Cybersecurity 2.0

The Latest on Cyber-Attacks, Ransomware and The Need for Risk Assessments…

Same Message, Different Result?

By: Dorothy Cociu, RHU, REBC, GBA, RPA

It's been about a year since we were all on pins and needles about cyber-attacks and the news that Colonial Pipeline, JBS Foods and many others had been breached and their data held for ransom, which resulted in gas shortages and price hikes in the East and meat and food shortages everywhere, followed by the 4th of July weekend, 2021 cyber-attack against the software company Kaseya, which targeted many small companies in up to 17 countries, including the US, United Kingdom, South Africa, Canada, Argentina, Mexico, Kenya and Germany. Cybersecurity experts believe the REvil gang, which is a major Russian-speaking ransomware syndicate, was behind the attack, targeting the software company by using its network-management package as a means to spread the ransomware broadly through cloud-service providers. Luckily, the software company was able to shut it down quickly, but not before significant damage was done.

When I wrote my last article on this topic, "Cyber Attacks Hit Home…. The Next National Emergency? Valuable Cybersecurity Tools to Keep You Safe," published in **The Statement, July/August, 2021** page 5, at: https://camsdev.net/CAHU/Magazine/July-August-2021/index.html and **California Broker, August, 2021** https://www.calbrokermag.com/in-this-issue/cyber-attacks-hit-home-the-next-national-emergency/, I detailed how these attacks happened and gave some advice on how to keep your organization safe, as did many others, yet since then, we are still seeing the same issues popping up in the news on a far-too-regular basis… Breaches, hacks, cyber-attacks, ransomware…*Why does this keep happening?* Because for many people, unless and until it happens to them, they put off doing what they know they need to do… *because it can't happen to them, right?* **WRONG!** *It can, and it's not a matter of "if" – it's usually a matter of "when" it happens to you. Your company… Your data… in the hands of someone that shouldn't have access to it… And then it's too late. Your business is literally shut down. Your systems are basically dead. You're scrambling to either restore from backups, pay the ransom, notify the authorities and the victims, and in all cases, you're retracing your work, putting in hundreds of man hours (or thousands), or paying millions of dollars in crypto or other currencies, all to get your hands on what is already yours – your data!*

How many times do you have to read about this stuff… hear about it on the news… listen to people who had it happen to them, before you actually do something to prevent it from happening to you? What's the number? Ten? Thirty? One Hundred? More?

Let's do a little review first on what has happened since early 2021…. Just in summary:

- Colonial Pipeline - $4.4 million paid (but 64 bitcoin (approximately $2.3 million, was recovered by the US Government from a virtual wallet – the only known recovery to date of significance) – resulted in severe gas shortages, long lines and extremely high prices all over the East Coast.

- JBS Foods, reportedly paid $11 million from the Memorial Weekend, 2021 attack, which caused sever meat shortages in an already pinched supply chain during the pandemic.

- Kaseya Software hack occurred affecting customers in approximately 17 countries.

- Microsoft Exchange Server Breach in early 2021, giving attackers full access to user emails and passwords on affected servers, administrator privileges on the server, and access to connected devices on the same network. As of March, 2021, it was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom, as well as the European Banking Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market (CMF).

Healthcare and insurance providers have of course been a huge target for cyber-attacks. We've heard of Anthem to Primera Blue Cross, Mass General, Cottage Health, UMass, Scripts and more, all falling victims to cyber criminals. It's commonly felt that healthcare and medical information is susceptible to cyber-attacks because of the amount of highly sensitive data that they possess. Of course, the medical and insurance industries are subject to privacy and security laws such as HIPAA Security and HITECH, so there is a standard for protecting information. But as I said in my last article on this, there is no single federal law regulating cybersecurity or information security. We have a hodgepodge of state laws and minor federal laws, but no single protection source, as they do in the European Union and other nations.

Lately, it seems, mobile banking is among the latest victims, including Bank of America and Wells Fargo customers being scammed from outsiders using the mobile banking app Zelle to steal money from their accounts; and worse yet, the customers themselves allowed it to happen, because they thought they were talking to their banks, and instead of stopping it, they basically allowed the Zelle hackers to take money directly from their accounts.

