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)

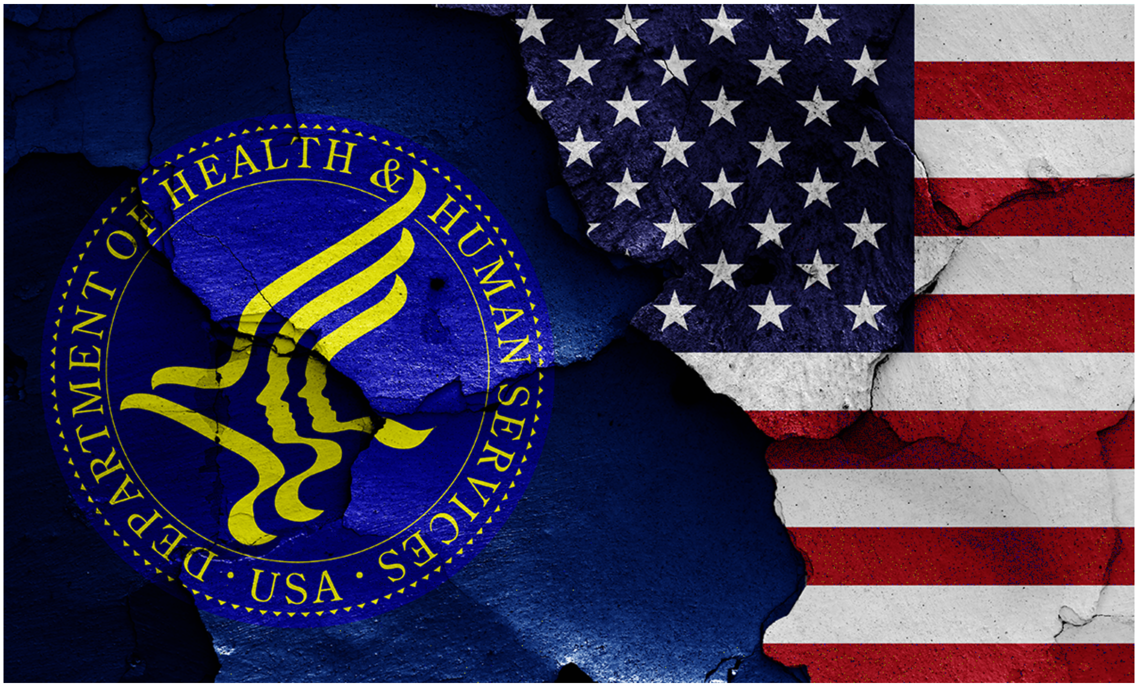
[4.] Microsoft Urges Users to Stop Using Call & SMS-Based Multi-Factor Authentication (zdnet.com)

[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)

Breaking News: PHE Renewal



By Elizabeth Woodcock, MBA, FACMPE, CPC

On October 15, 2021, the Secretary of Health & Human Services renewed the Public Health Emergency (PHE). This move represents the seventh time the PHE was renewed since its declaration on January 27, 2020. The importance for medical practices is that the regulatory relaxations for telemedicine related to the federal government are extended for another 90 days. This includes Medicare reimbursement for certain Medicare services provided via telemedicine or, as applicable, by telephone. For a current list of reimbursed services, see this link. https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes

It is important to note that this federal extension does not apply to individual state board rules and physicians are encouraged to check with each state in which they practice as to the current licensure requirements in effect.

Not All Heroes Wear Capes

By Tim Behan, JD

To be human is to be connected. Since March of 2020 that concept has been stretched and strained to the point of breaking. These “trying times” we have been living though are trying the times of our healthcare providers and administrators in their relationships with patients. The stress and fear people are carrying internally are manifesting in unprecedented behaviors. Pre-COVID-19, from time to time, I assisted our providers and administrators with patient issues. But since COVID-19, I have dealt with an explosion of problems regarding negative patient behaviors and encounters. What has been consistent throughout the calls, is the grace and patience exhibited by all I have spoken with who are dealing with this mushrooming issue. As was very recently said to me by a provider, “We just want to do the right thing.” Not all heroes wear capes. From what I have seen over the past 19 months, many of them wear white coats, scrubs, and the business attire of medical practice executives.

