John Greiner:

Okay, good afternoon everyone. Welcome to Cybersecurity: Practical Considerations and Best Practices. We're going to actually start off before we even do any intros with a poll, and so if you can just take a second and respond to the poll.

And while you're doing that, I'll introduce our presenters. Courtney Kanopka is the Deputy Chief Information Security Officer, very apropos for the session for the New York State Courts. And Christine Sisario is the Chief Information Officer for the New York State Courts as well. So very large complex organizations, urban, rural, they've got sort of perspective on limited budgets, on managing lawyers, and supporting legal processes. So very relevant we thought for legal aid. We've had in past sessions a lot of discussion from sort of a smaller provider perspective, but kind of getting a sense of how a much larger organization approaches cybersecurity with a focus on how that translates to smaller nonprofit groups would be a fresh take on cybersecurity, which is obviously critical and becoming more and more important and taking up more of our space every day.

So, if you wouldn't mind responding to the poll, we're going to close that out in just a few seconds.

And just to let you know, this is a session that's eligible for CLE. We'll be announcing the code verbally twice at the very end of the session. You can get the form on the court's website for the conference, download that form, and you need to make sure you submit that form promptly to get credit. I think you have five days. We are going to be taking your questions. I'm going to be reviewing them and posing as many of them as we can at the end of the session, but please don't wait to chat your question. Really interested in what your thoughts and concerns are as we go through it and questions of course. And obviously, we're recording the session, so it may be something that we hope is valuable to some of your colleagues back in your organizations. So we would encourage you, obviously not for CLE, but we would encourage you to share that when it's published. And there may be some questions that you pose that we don't get to, but we will try as a collaboration to address in some fashion down the road. So welcome.

Thank you for responding to the poll. Could we get the results? Oh, I'm sorry, I didn't respond myself.

Technology Moderator:

Results are in the chat.

John Greiner:

Okay. Okay, well maybe that's a good place for you to start.

Christine Sisario:

Okay. Hi everybody, I'm Christine Sisario and I'm the CIO of the Unified Court System for New York State. Thrilled to be here and thrilled to discuss my personal favorite topic. Looks like right now from the poll response, 25 responses are majority by not a huge margin is more people have professionally experienced a cyber incident than personally or not ever experienced one. So it happens, it happens all day long, by the way, where I work. It is a scary world out there.

So, I'm moving on to the first slide here. In my position, I get perhaps 30% of my inbox every day and my phone calls are invites to trainings. Our sales calls are things related to technology obviously, but more and more and more they are specific to cybersecurity. I put here on this very first slide, one blurb that came from a company that was trying to get me to attend a training and then of course purchase their software. But I thought it was timely and important to read out loud to all of you. So as the digital demands on the public sector have grown, so have the risks. Leaders must shift their focus to prioritize

cybersecurity and defend against cyber-attacks. It has never been more important to stop breaches before they happen. Security must now be at the center of every organization and I can't stress that enough. That was very well done. They almost got me to attend their training. So whoever wrote that did a good job.

As soon as I became CIO here at the courts, it was about five years ago now this became my top priority and has remained my top priority. I have a lot of other things I'm supposed to be doing and I do them, but I am more frequently in touch with Courtney and my CISO than really with most other people that I work with. We're constantly checking in with each other, needing to know what's going on. And that is really how anyone, even if you're not the technology people, if you are the president, CEO, Executive Director, whatever your position is, as a leader, you should be making sure that cybersecurity and prevention of the attacks is really your priority all the time.

It can't wait, don't put it off. I cannot stress that enough. Stay current and we're going to discuss what that means in many different ways. Regularly assess where you're at as far as the versions of software you're running, your overall cybersecurity presence and be proactive in your approach. Don't wait for something bad to happen before you start implementing the best practices, the right ways to operate. I cannot stress that one enough. So moving on, Courtney, I believe this is you.

Courtney Kanopka:

Yep. Hello. So every organization has issues, attacks happening daily. Like Christine said, it's how you're going to keep all that at bay and be able to manage the risks and continually monitoring what's going on in your environment. I'm just going to go over from a threat perspective, the common risk to you and your environment. I've actually worked all these types of incidents that are considered specific risks.

