Phillip Stringfield (00:00:01):

Awesome. Thank you so much, Olivia. Again, welcome everyone. We are glad to have you here for part one of Considerations for Sustaining a Culture of Cybersecurity.

Phillip Stringfield (00:00:11):

Before we get started, I just wanted to fit a quick plug in for our EHR user groups, and just wanted to make you aware, if you're not already, that NACHC currently supports six EHR user groups that are NACHC hosted, meaning that they are led by a PCA, HCCN, and Health Center leaders. Each of these groups meet on a monthly or a quarterly basis, so as you can see, we have those six listed to the left of your screen: athenaOne, athenaFlow/athenaPractice, eClinicalWorks, Greenway Intergy, NextGen Healthcare, and our newest, EPIC, which is set to launch June 1st. If you're interested, I'm going to go ahead and drop a link in our chat, so that way, you can sign up for your respective sender, but you also have my email address here below. You can send me a quick email address, and I'll make sure to get you connected to those groups.

Phillip Stringfield (00:01:05):

Without further ado, I'm going to go ahead and get things kicked off in passing things over to our partners over... We have Michael Sanguily, who is with the Health Choice Network, and Arnel Mendoza, with QueensCare Health Centers, who's really going to be diving in for our series part one, Understanding the Essentials. Without further ado, I'm going to go ahead and hand it over to these gentlemen to get us started today. Thank you, again, for joining.

Arnel Mendoza (00:01:32):

Good morning, everybody, if you're in the West Coast. If you're in the East Coast, good afternoon. My name is Arnel Mendoza. I'm director of information systems at QueensCare Health Centers. In terms of relative size, we see about 24,000 patients and get about 115,000 visits, at least that was in the past year, so that kind of gives you an idea of where we stand with that. I'm going to pass it on to Michael to introduce himself.

Michael Sanguily (00:02:03):

Thank you, Arnel. Welcome, everyone. My name is Michael Sanguily. I serve as director of CISO services, which is our cybersecurity team over at Health Choice Network. We support over 50 FQHCs across the nation, with several thousand patients in our systems. Then, our primary focus is really cybersecurity education, as well as improving the posture, the cybersecurity posture of our FQHCs and in anything else that we can help around with cybersecurity. I believe we're ready to get started.

Arnel Mendoza (00:02:38):

What we're going to be talking about this morning, or this afternoon, is cybersecurity data breaches, who they affect, how do hackers find their targets? Basically, it's going to be... We're going to be discussing basic tool sets, because what I always say is a basic infrastructure protects, a good infrastructure enables, and a great infrastructure innovates. We're not going to do the last two. We're going to do the basic one. That's what we're going to cover today.

Arnel Mendoza (00:03:09):

If you go on the next slide, basically what I do... I'm in charge of IS, information systems, for my organization. If you're a tech person, if you're a tech leader, I'm one of you. I get to be in the boardroom. I get to be in the room with the C-suites and explain expenses and budgets and all of that stuff, and we're going to cover a little bit of that, too, because what I'm finding is there's still a bit of a gap between the perception at the C-suite level and the technology staff level or technology leadership level. We're going to cover that and why in a second.

Arnel Mendoza (00:03:52):

First of all, ever notice data breach is now part of the consumer vocabulary, right? They basically started tracking this in 2003, when it was just called credit card fraud and identity theft. Now it has, in a period of two decades, it's evolved into medical identity theft with life-threatening implications and, even greater than that, to national implications, as well. Next slide.

Arnel Mendoza (00:04:23):

First, I want to do a tabletop exercise, only because I want to make sure this mechanism works and I'm able to do it, because there's going to be a couple of tabletop exercises at the very end of this presentation. I just want to ask a simple, simple question. Do you know of any community health center that has been affected by a data breach? It's just a yes or no. I'm going to give you a minute to do that here. Timer on.

Phillip Stringfield (00:04:57):

Just as a heads-up, everyone. You should see the Slido polling on the right of your screen, and you should be able to select the option yes or no, and if you would like to elaborate, feel free to drop it in the comments. It looks like we got a comment in the chat from Candice, "It's that you either do or don't know that you do."

Arnel Mendoza (00:05:43):

Is that Candice Roland? Hello, Candice.

Michael Sanguily (00:05:48):

That's very true. It is very true.

Arnel Mendoza (00:05:54):

Okay, we can pick it up from here, I think. I don't see how many people said yes. Oh, I do, 63%. Wow. That's the majority. For those 37% that said no, as Candice pointed out, how do you know? I'm going to go over that in a second. Next slide.

Arnel Mendoza (00:06:15):

As far as me, the answer's an easy yes. This, I'm going to be talking about a specific community health center where I am, in the Los Angeles area. It was hit by ransomware about a little over a year ago, in February 2021, and my counterpart was kind enough to speak to myself and a bunch of our IT leaders in the area to talk about it. Here's what she shared, okay?

Arnel Mendoza (00:06:43):

They were hit by Zeppelin ransomware that was triggered by a phishing attack. That's when somebody sends you a phishing email and somebody clicks on a bad link or attachment and introduces malware into your system; 26,000+ patient records were exfiltrated. That means, it was basically stolen. All systems were encrypted at block level, including backups. That means, they couldn't even backup to a previous iteration of their databases.

Arnel Mendoza (00:07:10):

Forensics determined later on that threat actors had access to the system as early as a week earlier, and possibly even a lot earlier than that. They did pay the ransom, and although she didn't tell me an exact amount, it was in the hundreds of thousands of dollars. That's actually, I will show you later, fairly small compared to the average. Thousands of man hours were spent on immediate remediation, all her staff, all of her staff, spent 15 to 17 hour days for a good week, because full access to their systems were not covered for at least that week, for five days. Can you imagine, if you are a tech leader? I felt really, really bad for her, as somebody who stands in her shoes, not to mention the patients that they weren't able to see, not to mention this expense that they had to do.

Arnel Mendoza (00:08:04):

What doesn't get talked about is the damage to your reputation. You have to report these kinds of attacks to your state or some other federal agency, and that becomes public. In other words, there's a breach of trust, if you will. That stuff, it's hard to recover from, at least not immediately, okay?

Arnel Mendoza (00:08:29):

I'm going to move over now to a much, much bigger hack. This one kind of hits home, because a lot of us are FQHCs. Like I said, this is just an FQHC where I am, but a bigger hack on a more larger scale, I'm going to let Michael talk about. Next slide.

Michael Sanguily (00:08:47):

Lapsus$ is basically a hacking group. They were recently arrested for what they believe... They caught all of them, but Lapsus$, from those that they found were people from the ages of 16 to 21. Now, the crazy part is these are basically kids. I mean, most of them that were arrested couldn't even get a drink at a bar or a beer anywhere, so these are high school kids through college students.

Michael Sanguily (00:09:15):

Their forte was hacking and then exposing the networks that they hacked, so they would put out all this information into the public for all other hackers to see. Any kind of data that they were able to take from these companies, they would put it out into the public internet for anybody to gain access to this information, which is obviously very dangerous for these organizations. They hacked into organizations, such as NVIDIA, Samsung, Vodafone, Ubisoft, Microsoft, Okta. Those are major, very large companies, with strong cybersecurity teams, and these folks were still able to breach these networks and expose that information. We want to talk a bit about some of the different hacks they did and how they did them, so that we can get an idea of what they target. Go ahead, next slide, please.

Arnel Mendoza (00:10:01):

By the way, that group is still at large. Although they were arrested, they were not detained. They're still out there.

Michael Sanguily (00:10:09):

Right, and then it's tough when you know that they're juveniles, and they just sort of get a slap on the wrist and then they go back out there. Then, more than likely, they go back out there and do the same things they were doing before, unfortunately.

Michael Sanguily (00:10:19):

This is one of the breaches they did was T-Mobile. They were able to compromise an internal tool that they did, called Atlas. Thankfully, there was no customer or government information on there, but they did expose all of the source code and all the information they were able to obtain to the public web, which just allows hackers to try and breach T-Mobile themselves with the information they were able to obtain.

Michael Sanguily (00:10:45):

What they did here was something called SIM-swapping. Now, I know most of us, hopefully, use multifactor authentication. That's when you log into maybe your bank account or a critical system, and it sends over a text message to your phone, and then to authenticate that it's truly you, even though you put in that password into the system.

Michael Sanguily (00:11:02):

Now, what SIM-swapping is, is it's a very advanced technique, very, very advanced technique, where they convince either your cell phone carrier, by taking all of your personal information that they more than likely hacked in some other sort of way, so they'll call and say you're T-Mobile, and they'll pretend to be you, and change your phone number over to their cell phone, so that when they do log into your system, and you get that multifactor authentication code texted to your phone, it'll come to their phone, because now they own your phone number. This is a very advanced way, and we still always do strongly recommend multifactor authentication as a layer of protection, but it's just to give you an idea of how in depth these breaches can go. Next slide, please.

