LSNTAP 2022 Cybersecurity Toolkit for Legal Aid
April 12, 2022

John Greiner:

All right. Good afternoon everyone, thanks for joining our session on reducing risks in client data and technology management. We have a panel presentation today, and I just want to underscore the option, and unfortunately, it's a little limited because of Teams, but the option to, in chat, share your questions, your ideas, your answers. I just want to encourage everyone to take advantage of that. We will do our best to try to incorporate your questions and keep track of comments and whatnot.

We've got a little poll, if you wouldn't mind putting it up for folks, asking you to give us a little information about your role in/or around legal aid. If you wouldn't mind answering that, we'll get a little sense. Everyone should see the answers in their chat window as it comes up.

I'm going to move on with introductions and then we can look back at the answers. I'm John Greiner, I'm the founder of Just-Tech. Former legal aid attorney, and technology manager. With me today we have Husain Rahim and Ken Montenegro, who are going to introduce themselves. But both are working on the front lines in both the IT and the management space. Ken also has experience as an advocate working as well as an attorney. I'm really excited to have them both here and if you, Husain and Ken, would introduce yourselves, that would be great.

Husain Rahim:

Hi everyone, my name's Husain Rahim. I'm a Senior Support Tech for Just-Tech. I've been working in the tech field about 10 years now. Primarily, I've been working with Just-Tech providing technical support for many Legal Services throughout the country. I'm excited to present today, and I'm looking forward to hearing from you guys. Like John said before, if you have any questions, please feel free to chat us. Ken?

Ken Montenegro:

Hi, folks. Thanks, Husain. My name is Ken Montenegro. I use he and him, and el. I am the Technology Director at the historic Center for Constitutional Rights in New York City. I've had a long journey to get here, but the short version is that I've been doing technology inside the nonprofits for over 25 years now. I am a law school graduate, and I've been lucky enough to work with some wonderful, committed advocates and I've learned so much from them and I continue to learn from them.

I'm glad to be here. I'm really looking forward to interacting with the audience and navigating questions together. Thanks, John.

John Greiner:

Thank you, Ken. Husain, if you wouldn't mind starting us off on some of the, again, the common current security threats and some of the results of those threats.

Husain Rahim:

Sure. John. At this first slide you could see we listed some of the common security threats that people have been dealing with. More recently, due to the pandemic we have a lot of people working from home, working remotely, and these are some of the examples that we've come across with users, primarily myself working as a help desk technician.

The first bullet point we have listed is phishing. I'm pretty sure everyone on this call by now knows what phishing is, but a more basic definition is we have an impersonator, usually communicating via email where they'll potentially mask their email address or send a potential link, having a user try to click into that link or email of that specific email address, and in turn they're giving out sensitive data to accounts or files or folders stored somewhere on a network drive that they wouldn't usually have access to.

For example, you could have someone masking their email address as a coworker in the office. What I can't stress out enough is to really pay attention to the email address and also really pay attention to the email and the link. They could have potential links that are basically masking, for example, maybe you might get an email from Chase and you'll see that the link says chase.com, but then you'll also notice it says chase.com-blahblahblah, linking you to somewhere else. Potentially, having you sign in and give out your information to a potential threat outside of the organization.

Another bullet point that's pretty important right now, it's whaling. This is when they specifically attack senior members or executives on a team. This has been happening a lot recently too, with a lot of people working from home. For example, John, who's our moderator today, he's the president of our company. I could give an example where I might get an email that could be John or it could potentially be somebody else, you won't know. They'll ask you, oh, maybe they need access to a SharePoint site, and can you please email me the account info?

I could be busy that day. I'm not paying attention, I'm working on tickets, have a bunch of emails open. I just reply quickly like, "Hey John, here you go. Here's the information." I could have potentially leaked out sensitive data to someone else. It's really important, like I said, with phishing to pay attention to that email address, pay attention to the link. If you're not sure, reach out to your help desk, reach out to other coworkers. Usually, when a phishing attack is happening, they wouldn't target just one person in the company, usually, they target multiple people.

If you ask around, someone else might potentially have that same email you have. It's a good thing to go ahead and delete that email, or you could go ahead and report it as spam. That's just another example of phishing. Smishing is also another example as well in the form that they won't necessarily email you, but they might send you a text message. This has been happening a lot lately, because with people working from home and using their cell phones, you might have a voiceover IP service where potentially, you just use an app on your phone and you'll text somebody or you'll call somebody through the app.

