Philip (00:00:01):

Awesome. Thanks so much, Alyssa. And thanks everyone for joining in. Looks like we already have a little over a hundred participants in our session today, so I'm definitely glad to be with you all. As we get started, I want to just of course, start with putting in a plug for our NACHC hosted EHR user groups. These user groups, they meet on either a monthly or quarterly basis, and they are also led by Health Centers, HCCN's and PCA leaders. So if you're interested in joining either of those groups, I'm going to go ahead and put the link in the chat. So that way you're able to visit your respective provider. And you're also able to register for the user group to receive our emails. If you have a specific question on any of those, you can always email me PStringfield@nachc.org. Next slide, please.

Philip (00:00:51):

And without further ado, we're going to go ahead and dive right into part two, looking at cybersecurity risk and preparation. We have with us today, Arnel Mendoza, who serves as the director of information systems with QueensCare Health Centers. And unfortunately we will not be having Michael Sanguily with the Health Choice Network with us today. He is a bit under the weather, so we do wish him well, but we will go ahead and keep things rolling with Arnel. So without further ado, I'm going to go ahead and hand things over to Arnel to get started. Thanks again, everyone.

Arnel Mendoza (00:01:26):

Hello, NACHC. If you're on the West Coast, good morning, where I am. If you're on the East Coast or somewhere in the middle, good afternoon. So today, we're going to be going over how to quantify risks in your organization. We're going to have some practical exercises to know what to do when, not if, a data breach happens and how to promote a culture of cybersecurity awareness in your organization. Next slide. So this is actually like I said, part two of a two part cybersecurity webinar series. And in the first part, we talked about infrastructure mostly. We talked about how a basic infrastructure protects, a good infrastructure enables and a great infrastructure innovates. So we covered the first part last week. Next slide. And we went over all of these cybersecurity best practices. We went over what a basic infrastructure is supposed to do.

Arnel Mendoza (00:02:29):

And I showed this slide, cybersecurity best practices, people, technology, and processes. And if you hit the enter key, this is what happens usually. So what I addressed was a disconnect between executive leadership and technology leadership. I'm one of you, I'm a tech leader. I'm director of IS at QueensCare Health Centers. And this is what I often get when I kind of geek out a little bit and talk about cybersecurity from executive management, because I addressed last week. There's a disconnect still, although they're aware of all the data breaches going on, what to do with it, not so much. Next slide.

Arnel Mendoza (00:03:13):

So again, in part one, we talked about dumbing it down a little bit and I presented as cybersecurity toolkit. Essentially, it's sort of a framework on what to spend or at least what the basic infrastructure was supposed to look like. It was supposed to go over these six items. You're supposed to know what you have. You have to update your defenses, go beyond simple passwords, preventing phishing and malware, backup and recovery and protecting your email and reputation. And we went over some tool sets that fell under these categories. Next slide. Talked about spending for cybersecurity. And if you can see in this slide, this was based on a HIMSS cybersecurity survey. Last year, you can look at the box here.

1% of organization in HIMSS, mind you, this a healthcare organization, no money is spent on cybersecurity.

Arnel Mendoza (00:04:05):

One to 2% said 18% of their budget, IT budget is allocated to cybersecurity. Three to 6% about a quarter, seven to 10% about 10%. The majority of it is under the 23%, I feel, where money is spent in cybersecurity, but no specific [inaudible 00:04:26] outs in the IT budget. So they're doing firewalls, they're doing all of the perimeter defense stuff, but not really categorizing it as part of cybersecurity budget. And I'm going to go over why that's a little bit important, a little bit. 18% don't even know. That's a little concerning too. As far as total budget kind of depends on organizations, but in the healthcare space, we're talking specifically less than 10% at least. Next slide.

Arnel Mendoza (00:04:57):

A word about budgeting, and this we covered a little bit last week too, when you're talking to vendors, always use the magic words "nonprofit pricing." Always look for free or significantly discounted resources. We talked about Nessus, which is free for vulnerability assessment solutions. You can see on the list here, monday.com, there's a product for nonprofits. Salesforce has a product for nonprofits, Microsoft 365, again, nonprofits, Google for nonprofits is free. Mobile Beacon is a wireless solution. That's free for nonprofits. On the right side, on the right column, we have CISA, that's the government information security group. They have vulnerability scanning. All you do is register and basically ask for help. Prey is a device tracking and protection tool, CloudFlare, Universal SSL and GRR Incident Response Framework. Next slide.

Arnel Mendoza (00:06:00):

If you go to CISA, that's a cybersecurity infrastructure security agency, they have a lot of free tools actually, and I'm not going to go over them here. I just provided the link to the website because there's quite a bit and there's quite a bit of categories. Again, a great resource for figuring out if you have anything you can do for free. Next slide. So what do we do first? So last week again, we talked about, if you want to know what to spend on for cybersecurity, you must first determine where you're most vulnerable. You must first figure out where your gaps are in order to determine what money where you going to spend. Next slide.

Arnel Mendoza (00:06:48):

And when I'm talking about determining where you're most vulnerable, I'm really saying you need to find a way to quantify your risks is what I'm actually trying to say. You need to find a way to figure out how to measure your risk in terms of a language that you'll be able to communicate, that'll translate to a spending budget. And it doesn't have to be all that complicated. This is a basic assessment I found on a web and essentially just asks you about eight questions. Do you have a written security policy? Are your employees in management given security awareness training? Do you have a documented data inventory? Very, very important. And based on your answer, this doesn't necessarily quantify it and you can ignore the last question there. The reason this is free is because they're obviously trying to pitch their product, which is something called Enterprise Data Defender.

Arnel Mendoza (00:07:43):

But if you've at least gone through it, it gives you an idea of where your gaps are. So these are the most important points. So if you're not doing security awareness training, or in my mind, if you're only doing

an annually, that's not sufficient and we'll go over why. If you're doing a data inventory and if it's not current, that's a gap. So a lot of these things, you're going to just do this basic assessment and they don't necessarily translate to tool sets that you need to buy. A data inventory or a device inventory even, that's not really ... You can buy a tool for that, but typically it's more of process and a policy. So it should be part of your basic policy as an IT group to do data inventory and to do device inventory. Next slide.

Arnel Mendoza (00:08:35):

So I'm going to geek out a little bit because I'm going to need to go from a very, very high level to really the science of quantifying a risk and for the science of risk management, I'm going to throw out these terms. It's risk, it's loss frequency, it's loss magnitude, threat event frequency. Don't worry. I'm going to dumb it down. I promise. It's vulnerability. It's primary loss and it's secondary loss. You don't need to remember anything. I'm just going to need to have something to tie my next couple of slides to. Okay? Next slide. The parameters. So when you're quantifying your risk, you're really talking about assets. And an asset, basically, I hate to sound like the CIA here or something covert, but an asset is just basically something you own. So it could be a database. It could be a system, it could be a physical facility.