The first one is malware, okay, I'll go over VPN and mobile devices quick. VPN is a virtual private network. Mobile devices is what you're using. A VPN is like an encrypted tunnel that your data is going over. There's constant internet of things and social media now, so you have to be vigilant in what you're using and how you're using those. So the specific risks to these devices, malware, which is software that is specifically designed to disrupt and damage or gain unauthorized access to a computer system or your email system. Ransomware, which is a type of malicious software designed to block access to a computer or system and usually they want a sum of money to be paid for you to gain access back to your system. Although ransomware is usually aimed at an individual, it's just going to be a matter of time before they really are going to be targeting specific businesses.

One incident that I had worked awhile back, which was a ransomware. The client didn't have any monitoring in place for that. So what the ransom was doing is basically phoning home. So, every other day it would just reach out and it would say, "Hey, am I still able to see what's going on here?" And then what the malicious actor did is they were able to be on that network, gain intel, then they waited for a specific date and they activated their ransomware. So the whole entire organization got ransomware and everything in their environment was encrypted, all their shared drives were encrypted. So it's pretty bad the ransomware that's going around, you just want to make sure you have monitoring and you're looking at what's going on.

Social media, you really want to be careful with what you're posting on social media for personal information. The malicious actors are looking at that and they're saying, "You know what? I see what this person's job is and everything that they do," they can then use that to try to spoof or pretend who that they're you.

So, you've got email attachments with embedded URLs. Embedded URL is a malicious URL which is clickable within an email that its sole purpose is for compromising the recipient's email. Credential harvesting, it's a form of a cyber-attack that involves the theft of personal or financial data such as your

username. It will take your passwords. These are typically carried out through a phishing or malicious website, email scams, you could possibly receive an email from someone you're working with that you've been working with but you weren't expecting that. And then you click on that link and then you enter your username and your password and that's credential harvesting. Phishing, which is fraudulent practice of sending emails or other messages which are purporting to be reputable companies in order to induce individuals to reveal your personal information such as your password or even your credit card numbers or your banking numbers. Next slide.

Christine Sisario:

Is it worth mentioning about paying the ransom? And I don't know that we want to tell everybody do or not do, but I do think there's some things to consider with that.

Courtney Kanopka:

Yeah, so usually what they're going to tell you is do not pay the ransom. Actually, Australia is considering making it illegal to pay ransom. So you could pay the ransom, but the malware is still on your system somewhere and once you pay that ransom, they're going to hit you again and they're going to ask for even more ransom because they know you're going to pay. So it's just better practice to have the backups so you can actually just recover from a known good image. So really, you don't want to pay the ransom.

Christine Sisario:

Okay, thanks Courtney.

Courtney Kanopka:

Okay, so here's phishing, versus spear phishing, versus whaling. Okay, so phishing is just your general more sophisticated could have misspellings in it. You've got whaling, which is high targeted phishing attack, it's usually aimed at a senior executive. Your spear phishing methods are targeted at specific individuals within an organization. So, the issue is that your emails with the targeted whaling phishing emails, it really can be spoofed. So, someone could take your email address -- there's a lot of free programs out there where they can take and make courtney.kanopka@ny.gov, whatever my email is, they can make it look like it came from within my organization, and they can start sending emails out and making it look like it's me. So you have to be very careful with that. You always want to make sure that you pause and you verify that email that you received in your inbox. Don't automatically click a link or open an attachment.

So this example here is just to show you that it's a phishing email. It looks like it came from your IT Department and if you look at this email, there's no misspellings in it. So the phishing emails are getting more sophisticated where they're not having that standout misspellings or they're not in English and it's a lot harder to actually detect what a phishing may be. This one actually looks like if this was your organization, it came from your IT Services Department. Okay, next slide. Okay, now this is an example of a spear phishing email that you may receive or may have received. I know it might be a little hard to view the picture, but the top here it says, "Targeted." This is where you're able to look and look at the person of the organization that the email actually came from.

Then if you just go down, you'll see impersonation. This right here, the impersonation field where it says the regards from. They're really trying to impersonate someone within your organization, but it's not, it could be the legitimate name of someone, but you just really have to look at it. And then the intent of the email is the urgent wire transfer. So they want to target you to do something. And then down below

where it says the invoice, that's actually the payload and that email contains a targeted piece of malware that can download to your system automatically once you open it. And it could have keyloggers on it could have ransomware, it could have trojans. So you just want to be very careful. Okay, next slide.

