Olivia Peterson (00:00:01):

Welcome to those who are just joining. We are going to go ahead and get started. I'm sure we'll have a few more folks join the call on as we go. Welcome everyone to this month's edition of NACHC's Telehealth Office Hour. We're very pleased to have you for today's webinar. On behalf of the National Association of Community Health Centers, my name is Olivia Peterson and I am a training and event program specialist supporting the training and technical assistance division here at NACHC, and I will be your technical host today.

Olivia Peterson (00:00:32):

I am pleased to bring you this session along with my colleague, Philip Stringfield, who is the manager of health center operations training also in the TTA division, and Philip will be getting a started in just a moment. But before we get started, I have just a few quick housekeeping items to review. First and foremost, please note this event is being recorded. We will share the recording with you all within the next week or two. We will be sending that out via email. So, keep an eye out.

Olivia Peterson (00:00:58):

Then if you're looking for the slides, we will also be sending the slides out by email directly after this event. Keep an eye out, that'll come from trainings@nachc.org. Then if you have any technical issues today, feel free to send us a chat. I'll be keeping an eye on that and you can always send us an email as well. You will be directed to a survey after the webinar. We really encourage you to fill that out as it informs our future events. Thank you in advance for your feedback.

Olivia Peterson (00:01:29):

If you have questions or comments today, we definitely encourage you to share those. You can ask a question verbally, if you would like, you'll just have to raise your hand so that we can call on you. You will notice that all lines were automatically muted when you joined today's call. Then we also have both the Q&A and the chat available to you. Please feel free to introduce yourself in the chat. We're always curious to hear where folks are joining from, but feel free to share your questions, comments there. If you do have questions, please plug that into the Q&A tab, which you'll see on the bottom right hand side of your screen. We'll being an eye on the Q&A and have some time set aside for Q&A towards the end of the presentation. Definitely make sure you're sharing your questions and your feedback throughout the event.

Olivia Peterson (00:02:15):

With that, I am going to go ahead and turn things over to Philip to get us started for today. Thank you so much.

Philip Stringfield (00:02:22):

Thanks so much, Olivia, and good afternoon and good morning everyone. Before we get started, I want to go ahead and do our usual plug in for the NACHC EHR user groups, NACHC hosted EHR user groups that bring together PCAs, ACCNs and health centers to discuss related issues, developments, and upgrades within their respective EHR systems.

Philip Stringfield (00:02:45):

Each group is led by a committee consisting of PCA, ACCN and health center leaders, and we're always looking for others to join in. If you're interested or if you would like to get more information, you can email me and I'll also be sure to drop in a link in the chat box as well that I'll direct you to where you can locate the user groups and sign up for them, if you're interested, go ahead over to the next slide.

Philip Stringfield (00:03:11):

We're going to go ahead and dive in with the rest of the time, we'll be talking cybersecurity best practices. As you may know, there has been a rise in cyber related crimes in the past year and a half, that has caused a lot of concerns for many organizations. We're joined today by Taylor Wells with Northwest Technologies Group who will be reviewing some of the top cybersecurity best practices for small organizations.

Philip Stringfield (00:03:37):

This is aimed at giving you practical ideas on how you can best protect your organizations and your patient's data. Before we hand over to Taylor, I just wanted to go ahead and put in one last plug, that as we go through these best practices and you have questions and concerns that come up, I want to remind you to check and see if your organization is a member of a health center control network or HCCN, because if so, these networks may have some type of security, resources and services available to assist you as well. With that, I'm going to go ahead and hand things over to Taylor to get us started. Thank you.

Taylor Wells (00:04:16):

Thanks, Philip. Thanks, Olivia, and everyone at NACHC and everyone here... Pull up my presentation. Thanks everyone for having us. Really excited to dive into today's topic really all around cybersecurity best practices and how can your organization ensure you're really doing what we like to say everything within reason to make sure you don't have a security breach, number one, and then number two, make sure that if you do, you're able to mitigate the least amount of cost and ultimately able to move your organization forward in a positive direction.

Taylor Wells (00:04:55):

Brief introductions around myself and the organization NWTechs, we help small, medium sized organizations tackle IT problems, cybersecurity being number one of them. My name is Taylor Wells, I'm the director of marketing and I've been with the organization for about five years. We do a bunch of additional trainings for small organizations around technology, everything from Microsoft 365 to password management, hopefully ones that we can come back to NACHC and do additional trainings on for everyone. But we also have some prerecorded ones at our website, nwtechs.com/webinars.

Taylor Wells (00:05:29):

Before we jump into the specific 15 best practices, I wanted to share this quote with you by the former director of the FBI, Robert Mueller in 2012. Granted, this is almost a decade ago and he says, "I'm convinced there are only two types of companies, those that have been hacked and those that will be, and even they are converging to one category, companies that have been hacked and will be hacked again."

Taylor Wells (00:05:54):

For most organizations, and we'll go into a few statistics here, frame the problem and look at some of the trends that we've seen in the past couple of years, and also something that even obviously the FBI have been seeing for a while now, have been the fact that it's not just, will you get hacked? It's when and at what time in the future will it happen?

Taylor Wells (00:06:21):

That's something you've probably heard, but it's becoming more of a reality. It may not be that the cyber criminal is successful. Hopefully, they're not, hopefully you have your defenses up. But chances are, especially if you're in a healthcare organization, you have had some sort of cyber security attempted breach or successful breach.