Arnel Mendoza (00:09:32):

It could be your employees. It could be supplier relationship. It could be your devices. So that's an asset threat obviously is an agent that can act against these assets, which would result in a loss. So that could be your hackers, your rogue employees, natural disasters. It could be something as simple as a failing hard drive. It could be a bug in your software. And the effect is obviously what happens after there's a threat in your asset. So it could be a loss. So it's resulting from the successful action of the threat is your loss of money, your loss of data availability, there's physical property damage. And one thing that's not necessarily talked about is the loss of reputation. Okay? So when you're preparing for scenario, like it says here, the threat would to successfully act on the asset to produce the effect, the organization would experience loss. Security risk quantification would determine the parameters of the loss. So next slide.

Arnel Mendoza (00:10:38):

So last week we talked about a framework that, again, it's going beyond the basics that I just went over a couple of slides before and the most common one, at least the most prevalent is NIST cybersecurity framework. That's a National Institute of Standards and Technology. And I'm going to go over it a little bit because I think it's really important to have somewhat of a framework to go beyond just those basic questions. Although I will show you in a second, this really boils down to a bunch of questions too. So when you're talking about the NIST cybersecurity framework, for those that are not familiar with it, you're talking about basically five functions. You identify and that's basically, we've talked about assets. You identify those assets. You outline how you safeguard those assets, which is under to protect function.

Arnel Mendoza (00:11:31):

You do detection, which is how you detect threats to those assets. You respond which is how you respond to the threat and then you recover. Those are the main functions. Again, there are only five. Next slide. But within those slides or those functions, there are categories. So within identifying, which is identification of your assets, there's asset management, the business environment, governance, your risks, even your supply chain risks. So those are just the categories under the identify function. And then under that category, there's subcategories, as an example subcategory is under asset management. So

do you identify your devices is one subcategory. So in the end, you're talking about five functions and you see on the table here, how many categories there are in each function, and then how many subcategories are within each category? You add them up, you get 108 total subcategories.

Arnel Mendoza (00:12:35):

Those are a number of questions that you have that you will need to answer in order to provide you with a good idea of where you are in terms of cybersecurity posture. If you go to the next slide, there are assessment tools for the NIST for free. Again, there's all these online one from Cipher and one from Expel. These are spreadsheets that you can download. They basically give you a list of the questions. If you go to the next slide, even Office 365, those of you that have Office 365, if you go to their security admin page, it has NIST governance tool. It's exactly the same thing. Basically, they're asking you a lot of questions and they give you a reference to the control, whether it's NIST, whether it's HIPAAs, you can see there, whether it's CSA, whether it's High Tech, whether it's ISO.

Arnel Mendoza (00:13:35):

So it's a nice roadmap, if you will and a cross mapping of all of these controls that, and in the end, we're supposed to be responsible for. And when you answer to questions, it gives you a compliance score as you can see there. So you can see even in Office 365, although it's limited to all the activities you do with an Office 365, if you're like my organization, we're heavily invested in Office 365 and all of the tools suites within it, gives you already a pretty fair view of your cybersecurity posture using that framework. If we go back to those spreadsheets though, next slide.

Arnel Mendoza (00:14:18):

This is from the Expel one, or is it Excel? Essentially again, it's boiled down to questions. So you can see here, the subcategories on the left, and then the questions or the categories on the left and the subcategories on the right, in the spreadsheet that's asking you questions. You're supposed to self score from zero to five, zero meaning we don't do this thing at all. And five, meaning we're God's, definitely stay best in class. Most people are somewhere in the middle. Again, you can see some of the questions that you go over here. Remote access is managed. So that's a zero to five, whether you manage it or not, if you don't, it's zero, if you do it well, do a five or is network integrity protected and is your networks segregation happening where appropriate. So again, there's over a hundred questions, but not that many. Again, you can go over this in a couple of hours. If you're fairly diligent, if you just sit down and actually do the work, you can definitely get it done in a day. And then the result is, next slide.

Arnel Mendoza (00:15:32):

You kind of get a heat map of where your biggest vulnerabilities are. So an example weaknesses is I went through the spreadsheet and I purposely scored at low on subcategory 10, which is your response in recovery plans. So the question was, is your response in recovery plans tested and purposely, I said no. So you can see on the heat map that on IP-10, it's closer to the center, right? So on the heat map, you can just focus on the ones that are closest to the center. And those are the areas where your weaknesses are already. And those are the ones that typically you're going to be wanting to either address the gap by shoring up your policy, and typically having some kind of spend. So this is kind of a good guideline as to where your spend is supposed to go. I thought it was pretty effective actually, when we've gone over with my management, in terms of going over this, our gaps in vulnerabilities, it was able to explain to them what they were based on a framework, which is actually your biggest advantage with using these kinds of tools. Next slide.

Arnel Mendoza (00:16:51):

Now, what the pros use. Now, if you were to hire somebody to do this for you, they would use a methodology called FAIR, which is Factor Analysis of Risk Information, or Information Risk, sorry. It's globally recognized. It's a model that codifies and monetizes risk, and it breaks down risk by identifying, defining building blocks, again, that make up the risk and how they relate to one another. The relationship between each building block or element of risk is measured mathematically. And actually there's an algorithm and a dollar value that's tied to that algorithm. It'll go over it in a minute. Not that you have to hire somebody to do it, and I'll show you why in a second, but essentially it helps you calculate potential risk in terms of financial loss exposure. Okay, next slide.

Arnel Mendoza (00:17:38):

Why is this important? Again, I'm a technology leader, so for you technology leaders out there, you must learn to speak the language of the C-suites and that's in numbers and that's in dollars. And that's how it relates to the budget. The budget is essentially just a priority list of what you need to spend on. You can't spend on everything, but you do need to identify what the most important things you can spend on are, and this will help you do that for the C-suites. This also is a way to meet your technology leaders. When they're kind of like what I just did in the last couple of slides, kind of geeking out a little bit so that it's a common language reference frame, right? Next slide.

Arnel Mendoza (00:18:25):

For the fair tool, it's actually free as well. I'm giving you the website right down here. All you do is sign up. Now I will warn you. You will sign up and it's very technical and it's going to require some. There is a little bit of a learning curve, to be sure, although there's some videos that they will show you also on how to use the tool. How it's supposed to work is, if you go to the next slide, so I got myself an account and here's what it looks like. And believe it or not, the professionals use this. So the example I'm using here is a phishing database breach, right?