Another very scary security scenario, in my opinion, is everyone's use of QR Codes. They've become all the rage to use… but they are also susceptible to hacking, which I will discuss further later in this article.

And let's not forget Mobile Ticketing and the requirement of season ticket holders and individual game purchasers to download their team's league app, without thinking twice about it and not questioning the permissions they are granting, which can be a security nightmare.

So, for anyone reading this, it's not over. That storm I talked about last summer and fall in my article referenced above has not passed. If we thought we were in the eye of that storm then, I hate to be the bearer of bad news, but it's more than a season of continuing storms with no clear skies ahead as far as the trend for more cyber-attacks and ransomware, *because most of us are allowing the bad guys to keep doing it!*

As long as we still have that Weakest Link I discussed in the previous article - Human Beings- we will always have risks, and we need to learn how to manage those risks, now and in the long-run. Until we do, we will continue to hear news reports on breaches and ransomware, and companies will continue to be at risk.

I will provide you with some more detail on these recent breaches, hacks, scams and current risks you should be aware of below.

Microsoft Breach by Lapsus$ Hacker Group, March 2022

Just this past March, Microsoft announced it was breached by Lapsus$ Hacker Group… News reports said that a screenshot was taken indicating that Bing, Cortana and other projects had been compromised in this breach.

As I often do, I looked to my HIPAA Security/HITECH and IT Services and Security partners, Aditi Group, to offer some insight from an IT or technical perspective as to what happened, if there is anything Microsoft users need to be worried about, or things they need to do to protect themselves. I was able to gain some additional insight to share with you in my conversations with Ted Flittner and Ted Mayeshiba, principals of Aditi Group.

"This group has also just successfully attacked T-Mobile and a growing list of big-name companies," stated Ted Flittner. "What happened with Microsoft is that hackers allegedly stole portions of source code for the search service Bing, and the navigation for Bing Maps and Cortana (Microsoft's answer to Siri). Microsoft's public statement is that obtaining portions of source code *does not* put the general public at risk."

Flittner continued: "In truth, knowing the code can increase risk by allowing hackers to scrutinize it and find weaknesses that Microsoft hasn't found or fixed. Since these services (Bing, Maps, Cortana) don't require user login info, there probably is not a risk."

Block (Formerly Square) Breach, April, 2022

More recently, Block (formerly Square) acknowledged that its Cash App had been breached by a former employee in December, 2021. It's reported that over 8 million customers were affected. The breach included customer names, brokerage account numbers, portfolio information and stock trading activity. They are claiming that no other personally identifiable information or account credentials were leaked in the incident. What is the danger of this sort of breach? Again, I went to my tech experts.

"This a straightforward case of a former employee still able to log into Cash App's system and download user reports," stated Flittner. "These are the same reports the employee was authorized to view while still working there. Even if no personally identifiable info was accessed, the data that was downloaded is PRIVATE info that people only want to share with their tax accountant or investment advisor. That sort of info helps criminals pick which people to target in phishing scams. Think Frank Abagnale Jr, the real-life person played by Leonardo De Caprio in "Catch me if you can." Frank just needed some info about people to pretend to be them…and scam money."

T-Mobile Breach

I also discussed the recent T-Mobile attack by Lapsus$, since it was the same hacker group as the Microsoft hack, with Ted Flittner, and asked him to let us know what happened and how it happened.

"The T-Mobile attack by Lapsus$ did not breach customer data directly. T-Mobile has had its share of that, including a breach of 47 million customers' personal data in 2021. This Lapsus$ attack involved BUYING T-Mobile employee VPN (virtual private network) login info. These were purchased on the dark web with the goal of escalating and accessing T-Mobile's account management system and ultimately allowing hackers to "SIM swap." That's when you tell the phone company that the phone number is now tied to a different SIM card. This lets someone hijack your cell phone. And if your cell phone is used for account verification – text messages for example, the hacker now can bypass multifactor authentication."