For example, what's been happening a lot lately is, you might get a text message from FedEx, for example, and they're like, click this link. You have a package arrive. The next thing you know, you're on a whole other website where you're giving away information through your phone. That's just another example of phishing. Phishing is an umbrella for a variety of other attacks that's been happening a lot, lately, and it's just something that we really need to improve on and pay attention to, whether it's through an email or through a text app or through a phone service.

John Greiner:

Husain, I know because we don't have too much time for the overall session, but with password stuffing and terminal services attacks, we've seen both in legal aid, passwords that get compromised, people using the same password across multiple sites or multiple systems. We're seeing both of those attacks, a lot of folks have been working via terminal servers. Their terminal servers are in front of their firewall or they're exposed through their firewall. These are ways that we're seeing currently over the pandemic and continuing for legal aid providers, to get compromised. But would you mind talking a little bit about some of the impact, the email compromise, the office compromise and so forth?

Husain Rahim:

Yeah. I just wanted to touch a little bit on the password stuffing as well, that it's very important that we have a lot of services running and we're not using the same email. One important thing to do is use a password management where, you're saving and storing all your emails, and it's not stored on a sticky note on a piece of paper somewhere, potentially someone could have access to that, but more on email compromise and office compromise, like I've listed before, it's always important that, like I just said, with password management, that you have your password stored confidentially somewhere else offsite and that'll help with people potentially trying to gain access to your email compromise.

We've seen it all the time where someone would reply back to a business email with a password or sensitive data. It's really important where it ties in with

phishing, you just have to be careful with who you're emailing and who you're giving access to.

John Greiner:

Again, on the email compromise, we've seen systems that Microsoft 365, certainly, Exchange environments, get compromised, and then they use that as a system to launch further attacks on other people within the organization and at other organizations. It might be that, hey, this is an email from an executive director at a real email, but it's from a fake person, a person impersonating an executive director or the finance person.

We've seen even funders getting attacked this way. That's one piece. Certainly, the office, I think most people are familiar with offices being shut down because their environment gets compromised. So, they don't know what they can use, or they don't even have access to the data because of ransomware, they're encrypting the data. Then, we've certainly seen, over the last year or so, more and more exfiltration, people stealing your data and using that as an opportunity to extract again, typically ransom. You may have backups, but if they take your data, restoring your services is only part of the equation. The other part is stopping them from sharing confidential information about your clients or your employees.

Ken Montenegro:

Yeah. We're going to get into it later on in the presentation, but I just want folks to think about, when we think about email compromise, a lot of the damage done by an email compromise is largely dictated by what you were retention policies are. If you have 10 years of email, you have 10 years' worth of exposure, as opposed to, oh yes, we archive our email, and everyone in their mailbox only keeps the last five years, the last three years, whatever's appropriate for the organization. Then suddenly, you've reduced the attack surface on that.

The other part is just going to password managers. I see that Kyle has a question about it. What I can say is that, at the Center for Constitutional Rights, we use LastPass because, A, they have a nonprofit discount, B, because it's actually a very good tool. But there aren't one password, there are just an infinite number of them that are pretty good because, going to what Husain said, in the issue of password stuffing, that's possible because people recycle passwords.

If you have unique passwords and use a password manager, like Husain suggested, then suddenly that becomes a lot harder to do. For me, one of the nice factors of LastPass is that it'll nudge you or poke you, saying like, "Hey, you're reusing these passwords. Are you sure you want to do that?" type of

thing. That's what we use and that's how these pieces somewhat tie together. Thanks, John.

John Greiner:

Thank you. Again, this is a snapshot. There are a lot of other security threats. This is what we're seeing a lot of. Again, we're trying to prioritize some of what you need to know about, and also what you might want to start working on. Sorry, let me... There we go. Ken, if you wouldn't mind starting off on this one.

Ken Montenegro:

Yeah. Not at all. I can actually start off by reading model rule 1.6, a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to information relating to the representation of a client. That's pretty large and broad, and it's a model rule, but most state bars have incorporated some permutation of that, and we also understand if we tie that to the duty of competence, if we are all using these digital tools, then suddenly the amount of competence that is potentially expected is a lot higher, and that's really hard, because technology moves so fast, and I say that as a technologist. Where it's like, oh, this was the one bright and shiny object that was going to solve all our document assembly problems, but that also has like five moving pieces to it, and suddenly you have a Rube Goldberg machine that is your document management system with so many different pieces to secure things that can go wrong.

Within this conversation, and it's just really nice to partner with the Just-Tech folks and thinking these things through, is how do we look at this as a management challenge as well? I think that there's this old model of thinking that IT operates on this side of the street and then programs on the other side. When, at the end of the day, and I think the pandemic has really underscored that, they are one and the same. I'm not going to let the cat out of the bag yet, but one of the resources is that the technology toolkit that Just-Tech and LSNTAP worked on, what I really like about that toolkit is that it's reasonable efforts.