Arnel Mendoza (00:19:06):

And if you look at the inputs on the left, I'm saying the question is how many times over the next year is this likely to occur? And I'm saying the minimum one, most likely two, maximum three. Now we've been over last week in part one, most of the time, over half the cases in all organizations, you're already in the middle of a breach. You don't even know it because you won't discover it for many, many months after you've been breached. So these are very conservative numbers. And if you can see here, what it does, it has an algorithm and it did a calculation. So the results were at the minimum of one phishing breach your minimum for the kind of organization you are.

Arnel Mendoza (00:19:53):

And in terms of my organization, I can tell you, we had, in terms of size, we saw 25,000 patients last year, and we did 125,000 visits. So that kind of gives you an idea of breadth and size to where we are. We have about a little over 300 employees. So the minimum financial risk that I'm looking at for one database breach is about $6,600. The average's $8.8 million. And that actually jives with some of the numbers we talked about again, which is the average in healthcare as of 2021, the average loss for a healthcare breach is nine million dollars, which is up 30% from the year before, the single largest increase of any industry by far. So healthcare is really, really taking off in terms of who's getting breached the most and the worst actually. So that 8.8 million is pretty right on. Next slide.

Arnel Mendoza (00:21:01):

And if you do hire somebody, this is what you end up getting. It's kind of the gold standard. They break it down into risk categories. They give you monetary loss in terms of what these categories are, what they mean, and a typical roadmap initiative, which is actually to me, the most important part, because it's one thing to measure your loss, but again, tying it back to the NIST Cybersecurity Framework, you need to figure out what tool you can do to tool, if any, you would need to spend on in order to mitigate that risk. So if it's insider access and you have to use multifactor authentication, if it's endpoint security, well, you need to spend a tool on endpoint detection. And again, all these tools now have different ranges of capability. Before, for example, endpoint detection, we talked about anti-virus software really.

Arnel Mendoza (00:21:56):

And the old school anti-virus software for those that remember, they relied on definitions, right? So you have to actually be updating definitions often, at least every month. These days, the most modern versions of antivirus software relies on something called heuristic behavior, which is a way to even actually use a bit of artificial intelligence to determine if a certain behavior in your system looks like it may be malware activity, and it will react to that. So again, obviously if you're just still using virus definitions, it's going to be on the cheap end of the scale. If you're using the more advanced functionality function software, it's going to be on the higher end of the scale. Next slide.

Arnel Mendoza (00:22:47):

So where does the data breach start? Well, according to this study, again, this is based on the HIMMS cybersecurity survey. If you hit enter, maybe next slide, it's email. 89% of all security incidents start with email. And if you look at the aftermath of it, you can see there from the survey patient safety issues caused by significant security incidents, disruption of non-emergency clinical care is 61%. If you're in FQHC, that's us, non-emergency clinical care. Disruption of emergency services, 28%. Serious patient injury or harm 17%. Diversion of the patients to other facilities, 17% and cancellation of elective surgeries, if you're a big hospital or inpatient facility, 17%. The fact that there's even a percentage at all already points to the seriousness of this that you can bring to your executive management team to say, "Yeah, we really do need to address these gaps." Again, addressing that gap between what the executives know and need to act on and what you know as a technology leader. Next slide.

Arnel Mendoza (00:24:07):

Some phishing statistics, according to Cisco's 2021 Cybersecurity Threat Trends, again, 90% of data breaches occur due to phishing. Phishing is when you get an email and they try to get you to click on a link or an attachment, and it introduces malware into your network. According to Verizon's 2021 Data Breach Investigations Report, 85% of breaches involve the human element. And that's where we're going to focus on right now. Next slide. Because the human error factor can't be understated. There's unintentional human error, which is the lack of knowledge, or just because a human is distracted, essentially. Intentional human error is the human knows of the potential risk, but is reckless, again, due to distractions. Malicious is when it's intentional and they know that there's going to be damaging consequences and they do it anyway. And that cannot be understated too, because again, that could be some person that is disgruntled with your company that simply doesn't care, that wants to get even, and who among us doesn't know of anyone like that. Maybe nobody. Just kidding. Next slide.

Arnel Mendoza (00:25:32):

Next slide. This is just basically a slide that talks about that last slide again, unintentional human error, which we're going to be focusing on in a little bit is mainly lack of organized knowledge of operating skills and intentional human error knows the risky behavior, but acts on it anyway, or misuses assets. May not necessarily bring sudden harm to the organization, but it still causes a breach. Next slide. What do the click cost? Again, from this report of Sophos State of Ransomware in 2021, the average ransom paid by mid-size organization was 170,404. While the average cost of resolving a ransomware attack was 1.8, $5 million. So what did this cost include? It includes not only downtime, but people time. You're not able to see your patients.

Arnel Mendoza (00:26:40):

You have device costs, obviously, because you need to remediate those devices that were attacked. You have network costs, you have lost opportunity. You paid your ransom and then your insurance premium, your cybersecurity insurance premium goes higher. And again, what doesn't get measured is the loss of reputation. It's almost like in my mind kind like when you strain an ankle, right? Is it really the same six months later still? You kind of still feel it. I have a fellow FQHC in the Los Angeles area where I'm at and they experienced a ransomware attack very recently. And when I talked to her, this was a good seven or eight months ago to this day. Although they remediated within a month, they still lost a whole week of not seeing patients. And to this day, they're still kind of thinking they still need to do some forensics because you never know anymore. And you're a lot more careful. So the actions that you will do, will be more towards cybersecurity than anything. Next slide.

Arnel Mendoza (00:27:53):

I'm going to geek out a little bit here for the next couple of slides, if you'll just indulge me because what it's going to boil down to is really, really hard to get people to pay attention in terms of phishing emails. Why do people click? Little brain science. The emotional brain is both quicker and stronger than the logical brain. Emotions like fear and urgency sidestep the frontal lobe and smack is right square in the amygdala. That's the area in your brain that triggers a fight or flight response. That's the area in your brain that signals there's danger, right? So this is brain science. Next slide.

Arnel Mendoza (00:28:36):

So when you're a hacker and you're trying to get access to your information, they'll introduce a psychological stressor, say, in the former threatening email, right? So in this example, your PayPal account is limited. Solve 24 hours. That's kind of giving you psychological stressor, right? It's kind of that you need to do something right now or this threat will continue or something bad will happen. That's what the hacker is trying to get you to do, even though you may or may not even have a PayPal account, still the fact that you're getting introduced to this kind of a psychological stressor again, it bypasses the logical brain and it gets right to your emotions. You're going to have some kind of reaction. Next slide.