Flittner continued: "Though hackers didn't get far enough this time, it highlights the problem of phone numbers being hacked. And why we recommend using multifactor authentication with a hardware key – like Yubico."

Are Banking Apps Safe?

The world of banking has evolved to the now “must have” banking apps on your mobile devices. Banks need to draw new customers, and many of them are young and tech-savy. They’ve literally grown up on the technology some of us are still trying to adapt to in our everyday lives.

Zelle is used by many banks in the USA today for easy transferring and sending money. These banks include Bank of America, Capitol One, Wells Fargo, US Bank, JP Morgan Chase and PNC bank. Of course, Apple also offers their Apple Bank mobile app, and there are many more. But are they safe?

I briefly described earlier the recent scams using Zelle that cost customers of Bank of America and Wells Fargo hundreds to thousands of dollars as scammers spoofed the banks’ phone numbers and the customers were sent text messages, followed by a phone call, which informed them of an attempt to transfer funds. As a “preventive measure” the scammers gave instructions to the customers which instead sent their funds off to the scammers. The banks are not actually obligated to replace the money in their accounts if their customers authorized the money to be transferred, which in these instances happened.

So how do we keep our money safe if we’re using banking apps on our mobile devices? To assist me with this question, I once again went to Aditi Group, to give you more information from the tech side.

“These banking scams are really using age old tactics: pretending to be someone they’re not,” stated Ted Flittner. “The callers use false Caller ID for the phone call and text messages to innocent bank customers. They SAY they’re from Wells Fargo or BoA or another of the most common banks. Some people have been fooled into divulging their account credentials ‘to avoid attempted fraud.’ And in the process they ALLOW the fraud.”

Flittner continued: “This is not a failure by the application. This is a failure to understand how a fraud investigation really works. The financial institution doesn’t ask for your login credentials. But when you call them, they ask you to verify who you are – name, birthdate, address, last 4 numbers of your of social security number. We all need to be sure WHO we’re talking to on the other end of the line. Is it the BANK or a SCAMMER? We recommend always calling them back. Check the number they give you and see if it matches the phone number on the back or your credit card or the bank. It not, call the phone number you KNOW for your bank and ask about it.” That is something that we’ve encouraged people to do for several years.

“Banking Apps are as safe as using web browser normally,” continued Flittner. “Potential security problems include logging into apps when others can see you, or working on public wifi, where hackers may have obtained access to your phone or computer. Other problems are the general ones that apply whether it’s a mobile app or web browser on a computer, like using weak passwords or leaving your password around for others to find. And with phones, leaving them unattended without a strong password to keep others from doing bad things while you’re not looking.”

The Risks of Using QR Codes

QR Codes are all the rage… If you don’t have one and you’re trying to advertise something, you feel like if you don’t have one, you’ll be left behind and lose out to your competitors… And now it’s not just advertising… QR codes can be found everywhere now… The problem is, they too can be compromised. Thieves and bad actors have begun placing their own QR codes over the originals and sending your phones to unsafe sites where again, bad things can happen. Keep in mind, a QR code uses the phone’s camera… therefore it needs access to your camera, and will often ask for (and people automatically give) permission to view all of your files and photos on your device. *Wait, what? All of your photos and all of your files?* Are your company files in dropbox, which you can access from your phone? Are your emails from your customers, or their private information such as their names, phone numbers, account numbers, maybe credit card number in those files on your phone? If so, do you want every entity that you scan a QR code for to have all of that information? If not, you might want to think twice about using QR codes without scrutinizing them.

Again, I went back to my tech experts to provide some more detail from the technology side.

"Look before you leap," stated Flittner. "Does the QR code look legit or is it like sticker graffiti on a traffic light pole? If it looks like someone pasted a sticker on the original, stop." It sounds simple, but many people just don't stop to take that second look, and that is a real problem.

"If you do scan the code, look at the website address (URL) that it shows before agreeing to load the page. Only use the QR code read apps or camera apps that let you choose to visit the website or not, instead of having it load automatically," continued Flittner. "Once it loads, look at the website to be more certain it's real before you enter any personal data, credit card or sensitive info."