Michael Sanguily (00:11:50):

They also breached Samsung. They claim that they leaked 190 gigabytes of Samsung as a proof of the hack. They announced this on a Telegram channel, which is sort of a chat channel, and they sent it out in a Torrent file for everyone to download. That's just a simple file that anyone could download. They put it out there on the public internet with the source code, which is basically the secrets to the company, allowing any other hackers to download this information to also hack Samsung or any other information that may be inside that source code that would allow other hackers to breach Samsung or any other tools or companies they may be connected with, as well. It's just to give you an idea of how they're just exposing these companies and causing more danger to others, as well, because if you're connected with Samsung in some sort of way, you may have been exposed through this breach, as well. Next slide, please. I know this one's a more personal one for Arnel. He's very familiar with Okta, so I will go ahead and give it over to him.

Arnel Mendoza (00:12:52):

We use Okta as our identity management provider. What that means is they're basically our single sign-on provider, right? We have most of our applications in the cloud, and our Okta instance, if you will, syncs to our active directory, so that's how we connect to everything, that single point.

Arnel Mendoza (00:13:10):

When we found out, or I found out, that they had announced they had possibly been breached, immediately the thought was, were we part of that breach, right? I mean, this is how we gain access to most of our systems. I was on the phone with them for a while, for a good half a day.

Arnel Mendoza (00:13:30):

What they found was... and back then, when I did talk to them, they weren't saying anything. "Oh, we weren't hacked. We weren't hacked." Turns out, a week later, they did admit that they were hacked in January 2022. Further investigation determined that it was the account of a customer support engineer working for one of the third party providers, so it wasn't specifically Okta, but it was one of their providers that had Okta information.

Arnel Mendoza (00:13:56):

The forensics that Okta did, at least what they claimed, was that the intrusion was limited, that the breach lasted for only 25 minutes, and it affected only two customers of that third party provider. However, the point being, they were still breached. They still got Okta data. A breach is a breach. Back to you, Michael. That one, like I said, was personal to me.

Michael Sanguily (00:14:22):

Well, I could imagine. Actually, I'd like to piggyback off of what Arnel said. Just because you may be secure, you also need to vet all your third parties that you're connected to, so any systems that you're integrating with, with a third party, you should always be vetting your third parties to make sure they are upholding the same cybersecurity posture as you, to make sure you're protected, because again, if you're third party, who's integrated with you, is hacked, that can turn into you getting hacked, as well. You've always got to make sure you're protected from your third parties, because that could translate into a data breach into your own organization.

Michael Sanguily (00:15:00):

How did they pull off breach after breach? For T-Mobile, they purchased stolen credentials from a Russian cybercrime market on the dark web, which I'll talk a little more about the dark web in upcoming slides. They are able to just basically go on websites and purchase this information, and then use it to their advantage to get into your networks, so stolen credentials. Let's say, sometimes hackers steal credentials. They sell it on the dark web. They don't want to go and take the time to hack into your system, so instead, they'd rather take the profit right away and just sell off these credentials to other hackers, who would go ahead and then hack into you.

Michael Sanguily (00:15:37):

They compromise these credentials, allow the threat actors to interface to your applications through VPN or maybe you have some kind of remote desktop tool. They sold that kind of both user names and passwords of those tools, so if you think that you're using the remote desktop protocol... I know some people use TeamViewer as to remote into systems. They may have hacked that system and sold off those credentials for hackers to use it to then remote into the systems themselves.

Michael Sanguily (00:16:06):

Again, it's just always protecting yourself from your third parties, as well. You've always just got to keep in mind... Ask them for their annual audits. Ask them for their security audits that they have. Ask them, have they done penetration testing in the year, so that you can just double-check that they are also secure, just as well as you are. Next slide, please. This is a, basically, a live listing on the dark web of credentials being sold online for a Windows 2008 server, so they [inaudible 00:16:39]-

Arnel Mendoza (00:16:39):

For a whopping price of $10.

Michael Sanguily (00:16:42):

For a whopping price of $10. Imagine a hacker knowing that he can just purchase credentials without doing any work, and then just log directly into your systems. The original hacker who has this listing, who's selling this, hacked probably tons and tons of different systems, got tons and tons of different credentials, and is just selling them off to make other hackers' lives easier, for $10, for them to just log directly into your systems and do as they please within there. Next slide, please. That's just to give you an idea of how dangerous that portion can be.

Michael Sanguily (00:17:14):

Hackers leverage these credentials. One of the main problems we're seeing is that credentials are being stored in plaintext passwords, and that exposed 429% in increase of networks because of these plaintext passwords. Any kind of tools you... You've always got to think of any kind of applications you have. I usually like to say, make a list of all applications you have and where those credentials are stored. Are they being plaintext? Are they encrypted?

Michael Sanguily (00:17:42):

You always want to make sure they are encrypted. I definitely recommend using encryption, especially at FQHCs. We handle patient information, so we should be using encryption in every place possible that we can, especially anywhere where your plaintext passwords are. You want to outline all your applications and your tools, and make sure those tools are encrypting passwords.

Michael Sanguily (00:18:03):

Sometimes it's not up to us. Sometimes it's up to the tools that we use, so before... At least for us, in house, before we purchase any tools, any applications, we always vet them, as well, just like we do our third parties. We say, "If we want to use your applications, we need to see what your security standards are. Are you encrypting your passwords? If I'm sending data out of your applications, is that being encrypted?" You always want to vet any tools you're using, because then this could also lead to a breach if they're not encrypting your passwords. Next slide, please.

Michael Sanguily (00:18:37):

These are a dark web price index for 2022, and these prices vary. They could go much lower, much higher, but as you can see, this is average pay for credit card data, so credit card details with account balances to $5,000, $120. Credit card details account balances up to $1,000, $80. Payment processing services, like PayPal accounts that have been hacked, they sell them for $45. Crypto accounts, $250; social media accounts... so you get the idea. They also sell malware. They create their own malware, which they feel has a very strong success rate against your antivirus not detecting it, so they'll find a

piece of malware that they create themselves. They'll test it against multiple antivirus tools, and notice that 70% of those tools do not detect their malware, so then they'll sell this malware out to other hackers that want to use it for a very high price, depending on the success rate, and this will allow the hackers to use this malware to infiltrate your systems.

Michael Sanguily (00:19:38):

That's where proper network monitoring comes in play. You can't just rely on your antivirus systems. You also want different tools that will help you identify if any strange activity is going on within your systems. We'll talk a little more in depth about that in some coming slides, but you always do want to get an idea of what's going on in your network because look how easy it is to just purchase something. Next slide, please.

Michael Sanguily (00:20:03):

I'll talk a little more about the dark web here. I know it's almost becoming a household name, unfortunately, what the dark web is, but it's essentially... You can think of it as sort of a back street to the internet, more of like an alley in the internet. You need special tools to access the dark web, but it is very easy. As you see, kids are basically able to log into there, but it's almost as simple as them watching a YouTube video, downloading a link, using a special application called Onion, and it gets them into the dark web, which allows them to access all these different types of websites, which are typically nefarious.

Michael Sanguily (00:20:38):

As you see here, this is a listing. This is a screenshot of an actual dark web website called HANSA, extremely popular. It's almost like an Amazon that you can think of. These websites do get taken down all the time, but they just pop right back up.

Arnel Mendoza (00:20:53):

Michael, I also wanted to point out. The stuff that you can Google, that's not the dark; that's the regular web, and that's a very, very small part, compared to what the dark web is. Dark web is almost more than half of the total internet.

Michael Sanguily (00:21:10):

That is. That is correct. What's scary is that the majority of things... It's not always used for bad things, but the majority of things on there are typically things like you see here.

Michael Sanguily (00:21:20):

This looks like an Amazon listing. It says, "V.I.P. Healthcare; full info, medical records, date of birth, social security numbers, photo, insurance, drug, and lab results for sale for only 99 cents," which is the scariest part. Now, hackers will use this to purchase it, and then they'll perform some sort of identity theft. How this starts is because they go ahead and hack into, let's say, an FQHC. They're able to compromise thousands and thousands of medical records, and then they'll list it online for a very cheap price because they have so many of these medical records.

Michael Sanguily (00:21:52):

When you hear these breaches of a million patient records breached, two million patient records breached, they'll sell these all off for $1, just because they want to get rid of them as fast as possible. Then fraudsters will purchase this and perform identity theft against it. I'd just like to emphasize this, so that we all know how dangerous it could be and how we want to increase our security posture, because we would never want our patients' information to be listed on the dark web, that would impact many, many people. Next slide, please.

Michael Sanguily (00:22:23):

Five common ways credentials are stolen. Phishing, which is the most common way, which is simply sending an email out to your staff, making it look like maybe it's coming from your IT Department or maybe some sort of system you use, saying, "Hey, your account has been locked out. Please click this link to log in. Put in your user name and password and confirm your identity." People will think it's real, because they may see a Microsoft logo on it, click it, put in their information and password, and now those hackers have that information, and they'll sell it off or use it for themselves to try to hack into your system.