Arnel Mendoza (00:29:24):

Other brain hijacks. So the reverse is also true. Humans have been found to have similar reactions to surprise rewards, believe it or not. The anticipation of a reward. So again, some brain science, a pleasure center of the brain called the nucleus accumbens, not going to test you on this, is highly activated by the possibility of receiving a reward. Next slide. So this is an example of an unexpected reward. You get an email, you have an unexpected tax refund online to the amount of $420. So whether or not that's real or not, you're going to have some kind of reaction. Again, it's bypassing your logical center and it's going right to the emotions of it all. Next slide.

Arnel Mendoza (00:30:16):

So when emotions take over people click and it could be due to several different kinds of emotions. It could be stress. I'm too busy. I'm preoccupied. It's fear. Do this now or else. If you get an email like that, to me, that's already kind of a yellow flag, if you will, that this email, you probably need to not do something immediately. Overconfidence, you could be an IT person, overly optimistic at your ability to recognize a phishing email. But again, these phishing emails are meant to go beyond your logic. And it's meant to go to get you to do an emotional response. It could be greed, the unexpected reward factor, and it could be based on hierarchy and authority. People tend to comply with request some authority figures, particularly if it's someone in your organization. Next slide.

Arnel Mendoza (00:31:15):

The power of authority. This is a true example. This person here, Eloisa is my CEO, and she's supposedly sent me this email. "I need you to go to the nearest store and make a purchase of 10 visas and MX cards at $500 each." And well, we're going to be doing some kind of staff thing that, don't worry about reimbursement. We'll get you to do it. And again, your logical brain, looks at it and says, "Why is she emailing me from Gmail? Why does this say staff mailbox 00911? Why does she even need a gift card for me? She has a administrative assistant. Why did she come to me?" All logical stuff. Right? But I did have to for a split second there, think about it and almost kind of like, "She wants me to get gift cards for staff. That's great." Again, it bypasses your logical brain goes right to your emotions.

Arnel Mendoza (00:32:12):

Next slide. What are the top phishing email subjects? Password check, very, very, very common, 43%. How many of you have gotten a delivery attempt was made by FedEx and you need to pick up your package immediately, or at least click on the package, click on this link that says that you've got this email? 9%, which I think it's higher than that actually. De-activation of emails, again, trying to get you to do something because it's a threat. New food trucks, that's a reward. Updated employee benefits, this is a very common one in my organization. Same thing with the next one, revised vacation and sick time policy HR phishing emails are pretty common because again, they're usually about a subject that is very common in organization that affects everybody like employee benefits. And if it'll affect you personally, vacation and sick time, that affects you personally. So again, that you're typically thinking this is very important of the authority figure. You have a new voicemail, new organizational changes, again, change order password required immediately. Next slide.

Arnel Mendoza (00:33:29):

So how do you cultivate a culture of cybersecurity awareness? In my opinion, a one hour training given annually is not enough. If you're trying to train somebody to not click on an email, do you really feel a one hour training is going to work? I don't. A couple of cybersecurity awareness is something that is cultivated by repetition. You must train like a ninja. What does that mean? Next slide. Single most important skill you need to train people on. Hover over a link. Single most important skill, because that is the basis of what people are going to get you to try to do is to click on an attachment of a link or a link. If the email appears to be coming from a company, these are the questions you have to ask. Does the hover link match the website of the sender?

Arnel Mendoza (00:34:22):

Does link have a misspelling or if it's specifically, if it's a well known website, look at that example, micorsoft.com. Need to pay attention to these things. Again, your brain will see Microsoft. Does the link

redirect with suspicious external domain appearing to look like the sender's domain? A very common one is something-support.com rather than something.com. So if it's a very common domain, like let's say Google or Adobe, you're going to get a lot from adobe-support.com. There is no such thing. Does that hover link show in a URL that does not match for the context of the email claims it will take you? Do you recognize the links or address or did you even expect to receive the link? So again, a lot of these things from delivery, phishing emails or things like that again, I know in the world of Amazon, we all get deliveries and stuff, but really, you really need to think about it. Did you receive a blank email with long hyperlinks and no information as context? So you're going to get a long hyperlink and nothing else. That should be a yellow flag already, right? So again, single most important skill, get them to hover over a link. Next slide, please.

Arnel Mendoza (00:35:48):

The other single most important skill, the pause. Again, we're going to the brain hack, the brain hijack that we're talking about. The research shows that it takes at least six seconds for the brain chemicals, talk about brain chemicals here that cause the brain hijack to get you to do something takes about six seconds for that to diffuse. So the next biggest skill that you want to have people learn is to simply pause. Again, that's very difficult to get people to learn, but that's the kind of training you need to focus on. And again, that's not something people are going to learn typically on an annual training for an hour. Next slide.

Arnel Mendoza (00:36:30):

So good email anti-phishing hygiene, assume there's something fishy about every link, every single link and every email. In this day and age, I would agree with that. You have to pay attention. You have to look at what the email is trying to get you to do. You have to look at how it's trying to get you to do it and remember the six second rule. Next slide. So in terms of security awareness, I'm putting up their platforms. Because again, when you train, the idea is you can't train once a year. You have to train constantly. We train once a month and I'll go over that in a little bit and these platforms help you to do that. You can do it yourself too, if you have Office 365. The challenge there is you not only have to create the emails yourselves and deploy them, but you also have to look at the results.

Arnel Mendoza (00:37:24):

You have to look at who clicked on it, what they clicked on, because that's basically how you want to run a awareness program. And again, although people might not think this is important, what I did bring up last week in part one was that you can spend $30,000 on a firewall solution or network perimeter defense, or anything that monitors all of that stuff, thousands and thousands of dollars, but all of that stuff just got rendered useless because somebody clicked on one link on an email. All that's useless, because they just got into your network. So to me, typically for the size of my organization, five to six scale on something, one of these platforms that's a good spend in my opinion. So there's your best in class, KnowBe4, your Ninjio, your Infosec. Ninjio, if you want to look in YouTube, which is out content, just so you can see what they're like.

Arnel Mendoza (00:38:29):

And they're basically three to four minute segments, video segments are animated. They're pretty entertaining. And I use those too, because they're already on YouTube. So it's for free. Show them. Typically, you can look at one on ransomware and it's very effective at showing or at least bringing awareness to what the problem is. In my mind, again, it's more towards bite size chunks. So you want to

train small sizes and repeatedly. So not one hour trainings, but very short trainings often is what works. That's the only way you're going to get people to train on pausing and learning to hover over a link and actually getting good at that. Next slide.

Arnel Mendoza (00:39:18):

So what we do in my organization is we do the test monthly. The clickers, again, the value of having a platform is you can find out who the clickers are and automatically have them take an online training class, automatically notified the supervisor and they'll get reminders, if the staff does not complete the training. So even the supervisors know who the clickers are. And so it's not just the clickers themselves. It's also becomes pervasive in the organization. If you knew who your direct reports are that are clickers, then you're likely to kind of bring it up. And essentially this also becomes part of our perform performance evaluations.