Taylor Wells (00:06:40):

We've seen everything from large hospital systems to small practitioners being breached and there really is no specific industry that's not being targeted, and we'll even look here in a second at statistics of smaller organizations. If you have a couple hundred employees or maybe just a couple of locations, you're not even a large system, then even those companies are being targeted because ultimately, especially healthcare organizations, store so much sensitive data.

Taylor Wells (00:07:11):

I think, especially, healthcare organizations want to talk about also defining what is the problem, and that's really PII. PII is personal identifiable information. If you're in IT, then you've heard this term thrown around a lot, and it really defines any information that's either a full name, social security number, credit card information, driver's license, bank account information, passwords, email accounts, email addresses. It encompasses a lot. It's a pretty big spectrum.

Taylor Wells (00:07:43):

Ultimately, it really encompasses almost every organization has PII, and then obviously healthcare providers have multiple of those, if not more than that. When you look at your risk factors in your organization, PII is the number one. There's a whole lot of other forms of cyber security risk to your organization. But the number one is losing, ultimately your patient data, your client data, any sensitive PII that you store internally, that's really related to your organization, like your employee data.

Taylor Wells (00:08:23):

Really, PII is the number one. There's a bunch of other things we'll talk about in this presentation you can avoid. Things related to phishing scams, that maybe not so much losing data, but wire transfer fraud or gift card scams. There's all sorts of things that are not necessarily PII, that are important, that we'll talk about. But when you think about your risk factors, PII is number one. You should be looking at wherever the data lies, that's what you should be focused the most resources on, on protecting, in addition to everything else as well.

Taylor Wells (00:08:57):

I wanted to frame that as we go into that. A couple of trends we're looking at here. In the past year, Microsoft has occurred or seen 10 years of innovation in a lot of their tools and especially cloud hosted applications.

Taylor Wells (00:09:14):

A lot of enterprise companies, small businesses, all the way to enterprise organizations, government organizations are moving to the cloud. The pandemic has spurred this, just globalization, innovation, the cost of cloud solutions has perpetuated this. There's a lot of things that the whole world of technology has changed. I'm sure for healthcare providers, everything from telehealth, to using more cloud tools, to things being virtual, to having remote teams. A lot of our healthcare providers, the ones we've supported, maybe 50% of their workforce is now remote. A lot of their admin staff, a lot of their, maybe not so much patient facing employees, but a lot of their admin staff or their executive teams are now remote. A lot of people can work remotely, even doctors and/or practitioners.

Taylor Wells (00:10:06):

A lot of innovation which changed the game, right? There's different cyber risks now than there were five or 10 years ago. A couple of other trends here as well is, out of one in... For small businesses, this is small businesses, not even enterprise businesses, but one in every 323 emails is a malicious email. Small organizations, small businesses are getting targeted. Average cost of a breach is 3.86 million as of 2020. 43% of cyber attacks target small organizations.

Taylor Wells (00:10:43):

Obviously, big organizations are no brainer. Bringing down a Twitter, bringing down a Microsoft, bringing down a large organization is a no brainer, and there's a lot of that going on, or at least a lot of attempts. But 50% of it is actually targeting small businesses as well, almost 50%. 98% of social attacks rely on social engineering. If you take anything out of this presentation and this information that we're sharing today, social engineering. If you can protect and enhance your social engineering trainings, protocols, systems, testing, we'll talk a little bit about that today as well. If you can do that, that has huge impacts to your overall cybersecurity.

Taylor Wells (00:11:29):

A couple of stories, I just mentioned Twitter. Twitter got breached 2019 by a 17 year old and a 15 year old, essentially kids from Florida and the UK. What they did is they went around and called hundreds of Twitter employees pretending to be IT, to get them to give up sensitive information, which then led to them breaching politicians, government officials, billionaires accounts, which could have wreaked havoc. Thankfully, all they did was a Bitcoin scam, which was not a big deal. But ultimately it's a 17 year old kid and a 15 year old kid out of Florida in the UK were able to breach a huge company due to just a socially engineered scam. It didn't take a whole lot of technology.

Taylor Wells (00:12:20):

We're seeing phone scams on the rise. They've always been around, but more of it happening. Text messaging scams are on the rise, email scams, you've seen those. Those three areas, especially, are obviously the most common areas of socially engineered attacks. If you can increase your training in those areas, huge. Number six is damage related cyber crime is projected to hit 10 trillion by 2025. Crazy big number. Phishing increased in 2020 to account for one in 4,200 emails.

Taylor Wells (00:12:50):

In every 4,200 emails sent in the entire world, one is a Phish email. That's crazy, that's also something that we're seeing a ton of, and something you can do things about. You can actually put in systems to

greatly reduce that. Nothing's 100%, but you as your organization, we'll talk a lot about culture, we'll talk a lot about putting different systems and tools and ultimately risk controls, and things like that to ensure you have the best practices.

Taylor Wells (00:13:20):

But a lot of it is culture. A lot of it is creating a culture of awareness and training and people being transparent when things happen. I can't tell you how many times I get emails that are, somebody's accounts been compromised or a phishing scam, or somebody is being spoofed. Call those people. We'll talk a little bit about that later, as well, as far as specific things you can do.

Taylor Wells (00:13:42):

Let's jump right into the first one here, and this is actually what we've been talking about already, which is the first best practice you can do in your organization is provide, and ultimately, the question is, does your organization provide regular cyber security training and testing for all your team members? Ultimately when it comes to, 98% of breaches had some sort of social engineering element to it. Then if you can put in cybersecurity training and testing, you can at least bring that number down, if not bring it down substantially.

