore, the pattern will continue with subsequent password changes that result in passwords like “Winter2021” and “Spring2022”. Cybercriminals also purchase passwords on the Dark Web, a segment of the Internet where activity is anonymous and cannot be tracked. These passwords come from previous breaches where cybercriminals have obtained usernames and passwords. Lastly, cybercriminals simply ask for your password. It may seem unlikely that you or one of your employees will divulge such information, but cybercriminals are very successful with this technique, which usually involves some form of social engineering. This scheme is often pulled off by sending a phishing email, impersonating a trusted person, company, or brand, containing a link to a very realistic, but fake, login screen. Once the victim’s password is entered on the bogus login screen, the cybercriminals are well on their way to compromising your network.

The solution to the password problem is Multi Factor Authentication (MFA). MFA works by adding a second authentication factor to your existing password. The two most common and easiest methods to implement are a security code sent via text message or a push notification sent to an application on a mobile phone. Individuals will first enter their username and password as they normally do. Next, MFA will kick in and require the second factor. If a security code is used, the individual will be presented with a screen to input the code. If a mobile application is used, the individual will be presented with options to accept or deny the request. MFA works by requiring a second factor that cybercriminals don’t have access to - your phone. Following a password compromise, MFA is your safety net that helps to keep cybercriminals at bay. For an example of how a weak password and lack of MFA contributed to an organization’s ransomware attack, read the past article in this series titled, “Weak Password Allows Major Cyber Extortion.” [3]

Like nearly any other security control, MFA is not hack-proof. [4] It is important to be wary of texts or push notifications that you did not initiate. They are a good sign that someone has your password. If an MFA push notification is accepted in such a scenario, the cybercriminal may be permitted access to the target accountWhile MFA significantly improves your organization’s security, users should be aware of its potential flaws to

further increase MFA's effectiveness, and users should be directed to immediately report signs of a potential hack attempt.

Our next problem focuses on running outdated and unpatched software. Flaws, known as vulnerabilities found in software applications and operating systems, can be exploited by cybercriminals to compromise your systems. Following the discovery of a flaw, software manufacturers will release an update known as a patch. Some manufacturers, such as Microsoft, release patches on a cycle. For instance, Microsoft releases patches on the second Tuesday of every month, a day known as Patch Tuesday. Other vendors like Apple release patches ad-hoc. You should never run unsupported software. Once software becomes unsupported by a manufacturer, they stop releasing updates, which leaves the software vulnerable.

The solution to outdated and unpatched software is to establish a patch management program. The purpose of this program is to inventory your software and create a routine schedule for patching. Software patches can be deployed through automated or manual operations. The option you choose will depend on the software manufacturer and the methods they provide. Not all vendors provide automated methods and for those that do, it is often a feature you must initiate. When automation is not available, assign the responsibility to an individual and create a routine schedule for patching software. Software solutions are available that will scan your network and report all outdated software. These solutions can be configured to automate patch installs even when the manufacturer does not provide automated methods.

We previously discussed how cybercriminals use phishing emails to ask for your password. They use the techniques crafted by con artists combined with an email. Phishing emails typically create a sense of urgency and use your social tendencies against you, causing you to act on something that is a forgery. Phishing is more of a psychological attack delivered via email than a technical attack; however, we can use technology to combat the issue. The best way to determine your risk is to run simulated phishing attacks against your organization. Solutions are readily available that will create and send a phishing email to your employees with the results tracked and provided as a report. Unlike cybercriminals, your phish test is benign and will not cause real harm. The testing system will report on the users who download attachments, click on links, and enter credentials on fake login screens. The purpose of a phish test is to identify risk and provide a safe learning environment for employees. Do not use your phish test to punish employees, especially if you've never trained them. The results of the test should be used to develop a training strategy and a risk mitigation plan. Phishing solutions are easily attainable and affordable regardless of the size of your organization. Most solutions offer a free trial. I recommend KnowBe4's free test for those looking to get started. [5]

Lastly, let's discuss backups. Backups are known as an effective and reliable solution for recovery of failed or damaged computer systems, but historically they have not been thought of as a security control. The rise of ransomware has highlighted a new need for backups. Following a successful ransomware attack, victims are left with the choice of

either paying the ransom or restoring data from backup. Many organizations choose to pay the ransom, but once the data is returned, they find large portions of their data missing. Sophos' 2021 State of Ransomware Report states that on average organizations that pay the ransom only get back 68% of their data. [6] Therefore, even those with a strategy to pay the ransom will need a good backup to retrieve the remaining 32% of their data. As a result, whether you plan to pay the ransom or restore from backup, now is a good time to ensure your backups are working properly. For a detailed look at backups please read our previous article in this series titled, "Back It Up – The Importance of Proper System Backups." [7]

As cyberattacks continue to increase year after year, organizations are looking for ways to secure their environments. Top news outlets are reporting on sophisticated attacks against big name organizations, however, not all cyberattacks are sophisticated. Many attacks take advantage of poor security hygiene environments. Organizations that implement fundamental security controls will put cybercriminals looking for easy victims at bay, causing them to move on to the next victim. In this article, we discussed MFA, Patching, Phishing, and Backups. If you are unable to establish any of these controls, work with an Information Technology provider to address the issue.

If you have questions about cybersecurity or access to the resources available exclusively to SVMIC policyholders, call 800-342-2239 or email ContactSVMIC@svmic.com. Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other available resources to SVMIC policyholders and staff through their Vantage® account. If someone in your organization needs a Vantage account, they can sign up here. If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

[1.] July 2021 Healthcare Data Breach Report (hipaajournal.com)

[2.] Cyberattacks: Just How Sophisticated Have They Become? (forbes.com)

[3.] Weak Password Allows Major Cyber Extortion (svmic.com)

[4.] Microsoft Urges Users to Stop Using Call & SMS-Based Multi-Factor Authentication (zdnet.com)

[5.] Knowbe4 Free Test Offer (Knowbe4.com)

[6.] Sophos State of Ransomware 2021 (Sophos.com)

[7.] Back It Up – The Importance of Proper System Backups (svmic.com)

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.