Mobile Ticketing Apps

Whether you're a concert-goer or a sports fan, or anything in-between, it's likely your event is now using Mobile Ticketing only. The problem with mobile ticketing apps is that they can be unsafe because people don't always look at the permissions they are granting to the app when using, and automatically clicking yes to accept the terms without looking further or questioning the app's intentions.

My company has season tickets for the Anaheim Ducks (NHL) and the LA Rams (NFL), and both have mobile ticketing… But me being me, and being worried about the dangers of mobile apps, always asks the team if I can get paper tickets. Yes, it's old-fashioned, but much safter. Sometimes if you ask there is no charge to getting paper tickets. Sometimes you have to pay a paper ticket fee, but to me, it's worth it. Why? What's so scary about these apps?

I've seen these apps asking *for permission to access your files, your photos, and get this, your* ***network access*** in these apps. So, before you start clicking ok for all of these permissions you're granting them, you need to slow down and figure out how to see all of the permission requests and how to say no to what they do not need and what you do not want to give them access to. If you're not sure, contact an IT or security expert.

Another option is to have a second phone; one for business and one for things like mobile ticketing apps. For the latter, don't store anything on the second phone. Use it only for those concerts or sporting events. (But yes, that can be expensive to have 2 phones – see if a very limited plan can be used for the latter).

Crypto Currency

Crypto currency is the latest rage… Everyone wants it, even buildings now display their names, but no one is regulating it. In January, 2022, it was reported that $30 Million was stolen in the Crypto.com breach. ($18 million in bitcoin and $15 million in Ethereum, as well as other cryptocurrencies). I asked Aditi Group if they could tell us more about crypto currency and the dangers of using it, and if people are buying it and trading with it, is there anything that can be done to protect them?

"There are probably THOUSANDS of crypto currency offerings now," stated Flittner. "It takes very little to create one and make it public. And without regulation and with investor frenzy over potential profits to be made, it's easy to get caught up in emotion and skip due diligence. *Simply from an investment perspective, crypto investing is gambling. It can pay off for you or wipe your savings.*

"From a security perspective, it requires smart and strong password management. The main path of breach is someone getting your login and password to your crypto wallet. Guard those passwords. Make them as strong as possible," warned Flittner.

"Crypto.com, which is a crypto trading platform, was breached by hackers and discovered this January. Hackers were able to bypass the 2-factor authentication for user accounts and 483 accounts were accessed and $30 M in bitcoin and etherium (crypto coin) was stolen. Cryto.com reimbursed the user accounts and stopped other attempted transfers. They have since announced stronger 'multi-factor' authentication coming this year," stated Flittner.

"Part of the risk with crypto is once it's stolen, you may have no recourse," continued Flittner. "Crypto.com is rolling out a new Worldwide Account Protection Program that can insure your account up to $250,000 – if you meet certain conditions." So if you're thinking of investing in crypto currency, be sure you do your homework and put in the necessary security protocols before you invest.

How Do We Protect Ourselves and Our Companies?

So how do we protect ourselves from these common threats? As a privacy & security consultant and trainer, my first instruction is always to DO A RISK ASSESSMENT. You need to figure out where your risks are before you can mitigate those risks. You need to know where you are before you can move forward with a security plan.

"This is all about being aware of danger before it strikes," stated Flittner. "And preparing to reduce risk and recover faster if it does."

The Need for Risk Assessments – An Ongoing Security Tool

Every article I write about this topic and every training I do includes my preaching to you all about the need to do Risk Assessments. This means you must look at every device, every tool, every router, your network, and everything else to determine where the risks are, and figure out how to mitigate those risks.

According to Ted Flittner, "In basic terms, this is a comprehensive review of you or your business to consider what risks you may face (stolen computer, ransomware attack, even physical break-in), what inherent vulnerabilities you have (staff bringing their own computers, work at home, out of date software), the likelihood of each type of problem actually happening, and the impact if they do. Then we decide which items are really critical to address, less serious, and on down. Sometimes we conclude that chances are LOW that a problem happens, but the IMPACT would be catastrophic, so we take steps to avoid or easily recover (think Life Insurance)."