Michael Sanguily (00:22:57):

They also use malware to exfiltrate passwords and user names, if they're in plaintext, bad websites out there that have malware on them, as well, or they might just try to brute force your weak passwords. They might just try to guess at your passwords in your systems. That's why it's important to have a very strong password policy in your organization, to make sure someone can't use the password as password, or password123 as their password, because then hackers are able to breach that. Within less than one second, they could breach that. Then also there's public WiFi. The dangers of using public WiFi is you never know what you're connected to. You may be connected to someone who has a little device there that's emitting WiFi, and you think you're connecting to a legitimate WiFi, but really what they're doing is something called the man in the middle tech, where you're connecting to their system, so any information that's going to the internet is passing through their systems, and they're able to see everything. Those are just some of the common ways credentials are stolen, and things for you to consider, as well. Next slide.

Michael Sanguily (00:23:57):

This is a quick phishing exercise to show you a phishing email, what it looks like. We actually do phishing assessments for our member centers, where we send out phishing emails that we create ourselves, to see who passes, who fails, and then whoever fails takes some type of training. We always recommend doing this at least on a monthly basis. The more you do it, the better your staff will get at identifying these phishing emails. I mean, most of the time, when we first help out an FQHC with their phishing assessments, we'll see up to 50-60% of people failing a phishing test.

Michael Sanguily (00:24:30):

That means, if we were the actual hackers, we would be compromising 50 or 60 accounts out of 100. That would be tons of credentials we would have for an organization. That's why it's important to train your staff, as well, so that they know how, where, or what a phishing email looks like.

Michael Sanguily (00:24:46):

There's a quick few identifiers on here that we'd like to cover. Can you bring up the animation. I know it'll highlight a couple of them. Yeah, you can bring up all three, please.

Michael Sanguily (00:24:55):

There's a few things we always like to highlight. This is something, hopefully, you can just take back and learn for yourself and just teach your staff, if you haven't done so yet. Always look at the email it's coming from.

Michael Sanguily (00:25:05):

This is an organizational email it's sending over to you. Just because it says your health center's name, IT Department, doesn't mean it's truly their IT Department. This is coming from an actual Gmail address. If you look at it, that should be a red flag for you right away.

Michael Sanguily (00:25:20):

If your organization uses a banner, which I would strongly recommend that if you receive emails from outside of your organization, it let's the person know that this email's from outside your organization. You want to do that, because if I am internal to your organization, and I'm an employee there, I send you an email, you would not get a banner, but if somebody is spoofing my account, sending you an email that looks like it's coming from me, they should be outside your organization. That person should receive that banner and should know right away, "Hey, how come Michael Sanguily is getting the red, I'm outside your organization, banner when he's internal," so that should be an identifier.

Michael Sanguily (00:25:53):

The last one I always like to highlight is hover over any links. Just because you see a link that says www.google.com doesn't mean you're necessarily going to go to google.com. If you hover over the link, it'll show you exactly where you're going to be sent. In this case here, if you hover over that confirm account link, it'll show you where you're going to be sent. It's a strange-looking link. It says something like sendgrid.net, and then it has a bunch of letters and numbers. That should already be a red flag for you there to know, okay, I'm going to be sent to some strange website. I probably should not click this. I should probably report it to my IT Department. Next slide, please.

Michael Sanguily (00:26:25):

This is just one last example of how easy it is, bots are easily bought online. Literally, just entering in credit card, what you're looking for, the max price that you're willing to pay. You hit a search. You can select your countries. They have filters, just like you're in a regular store. Then it'll come up with all the available listings of people selling credit card numbers or credentials or patient information, as well. This is just something to keep in mind of how simple it is for someone to purchase this information online. You never want your information on there. Next slide, please.

Michael Sanguily (00:27:06):

We always like to mention this. This is a website called haveibeenpwned.com. You can see the link there on the bottom right. You can type in your email address in there, and it will tell you if your email address has ever been a part of any other data breaches out there.

Michael Sanguily (00:27:20):

For instance, T-Mobile, Equifax, if you had an email registered with them, and you had credentials with them, it will tell you if your account was part of that breach. Basically, that's good to know, because then you know if your account was part of that breach, you probably want to reset your passwords across all

accounts, not just that one account, because they'll take that user name and password from, let's say, Equifax, even if it's a specific... or not specific to Equifax. If you're using that same password on Equifax across other programs you're using or, let's say, your bank account, they can test that email address and that password against multiple websites and see if any of them log them in because you use the same password. Never reuse your passwords on multiple sites. Always change your password for every different site. Next slide, please. All right, I'll give it over to Arnel, and he's going to talk more about this part.

Arnel Mendoza (00:28:08):

Also, by the way, shameless plug. We're going to be talking in greater detail about phishing in part two of this webinar series next week. We're going to be talking about that a lot more and quantifying risk.

Arnel Mendoza (00:28:22):

Why do people do this? Well, because, simple reason, it's very profitable. 2021 cybercrime is expected to cost almost $6 trillion, $6 trillion. That's with a T. That's more profitable than an entire global drug trade. Can you imagine that? Cybercrime costs more per year than all natural disasters in the world combined, and it's projected to go more than $10 trillion in another three years, staggering numbers. Next slide, please.

Arnel Mendoza (00:28:59):

Now I'm going to talk about attitudes, because this is kind of like the important part. What do the C-suites think? After all, they're the ones holding the purse strings, right? According to a Shred-It Data Protection Report in 2019, 55% of C-suite respondents support the statement that data breaches are not a big deal or blown out of proportion. I thought, that's got to be wrong, so I tried again for this years report. In this year's report, four out of 10 business leaders rate the risk of an attempted data breach in the next 12 months as four or five on a five-point risk scale, okay? Only four out of the 10 think it's very risky, that there's actual real risk, so that even went lower. Next slide.

Arnel Mendoza (00:29:50):

Is there a disconnect at the top, you think? When you go to the Deloitte 2021 Future of Cyber Survey, 96% of U.S. executives say that they discuss cybersecurity with their boards at least once a year, 50% say quarterly, so it's on their minds, so what gives? Next slide.

Arnel Mendoza (00:30:12):

More C-suite responses, the same survey, Deloitte 2021 Future of Cyber Survey, 98%, like we said, of U.S. executives say their organization experienced one or more cyber incidents in the past year. However, when asked if their organizations have a strategic and operational plan to defend against those cyber threats, 14% said no, and if they were asked how do executives detect or mitigate employee risk indicators, 15% say their organizations have no way of doing this, and another 44% say they rely on leadership to monitor employee behaviors and cyber risk indicators. What does that mean? They're pushing, 44% say leadership... That's the tech leadership. That's us. That's me. If you're a tech person, that means your CEO is depending on you to guard the gate. Next slide.

Arnel Mendoza (00:31:05):

Of course, technology leaders, we know about cyber risk. We know about cyber preparedness. The 2021 Mimecast State of Email Security Report says four out of five technology leaders say their companies were already hurt by their lack of cyber preparedness, so we know we need to do some work. Next slide.

Arnel Mendoza (00:31:25):

What are the obstacles? You go back to the survey on executives, 38% said it's just too tough. New technology, increases in data management and the perimeter are too complex; 35% say they have an inability to match to the rapid technology changes. Another 31% already acknowledge that they need to have better prioritization of cyber risk across the enterprise. The obstacles, new technology, overwhelming new approaches, more resources, that's money. That's dollars. What's budget, after all? Well, budget is just a priority, priority of spending.

Arnel Mendoza (00:32:11):

My next message is directed to the C-suites, because what I'm trying to tell you is that guy in the picture you see, that could be those teen hackers, but they can also be state sponsored hackers from Russia or China or North Korea or the Middle East. It's not just those kids. It's very well funded groups, and I'm here to tell you, as a technology leader, if you have that guy doing his thing 24/7, there is no way I beat him, no way, 0% chance, okay? That is bleak, and my point here is to scare you. Yes, I'm trying to scare you, so that you can take action. Next slide. Go ahead, Michael.

Michael Sanguily (00:33:01):

Right, so as Arnel mentioned there, it is bleak in the sense that it's real life. They do this as a full-time job. They have large groups of them, so if they want to target you specifically, they're going to poke at every single place possible and hope that they find one little hole that they can sneak into your organization through. It's just kind of just the reality of this, unfortunately. That's what's bringing us to the cost of a data breach going higher and higher every year, so 2021 had the highest average cost in 17 years. A data breach cost rose from $3.86 million to $4.24 million. That's the highest average total in a 17-year history. It just gets worse and worse every year. They are finding it's profitable, so they keep and continue on doing what they're doing.