Arnel Mendoza (00:39:59):

If there's somebody that does this more likely than not, then it becomes part of their perform performance evaluation. And that's essentially how you do the culture. We do targeted mini trainings implemented for groups identified as high risk. So like an example would be if there are MAs that have been with the company less than six months or the users have clicked on three times in the past year, we'll do some targeted mini trainings that not an hour, but maybe for 10 minutes and then do a class again. The idea here is just again, small bite size chunks over and over and over. Next slide.

Arnel Mendoza (00:40:39):

So this is actually real. This is how we track. It's a monthly tracking of what our Phish percentage is. So in the month of March, for example, we sent out 368 emails. Eight people clicked on links. So the Phish percentage was 2.2%. When we started this, this was two years ago, it was 35%. So over time I'd say it took a good nine months to a year before it started really going down appreciably. So again, over and over, this has to happen to make it part of your culture. And now we're 2.2%. So it's so low, I can actually even call these people, say, you clicked on that. How come? What happened? And what we do is, next slide.

Arnel Mendoza (00:41:25):

We let them know what they clicked on and we identify patterns. So last month's pattern, for example, it's the DAs and the MAs. So I might want to look at that or if we do it by location. So in this particular month, location one had four out of the eight. I'm going to want to look at that and see if I want to do a targeted training for that location. So it kind of gives you a narrower focus to be able to do targeted trainings, which is in, by our experience far more effective than doing those blanket trainings. Next slide. We let them know what they clicked on. Here's that employee email from HR that I keep talking about and it's to a survey. So they fell for that one. Next slide.

Arnel Mendoza (00:42:17):

This one came from supposedly IT. They're using an old version of Zoom. Again, the important thing here is we're able to tailor the content that we send out also where we use Zoom, obviously. So we send out a bunch of these and again, the idea is to get them to learn to pause and to hover over the link to at least look because if you look at all of the other elements of the email, it looks pretty legit. Next slide. This is a tabletop exercise. We're going to go to a tabletop exercise. So I want to know if you guys can identify whether it is a phishing email or not. Alyssa, you want to run the tabletop?

Alyssa (00:43:17):

Sure. So take a look at this email and your question is going to be, whether you think this is a phishing email or not.

Arnel Mendoza (00:43:29):

I even hovered over the link for you already. So this is what comes up after you've hovered.

Alyssa (00:43:35):

Yes. And then the next slide, we will be using Slido for our polls. So you'll either take the link and put that into your browser or there will be a QR code that you can scan to be able to take each to the poll. So go ahead and take a look at this slide and we'll move into the poll in a moment. So here we are with the slide. So you can either scan the QR code or you can go to slido.com and put in the numbers 8020 758. And you'll be able to see your answers as they come in.

Arnel Mendoza (00:44:47):

By the way you guys, that was a softball.

Alyssa (00:45:26):

So [inaudible 00:45:27].

Arnel Mendoza (00:45:27):

I think we can look back now.

Alyssa (00:45:28):

Yeah.

Arnel Mendoza (00:45:28):

So the 2% that said no, you want to look at the link, right? It says eFax hosting.com.mailru382.co. That's your giveaway right there. And again, that's kind of part of what you want train your users to do is kind of recognize those kinds of links. Okay? Because it's not legit. Usually it's eFax.com or eFaxhosting.com. There is no mailru382.co. So let's go to the next one.

Alyssa (00:46:01):

All right. So it'll be the same procedure. So now this email supposedly is from Dropbox. Is it a phishing email or not?

Arnel Mendoza (00:46:13):

Again, I hovered it for you already. This is the link that came up. What do you think?

Alyssa (00:46:22):

Let's go to the poll again. It's the same QR code and numbers.

Arnel Mendoza (00:46:55):

Jay Sanchez, it's a good point. If you don't have Dropbox, you should wonder why you're getting an email about Dropbox. At the same time, some of your staff may not know you don't have Dropbox. Not a softball this time. Huh, guys? Yeah, I think we can go back now. The answer is a legit email. However, Sean just posted a comment. What I would instruct your users to do is if you encounter this, it's typically easier if you just go to the website, even if you do have Dropbox and specifically this one, it's an upgrade. So if it's a corporate account, typically it's not going to go to you. It's going to go to your administration of that account anyway. But in this case, dropbox.com/by is actually real for the purposes of this exercise. Last slide. The dreaded someone has your password. Sign into your Google account. By the way, we do have a corporate Google account. So this one and for us, this would make sense.

Alyssa (00:48:41):

So take a look and then we'll go to the slide. The poll slide. Is it a phishing email or not?

Philip (00:49:17):

Looks like some folks want to see the email one more time before they [inaudible 00:49:22].

Alyssa (00:49:21):

Sure. Here's the email again. I think you can give us the answer now, Arnel.

Arnel Mendoza (00:50:07):

Okay. If you go back, it is a phishing email. And although the information that's telling you that the email came from Romania, if you look at the link, when you hover my account.google.com-securitysettingsGoogle, that's the giveaway. Like I said, what you want to instruct a user to do is if there's something that says Google-something, it's usually a yellow flag already that it's a domain that's not sanctioned or real or it's not something that's connected to Google at all. And that's common. Like I said, you'll get something around adobe-support.com. That's not Adobe. If it's Google- in this case security settings, that's not Google. They'll, have a different way of doing that than that. So I hope that was helpful. We can go on now.

Arnel Mendoza (00:51:13):

So now that you've at least figured out, or at least showed you how you can cultivate a culture and that's again, addressing the hardest parts of cybersecurity, which is actually boils down to getting people to not click on a link and hover and pause. What happens when somebody does click a link? Again, we go back to our friends NIST, National Institute of Standards and Technology, a response plan, again seems pretty straightforward. Before an attack, you must be prepared. You must be able to do detection and analysis. After an attack, you must have procedures that allow you to do containment, eradication and recovery. And then there's post incident activity. Next slide.

Arnel Mendoza (00:52:03):

What does be prepared mean? You must compile a list of your assets. You go back to the assets, not just endpoints, but your networks, your servers, your systems, you must identify their importance and which ones are critical or hold sensitive data we're in healthcare. So you actually, you should know, we already need to identify those systems that have Phi you must set up monitoring. So if we have a baseline of what a normal activity would look like, and you have to determine which type of security events should

be investigated, so that you'll be able to create detailed response steps and communication guidelines for common types of incidents. Next slide.

Arnel Mendoza (00:52:55):

Detection analysis. That's implementing monitoring systems for networks systems that's so you're able to log inactivity. So you are able to detect alert and report on potential security incidents and identifying a baseline or normal activity for these systems must be able to correlate related events so that you can see that's actually a really, really bad security event. And if the deviation is that bad from normal behavior, it could be just a system going down, but essentially you want to know before and after what was happening. Next slide.