Flittner continued: "The result should be ACTION to address the dangers. HIPAA and HITECH require it for businesses that fall under HIPAA. And it's often mentioned by the federal investigators as missing or lacking in HIPAA violations."

Identifying technical vulnerabilities to include in their risk analysis, according to OCR in their March 17, 2022 Newsletter, "OCR Cybersecurity Newsletter: Defending Against Common Cyber Attacks," (which I'll mention again below and include the link to view it), include the following:

- subscribing to Cybersecurity and Infrastructure Security Agency (CISA) alerts (https://us-cert.cisa.gov/ncas/alerts) and bulletins; (https://us-cert.cisa.gov/ncas/bulletins)
- subscribing to alerts from the HHS Health Sector Cybersecurity Coordination Center (HC3); (https://www.hhs.gov/about/agencies/asa/ocio/hc3/contact/index.html)
- participating in an information sharing and analysis center (ISAC) or information sharing and analysis organization (ISAO);
- implementing a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches; and
- periodically conducting penetration tests to identify weaknesses that could be exploited by an attacker.

Regulated entities, according to OCR, should not rely on only one of the above techniques, but rather should consider a combination of approaches to properly identify technical vulnerabilities within their enterprise. Once identified, assessed, and prioritized, appropriate measures need to be implemented to mitigate these vulnerabilities (*e.g.,* apply patches, harden systems, retire equipment).

How often should a Risk Assessment be done? According to Ted Flittner: "We recommend a yearly review or when major changes happen with the business."

Who should be involved in a Risk Assessment? Is it just IT? "Risks involve the whole team," stated Flittner. "Key supporters of Risk Assessments should include executives, especially financial leadership. But really, everyone should be involved in some way."

What are some of the areas in an organization that need to be looked at in a risk assessment? Again, I went to Aditi Group for their comments. "Everywhere that sensitive info moves throughout your business," replied Flittner. "This could just be one department like Human Resources, or it could affect everyone."

What sort of questions, tasks, need to be included in a Risk Assessment? Ted Mayeshiba of Aditi Group responded as follows: "Physical inventory - what devices hold sensitive data (PHI in HIPAA terminology). Important questions include: 'Where does the data reside? What's in 'the cloud' with 3rd party companies? Who should access the sensitive info? And how do you control access? Is there a BA agreement in place? Does the 3rd party company have access to the data?' All of these should be considered and discussed within your organization."

We always recommend that a Risk Assessment be done by an independent third party. Why? "Three main reasons: first it's not the main job of employees, so it rarely gets priority; second, outside eyes tend to notice problems that people who see the process every day can miss (can't see the forest through the trees in front of them); and third, employees sometimes are reticent to admit to weaknesses in the process," stated Flittner.

I asked Ted Flittner what message he would share with every business owner, large or small, related to Risk Assessments and their importance in protecting their data? Ted replied: "Know before it's too late. Be Prepared. As a former Boy Scout, I learned to live by the motto long ago. Security is always evolving and where you didn't think you have risk in the past may be totally different today. And the cost of problems like data breaches and ransomware are much higher than the cost of prevention."

Weak Cybersecurity Practices

It is well known that a regulated entity that has weak cybersecurity practices makes itself an attractive soft target for hackers and cyber criminals. Weak authentication requirements are frequent targets of successful cyber-attacks (over 80% of breaches due to hacking involved compromised or brute-forced credentials, according to OCR). (Verizon. *2020 Data Breach Investigations Report*. (2020, p. 19). Retrieved from https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf).
Weak password rules and single factor authentication are among the practices that can contribute to successful attacks. Once inside an organization, if the entity has weak access controls, this can further contribute to an attacker's ability to compromise systems by accessing privileged accounts, moving to multiple computer systems, deploying malicious software, and exfiltrating sensitive data.