Michael Sanguily (00:33:50):

The average cost was $1.07 million higher in breaches where remote work was a factor. Remote work has become an everyday life for the most of us, after COVID-19, so that opens up a new realm of areas that we have to identify, to where we can protect ourselves against different types of breaches. Compromised credentials caused the most breaches. This is the same stat year over year. It's always compromised credentials, whether it be through phishing or vishing, which is phishing, but over the phone, that they call you and try to impersonate someone, or just compromising your plaintext passwords you might have stored somewhere. The cost of a data breach keeps going higher because it keeps happening more and more, and it's something we just have to be aware of and keep in mind. Next slide. Go ahead, Arnel, [inaudible 00:34:38].

Arnel Mendoza (00:34:39):

As you can see here, what you're seeing in this slide is the cost of a data breach. In blue is in 2020; in purple is 20... I'm sorry, yes, 2021. Who gets to win it all is healthcare. By far, the largest cost of a data

breach is in healthcare, and by far, the largest jump from '20 to '21 is healthcare, and it's not even close. The average cost of a healthcare data breach ballooned to $9.23 million, up 29% from 2020. Next slide.

Arnel Mendoza (00:35:12):

Could it happen to you? Well, according to the Mandiant Security Effectiveness Report, doing a deeper dive into cyber reality, 53% of attacks go unnoticed, 53%. That's more than half; 68%, really more than half, of ransomware attacks go unnoticed; and the vast majority, 91%, did not even generate an alert. If you're a tech person, that should definitely make you concerned. Next slide.

Arnel Mendoza (00:35:44):

Data breach response times in the healthcare industry, average number of days to detect a data breach, 255. That's according to the IBM Security Cost of a Data Breach Report in 2020. Average number of days to contain a breach, 103. Combined, that's almost an entire year, an entire year. Next slide.

Arnel Mendoza (00:36:05):

This is a website that's publicly available. This is from the California State Attorney General's website. What it is, it's a listing of data breaches that were reported in the state, state of California. To the left, I only filtered for healthcare organizations, okay? These are all healthcare organizations. To the farthest, farthest right, that date is the date it was reported, so we're talking about some dates here that were just a few weeks ago. Then in the middle, those were the dates the breach actually happened. That is to make my point that, you look at Advent Health Partners... I'm sorry if you're mentioned in any way. If you're in this webinar and you're one of these organizations, I do apologize. You can see that they found out that the breach... They reported it on 04/27, but the actual breach happened way back in July. That's a full nine months ago. LA County Department of Mental Health, way back in October. They reported it a few weeks ago. That's six months ago. If you're at Rady's Children's Hospital in San Diego, you can see here, they were breached many, many different times over a span of 10 years.

Arnel Mendoza (00:37:21):

Again, if you didn't think it can happen to you, how do you know? It takes a while before you even know you've been breached, right? These are real numbers. Next slide. I keep asking that question. How do you know you haven't been breached already? Next slide, Michael.

Michael Sanguily (00:37:48):

How do hackers find their targets. There's many, many ways. This could take hours to explain, but one of the most common ways is they poke around on the internet and look for public information, look at your LinkedIns. First, they identify what company they do want to hack. They'll go onto your LinkedIn again, get your information, send you a phishing email over to you. They see maybe your account end user is ADP. He posted that on his LinkedIn, that he's an expert in ADP, so now they formulate what's called a spear phishing attack, which is a targeted phishing attack, and they'll make the phishing attack look just like ADP, since they know that person is more likely to click on that link and compromise your credentials that way, as well. They'll use financial-

Arnel Mendoza (00:38:30):

By the way-

Michael Sanguily (00:38:30):

Go ahead.

Arnel Mendoza (00:38:33):

On LinkedIn, you can easily determine the company's organizational structure just by looking at a certain company, and you can see the CEO's there, the CFO's there, and then the next thing you know, you have an entire org chart that you can actually just figure out on your own.

Michael Sanguily (00:38:49):

Yes, and they actually do create these org charts, like you see in the movies, where they put it on their walls, and they create an entire org chart, so they know what structure and how they want to attack at a company. You always want to have some sort of social media policy. You want to minimize the exposure your organization is putting out on the internet. It's always, obviously, important to do publicity for your organization, but you want to minimize tools and systems that you're using, or any information that attackers can use.

Michael Sanguily (00:39:18):

They also look for any vulnerabilities in a company's IT infrastructure. They have bots, which... Actually, you can go over to the next slide. I believe it might be coming up. They have bots where they send out automated systems throughout the internet, and it just pokes at every single IP it finds out there. If your IP out there on the public internet for your external network of your organization has not been patched or has some kind of vulnerability or you haven't maybe been paying too much attention to it and haven't updated it in some time, it may have a vulnerability.

Michael Sanguily (00:39:51):

Now, what they're doing is looking for the low hanging fruit. They will go ahead and find the IP address that has the easiest vulnerability to exploit, and they'll take advantage of that vulnerability to get into your systems. You always want to make sure you have proper patch management in your organization, a policy based around it, so if a system is out of date for 30 days, or a new update comes out, that your IT teams have to patch that system within 30 days or 60 days, whatever you feel fits your risk management there.

Michael Sanguily (00:40:22):

Keep in mind, keeping systems up to date is extremely important. The moment you have one system out of date with a critical vulnerability inside of it, hackers can take advantage of that right away. Next slide, please.

Michael Sanguily (00:40:38):

Again, easiest ways to get hacked, we've already touched on this multiple times about phishing. I can't stress enough, phishing, because we see it happen all the time with our FQHCs. We've seen people click on links, put in their user name and passwords, and then, all of a sudden, with our internal tracking tools, we notice someone is trying to log into their account with their actual password from an entirely different country, and we know that's not them. Then, once we go and do our investigative work, we find out that they clicked on a simple email, and they put in their user name and passwords. Viruses and worms, you always want to keep in mind, if you keep your systems up to date, this can help reduce your

attack surface, so maybe these malware or these different types won't be able to take advantage of those vulnerabilities and those unpatched softwares you have.

Michael Sanguily (00:41:22):

Denial of service attack is one very big topic on its own, but this is where essentially they will flood your network with so much information, it'll crash it. Denial of service is something you should... a meeting you should hold with your IT teams to do a scenario where, if you did get attacked with a denial of service attack, how could you prevent this attack, or how can you at least mitigate this attack. Those are just a few of the many ways that they go ahead and compromise you. Next slide, please.

Michael Sanguily (00:41:50):

Like I mentioned earlier, they look for the low hanging fruit. They look for the easiest targets out there. There's so many targets out there, that they poke around until they find whoever has the least amount of security. If you're just faster than the guy behind you, chances are, just like you see in this one, the bear is probably going to get the guy falling with the camera. That camera in his hand is that major vulnerability. Everyone else there has minor vulnerabilities, so that bear is going to go for that guy who's falling onto the floor there, just like attackers. They might find systems with vulnerabilities, but they're going to go after the person who they see has the easiest vulnerability to take advantage of. If you keep your systems up to date, you keep your cybersecurity posture better than most, you'll minimize your risk, when it comes to being attacked by hackers. Next slide, please. [inaudible 00:42:39].

Arnel Mendoza (00:42:39):

Can't stress that point enough, actually. You just need to make your infrastructure just hardened enough, so that you're not the easy prey. You're not the low hanging fruit. You're not the easy target.

Arnel Mendoza (00:42:51):

The question becomes, how much do I actually need to spend on cybersecurity? If you want to know what to spend, I mean it'd be overwhelming, right? I mean, there's so many areas, but you need to determine where you're most vulnerable. That's the most important part is you need to actually quantify where your greatest risks are. Next slide.

Arnel Mendoza (00:43:14):

I'm going to be talking about something called the NIST Cybersecurity Framework, because this is one of those tools you can use to do these quantification mechanisms, so that you can identify where you're weakest, right? You need to quantify something. NIST is the National Institute of Standards and Technology. It's a set of standards and best practices to help organizations manage cybersecurity risk. It's a framework, so you document your controls in your organization.

Arnel Mendoza (00:43:43):

I'm going to give you a practical example for it. We're going to be... Again, another plug. We're going to be covering this in greater length in part two of the webinar next week. Next slide.

Arnel Mendoza (00:43:58):

There are five categories and 22 categories for the NIST Framework. By the way, if you're part of the government, and you're a government organization, you are required to have an NIST assessment, cybersecurity risk assessment. Next slide.

Arnel Mendoza (00:44:17):

All it is, basically, is asking you questions, right? This is the simplest way I can describe it. You'll see the questions on the left here to assess your controls. Questions are like, do you inventory your devices? Do you inventory your software? Do you allow remote access? Do you encrypt PHI? Do you monitor your systems? You basically just answer them. There's about 110 questions. There used to be 72, but now it's much, much longer, so 110. Zero to five, zero means, nope, we're not doing it. One is it's ad hoc; we only do it in cases where we have to. Two, we do it, but it's not consistent or structured. Three, we do it consistently, but it's not best practice, could be better. Four, we do it pretty well. Five, we're world class. If you take the time to answer these questions, you get a good picture of where you are, in terms of your cybersecurity. Next slide.