Now this is an example of a whaling email. This shows you the top is the attachment, in the red I've highlighted that. It looks like it's from within this organization. This is just a fake organization, this is just Eastern Kentucky University. We shared a document with you. If you look at who signed it, it looks like it's coming from your president of your business. But if you look, the subject has two different names in it, which is highlighted here in the red to the right Kentucky Christian University. And if you look at the from, it's a different edu than who it should be. So you just want to be very careful that you're looking at the emails you receive and make sure it's not from one of your executives.

This is the pause and verify. Don't just rush into it. And also don't just forward these messages within your organization to see if anyone else received it because they may see that it's from you and you're a trusted person. They may then just click on whatever's in that email and not even look at it. So first thing to do is if you have any questions about it, contact your help desk or your IT person right away and say, "Hey, I got this email, what should I do?" If your IT person wants it forwarded, they'll tell you how to do it and what to do. And also don't remove any emails from your junk folder because your email servers doing what it's intended to do. It sees something malicious in the email, it put it into junk. Don't ever remove email messages from junk into your inbox. If you think that a legitimate email shouldn't be in junk, contact your IT department or your cybersecurity unit if you have one and have them verify it for you. So that's that, pause and verify.

Christine Sisario:

Courtney, it is scary. I do have to say though, since I've scared all the people I work with here, the judges, the attorneys, all my coworkers doing a lot of these trainings, they do now pause and verify before they open something instead of just clicking the link to say, "Oh, why did he send me that?" They really do look more carefully. It helps to spread the word and tell people about all of this and we'll talk about training in a few minutes. So this next couple of slides, we recognize that a lot of you on this call are from legal service providers, nonprofits. You may not have a gigantic budget, you may not have any technology budget or a very small technology budget.

So while I do have a technology budget, it's still a lot to manage for the number of employees and the size of our network that we have to monitor. So we are very much aware of trying to do things in an efficient way, in a way that doesn't spend tons and tons of money. So we did do that intentionally to share with all of you. And I just want to remind you that some of the things I'm about to go over, specifically sample policies that you could use, are part of our attachments to this session that are out on the webpage for this session.

So one thing we've done here, and I do believe it has made a huge difference, is we now require cyber awareness training for all employees. In fact, we're about to implement that you have to attend your first cyber session before you're even allowed to start working. So at your new employee orientation soon that's going to be a requirement. I know a lot of other organizations work that way. We happen to have a training that we use that comes out quarterly. The sessions are about 15 minutes each. It is hardly sucking up people's time and there are free cyber trainings out there and we've included that, like I said, in the materials. I can't vouch for how wonderful, perfect they are, but they do exist. They're better than nothing and it is really worth looking into this or to invest in something. Your end users are the target, your end users need to know what to look for and if they don't, it can be very, very dangerous. So really making them aware and knowing what to do or not do is really important.

John Greiner:

And Christine, if I can just add on that, I mean, again, in legal aid, make sure that includes all of your interns, your law students because you're giving them access. So it really needs to apply across the board.

Christine Sisario:

Yeah, that's really good point John. This next bullet is, it's kind of hard to do. I fully understand and recognize this, but I just wanted to bring it up that internet access and email are the two biggest ways that malicious activity is brought into a network, is brought into an organization. So if you can limit who has access to the internet, in other words, if it's not needed for someone's job, don't grant internet access. You're just asking for trouble. It is not needed. It may not be possible in a small organization. Maybe you need that for very valid reasons. I fully understand that.

If you can't limit it at all or even if for the number of people that do have it, we still recommend that you incorporate automated blocking of malicious sites using a proxy server. I don't believe there's free ones out there, but you don't have to spend an arm and a leg to implement the blocking of bad sites. There's all kinds of different software products that do this. It really makes a gigantic difference. You wouldn't believe how much traffic is blocked by our software all day, every day. New websites are spun up constantly. So having software that is dedicated to paying attention to that and blocking it is really critical.