When we're talking about risk management, I would say, how do we make sure that we're being reasonable about what rules do we have about staff using their own equipment for work purposes? Okay, cool for email, not so cool if you're going to be drafting client documents, a retainer, a pleading, et cetera, maybe not cool. But then, email, awesome. Go ahead and do it.

Client communication through unauthorized channels. It's like, hey, cool. I get it, you really wish you had your desk phone, but it's a pandemic, we're all out of office or mostly out of office. You have to use this app because we don't want clients having your personal number and disturbing you at two o'clock in the evening because the housing matter is now a family law matter that is now

an immigration matter, that is now a, hey, by the way, I'm thinking of buying a house. Can you help me? You're a lawyer, you're an attorney.

How do we, once again, draw those divisions as well? Also, just how do we make sure that we communicate these things effectively? Once again, in a way that's reasonable, in a way that we intend for our organizations and our users and our clients to all succeed together. John.

John Greiner:

I think that's really important, that last point, that we really need to be aligned to work to achieve the individual client's needs, but the mission of the organization. We need to work together and we're going to get a little into the culture later. But one of the things I think that an executive director out in California made the point of, and it's worth, I think repeating, is that we certainly don't want to ever be judgmental or scolding of staff who are doing creative work-arounds, but we need to address their needs.

Again, the pandemic, and now, as we're coming back into the office, this hybrid approach, there's a lot of great work that's been done to serve clients and to get us through this pandemic while addressing critical legal needs. But we now need to take the reins without shutting down the functionality. Again, it's working together with your management, with your staff, listening and making sure that, as an organization, you're addressing the needs of the advocates and the staff.

Ken Montenegro:

Cool. Within these risk management frameworks, and I really want to underscore that all of these items listed that we'll go through together are really contingent on what was just shared, which is, how do we have these communication loops that are honest, that are respectful, but that are also shame free of, oh my God, you did what to this? You're storing our client files on MediaFire, or you're using a peer-to-peer network for what?

Once again, how do we have those conversations so that we can really implement initiatives that mitigate risk? Let's say cybersecurity insurance, that landscape is shifting so quickly. The first wave of insurers or underwriters really, were the ones who were hit hard. The underwriters, because this was almost Terranova. It was like, what are we doing here? But let's charge people for insurance. Now, the stakes are up because there are so many incidents, particularly with things like ransomware that folks in this area are seeing an increase in the requirement for multifactor on everything. Everything has to be super locked down. Devices have to be encrypted.

Once upon a time, it was like, "Do you have antivirus on the machine?" "Yes." "All right, cool. You're good to go." Now, it's, do you have a tool that fortunately Husain's hopefully going to get us into, which is EDR or other

advanced threat mitigation tools or software. Cybersecurity insurance is one of those things that we're seeing that ground shift beneath us. How are we ready for that? Because, a) it has an impact on users. I think we need to understand, when we're talking about security, we're talking about friction, and I'd like to use the example of a doorway.

A doorway without a door, it's awesome. You just fly through it, you don't ever have to worry about it being closed, et cetera. But then if you have a valuable behind the door, you're going to have like one of those, what I used to call when I lived in Los Angeles, like the cliche New York door word that has like eight locks. But, of course, only one of them works. If you're trying to get out, you're trying to figure out which one works.

Some security architectures are like that, where they look really secure, but they're just a pain in the butt. How do we, once again, bring this back to the reasonable, the practical and the affordable? Because that's the other thing is security initiatives cost money, both in terms of the security implement, the tool, but also in terms of staff time, both program staff and infrastructure staff.

With back to the office, what does this look like? Once again, we're not going to do a deep dive, but what would it look like for staff security, especially disclosure of email addresses, if you have an iPad at the reception or if you're collecting temperature information, are you going to purge that at some point, or who's the custodian of that information? All this, we'd consider nonsense, but it's actually a real threat to the organization because we're collecting things.

Building security culture, and I think that security culture for me, having done this work for as long as I have, and particularly in more radical political spaces, for me, security culture is about trust. It's about the basic understanding that we are in a shared enterprise, and that one of our team members getting hurt means that all of us are susceptible to that same pain or harm.

Security sustainability, focused education analysis, with the understanding that it's a rapidly evolving landscape, and I don't have a golden bullet for that one, because I don't know what are the security things I'd want my people to be really hot on and knowledgeable about, because that could shift tomorrow, that could shift by the person's area of work. People on our Palestine team might have a different security posture than people on our Guantanamo Bay team, et cetera. It's really hard. But if I'm committed that we can get through these things together with conversation and the communication models that are generative-

John Greiner:

Ken, if I might just jump in, as you mentioned, the model rule and how do advocates manage also ethical questions, it is an ongoing, evolving approach.