Taylor Wells (00:14:14):

What we do for our clients, we do internally, we have regular testing that just makes people aware. I can't tell you how many different types of scams out there that people should be aware of. Everything from gift card scams to wire transfer scams, to phishing scams, to... There's just all sorts of things, phone scams, texting scams, all these things out there that we all need to be aware of, especially if you're in an industry that's either healthcare or in some sort of highly regulated industry, not only do you have an obligation to your patients, to your employees, but also to the government to make sure you have this sort of training in place. But it's also just best practice. We talked about having a culture of people being aware of the risk and understanding that it's so pervasive, and especially with amount.

Taylor Wells (00:15:04):

Just think about how much device prelification has occurred in the past couple of years. Just look at your own device usage, how many more devices do you have now than you had five years ago? How many more devices do you have now than you had 10 years ago? We have all these more risk factors, all these more points of opportunity for cyber criminals. Being trained on all those areas is super important, and then testing, regular testing of you and your staff, you and your higher organization, so you know which individuals may need extra coaching, extra training, extra awareness around potential risk. That can also provide some great feedback, if you're in a leadership position, that you're making these technology decisions, and you're ultimately trying to make sure your organization has the best security in place.

Taylor Wells (00:15:53):

Number two is, do you have MFA enabled on all accounts? This is something that we still see a struggle for organizations of all size, where there's still sensitive information at online accounts. MFA, multifactor authentication, it's that annoying text messaging code you get from your bank or any online account. It's become much more pervasive and popular over the past couple of years. You probably have it enabled, if you are a medium sized company or enterprise, organization, then you probably already have it enabled. If you don't, this should be a high priority, because the studies show that you can increase login security for an account by upwards of 60% that have an MFA enabled.

Taylor Wells (00:16:35):

It's a study Google showed that all their email accounts, all their accounts that are MFA enabled, 60% increase in overall security. That can bring just people ultimately getting inside your accounts. Since everything is cloud based, this is now more important than ever. Tools like a password manager, single sign on can help manage MFA, which we'll talk a little bit more about later, especially password managers, but MFA, super important to have across your board.

Taylor Wells (00:17:02):

Passwords are actually less important. What is actually more important is actually... Excuse me, password management or change in your password, a lot of organizations... Five years ago, you probably changed your password every 90 days, or at least that was a standard. That's becoming less important as organizations have more complex passwords, which is great, have a super complex password then have MFA on top of that, and you'll be in a great spot for your online accounts.

Taylor Wells (00:17:30):

Do that as much as possible, do that for as many online accounts as possible, even if they don't... Do it for your Netflix account, do it for your Facebook account. Everything, especially highly complex, socially engineered attacks ultimately, they use multiple elements. They might use your Facebook account, ultimately get into your business email account. There's very complex systems.

Taylor Wells (00:17:57):

Making sure your, what we call digital hygiene, your overall hygiene for all of your online accounts and for all of your technology in general, if you can have MFA enabled, it's a great positive direction to make sure that's there. Number three here is, do you have data encryption on all computers, servers, work stations, anywhere that has a hard drive and ultimately stores data.

Taylor Wells (00:18:23):

This isn't so much of a problem for larger organizations, because usually they buy in large quantities of servers and/or work stations and laptops and all of that fun stuff. But if you're a smaller organization, you may have purchased equipment that doesn't have business class, business grade encryption built in. If the laptop were to get stolen, people working from home, people are traveling with their works stations now more than ever. Whether it's working from home, whether it's a hybrid environment, where they're working some in the office. Especially doctors or practitioners have that, where they're needing to work from multiple locations, or they just have sensitive information on their laptop or their work station. Ensure you have data encryption built in. If it's not built in, you can also add it on top. That's also something you can do as well.

Taylor Wells (00:19:17):

Number four is, do all of your employees in your organization use a corporate password manager? This is where password managers is super important. Password manager is probably one of the coolest cyber security related tools that you can have in your tool chest now more than ever. A password... Actually, my wife and I were laughing the other day, because... I was probably laughing more than her because I'm more nerdy about tools than she is. But we said that my favorite tools or our favorite tools was a password manager, one password and our budgeting tool, because both of those tools are so helpful for us, just keeping on track of everything, keeping things organized.

Taylor Wells (00:19:58):

We all have hundreds of different logins, whether it's personal or professionally. Having a vault, a secure safe for all of that data is super important. As an organization, but then also personally, I think password manager saves me personally 15 minutes a day, at least, because I'm not having to reset passwords, I can store really complex passwords, I can have MFA built into it, I can store credit card information. If I need to purchase something, I don't need to go look for my wallet, I can have all that information there.

Taylor Wells (00:20:32):

It's a super secure vault that ultimately allows you to be able to share sensitive information within your organization, so you have different vaults for different parts of the organization, but then you personally. Super important. One password is phenomenal, probably our favorite tool that we've seen organizationally and for our clients, and I've used it personally. There's a couple of other ones out there, but I think one password takes the cake, as far as being the best.

Taylor Wells (00:21:01):

Number five is, does your organization have a written information security policy that all employees have to adhere to? Written information security policy is one of, at least 15 policies that your organization probably should have on file. That's really the blueprint. It's the architecture for how you manage your IT. If you are the IT department, IT managers, CIO, you probably have most of these, if not all of these in place already. If you're a smaller organization, all the times we found that they struggle to have those in place and we've been able to help organizations get those in place.

Taylor Wells (00:21:37):

But ultimately, it does a couple of things. First, it is a document that's really... It's the blueprint for how you manage your IT, like I mentioned. But it's also something that you talk about culture that is something you can make aware to your staff, to your employees, to your organization, that here's the things that we find important when it comes to data security.