I highly recommend that you review reports of internet use by the employees and incorporate an internet use policy. If it's wide open and you don't block anything and it's one thing to waste time, right? Shopping, reading about sports, whatever it is, that might not be malicious. People might go to sites not intentionally doing anything wrong. So really looking into what people are doing, what kind of traffic is going on out of your network as well as coming in. Really highly recommend that you do that. There was a sample-

John Greiner:

Just add there's... Sorry. So one example where we've tried that in legal aid with attorneys who are doing research where they've got a case and they've got to go visit a bunch of different websites, so there can be some tension or some conflict there. And so it's just make sure that you have good support mechanisms. So if you have to open up a site or you maybe have a dedicated, not necessarily air-gapped computer, but you have a dedicated computer that you know might have some compromised software on it that that's not part of your network. So there are ways to do it even in legal aid, but you've got to provide the support for users who have a legitimate and urgent need typically to get access to sites that you don't want most people going to.

Christine Sisario:

Yeah, we do that too, John. I think it's worth considering having a device or a couple of devices that aren't on your network. Granted you might have to go elsewhere if you don't have a separate Wi-Fi or something like that, but those devices are used to go out to those sites, the social media sites. Maybe you're working on a case and you need to go look at this stuff. You need to know what's going on, but you don't want it to infect your environment. It's a real balancing act. It is difficult. We're up against that with our court attorneys and our judges, right? They're getting evidence from cases, they're having to go out and do research. It's a thing and we're trying very hard to figure out the right balance there, but just think about that as a possible option.

Loss or compromise of a device is really maybe one of the best ways to have a data breach or loss of data in your environment. If data's being stored on the hard drive of a laptop and you leave the laptop on the subway or, in an Uber, or somebody steals it, guess what happens all the time? You give it to your kid in college and they lose it. There could be personal identifying information in files on that drive. There could be write-ups about cases that you're working on. There could be all kinds of confidential information. There could be financial information depending on the kind of case you're working on. You should automatically encrypt the hard drive of all devices that you use for work purposes. It's free with Windows, easy to do, but most of the time you get a device when you purchase one, it's not encrypted. So that's just a free quick policy to implement for all of your devices.

We've had examples of devices that were used and a whole case was being worked on the hard drive of a laptop and as opposed to being stolen or lost, there was malware, there was an infection of malware on the device, we had to take it off our network and the people working on that case no longer had any of the documents that they were working on for that case and it was a gigantic problem for them. So it's another reason to use cloud storage or local network storage that's backed up, that's safe, that's secure, that's behind firewalls, that's behind logins and passwords and so on and so forth as opposed to just in one and only one place, which is on that hard drive. You lose that machine, you've lost everything. So that, I can't stress that one enough. We bump into it all the time here.

Protecting the PII is so critical, the personal identifiable information. Being someone who works in a court system, court cases, guess what they have in them, information about the parties and all kinds of information. Many of them have financial, some of them are about minors, all kinds of things. Cases ultimately get sealed. So think long and hard about how you store that PII. For example, if you have a case management system that you use, whether you built it yourself or it's a third party system that you've purchased, is their auditing incorporated in it so you can see who's in there looking around at the data? Do you limit who has access to that system? Do you control the levels of access? For example, their job function. People should only have certain permissions based upon what their job is. Not everyone should be able to see the cases once they get sealed. Not everyone necessarily needs to see certain types of information. So the more kind of granular you build out those permissions and lock it down as best you can, that is going to potentially help you out.

If you must send out a document that has PII or other confidential information in it, we can't stress this one enough, use secure email or other sharing options rather than just unencrypted by default email. So there are ways to secure an email message that goes out and or encrypt it. There's information about that in the attachments to this session. During COVID, I was a complete nut about this and insisted that anything that was getting sent out that had an attachment that was going out to parties, that was going out to attorneys that normally would've been handed out in paper in a courtroom, orders of protection, all decisions, you name it, documents, forms and so on. We sent them whenever possible through secure email so that there was no risk of that being intercepted. Really important.

And outside of cyber digital security, also think about physical security and by that I mean your computer. Lock the screen when you walk away from it. Someone could walk into your office and send something on your behalf. Thank you, John. Encrypted email is free. Yes it is with Office 365. Thanks. And I think Gmail and other commercial providers as well. If you have servers on-prem where you store your data, they should be in locked rooms. They shouldn't just be sitting out in your waiting area or somebody's office in the corner. Locked rooms where there's cameras-

John Greiner:

Or not in a fireplace, we've found at times. An unused fireplace, but you never know . . .