Arnel Mendoza (00:53:39):

Containment, eradication, and recovery. The goal of containment is stop the attack before it overwhelms resources and causes damage. Your containment strategy will depend on the level of damage that an incident can cause, and the need to keep critical services available to employees and customers. And also the duration of the solution that temporary solution could be for a few hours, days, or weeks, or it could be permanent containment methods. That includes a coordinated shutdown and blocking communication channels and network routes. Once the cover, my systems are identified. I think we had a tabletop exercise in part one last week. What do you do? If you get a call, your help desk gets a call, "Hey, getting that a ransomware activity and you've determined it was real." First step, get them to turn their machine off eradication step that removes all elements of the incident from the environment, including malware from all compromised hardware. And of course, login credentials must be changed and all those compromised accounts.

Arnel Mendoza (00:54:41):

So once you've done all that, and the threat is eradicated, the goal is to recovery is a recovery to normal operations as quickly as possible. Next step. Post incident activity. That's just asking a lot of questions. What happened and what times, how well did the incident response team deal with the incident, were processes followed? Were they sufficient? How long did it take? What information was needed sooner? Were any wrong actions taken that caused damage or inhibited recovery? Again, this is just basically sort of a debrief on anything that could have gone wrong or that could have been done better. Good staff have shared information better with other organizations or departments.

Arnel Mendoza (00:55:31):

A lot of people that they've found why it takes so long to discover a breach was that the users simply didn't know or sat on the information. Have we learned ways to prevent similar incidents in the future? Very, very important. Have we discovered new precursors or indicators of similar incidents to watch for in the future and for the tech leaders, what additional tools or resources are needed to help prevent or mitigate similar incidents? Next slide. I'm providing a sample incident response plan template. This is from the California Government Department of Technology Incident Response Plan. It's a 17 step incident response procedure with detailed plans for specific incidents. Again, I'm not going to go over it. You can download it for yourself. I've added the link here. Next slide.

Arnel Mendoza (00:56:27):

So we're going to do another tabletop exercise. You get a call from one of your providers. Your company provided laptop got stolen from Starbucks. Are you worried? You're not because, A, you're definitely

worried, B, the laptop was encrypted, C, you're not worried because you have tools installed to track it and brick it. D, he said it was turned off, E, B or C, B and C. Sorry. Take it away, Alyssa.

Alyssa (00:57:01):

All right. Going to our poll. Again, you can scan the QR code or put slido.com into your browser.

Arnel Mendoza (00:57:12):

By the way, does this happen? I can tell you in my organizations twice in the past year, not maybe stolen from Starbucks, but stolen, and it's not just providers. It's staff, too.

Philip (00:57:59):

We have some good comments in the chat. So option F, a policy doesn't allow staff to Starbucks, but also the comment from Michael saying four to five of the equipment our staff equipment have been missing this year alone. Think that's also important to note.

Arnel Mendoza (00:58:44):

Give you another minute here.

Alyssa (00:58:51):

And I'll plug our Q and A box again, as we're getting closer to the end of the presentation, make sure to type in any of your questions for Arnel into the Q and A box. If you don't see Q and A at the very bottom of your WebEx screen in the lower right corner, there should be three dots, and you can click that. And Q and A should be an option there.

Arnel Mendoza (00:59:34):

Good point, Jennifer. Asset management, know what you have. Think we can go back and review this now. So 76% said B and C and that's true. B, you should have your laptop encrypted, first of all. But as you know, the bad guys can definitely beat encryption. So you still should have tools installed to track and be able to brick it. MDM is a must have tool, yes. It's something that will enable you to do that. I listed Prey project and the tool sets earlier, much, much earlier in one of the slides. It's a pretty low cost tool, and it gives you GPS tracking. In fact, we were able to track one of our laptops that way. It was when it got turned on, GPS got turned on for it. It's similar to find my Mac, or find my Android.

Arnel Mendoza (01:00:44):

I said D it's funny because that's actually a response that I got from one of my providers last year. "Hey, it was turned off." So again, this kind of goes hand in hand with being able to train your users as to what's important and why you're doing all of these activities and policies and procedures, and also able to explain to your executive manager why you need these tools. This is the kind of response that you're going to get for real. Okay? You're definitely worried. 10%. That's too high in number for me. I think we can go on now. So after all that, how do we future proof cybersecurity? So I'm going to cover for a little bit here. The buzzword that's basically the big buzzword in cybersecurity now, which is zero trust. And the core concept of zero trust is simple. Assume everything is hostile by default, assume everything is a zombie from Walking Dead that's trying to get into your network. Next slide.

Arnel Mendoza (01:01:58):

So in the traditional network security environment, you have the Castle and Moat approach, and that is everyone inside the moat is trusted. Everyone outside is not. What's the moat? The network, the firewall, your VPN. So if you can get in to the castle using the VPN or the firewall, then you're trusted. If you can't, you're not. You get access to the inside by already being inside or again, by connecting via the VPN. Most people have this architecture, the vast majority actually. Next slide. So why does this not work? Or why is this not the best idea? Well, it doesn't accommodate for nontraditional workmodes. What happened during the pandemic? We all got sent home, right? We all got to do remote work. So VPN bandwidth, that can be a limitation. Also, the fact that there's one single point of failure.

Arnel Mendoza (01:03:05):

So again, we saw how easily an attacker can simply buy credentials off the web. We showed that last week. That is why the big security companies still get breached. We're talking Microsoft, we're talking Okta, we're talking, T-Mobile, we're talking Samsung. Somebody just keeps buying credentials until they can get in from the web. Last week, we showed it was for like $10 for credential or something like that. So once in, you're already within the boundary, you're already within the moat. You're already in the castle. And the note here also by the way, is not just the compromise. The single largest reason for a data breach nine out of 10 times already showed 90% is a phishing email on one single user. So with just that one email and one click, you've already circumvented that whole moat approach.

Arnel Mendoza (01:04:04):

Next slide. So before I go over what it is, I'm going to go over what it isn't. It's not a single piece of technology or any one software implementation. It's a framework. Again, a framework. It can be implemented by incorporating several security technologies that already exist and already being used standalone or in some combination. Next slide. What are the core principles? Trust no one. No one. No exceptions. Always verify. Use least privilege access, require user device with a minimum permission required. Assume a breach, every react access attempt is considered hostile until verified otherwise. Seems Draconian? Yes, but necessary. Considering the numbers of breaches that are going on right now. Next slide. What are the components? The pillars are of zero trust. There should be an identity service. So there should be a way that you can get people to prove they are who they are.