A short time ago I was discussing this with a group administrator, and she said something that struck me. She stated that pre-pandemic, people had a sense of control over themselves and that this sense is now completely gone so they are trying other ways to get a feeling of control back. This is showing up with great frequency in health care offices and facilities and has contributed to an onslaught of calls about how to deal with patients when they act in ways contradictory to their best interests. One of the only human connections, outside of immediate family, that patients have had throughout the pandemic is with their health care providers. The stress, fear, and loss of control are spilling onto the ones who are trying to help them the most. While this presented a challenging situation for those I spoke with, the situations were consistently dealt with in a compassionate and professional manner.

While many of the situations I have been presented with are not new, the intensity and the frequency are different. There has been a definite rise in patients demanding their money back, seeking narcotics, wanting to record visits on their phones, making inappropriate comments, openly cursing in waiting rooms, making threats, and rushing to the internet to post negative reviews of providers to their friends and strangers alike. There is a growing trend of patients trying to dictate who is allowed to treat them in a provider's office and what medications should be prescribed. There has also been a rise in patient non-adherence with care. What is startling, however, is that many of these patients have treatable conditions that, left untreated, will turn out poorly for them. Another category of negative behaviors that is becoming more common is boundary violations, such as a parent attempting to use the mental health records of his/her children against the other parent in divorce and custody proceedings. Another boundary issue that arose recently involved family members of deceased patients asking physicians to change death certificates to state that a loved one died from COVID-19 when the patient did not.   As mentioned at the beginning of this article, the pandemic brought a slew of patient problems we have never faced before. But with all these situations, the providers and administrators handled the matters with skill and precision before talking to me. We then worked together to best address how to protect the interests of the practice while balancing that with the needs of the patient.

Being that this is a closed claim piece, and we know our readers appreciate a story, the following are a few accounts of the more interesting patient encounter inquiries I have dealt with recently.

> Back in January, I received a call from an Arkansas family practice physician regarding an elderly male patient who had called with obvious COVID-19 symptoms. However, the patient refused to appear for treatment or go to the hospital. Through persistence, several calls between us, and a touch of good luck, the provider was finally able to convince the patient to go to the ED where he was admitted and eventually recovered.
>
> Earlier this summer, a female patient of a Tennessee pain management physician became fixated on getting the provider's nurse fired. The reasons given made no sense and were not treatment related. The provider, of course, made sure that the nurse was not involved any further in the care of the patient, but the patient continued to demand that the provider terminate the nurse and went as far as to ask

> for her personnel file. Despite being warned to stop this behavior or risk being terminated from the practice, the patient continued to her detriment.
>
> Lastly, and perhaps the strangest, an incident happened in Kentucky late last year. The patient was a licensed health care provider himself who had been referred to our doctor by his PCP for specialty care. The patient's wife was the administrator of his practice and was very involved in his personal affairs. She fired her husband's PCP and began acting as though our specialist was now her husband's primary doctor. The more our doctor (a specialist, not a PCP) resisted her attempts to make him her husband's PCP, the more aggressive she became about it. We were able to finally end her campaign, but it took time, kindness, and patience.

The overriding theme throughout all these encounters with patients and their families has been the remarkable compassion, restraint, and fortitude shown by the providers and administrators, despite their own professional and personal worries due to the pandemic. But all embraced a concept summed up in my favorite saying based on a quote by J.M. Barrie: "Be kinder than necessary, for everyone you meet is fighting some sort of battle." This is why my current heroes wear more than just capes.