Christine Sisario:

Also doesn't look good in a fireplace.

But really important that your equipment be locked, especially when it's storing a lot of information from your whole entire organization or from a particular location. Think about paper security as well. Believe it or not, this is a real thing. You print out a whole list of your employees with their salaries and home address and social security number in your HR department and leave it on your desk and the cleaning people come in and, okay. So really, really carefully think about do you really need to print something out that has confidential information that has PII, if you must, shred it as soon as you can or get better at reading online. I think somebody just sent in another chat. Let's see. Think about potential hurdles recipients may have to go through to get access to encrypted email. Oh yes, that's a thing. We went through quite a bit of that. Molly, thank you very much. It's hard. It can be complicated. There can be several steps to get to the secure email sometimes, but it's important. Moving on.

So I found this blurb and probably the dollar amount has gone up since, but the global average cost of a data breach is $3.86 million. We recently have been working with a county here in New York State that had a data breach that was beyond 10 times that in terms of what they had to pay to get everything back in order. It's incredibly expensive. You don't want to have to go through this before you implement policies like I was saying before.

So let's talk about some more of the no- and low-cost options. Complex passwords, totally free, easy to implement. It's not a 100% panacea that you have great passwords and therefore no one's ever going to break into your system. But it makes it a lot harder for passwords to be guessed. So longer passwords that require a combination of special characters and numbers and upper and lower case are much harder to crack free. Totally free to just change up your password policy and make it better. Change those defaults on the software that you buy. By the way, a lot of them come with passwords that are four characters long and all numbers, change them. People know the default passwords when you buy Oracle or all kinds of commercial products. They all come with a default, change them immediately. So important.

Keep all of your software and operating system patches current. So this is any of the breaches that you've probably read about in the press happened because the latest and greatest patch that came out for some third party software that an organization was used, they didn't install it, they didn't have time, they were busy, they forgot, they didn't read the email, they didn't have a policy in place requiring that it be done as quickly as humanly possible. Those patches come out for a reason. They come out mostly because they're fixing security holes in their software. Same thing goes with your operating system. So Windows updates come out, your Apple iPhone has a new operating system update. Don't blow it off, don't continue to not plug your phone in at night so it'll update. It's there for a reason. It isn't just because they're changing and adding cute new emojis. It's often they're fixing problems with the operating system. So it's really critical on both the personal and a professional level that those things always remain current. And then I already mentioned this one, using the secure encrypted email when sending attachments or sensitive information out the door. You’re up.

Courtney Kanopka:

All right, so geo-blocking, either if you have an IT department or cyber security unit, geo-blocking is where you only are allowing IP addresses that are registered in the USA and you're not allowing any other countries to have access into your network. If you aren't able to have an IT department and say you have a router you bought from Best Buy, you can go in and you can set up rules. That's free for you to do so that you're only allowing IPs within the USA. There should also be certain features within those firewalls that specifically will tell you. And you can always YouTube how to do it too if you're not too

sure. But geo-blocking, basically, it prevents a bad actor from another country. And also if you are, say you're going on vacation and you've got big cases going on and someone that works for you is going to go to Russia, now, you also implemented it where they can't just leave the country and have access to their email and access to the systems because you're not allowing that. So you can white list maybe just their one IP address of their cell phone or their laptop that they're taking with them on vacation. If they really need to work on vacation, you can allow just that one IP. So that way if something did get compromised, it would only be allowing that one IP and you would see what's going on.

Be careful when connecting to Wi-Fi networks, particularly those that are not password protected. So, you go to Starbucks, and you see the free Wi-Fi, you go to McDonald's, right? You see the free Wi-Fi. Don't connect to those. There could be someone sitting in there with a laptop or even outside in their car. You might not even see them. They are scanning those free wi-fi's and they already can be compromised. They can literally grab your information and you think you're connecting to that free Wi-Fi, but in actuality, you connected to their malicious program.

So the best thing to do is your cell phone has a hotspot. A lot of the unlimited data plans now are allowing you to have hotspot included. Connect to your hotspot, use your cell phone hotspot, or get a little Wi-Fi device. Use that to connect your work laptop too. Just don't connect to those free open source. Even if you go to hotel, they give you free. You don't want to connect to those either. Next slide.