Arnel Mendoza (00:45:15):

This tool is free. It's from cipher.com. It's actually a dashboard. What I did here was I did answer the questions, and I purposely ranked zero on security awareness, just to make a point. What it does, what this does, is actually give you a heat map, so it tells you where you're weakest, where there are red columns. In the column there, where there's red, that's where your weakest points are. Again, if you can quantify, you're able to quantify where you're weakest at, that's where you probably need to be focusing your security spending, right? This gives you a good assessment of where those areas are, and you can address those gaps. Next slide.

Arnel Mendoza (00:46:00):

Because basically, this is why it's so overwhelming. Information technology, they always say it's PP&T: people, processes, and technology. People get fixated, most people, most executives, get fixated on the middle part, the yellow part, where there's technology, the firewall, the VPN, patch management, all of the end point security, data protection, network stuff, that sometimes the people and the process stuff get left behind, and they are just as important. My goal here is to kind of distill this, because when you look at this, there's just too much stuff. It does get overwhelming, right?

Arnel Mendoza (00:46:44):

The point I'm trying to make is, next slide, it's also not just PP&T. It's another P, which is policies. A lot of the things that you can identify as gaps can be solved by simply having a process in place to address them, right? That's a lot of... What this does is essentially go over all of the technology and blend it with all the people and processes and policy. Next slide.

Arnel Mendoza (00:47:15):

I'm introducing... I'm basically going to dumb this down a little bit, because essentially that slide where you saw those three big circles, to me, that's still overwhelming, if you're trying to explain that to the C-suites. Essentially, we're talking about six things. I found this tool from Global Cyber Alliance. It enables you to address all those things, basically, in a very concise manner.

Arnel Mendoza (00:47:38):

It boils down to six things, really. Know what you have. Update your defenses. You go beyond simple passwords. You prevent phishing and malware. You make sure you have a backup strategy and recovery strategy. You protect your email and reputation. Michael's going to go over each of them in detail.

Michael Sanguily (00:47:59):

First, you need to know what you have, so you need to identify your devices, your applications, your risks. This can be part of that NIST plan that you create. This can be part of a security risk assessment you do annually. You want to identify all the devices you have, all the applications you have, put them in some sort of Excel sheet, and then give them each a rating of how, from low, medium, high, and critical, of how the importance is to your organization.

Michael Sanguily (00:48:24):

You may have applications that store patient information or passwords. You want to mark those as critical, and then you want to look over those as part of your plan. You start with those first and say, "Okay, let me check the security on this. What do I have that's going to protect me from a brute force attack? What happens if somebody gets into my network? How is this application going to be protected."

Michael Sanguily (00:48:45):

Same for your devices. You want to identify the risk that these devices or applications may have, and start with your most critical ones. That'll give you a plan where you can just start from critical all the way down to low until you feel you're at a good point. Next slide, please.

Michael Sanguily (00:49:02):

Know your risks and vulnerabilities. This part is more on the technical side, when it comes to vulnerabilities, but we can't stress this enough. You should always do your external network penetration testing. This is where someone acts as a hacker from the outside and tries to get into your organization, so that you can know what to expect. Many of our FQHCs that we work with, we do penetration testing annually for them, and constantly do vulnerability assessments.

Michael Sanguily (00:49:32):

There's many tools out there. You can look some of these up. I know not every FQHC is going to have the resources to have a full-fledged cybersecurity team. This is where you can rely on HCCNs, or you can just look up a tool. Maybe teach one staff member how to use a tool. There's a tool out there for your vulnerability assessments, called Nessus Professional. Actually, for nonprofit organizations, I'd like to mention that you can get this tool for free. It's typically, I think, $2000 to $4000 per year.

Arnel Mendoza (00:49:59):

That's right.

Michael Sanguily (00:50:00):

But as nonprofit organizations, you can get this tool for free and learn how to use it. What this tool does is it scans your entire network and looks for those vulnerabilities that hackers would take advantage of, and it'll give you a report of all your devices that have vulnerabilities, from low, medium, high, and critical. This will basically... You can use it as a plan where you can tackle those critical vulnerabilities. If

you find, on your external network, you have a critical vulnerability, let's say some type of router or firewall has a critical vulnerability, you would most definitely patch those as soon as possible, and that'll just keep you that much safer, so then, when your penetration testing comes on annually, you'll hopefully pass that test, or you'll at least be in a much better standing.

Michael Sanguily (00:50:42):

As long as you do your vulnerabilities... I like to do them on a weekly basis. If you have that tool, that Nessus Professional tool, and you train somebody how to use it and look for vulnerabilities, or if you have a third party that will do it for you, if you do it on a weekly basis, anytime some kind of update or a vulnerability comes out, you'll be able to identify that right away, and then you can just go ahead and patch that. That should be part of your patch management program. That's what we like to stress every time we speak to an FQHC. Make sure you have someone or yourself doing a vulnerability testing continuously, and then do your annual penetration testing, always by the third party, at least with the penetration testing, because again, you don't know what you don't know. If you don't know you have vulnerabilities out there, then that can just leave you open to hackers taking advantage. Next slide, please.

Arnel Mendoza (00:51:29):

Michael, I also want to point out that you can easily find some data security companies. If you haven't done this in a while, they'll offer it for free. Why would they offer it for free? Because they're going to find something, and they're going to offer services to remediate those gaps that they find.

Michael Sanguily (00:51:43):

Absolutely, that is very true. That is.

Phillip Stringfield (00:51:45):

Can I jump in really quick? Sorry, gentleman.

Arnel Mendoza (00:51:48):

Sure.

Phillip Stringfield (00:51:48):

Michael, you had just mentioned it again, but I want to make sure folks on the line heard, because we're getting a couple of questions. Could you just restate the vulnerability assessment tool again?

Michael Sanguily (00:51:59):

It's called Nessus Professional, N-E-S-S-U-S.

Phillip Stringfield (00:52:04):

Thank you so much.

Michael Sanguily (00:52:06):

If you look it up, they do have a nonprofit portion, where they will give it to us completely free. We've assisted our FQHCs on getting that for them for free. It's a very easy process. You fill out some

information, and then if you're able to learn how to use it yourself, you can do it internal, or you can have someone else manage it for you, and they can run off scans and provide you reports, but it's very important, because then you'll have a constant report for yourself to know if you have any vulnerabilities out there. Yeah, it's called Nessus Professional.

Michael Sanguily (00:52:37):

Again, penetration testing, you want to do this at least externally, and penetration testing, specifically, should be done by a third party to give you an outside perspective of your security posture. They'll go ahead and act like a hacker, like I mentioned. They'll try to hack into your network, see what systems they can access, see if they're able to compromise patient information or passwords.

Michael Sanguily (00:52:57):

You will typically get a report at the end, which can act as an action plan, and they'll list out your vulnerabilities from, again, critical, high, medium, and low. This will allow you to first tackle those criticals, then highs, then mediums, then lows, and it'll just put you in a good standing, so every year you'll be able to know, how well am I being protected against the hackers? It's very important to be doing a penetration testing every year as part of your security risk assessment program. Next slide, please.

Michael Sanguily (00:53:26):

Maintaining your defenses. There's several areas to look at when you want to maintain your defense. Securing your perimeter, of course, you need a firewall. This is what's going to protect you from anybody just trying to poke into your network or trying to remote into your network. There's all kind of functionality, tools, and filters you can set in there. You can block any traffic from other countries that you do not do business with, or you can use the different tools in there to detect types of attack, so there's intrusion prevention systems in there, which will detect if somebody is trying to perform some type of malware or some type of attack against your organization. It'll learn it and block it.

Michael Sanguily (00:54:08):

VPNs are very important. I know I did read the chat earlier about someone asking about using public WiFi. VPNs are important, because that's a virtual private network, which essentially creates maybe like a secure tunnel through the internet, so if you are remoting into your organization, you can remote into the VPN and know that you are securely getting into your VPN without anyone intercepting your traffic, and same when it goes for using public WiFi, although I don't recommend using public WiFi. You should probably use your hotspot or something along that line, and with a VPN, that gives you even more security.

Michael Sanguily (00:54:39):

Then you have anti-malware, virus, and end point security. This has almost become 101 now for organizations, but one thing I do see is anti-virus or malware systems not being updated, so some systems that do require updates for these applications, you should always keep in mind that they do need to be updated. You can't just install them and forget about them. You always want to monitor, also, for any attacks that it's stopping, so if you see a trend that attacks are constantly happening from this specific IP address, you can block that IP address, et cetera.

Michael Sanguily (00:55:12):

Updating your devices, this is going to help you for those vulnerabilities we speak of. Typically, vulnerabilities are coming from devices that are out of date. I've come into FQHCs who still have Windows XP systems in there. Those systems have tons of vulnerabilities, which any 16-year-old can go on YouTube and in 10 minutes learn how to hack into a Windows XP machine. Just make sure you have the latest updates on everything you have, any systems you may have.