HIPAA rules state that regulated entities are required to verify that persons or entities seeking access to ePHI are who they claim to be by implementing authentication processes. (*See* 45 CFR 164.312(d): Standard: Person or Entity Authentication) A regulated entity's risk analysis should guide its implementation of appropriate authentication solutions to reduce the risk of unauthorized access to ePHI. For example, authenticating users that access a regulated entity's systems remotely (*e.g.*, working from home) may present a higher level of risk to a regulated entity's ePHI than users logging into their desktop computer at work. To appropriately reduce the higher level of risk of remote access, a regulated entity may consider implementing stronger authentication solutions, such as multi-factor authentication.

According to OCR's March 17th newsletter, implementing access controls that restrict access to ePHI to only those requiring such access is also a requirement of the HIPAA Security Rule. (*See* 45 CFR 164.312(a)(1): Standard: Access Control.) Here, too, the risk analysis should guide the implementation of appropriate access controls. For example, a regulated entity may determine that because its privileged accounts (*e.g.,* administrator, root) have access that supersedes other access controls (*e.g.,* role- or user-based access) – and thus can access ePHI, the privileged accounts present a higher risk of unauthorized access to ePHI than non-privileged accounts. Not only could privileged accounts supersede access restrictions, they could also delete ePHI or even alter or delete hardware or software configurations, rendering devices inoperable. To reduce the risk of unauthorized access to privileged accounts, the regulated entity could decide that a privileged access management (PAM) system is reasonable and appropriate to implement. A PAM system is a solution to secure, manage, control, and audit access to and use of privileged accounts and/or functions for an organization's infrastructure. A PAM solution gives organizations control and insight into how its privileged accounts are used within its environment and thus can help detect and prevent the misuse of privileged accounts.

Regulated entities should periodically examine the strength and effectiveness of their cybersecurity practices and increase or add security controls to reduce risk as appropriate. Regulated entities are required to periodically review and modify implemented security measures to ensure such measures continue to protect ePHI. (*See* 45 CFR 164.306(e): Maintenance.) Further, regulated entities are required to conduct periodic technical and non-technical evaluations of implemented security safeguards in response to environmental or operational changes affecting the security of ePHI to ensure continued protection of ePHI and compliance with the Security Rule. (See 45 CFR 164.308(a)(8): Standard: Evaluation.) Examples of environmental or operational changes could include: the implementation of new technology, identification of new threats to ePHI, and organizational changes such as a merger or acquisition. But even if you're not a HIPAA Covered Entity, these practices should apply to any organization due to the many other state and federal privacy and security rules, and as a matter or overall good business practice to keep your organization's data safe.

New Federal Guidance on Defending Against Common Cyber-Attacks

In the past few months, both the IRS and HHS's Office of Civil Rights have issued guidance and newsletters for HIPAA Covered Entities on keeping you safe against common cyber threats. I'll try to highlight some of the most important tips. I would suggest you read the HHS Office for Civil Rights In Action March 17, 2022 Newsletter, "OCR Cybersecurity Newsletter: Defending Against Common Cyber Attacks," which I mentioned above. It can be found at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html. In addition, the IRS published several releases in February, 2022, to protect tax payers from scams and fraudulent activity (https://www.irs.gov/newsroom/irs-warning-scammers-work-year-round-stay-vigilant), , as well as announcing a transition away from the use of third-party verification involving facial recognition (https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition). I will attempt to summarize some of the more important items discussed in these publications and provide additional commentary. I also want to point out that since we don't have a single national entity regulating all forms of electronic and cybersecurity, even if you're not a covered entity under HIPAA rules, the HIPAA Security and HITECH rules are very effective in protecting your organization from all types of electronic and cybersecurity threats. Simply, it's all we have, for the most part, so use those rules to your advantage.

Phishing, Spear Phishing and Whaling

As discussed in my last article, one of the most common attack vectors is Phishing. This is a type of cyber-attack that is used to trick individuals into divulging sensitive information via electronic communications, such as by email, or by impersonating a trustworthy source. According to HHS, a recent report noted that 42% of ransomware attacks in Q2 of 2021 involved phishing.