Taylor Wells (00:21:59):

It should be in layman's terms, that way ultimately people can understand it, but then also it can be a blueprint for your employees and then your vendors, and then also regulatory organizations. Vendors, regulatory organizations, or organizations that want to work with you. Chances are you know what I'm talking about, if you've ever had to fill out a security questionnaire, a security audit, they're going to ask for one of these. Really, all 15 of these best practices are things that under HIPAA, under most government agencies or regulatory frameworks are going to require these things or highly recommend them.

Taylor Wells (00:22:41):

This one in particular is across the board, required, and we see across the board. Number six here is, are all your company emails and cloud storage regularly backed up? Chances are, you've had probably on-premise infrastructure with servers. If you've moved to the cloud, all your data's in the cloud now, that's great. But are you backing it up? Do you have your own backup of it? If you're Microsoft, Google, AWS, on Tuesday... Was it Tuesday? Monday or Tuesday, they went down and they had multiple outages, if you saw that. Having a backup in the rare situation that, that happens, most of the cloud providers are

pretty stable overall, but rare situations, you need a backup to get it up back up and running, that's super helpful.

Taylor Wells (00:23:32):

But then also, if you were to accidentally delete something, user error. If you delete a file or an email, all the cloud providers guarantee, they're not going to lose your information on their end. They double and triple redundancy in place. But on your end, if your employee or team member, or you accidentally delete a file or an email, they don't guarantee that. After a certain period of time it's gone. That's why cloud backups are the new standard for backups, especially if all your information lives in the cloud, which is great. If you're downloading stuff at workstations, that's problematic and you may want to back that up as well.

Taylor Wells (00:24:10):

If you still have servers in place for certain applications or programs, you still want to back those up. But if things are in the cloud, make sure you back up the cloud as well. Number seven here is, is your organization running simulated phishing campaigns to raise awareness? We talked about training at the very first point, right? Training and testing for you and your staff around cybersecurity. Trends and best practices and have that awareness in place. But do you have simulated phishing?

Taylor Wells (00:24:37):

There's programs out there you can get, we do it internally and provide it for our clients where you can actually get fake phishing emails, it seems like a double negative. But basically, emails that appear to be a legitimate email, but it's actually a phishing email, getting you to think before you click, and also thinking before, what are they asking you for? What's the next step? What type of information are they ultimately getting, if you click on that link?

Taylor Wells (00:25:12):

Obviously, if you click on the link, nothing may happen, but you may actually download something, and that could be ransomware or malware. That's a big problem. Or it could be leading you to a website that could then ask you to enter information that then could then lead to a compromise of your organization. Phishing, like I mentioned is probably one of the... I just read a study earlier today by government officials saying that 90% of the breaches they're seeing had some sort of phishing element to it, which is a crazy high number. Even if it was 50%, that would be a worthy enough number to focus on.

Taylor Wells (00:25:52):

Having training in place, just so you think before you click, analyze who the sender is, analyze what they're asking for, analyze potential spelling errors, or just things that seem not appropriate for that provider. Then ultimately this simulated phishing campaign awareness then you can mark it as ultimately a fake phishing, and it'll tell you if it was fake or not.

Taylor Wells (00:26:20):

Microsoft 365 and other providers are getting the ability to report phishing emails, which is super cool too, you can report those. Then, let the rest of your team know if you get a phishing email. This helps so much though. Then it also gamifies this whole cybersecurity. The training as a whole, the testing and/or cybersecurity training as a whole, gamifies this whole process. But the simulated phishing really gamifies

it because then if you do click on it, the rest of your team can then see that your score goes down. It really provides a way to. once again, create a culture of people being aware of the problem, but then also being proactive with identifying the problem.

Taylor Wells (00:27:03):

Number eight here is, are all your workstations of service containing important information regularly backed up? This is on top of our point earlier around cloud backups. This is something you should still do, if you still have data on those workstations or servers, you still want to back those up. Number nine is, do all your computers in your organization have antivirus installed? This is a no brainer, but still we come across organizations, big and small that don't have a standardized antivirus, that's up to date, regularly updated. I emphasize that because that's a problem. You may have a version of something, but it hasn't been up to date in a couple years. So, it's pretty much not good at all. Make sure it's installed across all of your work stations. Then also make sure it's up to date.

Taylor Wells (00:27:51):

Number 10 is, does your organization carry cybersecurity? Cybersecurity is also something that's becoming much more common over the past couple of years. One way to look at how much security you should have in place... It differs. You should reach out. I'm not an insurance agent, reach out to your insurance agent, whether it's usually general liability and comprehensive and liability insurance covers this. You should ultimately reach out to them and get the quote for your specific organization, because every organization's different.

Taylor Wells (00:28:26):

I will tell you though, all these things, in this presentation, if you can do all these things, most likely, you'll get a better premium and a better rate. Because every year, most cybersecurity insurance providers and insurance policies require some sort of audit, where they have you fill out a questionnaire, identifying the things you have in place to make sure you don't have a security incident or a security breach.

Taylor Wells (00:28:51):

If you can do all these things and then some, you'll be in a much better position to be able to lower your premiums and save money there, and then also get a great policy as well. But one thing to note, as far as a general rule of thumb, you should have about $150 per contact, a PII really, in your organization. Generally speaking, that's for every client folder you have, you should have $150. If you have 1,000 clients, you should have $150,000, and if you have... Depending on your organization, it may be less or more, because you might have multiple clients in a folder and multiple data points.