John Greiner:

And just the 15 minute... We have 15 minutes left, a little less actually.

Courtney Kanopka:

Yep, I'll go fast.

Christine Sisario:

What about the free Wi-Fi on a plane? Someone just asked.

Courtney Kanopka:

No, you don't want to connect to that either. Anyone can have access-

John Greiner:

But what about VPN usage though? I mean, you assume the VPN on a public Wi-Fi better.

Courtney Kanopka:

Yes, but just know, right? If you are still on that free Wi-Fi and you're connected now with your VPN, you're now in your own network. And if they have gained access to your information, right, because you connected to their host, they now are inside your virtual private network. So now they're inside-

John Greiner:

I mean, and again they're the web-based or cloud-based VPNs like Firefox for instance. Mozilla has a VPN product that just gets you away from that local coffee shop or airplane and out into a broader in internet environment.

Courtney Kanopka:

Anybody else?

John Greiner:

And some of those actually, the slower speeds are free. You can get free VPN from reputable providers. They don't give you a lot of bandwidth. They keep it. They want to upsell you.

Courtney Kanopka:

Yes.

Christine Sisario:

And what about backups? That's just another critical . . .

Courtney Kanopka:

Yep. So basically you want to have your backups offsite in the cloud. Gmail actually gives you so many gigs for free, Outlook as well. If you can afford it, pay for all or even OneDrive, right? Pay a little bit extra. It gives you that safe. Save it in the cloud because if you save it on your laptop and it's stolen or it's ransom, you're not going to be able to do any backups.

Christine Sisario:

And if you don't have backups, good luck restoring from a ransomware attack.

Courtney Kanopka:

Yeah.

John Greiner:

Well and just on that point, I mean, I think what Courtney was saying, advising against paying ransom. I mean, we've helped providers that have had cyber incidents and essentially where they don't have a good backup, where they don't have a good recovery system where they would've been out for an extended period of time. So the more you can do to prepare for an incident, then the less susceptible you'll be to paying the ransom. But again, it's not an easy decision. A lot of people pay not because they want to, but because they risk the certain disclosure of data. And again, in New York, we all heard about Suffolk County being a disaster and they're not alone, the data that they lost on tons of private individuals.

Christine Sisario:

Not to mention their operations were completely brought to a halt. The police couldn't process arrests, they couldn't fingerprint people. It was very bad. It went on for months. So it's pretty scary. I see people mentioning about VPN and two-factor or multifactor, we're coming to that on our next slide, Courtney, let's move on to the remote work. Here we go.

Courtney Kanopka:

Yeah, remote work. So COVID hit, everyone's remote, still people are still working remotely, so working remotely opens up more risk, but a lot of people are working remote. So here's some suggestions how

to protect yourself. Be aware of the phishing scams that come in. Be careful of the fake news and alerts. When COVID hit, there was a lot of phishing emails coming in purporting to be like, "Hey, your COVID vaccine is now due." So just be very careful again to make sure you're not just clicking. Set strong passwords. Use a password manager. Identity manager, right? Google actually offers a free password manager. You can save your passwords into Google. Make sure their 14 characters or longer, have MFA. But make sure that you don't want to reuse your password on every single account and use multifactor authentication. It could be an app on your phone, it could be a text message, it could be you get an email, but make sure you have that. Install antivirus on all devices, that's free.

You can set up automatic updates on Windows. So every night it automatically installs your updates when you're not using your computer and it reboots. Apply the basic security features. Go turn on the firewall on your laptop, go into Windows, type firewall in the search bar, turn on the firewall, that's free. That will help. A lot of times they're turned off by default. Windows is getting better at having that automatically enabled for you, but a lot of times, it gets shut off like a new up patch comes in. Make sure that that's always turned on. Securing your home Wi-Fi as well. Don't just have open Wi-Fi at home and make sure the password on your home Wi-Fi is at least nine to 10 characters long. Don't have it just numbers or just letters. Have a good strong at-home passwords that your at-home Wi-Fi device cannot be compromised.