Arnel Mendoza (01:05:17):

That's kind of one of the central tenants. You should be able to identify your end points. And what I mean by that is, again, not just your devices, but also the people using these devices. And when you're doing an inventory of that, that's down to the IP address level. That's down to the Mac address level, all of that stuff that's characteristic of that device. There's your network. So that's essentially, again, trying to figure out the characteristics of your network. So is your network one continuous network? Is it manage edge? Is it segregated networks in several locations? Those are your components. And then your applications, is it cloud on premises? Is it software as a service? All of those things, those are the components of zero trust because those are the entry points. And those you're going to need to get information on at all times so that you can relate them. That's the component of a zero trust framework. Let me break this down a little bit. Next slide.

Arnel Mendoza (01:06:22):

Here's a workflow from Microsoft actually, who basically has their own consortium of companies that are working on a zero trust framework. And it's all based on signal. So you have your user and location on the left here, you have your devices. Like I said, you have your applications. And the risk is identified

all going in, all being part of an information process. All again, you assume everything is hostile. You assume everybody's a hacker and you verify every access attempt to every system, by every device. Of course, you're going to require multifactor authentication. And based on the information you get there, you let them through the app to access the apps and the data. A more practical look of this, next slide, is this. It's interactive parts.

Arnel Mendoza (01:07:21):

So you have your users, you have your network, you have your events, you have your devices, but then you have to define rules in your policies. So what are the rules? Well, you only let in specific users, you only let in specific IP addresses. You only let in specific Mac addresses. If you want to monitor it to that level, you monitor geographic locations to specific networks. If you can, you monitor apps and systems we have in my organization, role based accesses, so we even inventory role. So this was not an easy exercise. It took about a year to do, but we basically worked with HR to come up with the roles that people typically have. And then we worked with the departments to figure out what systems they would typically need to access based on their role and on an administrative level. This was fairly easy when we tried to do it at the HR, not quite so easy, that took a long time.

Arnel Mendoza (01:08:21):

Next slide. What does that look like in the real world? This is a Office 365 CloudApp security screen, a real screen from my organization. You can see the information coming in and the alerts that you've set up based on the rules. First one activity from an infrequent country. And that gave us a warning. And essentially what I will even cover that specific one directly. What that means was somebody went on vacation, one of our providers and tried to log into the network from London. And of course having no remote sites in London, we blocked them. So the subsequent action needed to be, if you're going on vacation and you're going beyond our geofencing you're going to need [inaudible 01:09:13] know. Multiple bail log in attempts. That's actually also a very good indicator, depending on how often and how quickly. So if you see something that says something was trying to log in unsuccessfully a hundred times in the last 20 seconds, no human can do that. So that's already a way to figure out that's probably malware. Next slide.

Philip (01:09:38):

Arnel, we have a quick question that says how many staff are monitoring this? Also, when the alerts come in, do they get emailed to your ticketing system?

Arnel Mendoza (01:09:45):

Yes. How many staff? I have four people on my staff and we only look at the reds. In Okta, which is our identity management system, you're creating network zones. So you're adding the IPS that need to be included. And it also records if people are working remotely, the history of people logging in from where. So even the IP address is an unknown, it's a remote system from someone's home. They can figure out what the IP address and they're working from a spectrum network or charter or [inaudible 01:10:27] or whatever your ISP is. They're able to figure that out and they're able to kind of build some intelligence, so you can kind of build in a blocked IP zone in a trust zone.

Arnel Mendoza (01:10:40):

Next slide. You can also use network bandwidth analyzers, and that's we have solar winds for that. I think we mentioned last week, a free version of Nessus, which is a vulnerability scanning software. I

believe it has a bandwidth analyzer as well. This particular one is Datadog, and it's a way to quickly see, for example, again, a piece of software that allows you to alert you, that behavior looking at behavior, certain network traffic looks like it's more than just an anomaly. Looks like something that needs to be looked at further. Next slide. So that's your new world of IT maintenance. When you follow this path, you will get a lot more warnings and alerts, but you will sleep better at night. Next slide. And with that concludes my presentation. I thank everybody that came and participated and I think Philip, you can open it up for Q and A now.

Philip (01:11:50):

Awesome. Thank you so much, Arnel, for continuing us with this part two presentation. I think the first question will pretty much be a good one to start us off. So it was actually just recently asked and they want to know a little bit more about your role in your organization. So could you describe how big your organization is and with four of your staff members, how does that really look like within your organization?

Arnel Mendoza (01:12:19):

So in terms of myself, I'm director of IS, but typically I kind of wear a CIO hat. So I run three departments. One's the IS infrastructure department. I'm in charge of data analytics, and I'm in charge of the HR support team. In the IS infrastructure, there's four people, like I said, four and a half, really, once part-time. In terms of size, we have 320 users. We have five locations, we have five community health centers. I think I mentioned earlier, we see 25,000 patients and we do 120,000 visits. So that kind of gives you an idea of where we're at. Maybe a point of comparison. What I've gotten my staff to do is learn to work with priorities. Again, everything is a priority. So yes, the alerts come in, but we've managed to figure out which ones to pay attention to. You've been able to classify which ones are the critical ones. Those we need to take a look at.

Arnel Mendoza (01:13:26):

If you want to look at the medium ones again, the medium ones, they typically, we have less priority to look at them, but we will look based on who they are. What we've done is we've identified who the risk populations are based on all of the cybersecurity testing that we do. So we kind of know who they are. And I'm sorry, if you're a provider on this call, I will apologize profusely. We find the providers in the high risk population. You don't have a lot of executives in the organization, but you have maybe at least a dozen, you'll be able to figure out who the risk populations are. So we basically track them closer. So it's more of a custom kind of net we put out there. I hope that answers your question.

Philip (01:14:17):

Awesome. Thank you. And we'll go ahead and dive into some of the questions we have. So looks like we have about seven questions. So I think we can get through this. So the first one is we use dual facts or authentication. Is there a standard on the frequency? Does it have to be every time there is a login or can it be weekly?

Arnel Mendoza (01:14:37):

Best practices every time weekly, you can do that, but again, it's kind of dependent. Zero trust means what are they trying to get into on what system, right? How important is that system? Is it a critical system? On those system, if you've identified it as a critical system, I'm talking your EHR, I'm talking your

financial system. You're going to want to have two multifactor authentication at every single login. Again, how to future prove your cybersecurity environment is simply trust no one.

Philip (01:15:21):

And so the next question, it kind of leads into some of your current experiences as well. It says what types of reports are important and most useful for C-suite leadership to receive from an IT team, so which one have you found the most useful?