Taylor Wells (00:29:34):

Reach out to your insurance provider, reach out to your insurance broker, to find out the right number you should have in place. That being said, I guarantee you, if you tell them you're doing all these things, tell them that you're vigilant to have the best practices in place, and you're having training and policies and procedures and things are encrypted, things are backed up. You have the right IT resources delegated to this, then you'll get a better premium and you'll get a better rate. But something you should have in place because it's going to happen.

Taylor Wells (00:30:05):

It's not that you're going to get breach, but you're going to get an attack. If you can reduce the chances of attack, awesome. That will keep your premiums low for insurance. That will keep your headache, that will keep your reputation, all the negatives of a breach, you'll avoid that. But then, you'll also ultimately save a lot of money on cybersecurity insurance and things like that by avoiding that and mitigating as much as possible.

Taylor Wells (00:30:34):

Number 11 here is, do you have any annual security risk assessment process in place? Another thing HIPAA requires, another thing that is best practice is that annual audit, a self-audit of your cybersecurity best practices. This is something we help our clients with and something that every organization should do, especially those that are under HIPAA or hold a lot of sensitive information.

Taylor Wells (00:30:55):

This does two things, it's a self audit. Every year, you self-audit yourself to realize the potential risk factors before they lead to potential breach or incident. Then it's also an outward facing document that if you were to get audited by HIPAA, or if you were to have a client or vendor ask you to fill a questionnaire, the cybersecurity insurance being one of them, this will be something we'll ask if you have in place.

Taylor Wells (00:31:21):

Number 12 is, do you have a system to track security incidences? This is a great portal, a portal that you should have in place where you're tracking training, tracking security incidences. Having a culture of transparency around data security, super important, like we've talked about earlier. Having a portal where you can track these things from an IT standpoint and know that hey, if employees or people in your organization, if they experience something, if they accidentally give up information, they accidentally click on that link, no one's perfect. You need to make it aware to your team, to your entire organization that we track these things. Because, little side note story here, a lot of times, cyber criminals, they'll attack one employee and try to get them to reveal information, and then if that employee doesn't work, they'll go to another employee.

Taylor Wells (00:32:21):

One side note is you should never tell the cyber crime that, "Hey, I'm not going to fall for your cyber crime." In fact, don't even respond to them. You should let the person know, if they're being spoofed or if they're account's been compromised, let them know, call them, let them know verbally that that's occurred. Then also let their IT team know. Let them know, that way they can let the rest of the team know that, hey, this is something you should look out for.

Taylor Wells (00:32:51):

Having a way to track those things is super important because it's not always just one employee. They don't try one employee and that person doesn't let them in, they move on. No, they try multiple employees. Think about the story I said earlier about the Twitter incident. They tried hundreds of employees before they got somebody. If one of those employees had made it aware to the entire organization that hey, some suspicious activity was going on. Do you think they maybe could have prevented that? Maybe. Who knows. It could have definitely put them in at spot, though.

Taylor Wells (00:33:20):

Number 13 here is, are you sharing files securely? If you have a good ERM, or if you're using your practice management tools, a lot of them have file sharing built in, where there's a portal where your patients are logging in or third parties are logging in to get information. That is best practice. You should never email things or send things via text or anything like that. It should have some sort of secure portal where your patients, your employees, really, even internally, you should never send files internally or sensitive information over email. It should all be through some secure portal or secure channels. Because email ultimately is not secure.

Taylor Wells (00:34:07):

One more note on that is, you can send a secure email if it was encrypted, and there is tools you can add on to Microsoft 365 or Gmail to make things encrypted, but you can't guarantee the person on the other end is not going to turn around and send you an email. Once again, it's all about culture, it's creating awareness around, hey, we shouldn't send sensitive information via email. It should be through some secure portal.

Taylor Wells (00:34:34):

14 here is, have you reviewed your specific industry data regulatory requirements? If your healthcare provider, HIPAA is one of them. Is probably the biggest one you should look at, and that will be pretty comprehensive. I'll leave you at that one. Something we help our healthcare providers get through is HIPAA... Or if you work with organizations that are HIPAA regulated, that's going to cover most of them. If you work with other government organizations or if you have clients or vendors, they may have other requirements, your cybersecurity insurance may have specific requirements as well. Those are all things to consider. But there are specific regulatory requirements you have to go through. Have you reviewed all those to make sure that you're in compliance?

Taylor Wells (00:35:18):

Number 15, are you alerted when suspicious activity occurs in your organization? Your IT department, internal or external should be vigilant to have systems in place to be alerted. I'll give you a story. A couple of months ago, one of our engineers reached out to me and said, "Hey, Taylor, I noticed somebody in Eastern Europe is trying to get access to your account. Do you know why that is?" I said, "No, I don't know why that is." He was able to put additional security measures in place onto my Microsoft 365 environment. That way, that cyber criminal wasn't able to get in.

Taylor Wells (00:35:53):

There's things you can do if you have the right kind of oversight views and things in place. Before we jump into the Q&A, because I know we got some questions, please submit questions. I'd love to answer any of these questions around these 15 areas. There's other areas too, but these are the main 15 ones. These ones ultimately trickle down into different areas, because once you go down into past policies, like I mentioned, there's 15 different policies. When you do an annual risk assessment, that's going to bring up different issues. When you analyze backups, that's going to bring up different issues.

Taylor Wells (00:36:28):

They all have different spheres. This is a great roadmap and assessment that you can take your organization through. Take these 15 things with your IT department, your third party or internal, or if you want to talk, you can feel free to reach out to us as well, we can definitely help you walk through. Before we jump into Q&A, I do have a couple of bonus ideas or things you can do that are recent things

that we've been exposed to and things that we're integrating or recommending or we've heard about been super successful.