Again, using a VPN, virtual private network, they're very good to make sure that your data that's going across the wire is encrypted. So it can't be, if someone's on your network and they're looking at your traffic or sniffing your traffic, they can't actually view what you're sending. Keep your work environment private. Make sure that you don't let your kids use your work laptop to download a game, then that's malicious, right? It could be a malicious game. So just make sure that you keep work and home totally separate. I know it was tough when COVID first hit, some people were able to get a work laptop, but now that we are back in the office. Some of us just make sure you keep your work laptop as your own and then set a remote work policy if you have people that are working remote so they know what they should and should not be doing while they're working at home from their work laptop.

And also, so some people think that cyber insurance is going to cover me. I don't need to worry about all this remote work and having all the safeguards in place, but cybersecurity insurance, if you haven't fixed the issues that they found, it's not going to cover you in the event you get a breach. So just make sure these are the basic things you can do. Okay, send to Christine.

Christine Sisario:

Okay, next slide. Some more thoughts about people working remotely as far as additional policy suggestions and other measures. So we've talked about MFA. One of the big breach --a lot of the big breaches that happened early days during COVID and also still happened today were because a network, an environment didn't have multifactor authentication. What this means is someone could get your credentials, but unless they're holding that device or have the way to see that second factor authentication, the text message using that authenticator app, unless they're physically in hand with what you're set to receive, they can't get in. And we have luckily, knocking on wood here, that's protected us many, many times here. So it's so critical. So, so critical. The users hate it. Sorry, that's my answer to them. I'm sorry. But it's protecting you and all of your work. Prevent personal devices from connecting to your environment.

This one's tough. I totally recognize that. We had personal devices that were connecting to our environment during early days of COVID for sure. Everyone had to go home. We didn't have enough laptops to go around for the thousands and thousands of employees that we have here. So many people did have to use their own personal devices. We insisted and we implemented MFA immediately for

everyone. Everyone was calling in through VPN, it helped. But when someone's using a personal device, you have no control. Are they applying those operating system patches? How old is that computer they're using? What on earth is going on? Who else is using the computer? The kids go in and do all kinds of crazy things on the computer at home and it could be compromised, and you don't even realize it. And then you're connecting to work and you're taking that file you were working on and attaching it and sending it to somebody at work. And you think all is fine because you're on the VPN and you've used your two-factor, but you've just sent a file that's corrupted. So it's really scary. And yes, John, I know what you're going to say, but go ahead.

John Greiner:

Well, so first of all, the one question that Karen raised and Pat sort of responded to, the VPN is really important. I think the two factor VPN, some of the better VPN products out there are now supportive of, or even require that second factor. And so that's really next level, really important, really valuable. But don't feel bad that you've got a VPN protecting when you access your network. That's really critical because we saw actually at the beginning of COVID incidents where people had terminal servers hanging out on the internet and they were not properly protected in a number of ways. So you're definitely better off with the VPN than without. So that's a good step. But you can take it further as Pat suggested to 2FA. So if people feel free to add more questions. But Christine, I want to go back to you. So let you finish and-

Christine Sisario:

Yeah, I think we should move on to the next slide, Courtney, just given the amount of time we have left.

Courtney Kanopka:

Yeah, that's fine.

Christine Sisario:

Everyone has these slides. The rest of these are kind of common sense things that we had. We want to make sure we touched on vetting vendors and other third parties. I think this is important. So Courtney, take it away.

Courtney Kanopka:

You can go ahead and click through and I'll just start talking. So you want to make sure that if you have to work with a third party vendor, you verify their policies and how they handle a security incident. Third party vendors are the most risky. So just ask them, "Have they been compromised?" “How is their data hosted?” “Do they have backups?" Just simple questions, “How is the data?” “Is it in a cloud environment like commercial or government cloud?” Commercial is, it could be anywhere outside of USA, government cloud is in USA, so the government cloud is in the USA and it's a little bit safer if you're a government entity and you can get that. It's better to get that hosted. Is there data encrypted at rest and in motion? Questions to ask to make sure that they have in place.

What is their financial ability to recoup a loss if they have a cyber incident, if they're supporting your software or your case management system and they get a cyber incident, can they recoup from that or will all that your data be lost too? Compliance risk consideration policies for a lot of the different data that you may have. You have HIPAA, which is your Health Insurance Portability Act, which requires safeguards to protect privacy protected health information. You have CGIS, which is Criminal Justice Information Services, and that's the division of the US FBI that gives state, local and federal law

enforcement criminal justice agencies, access to certain criminal justice information, which they set limits on five unsuccessful login attempts by the user. And it really sets a specific standard for that data. FedRAMP, which is the Federal Risk and Authorization Management program. And then you have StateRAMP, which is State Risk and Authorization Management. That's for non-for-profit. So FedRAMP is federally funded and StateRAMP is for nonprofit organizations.