Michael Sanguily (00:55:43):

Encrypting your data. Again, plaintext passwords, not only plaintext passwords are something to think about encrypting, but patient information. If you're storing patient information in your networks or through some type of tool, you should always make sure it is encrypted, so at least it minimizes the risk. If a hacker were able to take and exfiltrate all of that patient information, it's encrypted with the strongest standards, and they cannot decrypt it, so they will not be able to gain access to that information.

Michael Sanguily (00:56:09):

Encryption is very important, also device encryption, your laptops, your computers, if somebody conducts confidential information on their laptop. Let's say your finance department has Excel sheets with financials on it or other kind of confidential information, and they lose it or it gets stolen, and somebody logs into their laptop or takes out their hard drive and takes the data out, they can see that information, so device encryption will encrypt everything on your device. If somebody were to steal it, they would not be able to gain access to it, so make sure you have everything that you can possibly encrypt would be a good place to start.

Michael Sanguily (00:56:42):

Then, secure your websites. There's also penetration testing for your websites, as well. If you have websites that have user name and passwords, you should have penetration testing done on them, as well, to make sure that information can't be taken out of your website. That's just some of your main defenses that you want to look at. At least that'll give you a good idea of where you should start, and you can write that down as a list and go area by area to make sure you're actually looking at those portions and that actually everything is updated in good standing. Next slide, please.

Michael Sanguily (00:57:14):

Strong passwords. People are doing a much better job nowadays with strong passwords, but we still do see some organizations with no password policies. You do want to have a password policy. If you ever need any type of policy, in general, you can google it half the time and find templates, and you can just use that template to structure it around your specific needs in your organization, so password policies. You could state that you should have at least 12 characters in your password with numbers and letters in there, and then special characters, and manage your passwords.

Michael Sanguily (00:57:46):

There's tools that generate and store and manage passwords. There's one called Thycotic, T-H-Y-C-O-T-I-C. It is a paid tool. I know is popular amongst enterprise level, and it'll just manage your passwords for you. It'll automatically generate new passwords after X amount of days, or there's different systems you may have implemented that could do this, but just make sure your passwords are being changed. Make sure your passwords are strong.

Michael Sanguily (00:58:12):

Then, with that combination, you want that multifactor authentication, also known as two-factor authentication. This is very critical. Everyone should have this to log into your systems. If you do have some type of remote access or applications you use that have critical information on it, you should have two-factor authentication, so if you log in, even if somebody steals your password, and they log in with it, it would send you a text or notify you through some type of app on your phone that somebody logged in, and you would have to approve them. Again, it'll protect you from those password attacks, as well. Next slide, please.

Michael Sanguily (00:58:47):

Preventing phishing and malware with network monitoring. Network monitoring can be a tough one. It is time consuming. It does take some expertise, but sometimes your firewalls may have these systems in place, where you can just go through the logs and look at them. Just because you have a firewall and it's protecting you, you still want to look at those logs to see where attacks are coming from, if you detect anything strange going on with your intrusion detection, so at least, like I mentioned earlier, if you see specific attacks continuously happening from certain IPs and certain countries, you can block that, so just to minimize that risk of them even being able to try to attack you.

Michael Sanguily (00:59:25):

You have your antivirus and your ad blockers. You typically should just have very strong URL filtering, so that users cannot visit specific websites, and tools built into your browsers to automatically block spam or anything malicious coming through. Then you have DNS security. This one's more of a technical topic, but there's ways for them to essentially change the website you're trying to visit. If you try to go to Google, it could redirect you to a different website. There's different, there's many tools out there based off DNS security, but your IT teams should just look at DNS security as an overall and assess that as part of your plan or your security risk assessment.

Michael Sanguily (01:00:06):

Lastly, but the one that we stress the most, I think it's the easiest and most cost-effective solution to minimize risk is security risk awareness. This is where you train your end users on that phishing, like I showed you earlier. You typically will phish your staff first, either if you can do it in-house or you have another third party assist you with the phishing. There's also tools out there that you can pay for. KnowBe4, I know, is a common security risk platform, where you phish your staff. If they fail, they take a five-minute course. If they fail again, they take a 10-minute course. If they fail a third time, they'll probably get a visit from their manager or HR Department, saying, "Hey, why do you keep providing your user name and passwords and putting our organization at risk."

Michael Sanguily (01:00:49):

Make sure you conduct your security risk assessments as often as possible. I would say at... I like to say, do your phishing on a monthly basis, if it's possible for you, so that your users just get into the flow of identifying phishing emails, because if you do it once a year, it may be a little tough for them to remember it the next year. Six months down the line, they may forget about it, so just do a training to everybody. I like to say that IT is not just the IT Department, or security is not just the IT Department. It's everyone, as well, because end users can cause breaches into your organization and also need to be trained. Next slide, please. So-

Arnel Mendoza (01:01:26):

I can't stress this enough.

Michael Sanguily (01:01:27):

Yeah, yeah, go ahead.

Arnel Mendoza (01:01:28):

A word in security awareness training, to us, this is our favorite thing, because the point I'm trying to make here is $30,000 you've spent on hardware and software, for firewalls, VPNs, to protect your network perimeter. All that just got rendered ineffective, because someone clicked on a bad link or an attachment in an email. A comprehensive security awareness program is approximately 5K for 200 users, so you do the math. Next slide.

Arnel Mendoza (01:01:57):

You always want a backup, backup, backup, backup. The best practice is the three-two-one strategy. Three copies of data: one primary, two backups. You want to keep your data, that two part, on two types of storage media, including the cloud. The cloud counts, and one of these should be offsite. Next slide. Michael, you want to take this one?

Michael Sanguily (01:02:22):

Yep. DMARC is part of email security and reputation. DMARC, in a simple way, basically authenticates that this is truly you sending out emails, so if somebody tries to spoof it, it would basically block it or notify you that your domains are being spoofed. That's maybe the easiest way to explain it. It's something that's part of your email and reputation that you want to look at. Once you have that, once you break out that security risk assessment plan, this should be a portion of it is reviewing email.

Michael Sanguily (01:02:52):

I didn't mention email encryption too much on here. I did see something going on in the chat about email encryption. That is very important. Most systems have email encryption built in. If you use Microsoft Office 365, there's email encryption in there. It'll automatically encrypt sensitive data, depending on the filters you set, so you could say, if I send over a social security number through email, it'll automatically encrypt that, so that no one can intercept that email and take that information.

Michael Sanguily (01:03:19):

Yes, you do want to implement your DMARC as part of your email review. You want to look at your email encryption, as well, and look out for any tools. If you're using email, audit your email system and see where you may be having a gap in security there, or you're missing DMARC. There's other ones called SPF and DKIM, as well, which is a little deeper, but your IT teams, your technical teams, can look into that to make sure your email's protected, because again, you could be subject to a man in the middle attack, if you're not properly implementing email security.

Michael Sanguily (01:03:49):

Then, audit your social media accounts. I mentioned that earlier. Hackers can just use social media accounts to gain information. Sometimes staff and employees may be posting things that shouldn't be on social media with information. Something that we saw some time ago, somebody posted on social

media a picture that they took of a computer, and that computer had patient information on it. Whether they did it on purpose or not, I'm not sure, but you could see the background of the information. You could see the person's social security numbers and lab results and all kinds of information, so always audit social media accounts, as well. Have some type of policy built around this. Again, you can google these policies, and they have some good templates out there that at least you can structure around your organization. That'll just assist you with maintaining a reputation online, as well. Next slide, please.

Arnel Mendoza (01:04:40):

By the way, about social engineering, can the threat actors find someone who is no longer part of your company, who might've left on bad terms? Oh, yes, they can, Glassdoor. What if they left a bad review? Can they be tracked down? Of course, they can. Would these guys be willing to work against the companies they're disgruntled about? Of course, they are. Again, another word about being aware of what's out there.

Arnel Mendoza (01:05:07):

Budget considerations are do it yourself or you're managed, right? Do it yourself means FTE/internal staff. There are lots of free tools and resources, but most have a learning curve to be used effectively. Managed means migrating to the cloud. I always say, if you're hosting your EHR, for example, you'd better have a large staff to support that. Myself actually, my organization, it's much easier to have that stuff managed. Next slide.

Arnel Mendoza (01:05:38):

The question is, how much cybersecurity is enough? The answer is another question. How much risk can your organization tolerate? And how much can you afford to lose? Then, the final word is about cyber insurance.

Michael Sanguily (01:05:53):

Next slide, please. Cyber insurance is a very important part. Again, it's an insurance policy to protect yourself from cyber attacks. It's something to always consider. Again, like Arnel said, how much can you afford to lose? Typically, you should always have a cyber insurance policy in your organization.