Arnel Mendoza (01:15:40):

They don't want to really get into the details. And by that, I mean, they're not going to want to look at how many people, how many missed logins happen this week? Unless it's one of them then I let them know immediately. What are you doing? Or one of the questions or alerts we have is if you've erased more than 20 files from our SharePoint drive or SharePoint One Drive directory, and it could be somebody just cleaning up their environment. And if it's a C-suite, I will talk to them directly. But typically the most important reports they want to hear from are essentially status reports on what the gaps are, because they're very, very in tune, I think on risks in terms of the high level, like I said.

Arnel Mendoza (01:16:36):

That's why you need to be able to speak to them in terms of quantification. So if their risk is security awareness training, and if we identified that and two years ago, we did, then they wanted to see a report every week or every month on what our phish rate was. That's why I basically had that slide on the ready, because we still do it. So things like that, if we've identified where the gaps are, they want to know what we're doing about it and how effective we are in mitigating it. I hope that answered your question.

Philip (01:17:11):

Thank you. You had just mentioned the phishing example. So I'll go ahead and bring up this question. It says, what is an appropriate phishing percentage a year or more after implementing things like know before?

Arnel Mendoza (01:17:27):

What I find is, and I've talked to a few organizations that have implemented it, community health centers, and I think I'm going to stick to that whole it takes about a good nine months to 12 months before it starts really starting to appreciably get lower. And I'm talking, if you started at 30, then you're looking at 15. If you start, like we started at 35 and after one year, it got down to 15. And now as you see, it's down to two to 3% and we mix things up. We change our content all the time. We'll customize it during COVID. We were customizing it based on COVID type of phishing emails. So yeah, that's the number that I'm going to stick to after nine to 12 months, you should see an appreciable decrease by maybe a factor of half.

Philip (01:18:20):

All right. Down to our last few questions. It says if a real email is malicious and someone opens it, but doesn't click anything and just opening the email leads to bad outcomes.

Arnel Mendoza (01:18:35):

No, it doesn't. But what I've tell my users is send it to the help desk anyways. So we can tell people because the idea of cybersecurity culture, isn't just you. You're part of a collective whole. So the more people know and believe me, if you got it, chances are somebody else also did. Right? So it could be that they clicked on it, although you didn't or all you did was open it. So again, the idea is to communicate that. So although it's the right response not to do anything, it's also a good idea to spread the word so people know.

Philip (01:19:13):

All right. So I think folks are really interested in kind of your perspective and your role and also the four staff that you have. So I'm going to jump to these last two questions we just got, because I'm sure that's probably what most people want to hear. So I'm going to read it slow, but there's two parts to it. First question is what is your organization cybersecurity budget or the percentage of your IT budget is for cybersecurity? And in part two is, can you quickly elaborate on the roles of the four staff in your infrastructure team? Do you have a dedicated security person?

Arnel Mendoza (01:19:57):

Answer to that last one is no. I don't have a dedicated security person and when you have four people, it's very hard to do what I call man to man defense, right? So they're cross trained. To answer the first question was about the budget. Our cybersecurity budget is about 6% of the total IT budget and that's including everything. And actually the biggest part of the IT budget is the people. So it's not really the tool set. And if EHR is part of your budget, a huge chunk of my IT budget is the EHR huge. So again that kind of like factors into it as well. What we've gotten good at is getting my team to work with vendors. So when you have a solution that you've purchased for monitoring like solar winds or something like that, I also buy the highest level of support so that they're able to ask questions so that they're able to kind of even use the vendor or leverage the vendor as sort of a pseudo part of my team so that they can kind of follow along a case.

Arnel Mendoza (01:21:12):

So because the hardest part about cybersecurity, isn't the day to day, it's the anomalies, right? And you're not going to have, you're going to need a real expert to kind of dig deep and dive deep when you get to that point where you're doing forensics. It's not going to be one of my staff that's going to do that. So you need to have a resource like that on the ready as well. So you either do that by purchasing the support level to enable you to do that. Or you have somebody you can outsource to do that as well. That's can be part of your cybersecurity budget too, is to be able to outsource somebody that can help you. So it's not just your staff. So it's a mix and match of both.

Philip (01:21:55):

Definitely. That's awesome. You mentioned solar wind. So I'll go ahead and bring this question up. It says, you've mentioned Okta and SolarWinds, but both have experienced breaches themselves. How do you have the confidence in these in other companies that they are still safe to use? I'm sorry.

Arnel Mendoza (01:22:16):

Believe me. The Okta one was very personal because my CEO asked me, "Were we part of that breach?" And so I was on the phone for a half hour with them trying to figure out if we were part of that breach and they assured me and in the end it wasn't really Okta that got breached. It was what we found out was it was a third party provider of Okta services that got breached through remote desktop. And we

got down to that level of who it was and who got affected. It was two customers of that company, of that third party provider that got breached. Still, they were able to get into that particular instance. So at that level, Okta was breached on our individual level though, we weren't breached. So we were satisfied that wasn't part of it. Same thing with SolarWinds. So yes. So part of what I do is I got to find out if Microsoft got breached too. So you kind of need to be able to ask the right questions to see if you were part of it.

Philip (01:23:16):

Yeah. And I also recall you breaking up last week is making sure having those discussions with the vendor even before starting business making sure that they have a program that really fits in alignment with your organization. I think that's a really important point to bring up here as well.

Arnel Mendoza (01:23:31):

Exactly. Right. Our EHR is a cloud based. It's hosted. So that's a real significant conversation you want to have with them. What happens in the event of a breach? You're really willing to be monitoring them as well.

Philip (01:23:48):

All right. I think this will be our last question to close this out. [inaudible 01:23:52] says, what services other than have I been, is it, I don't know how to say it actually-

Arnel Mendoza (01:23:58):

Have I been pwned, yes.

Philip (01:24:00):

There you go. Ashley before said, so are there other services than that one that performs password breach notifications?

Arnel Mendoza (01:24:09):

That one's the most common one. I'm not aware of anything that's actually as effective as that one because the owner of that one keeps it pretty up to date and we use it well. So that's a good place to start. And I have a lot of confidence with that particular website.

Philip (01:24:30):

Awesome. Well, looks like those were all the questions. So I want to go ahead and take this last couple of events to really close this out and thanks again, Arnel Mendoza with QueensCare Health Centers for this presentation today. And this entire series that we've had is really great to get the feedback from you all. And you will receive a evaluation right as this session closes. So if you're able to hold on for just a few seconds, we'll close this session out. So that way we can get your feedback, we really appreciate it. We'll make sure to get the slides and the recordings for both sessions sent out to you all. You can always reach out to myself or Arnel if you do have questions and follow up. So we definitely thank you all for your time in being here with us. We hope you have a great rest of your week and enjoy your holiday as well. So thank you and take care everyone.

Arnel Mendoza (01:25:18):

Thank you for attending the seminars, guys.