Taylor Wells (00:37:00):

Number one is verbal confirmation. A lot of, for example, bank wire transfer fraud, when somebody does something like that, or purchasing, or... Those are probably the two main ones. Do a verbal confirmation. Call up the person to get verbal confirmation. This is a defacto two factor authentication because it really acts as that second layer of confirmation.

Taylor Wells (00:37:30):

I think a lot of times, because the technology inefficiencies, we want to do things remotely. I'm the first person that would avoid picking up the phone if I can to just send an email. But if it is something important, if it is something that potentially has some financial implications or may lead to access of data. Somebody's trying to get admin access, someone's trying to get global admin access. Someone's just trying to get... You're ultimately giving either keys to the kingdom, some sort of keys to your organization's data or there's some sort of financial implications, should both be a red flag whenever you get an email request and should have some sort of verbal confirmation on top of it.

Taylor Wells (00:38:11):

Another thing you should do is have unique signature. Especially for internal communication, a lot of scams and things happen internally. We've noticed people, one little side note is, you can do a unique signature. Some organizations, they always sign their initials, the person always signs their initials, or they always sign their full name or their full name and their initials.

Taylor Wells (00:38:38):

There's things that you can do to make it ultimately be more, ultimately, one more step that the cyber criminal has to go through to try to mimic you and/or replicate a function that's in your organization. Another thing here is, let people know when they are compromised. I can't tell you because I talk to a lot of people and people email me. So, I get on people's lists. I get probably daily, or at least a couple of times a week, I get people that their accounts have been compromised, and they're emailing me to get me to download something or click on a link.

Taylor Wells (00:39:22):

I called those people. I've called dozens of people over the past couple of years and let them know. "Hey, I think your account's been compromised. I don't know why you'd send me this invoice, or I don't know why you'd send me this link." Let them know. Whether it's internal or external, let them know, give them a call. Don't send an email. I've sent emails before and gotten an automated response, that was the cyber criminal that set up an automated response, or was monitoring the email account and ensured that I got a response that was from the cyber criminal.

Taylor Wells (00:39:59):

Crazy levels of complexity that cyber criminals are doing. Having that extra layer or just having a culture, once again. Your community, let your grandparents know, let your parents know, let your kids know that they should be careful. Because I almost fell for a mortgage scam, a couple of months ago, just on a personal note where it was somebody that was calling from my mortgage company. It said the mortgage

company on the caller ID and had a very sophisticated process that thankfully I identified, or actually I called the mortgage company back and they had no record of it.

Taylor Wells (00:40:44):

Just be suspicious, unfortunately, in this day and age, be suspicious and let people know. Be like, 'Hey, why would that person send me that?" Call them, let them know. Another thing here is categorize cybersecurity as an enterprise business risk. Once again, if you're leading an organization, you should categorize cybersecurity as a business risk. It shouldn't be... Once again, this has been a lot of the theme in regards to culture and things like that, we've talked about. But looking at cyber security risk, looking at it as a business risk, that affects every part of your organization. There's not one person in your organization that can't be, unfortunately involved in a security incident.

Taylor Wells (00:41:34):

It really needs to be across your organization best practices. Hope this was super helpful. Love to jump into the Q&A now. I know we got a bunch of questions coming through and please submit more questions. I actually have one more extra bonus on top of a bonus. Pick a scenario and do a tabletop exercise. This is something that you can do ongoing, so quarterly or semi-annually with your leadership team, with your IT department, your external IT department. Pick a specific scenario, a possible common security risk for your type of organization and play it out. After, to do a tabletop exercise where you actually plan it out, what would happen? How would you respond to it? What systems do you have in place to respond to it?

Taylor Wells (00:42:23):

A lot of the security big breaches that have occurred on the news, I always go research what actually happened? Because we can learn from it, we can learn from ransomware, we can learn from socially engineered attacks. We can learn from vendor management attacks. We can learn from things like breaches where somebody had a VPN account to their internal server that then led to this huge E3 gaming company getting compromised.

Taylor Wells (00:42:52):

There's all sorts of things we can learn from it. Do a table exercise, actually play it out in your organization, what would happen? Do that on a regular basis. Do that, and you'll be one step. That will also bring to the surface areas of, maybe we need to review our backup strategy again. Maybe we need to review our cybersecurity training. Maybe we need to review our password management. Maybe we need to review our IT vendor. If you have an MSP or a managed security provider, maybe we need review them and look at a different provider, if you're not confident that every aspect of that security breach or attempted breach would not be handled well. Happy to take some questions. I know we got some questions coming in. Back to you, Philip and Olivia.

Philip Stringfield (00:43:35):

Awesome. Just a big shout out and thanks to Taylor for that great presentation. A lot of great nuggets in there that applies to your organization and personally as well, because you are also able to make entry through your personal information in order to get to your business. I think there was a lot of great information there that everyone can really take point to and implement within their organization.

Philip Stringfield (00:44:01):

We did get a great deal of questions. So, keep them coming in. I also have a comment that I would like to get more information from, from one of our participants. I'm going to get a couple of questions in, and then I'm going to umute. The first question that came in is, what resource do you recommend for a phishing campaign, if any?

Taylor Wells (00:44:26):

Great question. I don't know any personal, off the shelf retail ones that a business can purchase. We have one that we recommend and we implement for our clients. It's called Breach Secure Now. I don't know if you can buy that as an organization. I think you have to go through a reseller like us. You could reach out to us though, and we could help you get that and help you implement that.