Michael Sanguily (01:06:12):

Sometimes people will think general insurance may cover you. You do need a specific cyber insurance policy that will have all kind of identifiers in there, as to what it's going to protect you, what you need it for, et cetera. There's lots of questions they'll ask you to build that around there, but I strongly recommend cyber insurance policies.

Michael Sanguily (01:06:31):

In case you ever are part of a breach, this can assist you when it comes to coming up with funds for the investigative work or the remediation work. They typically will have this built into the cyber insurance policy, where a team would be deployed to assist you with this breach and identifying where this happened. Typically, that would cost very large sums of money, if you needed somebody to come out there. Like Arnel said, one of those breaches had thousands of hours to remediate this breach and identify where it came from. Imagine having to contract a third party company for thousands of hours,

which can run you $250 an hour, so you can do the math and see that that can cost a large sum of money. A cyber insurance policy can help you with things like this. Next slide, please.

Michael Sanguily (01:07:17):

Getting cyber insurance right... Cyber insurance can be a confusing world if you haven't been in it too much. You typically want to run this by your IT leadership. They have questionnaires on there. You've got to always understand, general liability, like I mentioned, does not cover cybercrimes, typically, so you do need a specific cyber insurance policy.

Michael Sanguily (01:07:37):

There's a few things that I always like to note when you're looking at a cyber insurance policy. Ask your insurers to approve your preferred legal counsel and other service providers. They typically have their own specific third parties that can be approved for assisting you with any kind of breaches. You may have service providers you already like to work with. You can speak with your cyber insurer and ask them to approve that service provider, in case something ever happens, or again, your legal counsel, as well.

Michael Sanguily (01:08:07):

Invest time when answering the insurer's questionnaire. They usually give you a very large and very in-depth questionnaire. They want to know how much risk is in your organization, what you're doing and what you're not doing in your organization, so they know where to base their price off.

Michael Sanguily (01:08:22):

Now, everything we've mentioned before this, all these different security risk assessment plans, vulnerability assessments, end user training, all of that can help bring down your cyber insurance premium. If you're doing your end user training, if you're doing your vulnerability assessments and your annual penetration testing, you have a patch management program implemented, all the essential policies implemented, this can bring down the cost of your cyber insurance policy greatly.

Michael Sanguily (01:08:48):

Also, you want to be very honest on here, as well. They do want to know where you are missing a gap, so if something does ever happen, they can't go back to you and say, "Oh, but on here you said you had this protected, and you don't, so now we don't want to cover you." You do want to be honest on there. We have seen that cyber insurers will try to fight back on you and try to not assist you, as they can, if you did not put something that's honest on that application.

Michael Sanguily (01:09:13):

Also, pay close attention to the exclusions. Sometimes cyber insurance policies may not cover specific types of attacks. If you do need it to cover that specific type of attack, or again, if you do your own risk management and you want to make sure you're protected against this, add it to that exclusions list or tell them to remove it from that exclusions list. You do want to pay close attention to exclusions and read that in-depth.

Michael Sanguily (01:09:36):

Do not simply auto-renew your policy annually. Things change in your organization. If you're doing much better than you did last year, you can tell them, "Hey, now this year, I'm doing security awareness training. I'm also doing my own vulnerability assessment," so that can bring down your price. Also, things like exclusions may change in a cyber insurance policy year after year, so again, just always read it over every year and make sure that you're getting all your needs covered through that insurance policy, which can really help you out in case... Hopefully, you never do get breached, but in case you do get breached. Next slide, please.

Arnel Mendoza (01:10:10):

Oh, okay, so now we're into a tabletop exercise, just to make sure I know you guys paid attention. Olivia, you want to roll this one?

Olivia (01:10:21):

Sure. You all should see a Slido window on the bottom right-hand side of your screen, so please go ahead.

Arnel Mendoza (01:10:30):

What is the easiest, most common way to steal credentials? I'm going to give you maybe 30 seconds, because I'm going to give you enough time to do Q&A. Okay, so the vast majority of you did get it, phishing. That is the easiest, most common way to steal credentials.

Arnel Mendoza (01:11:10):

The very last question is for those of you that are non-tech out there. What is the first thing you should consider doing, if you've discovered you've introduced malware to your network? What do you think?

Michael Sanguily (01:11:35):

This one's a tricky one.

Arnel Mendoza (01:11:39):

I wanted to know how many people say call IT. That's why I put this up there. Yes, the majority of you said call IT, but if IT were not around, what you want to do is just turn off your computer.

Michael Sanguily (01:11:54):

Yeah, you immediately... The purpose of turning it off, you stop it from spreading into the rest of your network, so it's always a good way, to turn it off, and then call IT right away. Do them both at the same time.

Arnel Mendoza (01:12:03):

I like that one. Call your cyber insurance provider. With that, I think that concludes our webinar for today. Thank you everyone for joining. I know we do have questions.

Phillip Stringfield (01:12:16):

Thank you. That was a great way... Yes, we have plenty of questions for you all, so thanks again, Michael and Arnel, for that great presentation. I think it gave a lot of things for people to really think about.

Phillip Stringfield (01:12:27):

Before we get to questions, I also want to recognize all of the folks that have attended and have engaged in the chat. I think this was very powerful, sharing some of your previous experiences and also helping answer some folks' questions, as well, and what you do at your health center. It's definitely appreciated.

Phillip Stringfield (01:12:48):

I want to open up the questions and answers with a comment, and then a question. This is going to be for either of you all, so feel free to jump in. The comment was, "A traditional small IT Department in a community health center can't do all of this work." The question that is related is, "How can smaller organizations implement a cybersecurity program, and not all IT professionals have cybersecurity background or skills?"

Michael Sanguily (01:13:16):

I see this one a lot. This is where we step in and help FQHCs often because, again, it's not possible for everyone just to have their own cybersecurity team doing this all the time. One way I will say that you can start on your own, without a third party in the beginning, is at least formulating that NIST plan, like Arnel mentioned earlier, or some type of security risk assessment plan, so that you could at least identify the areas of risk that you have with the most critical portions.

Michael Sanguily (01:13:49):

If you do have some type of IT teams, let's say your highest risk is just some systems that are not updated, your IT teams could go in there and update it. But then, if you run into things like penetration testing or vulnerability assessments that you may need a third party, then you would probably need to reach out to third parties. I always say, look at other people in the nonprofit space, like HCCNs, because you can get far better pricing than some of these private companies out there to assist you with certain things.

Arnel Mendoza (01:14:15):

Absolutely.

Michael Sanguily (01:14:16):

And always mention that you're nonprofit, because if you're nonprofit, they typically will give you breaks, but starting with a security risk assessment plan will put you in a good place to at least understand where your risk is and move on from there.

Arnel Mendoza (01:14:27):

I'd also like to point out that, myself, I have four people in my IS group, four, so it's kind of a mix and match of what do we need to outsource versus what do we need to be able to do ourselves? Of course, you have to purchase subscriptions and tools and all of that stuff, but the management of those things, those are the things you're going to outsource. Hope that answered your question.

Phillip Stringfield (01:14:49):

Thank you, and then I just want to elevate what Michael said. Definitely want to make sure that your health center is a part of a health center control network. That would definitely be a great help. You might already be able to get some resources and support there, so I would start there, for sure.

Phillip Stringfield (01:15:07):

Okay, so the rest of these questions, we're just going to dive in, because I think it touches a little bit of everything here. It says, "What would you say to someone that feels the external email banner warning would just be ignored and/or therefore not worth implementing?"

Michael Sanguily (01:15:29):

I do know that one happens. A strategy we did to hopefully not get it ignored as often is we change it often. One of the things that we do is-

Arnel Mendoza (01:15:39):

Yep.

Michael Sanguily (01:15:40):

Depending on the time of year, like the season, we may change the colors of it. We always change it, so that it's something new that pops up into your view, so continuously changing it will keep it being newer to a person and keep them... Every time it comes up new, they realize, oh, that's right. I have an external banner. It always keeps it at the front of their mind.

Arnel Mendoza (01:16:00):

Like all social media strategies, fresh content gets the eyes.

Michael Sanguily (01:16:05):

Exactly, exactly.

Phillip Stringfield (01:16:08):

Awesome, so the next one is, "Is just the act of clicking on a link in a phishing email considered bad, or do you have to click, then provide sensitive information for the action to be considered a breach?"

Michael Sanguily (01:16:22):

Oh, this could go both ways.

Arnel Mendoza (01:16:24):

Yeah.

Michael Sanguily (01:16:24):

But just clicking on it already is putting you in a bad spot.

Arnel Mendoza (01:16:26):

It's bad.

Michael Sanguily (01:16:27):

Yeah, you don't, because it could also link you over to a website that already has malware on there, and it will just immediately try to inject that malware into your system. Again, if you don't have systems updated or proper antivirus in your systems, that malware could be injected into your system, so I know we've done that. We would count it failing our phishing test, if our FQHC is just clicking on it. We also know if they put in their credentials, but we do count failing as just clicking, because of the fact that it could direct you somewhere maliciously.