If you're subject to HIPAA Security and HITECH (meaning you are a HIPAA Covered Entity, such as a sponsor of a health plan, an insurance company or a provider of health care services) your workforce members should understand that they have an important role in protecting the ePHI of their organization from cyber-attacks, according to OCR. Part of that role involves being able to detect and take appropriate actions if someone in your organization encounters a suspicious email. The problem is, if they are not trained to detect suspicious emails, they will go unnoticed, and bad things generally tend to happen as a result. These regulated entities should train their workforce (there is that word again… train…) to recognize phishing attacks and implement a protocol on what to do when such attack or suspected attack occurs. Do you have such protocols in place in your organization? Do your employees know who they are supposed to report suspicious emails to in your organization? Is anyone assigned to be that person or department?

Ted Mayeshiba of Aditi Group had these words to share. "In the latest Office of Civil Rights Newsletter, the government has tipped their hand as to the raising of the threshold of 'reasonable efforts' for evaluating companies `'best efforts' defending against common cyber-attacks. There is a new and repeated reference to 'penetration attacks' as a best practice which should be adopted by companies."

Ted Mayeshiba continued: "Penetration testing is usually a third party outside attack on your company's network by 'friendly' forces that test weaknesses in your network. This is really nothing new, this is done by Fortune 500 firms. It is the first time that we've witnessed this idea put forth in a regular OCR Cybersecurity Newsletter. Of particular interest was the reference to tie cybersecurity training programs with a follow up with friendly 'phishing', 'spear phishing' and 'whaling' attacks to test the effectiveness of the training. As attacks become more frequent and target even 'small' firms, it is becoming increasingly urgent to tighten cybersecurity for all firms."

According to Mayeshiba, "'phishing' is a type of social engineering attack commonly used to steal user data including login credentials or other financial data. It commonly occurs when an attacker, masquerading as a trusted entity, dupes a victim into revealing sensitive information by opening an email, link or text message. 'spear phishing' is similar to phishing, but the attack includes specific information unique to the individual being attacked, thereby increasing the likelihood of the victim opening the email, link or text message."

Another term not mentioned in the OCR Newsletter is 'whaling'. Mayeshiba defines this as "similar to phishing, but the attack is specific to executives (C-suite) or to others where the bad actor masquerades as the executive to coerce a trusted employee to divulge sensitive information."

According to the HIPAA Security Rule, regulated entities are required to implement awareness and training programs to all its workforce members, and such programs should be an ongoing and evolving process, so that it changes as new threats develop. Your management personnel should also be participating in training… I've seen far too often that they want their employees to be trained, but the executives fail to go through it themselves, and then when they are targeted, which they often are, because they have access to a generally a higher amount of ePHI in phishing email attacks, they don't follow protocols, and they often are the reason for such schemes resulting in bad things happening.

The key to an effective security training program is repetition and periodic security reminders. In fact The Security Rule includes an addressable provision for such reminders. Are you doing this within your organization?

OCR suggests in their newsletter that covered entities should, for example, send simulated phishing emails to your workforce members to gauge the effectiveness of their security awareness and training program and offer additional, targeted training where necessary. An educated workforce can be an effective first line of defense and an integral part of a regulated entity's strategy to defend, mitigate, and prevent cyber-attacks.

In my opinion, the worst type of training you can provide is a canned, "check-the-box" training consisting of a few simple presentation slides. It's best to think of interesting, innovative ways to engage your workforce to understand the risks and prevent cyber-attacks.

OCR suggests that regulated entities can mitigate the risk of phishing attacks by implementing anti-phishing technologies. This could mean examining and verifying that received emails do not originate from known malicious sites. If an email is suspected of being a threat, it can be blocked and appropriate personnel can be notified to step in and deal with the threat head-on. Other approaches, according to OCR, can involve scanning web links or attachments included in the emails for potential threats and removing them if a threat is detected. Newer techniques can leverage machine learning or behavioral analysis to detect potential threats and block them as appropriate.

The key is developing and implementing "policies and procedures to protect ePHI from improper alteration or destruction." It's important to note that the Security Rule requires regulated entities to assess and reduce risks and vulnerabilities to the availability of ePHI, as well as confidentiality and integrity.