Philip Stringfield (00:44:51):

Awesome. I think this is the question that I sent in ahead of time says, what risk are finance AKA covered under cyber insurance and what costs always hit the covered entity if a breach occurs?

Taylor Wells (00:45:09):

That's a great question, and that's something I'm going to punt back to the insurance brokers again. Because every policy is different. There's some policies... We actually have some insurance brokers that are clients and that we work with, and some can be like an umbrella coverage on top of your normal liability, that has pros and cons.

Taylor Wells (00:45:35):

I would reach out to your insurance provider and find out the specifics of your insurance policy. That being said, there's some policies that can cover everything. That will cover the mitigation cost of a forensic IT analysis that you'll need done, or the PR issues. Because framing the problem, when you have a security incident, here's some of the things, some of the areas you'll experience cost. PR will be one of them, forensic analysis, you'll need a specific IT resource to come and do a forensic analysis, the mitigation costs based upon just getting your systems back up and running, depending on the type of breach it was, or security incident, and each type of incident is different.

Taylor Wells (00:46:23):

If it's a bank wire transfer fraud, it's going to be different than ransomware or malware or things like that. There's all sorts of different types of breaches, but I'd reach out to your insurance broker to figure out exactly what your policy covers, and they will give you exactly those numbers. Then that way you can analyze which areas have the most coverage and maybe you want to increase them, based upon your specific risk, and based upon those 15 things we talked about.

Taylor Wells (00:46:54):

If you have all these 15 things in place and then some, and you're doing at least the standard for best practices, then, that will also impact your coverage based upon premiums, but then also based upon how much coverage you want. I know it's a long winded answer, but I would definitely reach out to your insurance broker and have them go through a couple of options for you.

Philip Stringfield (00:47:22):

Perfect. Thanks again. Now, I'm going to go ahead and pass it over to Roberto Casanova to share some of his experiences with some of the software, because we're having a lot of good discussion here in the chat box, just around different programs that are available. I'm going to go ahead and see if I can get him unmuted to really talk just about his experience with the program software intercept. Let's see if you're still there, rolling. Give me one second. Roberto. Looks like he just might have left the chat.

Olivia Peterson (00:48:08):

Philip, I think he's unmuted. Roberto are you there?

Philip Stringfield (00:48:12):

Okay, perfect. You're all set. Yep. There you go.

Olivia Peterson (00:48:18):

He may not be Roberto. If you're there, feel free to chime in.

Philip Stringfield (00:48:21):

Should we make him a panelist and see if it changes anything?

Olivia Peterson (00:48:30):

He is unmuted. He might not be there, unfortunately. But Roberto, if you come to back, just send us a note in the chat and we can come back to you.

Philip Stringfield (00:48:41):

Perfect. It looks like he dropped off. Let's see if he'll call back in again. With that, we'll go to the next question until we get Roberto back. Then if there's anyone else that would like to speak to the software in the chat, feel free to raise your hand and we will unmute you then as well.

Philip Stringfield (00:49:00):

There's another question that came in that says, what is a recommended best practice or multifactor authentication solution for NextGen EHR, if we're looking for EHR systems. If that's something that Taylor can't answer, I will also do my best to pass this to our steering committee for the NextGen user group as well, to see if there's any resources or information I can provide on that end. It looks like Roberto's back on. Taylor, did you have anything you wanted to add before I-

Taylor Wells (00:49:30):

Yeah. For the single sign on and multifactor authentication for NextGen, they probably have something built in. Depends if the NextGen is hosted locally or is in the cloud. Unclear if it's hosted locally or in the cloud, but I would reach out to them and ask them, "Hey, how can we get MFA or single sign on enabled?" And get those additional security features in place.

Philip Stringfield (00:49:56):

Perfect. All right. We're going to move to Roberto, and I want to see if we have him...

Olivia Peterson (00:50:09):

Roberto, you should be able to unmute yourself now. We can't hear you, unfortunately. You'll have to make sure your audio is connected as well.

Philip Stringfield (00:50:29):

All right. Let me just keep an eye out on the chat as we're going through, just to make sure there wasn't anything else. It looks like KnowBe4, as well was discussed as well. If there's anyone else that would like to speak to their experience with any of these platforms, feel free to raise your hand and we'll unmute you. In the meantime, I'll go ahead and ask another question. It says, are there any recommendations for antivirus?

Taylor Wells (00:51:06):

Great question. Yes. I would say Webroot and BitDefender are two great options that we use internally and we deploy for our clients. Those are two phenomenal options. Great question.

Philip Stringfield (00:51:19):

Perfect. Looks like there's CrowdStrike there as well. I'm glad that everyone is at least able to speak to their current experiences and what they're using. Feel free to just drop in the chat, that's been useful for you, from a financial aspect, from an organizational aspect. Sorry, we weren't able to get you, Roberto. If we're able to, while time permits, we'll make sure to definitely allow you to share your experiences.

Philip Stringfield (00:51:56):

All right. We are down to the last question and it is, is NACHC going to be releasing more information about their breach incident last month? If you are not aware, NACHC did go through a system breach. We are still getting everything together. But what I would like to do is a sharing of lessons learned from that, because there is no other better way for us to really be able to share that experience while also learning.

Philip Stringfield (00:52:26):

We're definitely going to make sure, as time permits, to do something that's going to be able to make impact, and then also share the story of what happened, how we resolved it, and the lessons learned. We'll definitely make sure, keep you all posted as that comes.