Arnel Mendoza (01:17:00):

Also, not just that. It could introduce a bot into your network, right? I showed you, the bot can stay in your network and be hard to find for a long, long time, until somebody decides to activate it, so yes, it's bad.

Phillip Stringfield (01:17:18):

All right. Okay, so, "As more people work from home, how important is it for them to secure their home routers? What if folks feel that it is too invasive to have work tell them what to do with their personal router? How often are routers hacked?" It's like a three in one.

Arnel Mendoza (01:17:38):

Often enough.

Michael Sanguily (01:17:41):

It does, so what we like to say is think of it as you're also protecting yourself. It's your home router.

Arnel Mendoza (01:17:49):

Yeah, it's your home router.

Michael Sanguily (01:17:50):

Right, if it's your home router, you want to protect yourself, as well. Take all the tips that we can give you to help reduce risk in your own house. Make sure your systems at home are also updated. Make sure your antiviruses at home, make sure you're using your VPNs to secure your connections. You've really got to think about it just the same way an organization thinks about it. I think, I really would not want my house to get hacked either, so you have to protect everything.

Arnel Mendoza (01:18:14):

I can tell you, for my organization, we have a telecommuting policy. That's an HR policy. There's specific things that are required before you... You have to work from home, but you have to have these checklists done, including securing your router, including even making sure the bandwidth is adequate for all the amount of work you do, for specific amounts of work, so we have that kind of a policy.

Phillip Stringfield (01:18:42):

This question I think you all touched on, but I wanted to just go ahead and throw it out there. It says, "How risky is it to use a password manager? Have the password managers ever been hacked?"

Arnel Mendoza (01:18:57):

The answer is yes.

Michael Sanguily (01:19:00):

Yes, it could be risky. This is where you have to do your own risk management. I know people have their mixed feelings with password managers, that they can be hacked, as well. It's still sort of the standard to use a password manager. You could always use your own local password manager that doesn't have to be cloud-based, and have that encrypted, as well.

Arnel Mendoza (01:19:21):

That's right.

Michael Sanguily (01:19:22):

I still typically would recommend using password managers, because what I've noticed, it introduces more risk, because you're not going to memorize hundreds of passwords across different websites. If you have a tool memorizing it for you, at least you'll be more enticed to change your password, or have a different password on different systems. It does come with its risks, as anything else, but I feel it could be less risk, depending on your situation.

Arnel Mendoza (01:19:48):

It's much less risk to do that than have somebody posting their password on a post-it on their screen.

Michael Sanguily (01:19:55):

Definitely.

Arnel Mendoza (01:19:55):

I'll just leave it at that.

Michael Sanguily (01:19:56):

Yes, definitely.

Phillip Stringfield (01:20:01):

I think this question might be a little bit more specific. It says, "Can denial of service attacks happen if we are on the cloud?"

Michael Sanguily (01:20:11):

Yes, they definitely can.

Arnel Mendoza (01:20:14):

Yeah.

Michael Sanguily (01:20:14):

You've got to think of the cloud as they're just basically... Instead of you having your systems hosted in-house, they're just doing it for you, so there's still just as much risk. You still want to make sure you implement all the proper tools to reduce that, those denial of service attacks, so it does not completely remove you. It's just basically somebody else holding your systems for you and doing the physical labor of it.

Phillip Stringfield (01:20:39):

Okay, and on that note, it says, "We work with an IT consultant company for our managed IT services. They manage and monitor our network. Should we have the penetration test done by them or a third party?"

Arnel Mendoza (01:20:57):

I would say no. I would say you need to go with a third party.

Michael Sanguily (01:21:01):

Absolutely.

Arnel Mendoza (01:21:01):

Chime in, Michael.

Michael Sanguily (01:21:03):

Yes, absolutely, third party. You always want somebody who is-

Arnel Mendoza (01:21:07):

Not familiar with your system.

Michael Sanguily (01:21:09):

Right, and also a conflict of interest. You want to make sure, because we've done penetration testing for organizations, FQHCs, who have an IT managed system, and part of the reason why they're having us do it is because they want to make sure their IT managed team is properly managing their system, so they want somebody else to sort of fact-check them to make sure everything is being taken care of properly. That's why it's important, also, to have another, a third party, for your penetration testing.

Phillip Stringfield (01:21:39):

Awesome. Okay, well, I think you kind of just answered this question. I'll just throw it out there, anyways. It says, "What are your recommendations or stances on performing your own penetration test, rather than outsourcing? Is this good to do, alongside a third party penetration test?"

Michael Sanguily (01:22:03):

Yeah, if you have the capability, absolutely do your own penetration testing. We do it ourselves. We have a full cybersecurity team, and we also have a third party come alongside and do it for us, as well. Even with our vulnerability assessments or anything else we can do, it's always good to get a different perspective, and see if you're missing anything, as well.

Phillip Stringfield (01:22:24):

Awesome, so last couple of questions here in our last couple of minutes. Thank you for bearing with us. It says, "I noticed you didn't mention network segregation under maintain your defenses. Do you not recommend it? It was VLANs provides network segregation."

Michael Sanguily (01:22:50):

Definitely recommend it. It's just, there's so many aspects here that you can cover, that there's no way we can cover it in an hour and a half, but network segmentation is very important, just to prevent if somebody does get in one part of the network, they can't reach the other. Actually, WiFi is one I'll mention very quickly, is you want to make sure you have a guest WiFi for your guests that's completely separated from your network, so if guests are coming in with their devices that maybe have malware or are doing who knows what on their systems, it will not translate into a breach on your main network. Network segmentation is very important.

Arnel Mendoza (01:23:25):

Absolutely, and it also depends on how you're physically configured. We have five locations, so you might want to go that direction or however way you want to design how your data flows. Again, that could be a topic in and of itself.

Phillip Stringfield (01:23:41):

We're down to our last couple of questions. "How important is 24/7 monitoring, using something like Arctic Wolf, especially for organizations that are not open 24/7?"

Michael Sanguily (01:23:57):

You may not be open 24/7, but hackers are open.

Arnel Mendoza (01:24:00):

But the threat... Yeah, exactly. Threat actors are open 24/7.

Michael Sanguily (01:24:04):

They are. Your systems are still online. Your systems are still connected to the internet. If it's within your budget and your risk management, it's a very good thing to have 24/7 monitoring, especially when you think about some other countries that may be performing hacks on the U.S. Their time zone is morning for them when we're sleeping here, so a lot of the breaches, a lot of the attacks we see, we get flooded with bots in the middle of the night, and that's why it's good to have that 24/7 monitoring. You don't want to come into work at 7:00 a.m. in the morning, to know that you've already been breached, so it's good to have, if you can.

Phillip Stringfield (01:24:43):

All right, and then I'll leave the last two minutes, just to ask this open-ended question, and then you all can add any last tidbits for the group, but what would you say for folks that would say, after hearing you all, just saying, "Well, we don't have the staff to do it," or, "We don't have the staff that is trained to do it"? What would you say to those folks, just in order to really build upon their culture of cybersecurity?

Arnel Mendoza (01:25:16):

You have to start with the basics, like I said. You need to know what your risks are, and so you do that assessment. That kind of helps pinpoint where your weaknesses are, and at least be able to do that. It also gives you some kind of awareness about what needs to be important in your organization. From that point, you can work with your executive management to get more budget or more resources in order to expand your posture. Michael?

Michael Sanguily (01:25:44):

Right, right. No, exactly what Arnel said there. One of the areas where we've worked with FQHCs is they say, "We know we have issues out there, and I want to stress the importance to my executive leadership, so I can get the funding." Then, when they do that plan, that risk management plan, and they identify some critical areas, it strengthens your argument as to why you need a specific budget. As Arnel mentioned, reach out to your HCCNs. Those are typically going to be the most helpful for you, as far as when it comes to pricing or assistance. That will reduce your costs, as well, which could help you out.

Arnel Mendoza (01:26:21):

Show them this presentation.

Michael Sanguily (01:26:23):

Exactly.

Phillip Stringfield (01:26:24):

Yeah, it will be... Yeah, awesome, awesome, awesome. That's such a great way to end it. We're right at time. I want to thank, again, Michael Sanguily and Arnel Mendoza for this great presentation. Folks, if you did not have your questions answered, you can always email them directly. You have their emails on the screen, but we will also be back next week, right at this same time, from 2:00 to 3:30 p.m. Eastern Time with part two. We definitely hope you're able to join us. We ask that you please complete the evaluation that you'll receive, once the session ends, and we will make sure to get these slides over to you, and the additional resources that were mentioned in the chat today. Thanks again. Looking forward to next week, and have a great rest of your week. Thanks again, everyone.

Michael Sanguily (01:27:11):

Thank you, everyone.

Arnel Mendoza (01:27:12):

Thank you, everybody.