Anti-phishing technologies can impede or deny the introduction of malware that may attempt to improperly alter, destroy, or block authorized access to ePHI (for example, ransomware), and thus can be a helpful tool to preserve the integrity and availability of ePHI, according to OCR.

It is always advisable to combine an educated, engaged workforce with technical solutions in order to achieve the best opportunity to reduce or prevent phishing attacks.

Exploiting Known Vulnerabilities

I think most of you know and understand that hackers can penetrate an entity's network and gain access to ePHI or other sensitive data by exploiting known vulnerabilities, where it is publicly known to exist. The National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD), which provides information about known vulnerabilities. Exploitable vulnerabilities can exist in many parts of your information technology infrastructure, such as on your server, your desktop, mobile device operating systems, applications, databases, your web software, your router, your firewalls, and other device firmware. Often known vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version. If a patch or upgrade isn't available from the vendor, they may suggest actions you can take to mitigate a newly discovered vulnerability. These could include modifications of configuration files or disabling affected services.

It's important to remember that older applications or devices may no longer be supported with patches for new vulnerabilities, so you will need to take appropriate action if a newly discovered vulnerability affects older applications or devices. If an obsolete and unsupported system cannot be upgraded or replaced, then additional safeguards must be implemented or existing safeguards enhanced to mitigate the known vulnerabilities until an upgrade or replacement can occur. This may involve increasing access restrictions, removing or restricting the old device from network access, or disabling unnecessary features or services.

The bottom line is, you need to do a risk analysis to determine these potential risks and vulnerabilities. Not once, but often and on an ongoing basis.

Read, Sink In, Repeat – The Need for Continued Training

Although I discussed this in detail in my first article, I do want to touch on it again… It's imperative that employers take the time to train their employees on the electronic risks that are out there, because if you don't, it only takes one wrong click on an emailed link to download malware, worms or other things that can bring your systems to a screeching halt. As Ted Flittner stated in that article, "Know company policies and why it matters to follow them. The key topic these days is email diligence. Don't click on email links or download files that you don't really know. Slow down and take time to scrutinize. Teach people how to recognize fakes and legitimate messages," he stated. "And train people on how to react if malware, ransom, or phishing attempts succeed. Who should they call and what should they do next? That seems to be one of the glaring missing pieces in most employers' privacy policies."

Bottom line, train now and train often. You can never train enough. Things change, and so should your training. Keep up to date and keep up with the latest threats.

Same Message, Different Result?

Although to some extent I am sharing with you the same message as my prior article from 2021, I'm hoping for, someday soon, a different result. We don't need to keep repeating the same mistakes and putting off for tomorrow something that should have been done yesterday. The only way to have a different result, a better result, with less hacks, less cyber-attacks, is to do what you know you need to do. *Do a risk assessment*. See where you are and where you want to be and develop policies and procedures to help you meet your goals. And don't forget to train your employees regularly and often, keeping up to date with the latest threats. I'd like to think that perhaps someday soon I won't have to keep writing these articles every year…. So let's work on a different result, please!

Authors Note: I'd like to thank Ted Flittner and Ted Mayeshiba of Aditi Group for their assistance with this article. I can be reached at Advanced Benefit Consulting, dmcociu@advancedbenefitconsulting.com, or by phone at 714 693-9754 x 3. Ted Flittner and Ted Mayeshiba can be reached at AditiGroup.com, or by email at ted.flittner@aditigroup.com or ted.mayeshiba@aditigroup.com. Advanced Benefit Consulting & Aditi Group offer privacy & security training, consultation and implementation system assistance, as well as Risk Assessment services on an ongoing basis.

Dorothy Cociu is the President of Advanced Benefit Consulting, Anaheim, CA, and the current Vice President, Communications, of the California Agents & Health Insurance Professionals (CAHIP) 2021-2022.

References & Sources:

HHS Office of Civil Rights March 17, 2022 Newsletter, "OCR Cybersecurity Newsletter: Defending Against Common Cyber Attacks."

IRS publications February, 2022: (https://www.irs.gov/newsroom/irs-warning-scammers-work-year-round-stay-vigilant) and (https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition).

Plus sources referenced above in the article.