Philip Stringfield (00:52:46):

Looks like we have a question. Hold on really quick. It's quite long, so I have to paste it. It says, could you provide some guidance in terms of what to do to combat a ransomware attack? I've noticed a rise in those overall as of late, very informative session.

Taylor Wells (00:53:06):

Yeah, that's a great question. What's really interesting about ransomware is, ransomware is actually pretty not socially engineered. It's actually pretty automated, and it's one of those things that's random in a lot of situations. Some attacks are very intentional, especially some of the larger profile attacks that we've seen on the news are really intentionally targeted, and they found a very specific breach in the armor of the infrastructure, a very small little in with the organization.

Taylor Wells (00:53:45):

But as far as ransomware in general, especially for medium to small organizations, it's pretty random. A lot of it occurs because of phishing. If we're talking about combating it, I would say phishing is a big part of it. Also, having an effective backup strategy, because I think what the problem is with ransomware is, especially in the past year, we probably have had a dozen notable breaches from a large organization or government organizations worldwide.

Taylor Wells (00:54:17):

A lot of them, unfortunately, they actually paid the ransom or paid the ransom, and then they had the FBI go and try to retrieve it back. Which is actually something the government has been saying, you shouldn't be doing forever now, and I actually have talked to members of the Department of Homeland Security, and I've talked to other government officials that they constantly recommend don't pay the ransom.

Taylor Wells (00:54:44):

The only way you're able to not pay the ransom is to actually have an effective backup strategy, and ultimately, the ability to get back up and running without having to pay the ransom. Obviously losing data is a huge problem to begin with. If you do experience ransomware, no matter how you slice it or dice it, even if you have a backup, it's not good. But it can be a heck of a lot better if you have a great backup strategy.

Taylor Wells (00:55:16):

Then on the preventative side, definitely focusing on combating phishing scams, focusing on browser security and making sure people are aware when they're on a website that's not legitimate. Then phone scams and text message scams, because those things also... Really, all the phishing types of situations where people are impersonating somebody else to get somebody to download something or to click on something or give up information, those we're seeing as a huge trend for ransomware and ransomware being effective.

Philip Stringfield (00:55:59):

We got a good comment from Candice that said, paying the ransom provides investment income to bad actors to improve their criminal enterprises and attack more people.

Taylor Wells (00:56:08):

Totally. I'm not obviously the CEO of any of the companies that we're operating, but generally speaking, we're in a predicament if we continue with that bad revolving door problem. I completely couldn't agree more, Candice.

Philip Stringfield (00:56:31):

All right. With the last couple of minutes we have left, we're going to see if we can do the third time is a charm with Roberto and see if we can get him unmuted.

Roberto Casanova (00:56:50):

Hello?

Philip Stringfield (00:56:51):

Hello, Roberto. How's it going?

Roberto Casanova (00:56:54):

Oh, good, good. I finally got this working.

Philip Stringfield (00:56:57):

There we go.

Roberto Casanova (00:56:57):

Anyway, thanks for the presentation. I thought to myself, 15 best practices in an hour, I don't think it could be done, but Taylor, you did it and you did it well too. Thank you for that. Anyway-

Taylor Wells (00:57:09):

Thank you.

Roberto Casanova (00:57:09):

Sophos Intercept X, we've been using it for several years at my organization. By the way, I'm the director of IT Security at Urban Health Plan in the Bronx, New York. We've been using it for several years before it was called Sophos Intercept X, it was just Sophos antivirus, endpoint protection.

Roberto Casanova (00:57:30):

They have a pretty good suite of products, I won't get into that. I don't work for them, I don't get paid by them by the way. But it is a great product and it is highly rated. Before we renewed our contract with them and we repurchased their product, we did see a demo of the ransomware protection, and it's actually pretty cool. As soon as it detects some quick encryption of files, it will stop it.

Roberto Casanova (00:57:59):

It actually makes copies of the files so it can put them back and it will stop the process from running and prevent it from running again. I've also seen it running live in my own environment. Several years ago, somebody probably clicked on a phishing email and got ransomware. It didn't go any further than it started to encrypt a couple of files. I'm pretty confident in its ability to protect against ransomware, as well as other things. It's got a bunch of bells and whistles and the latest version is cloud based. You can view what's going on from anywhere. There's a lot of other good products, I just happen to think Sophos is the best fit for us.

Philip Stringfield (00:58:47):

Perfect. Thank you so much-

Roberto Casanova (00:58:49):

By the way, somebody mentioned it, KnowBe4, which we use has a ransomware simulator program that you can use to test your endpoint protection against... See if the ransomware protection is actually working. That's another good tool and it's free, anybody could download it and run it in their environment.

Taylor Wells (00:59:09):

What was that last one, Roberto?

Roberto Casanova (00:59:13):

A KnowBe4 Ransomware Simulator.

Philip Stringfield (00:59:18):

I saw there was other people in the chat talking about that as well. Thank you so much for Roberto for closing us out and sharing your experience. Always think it's a great thing to have a health center be able to really share their experiences from being boots on the ground and supporting other organizations as well in their roles.

Philip Stringfield (00:59:36):

Want to go ahead and close us out. We're right at three o'clock. I want to go ahead again, thank Taylor Wells with Northwest Technologies Group, in addition to my colleague, Olivia Boggiano-Peterson for assisting throughout today's webinar, our office hour. Of course, we're going to be resuming next month, and we'll be setting us off with a policy update, a telehealth policy update from NACHC's policy team, January 13th, same time from 2:00 to 3:00 PM Eastern. We hope to have you there. Thanks again, everyone, for connecting and discussing with us and enjoy the rest of your day and happy holidays.