John Greiner:

Courtney, so one question. Any downsides to VPN? I mean, I think there was question about the 2FA, but I think you've sort of raised the one downside in your response to the airline situation. But any downsides?

Courtney Kanopka:

It can be a little bit slower depending on what kind of VPN you have. You also want to make sure that your VPN you're using is located in the USA. You don't want to have, well, you don't want to log into a VPN and have your IP hosted in Mexico or Japan. So you want to use a USA hosted VPN and make sure that your IP address is going to be in the USA.

John Greiner:

And I want to add, because based on some feedback from providers, you want to do a lot of testing with it and you want to understand the user's experience and do the training and then you make your VPN as transparent as possible so that it automatically connects, it automatically reconnects, but if it fails to connect, it stops the traffic. And so that your users know. So get it out of the way of your users to the extent you possibly can. And again, different VPN products work differently, so it's really worth your testing.

Courtney Kanopka:

And also the free VPNs, you got to be very careful with those because some of the free ones can be malicious and can be monitoring what you're doing.

John Greiner:

And can be offshore as you mentioned.

Courtney Kanopka:

Yeah. So just you want to be very careful. So don't think that just because you're using a VPN, you're going to be protected. Because even if you still connect to that free open source Wi-Fi and you've been compromised that way and you just connected to your VPN, now you're compromised.

John Greiner:

Any free or low cost VPNs that you, not to endorse any one product, but if you have one or two that you might say take a look at?

Courtney Kanopka:

I personally only ever use the paid ones. They're not really that much.

John Greiner:

But any paid ones you might suggest people look at.

Courtney Kanopka:

Yeah, I mean, I can't say vendor rates but Cisco.

John Greiner:

Okay, fair enough.

Courtney Kanopka:

Well, yeah, I can, right? But Cisco AnyConnect is very good.

John Greiner:

And end user and obviously legal aid -- better have legal aid get their own account to give out to users.

Courtney Kanopka:

Yeah. Yep.

John Greiner:

Okay.

Courtney Kanopka:

Yeah.

John Greiner:

Great. Well, thank you so much Christine and Courtney. I think just the vendor selection, we need to have our own session on that, right? That's a huge issue. There's so many more cloud services working with one state, a visa sort of application cloud service that, again, they're small provider, they're doing innovative stuff, but we need to be able to vet them to make sure that we're not exposing client data. So a really tough, hard thing to do, but better to do together. So this has been wonderful. Appreciate your time. I know you're taking it away from all the various courthouses and judges and so forth that need it right now, but I really appreciate the partnership and the collaboration. Appreciate everybody who attended. Again, if you do have questions, post them in the chat. We'll see what we can do to respond. Certainly, again, this will be recorded if you would want to suggest this to some of your colleagues so that they can get a little more up to date in best practices for cybersecurity. Thank you.

Technology Moderator:

Do you want to launch the closing poll, John?

John Greiner:

Oh, sorry, yes. Could we launch the closing poll?

Courtney Kanopka:

Yeah. And in our documentation too, that's posted here, we do give some great vendors that you can use at free or no cost for this type of stuff.

John Greiner:

Great. Okay. So limiting filtering. Wow, that's interesting. Internet access, we've got more than I expected, which is good. That's great multifactor authentication. Hiring a third party to do an assessment. Additional tech staff. It really runs the gamut. Investing additional monitoring, knowing what you have, what's happening in your environment. And again, some of, as Courtney mentioned, some of the firewalls have more modern firewalls. Cloud-based firewalls have some of these as just additional licenses. Sometimes they're free, sometimes they're nominally additional. So understanding who's accessing your environment and they can translate a lot of geeky data into something that is lay speak. So again, thank you very much.

Technology Moderator:

Also, thank your panelists there. It was excellent.

John Greiner:

Thank you.

Courtney Kanopka:

Pleasure. Thanks everyone.

Christine Sisario:

Thank you.

John Greiner:

Bye-Bye.