Your Digital Front Door

By Elizabeth Woodcock, MBA, FACMPE, CPC

Open the (Digital) Door

It will be many years before we determine the long-lasting impacts of the pandemic on medical practices, but there is one effect that is already crystal clear – patients' expectations for a digital front door to their physicians. The migration to a digital interface for your patients need not be frightening, as it can be accomplished without significant investment. There are third party vendors that can handle the function for you, for a price. Alternatively, you can set up a basic interface to allow your patients to *request* an appointment online, but then manually process it on the back end by keying it into your scheduling system. To your patients, this looks like a digital front door, but it can easily be merged into your current workflow. Of course, there are advanced options as well, with many vendors ready to serve the market. To get a sense of the options, reach out to your EHR vendor to seek their advice – or do a quick Web search using key words like "patient self-scheduling."

As technology evolves, it's important to recognize that you're not going to hear patients asking for this function – it's an expectation. When you log onto Amazon to order a product or when you do an online search for a restaurant your friend told you about, and you can't find what you're looking for, you don't report your frustration – you just move on to the next option. That's exactly what's happening in health care right now; by making a small investment in some digital entry points for your patients, you can make sure they have the access they expect. Plus, you'll enjoy some direct benefits – opening a digital front door results in fewer incoming phone calls and more patient arrivals (as self-scheduling is associated with a reduction in no-shows).

Virtual Care Assistant

If you determine that virtual care will be a permanent component of your medical practice, it's essential to have the resources to execute the workflow effectively. This includes a staff member(s) who can support the effort. Preparing for virtual visits, conducting patient outreach, providing support during care transitions, interpreting test data from mobile health devices, and other related tasks expands the work scope of traditional staffing models. Although some practices have attempted to assign current staff the additional responsibilities of remote care, others have created a staffing model that is separate and distinct from the traditional face-to-face visit, with one person (or team) dedicated to remote care and another to in-person care. (See the sample Task Distribution guide below.) The virtual care assistant may be a permanent position – or may be rotated between medical assistants. The latter is a terrific way to boost staff morale as the role can be performed from home.

Regardless of how the responsibilities are structured, the key is to ensure that there is a proactive approach to understanding what tasks are involved with virtual care – and who's going to do them. Otherwise, the virtual care tasks get swept aside as the in-person care is prioritized. This leads to challenges that may have implications for patient quality and safety. Take the opportunity now to define and design a virtual care assistant.

Risk Matters: Remind Your Patients to Get Their Flu Vaccine

By Jeffrey A. Woods, JD

With the emphasis on COVID-19 vaccines and boosters, many patients may forget another respiratory virus that presents a significant health risk – influenza. It is important you educate your patients on the need to be protected from this potentially fatal virus, especially your patients who are 65 or older.

The dangers of the flu are increased this season because of the COVID-19 pandemic and especially the Delta variant. First, there is the risk of simultaneous infections or even back-to-back infections of COVID-19 and the flu. Second, many healthcare systems have been overwhelmed because of COVID-19 and there may not be capacity for patients who need hospitalization because of contracting influenza.

There are many reasons your patients may not be willing to get their flu shots this year. A significant amount of misinformation and fear is circulating about vaccines and their efficacy. There is also confusion among patients about whether they need a flu shot if they have been vaccinated for COVID-19. Others believe that because they are wearing a mask in public, washing their hands, and socially distancing, they are fully protected from the flu; while these measures help to reduce the risk, they do not provide the protection of a vaccine. Additionally, "vaccine fatigue" seems to be a real concern. Finally, some patients are reluctant to go to their doctor's office to get a flu shot because they are afraid of contracting COVID-19 while at the office. You can alleviate these concerns by reaching out to your patients and addressing any questions they may have regarding the flu vaccine, informing them of the steps your practice has taken to protect patients from COVID-19, and encouraging them to get vaccinated.

The CDC recommends that anyone age 6 months or older should receive the flu shot unless they have contraindications.

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.