It's collaborative. I think there's a model for managing security that's pretty familiar, I think to the legal culture. But it is as, again, something you said earlier, Ken, it's an all of the firm effort. It's not just IT, it's not just management, it's not just the advocates. It's really a collaboration.

Ken Montenegro:

Yeah, because then for me, the other part that always comes to mind is how are we doing compliance? Especially when we come to security issues, if someone is oh, I've built my better mouse trap, all my emails are encrypted, but when that person leaves, they don't give you the encryption key. Then suddenly it's okay, we can't do any compliance. If we have a malpractice lawsuit or something like that, go to the good graces of the judge and say "Oh, by the way, we really didn't manage our keys. Our stuff's not together. Help, have mercy."

Policies, I think, are really one of the foundational pieces. I'm a big fan of using the triad of people, process, technology, when we talk about technology pieces. For me, the process are the policies. How do we make sure we don't have 20 different policies, how do I make sure that my incident response policy is not 20 pages long? It's thorough, but it's not usable, because when someone's like, oh, I had a cyber security incident or a client pushed me or I pushed a client.

These are all incidents that at some point there has to be a model that's recyclable, that we can use the same notification networks. Because basic incident response for me is knowing who to tell that something went wrong and knowing that you can tell them without getting into trouble or being, I'm the messenger, I'm going to get jammed up because I shared the fact that I clicked on this link.

The other thing is, the shame that goes along with cybersecurity incidents and this actually goes to the nonprofit sector as a whole, where the nonprofit sector is not very good about sharing what has happened, in terms of security fiascos. People in the sector don't know. It's usually through a managed service providers, vendors, partners, that they have that collective intelligence of, they're able to say, oh yeah, five of our clients in California got hit for this or our reproductive health people in the south are getting hit with this type of harassment or harm. There really isn't a clearinghouse for that.

Like John mentioned, I think the ethical obligation to main tech and security competency is foundational here. Where, how do we apportion or create time for staff training, if we're going to get a document management system, how do we make sure that we're, "Hey, heavy hitter litigator, I know you want to go eat them alive. Go get them, tiger. But this is a tool, before you're out the gate, you need to know how we put our tools. You need to know how we record time, so that we can actually bill for it, those types of things."

How do we move together? One of the things that I'm going to drop in the links at the end of our conversation is the New York Civil Liberties Union, a friend of mine there actually wrote a piece on legal cyber security that I will share at the end. It's kind of hardcore, but if you want to nerd out on it, you can nerd out at the end. John.

John Greiner:

Excellent. I guess, again, each bullet here, again, they interrelate. Just the conversations that Husain and I and others are having with providers in New York, this is coming up. In fact, I think one of the executive directors that we were talking to saw it as her moral obligation. It's not just ethical, that this is a moral obligation that she feels the organization and everybody in it has to her clients or to the firm's clients, but it is this balance.

The security culture, a lot of organizations in New York have been talking about more training. Lillian Moy yesterday actually talked about how painful some of the security is. That MFA, that she called it a pain in the neck, or worse.

But part of that is getting a conversation going internally. We're not trying to frustrate your work as advocates. We're trying to enable it in a secure way. I think the other piece of that though, is listening to what their pain is, with whatever security work you're doing and seeing how we can modify the implementation or modify it after the fact to make it as workable and as usable as possible. In some ways, I think the example I raised yesterday was that MFA is really a great way to help improve security in terms of access. But Single Sign-On is a great way to improve security and make it easier for users to get into multiple different cloud or office environments.

The Single Sign-On technology paired with MFA makes it a little bit easier than it was before, and more secure. That's the part of the conversation that needs to be had. Husain, anything to add on that, or should we move to the next slide?

Husain Rahim:

I'd just say that, as Ken mentioned before, building the security culture, it's very important. Some implementations that we've done with clients is have a form of education, or have some kind of test or something that they're knowledgeable, and they're learning because, like Ken mentioned, everyone is integrated together. We're not just the ones that should know the tech, but also users as well, should be more informed and learn more of the vocabulary, and this way they can look out for what's coming their way.

John Greiner:

Yeah. That's a great point. Actually, as you were talking, one of the things that you were making me think about was the need to try out the technology before

you roll it out org-wide, and try to get some users involved, just really with any technology project so that the techno implemented in two different organizations, it's going to look a little different. Having that phased rollout can really be helpful and involving the non-techies in that project early on to make sure that the training actually meets the need and then, of course, support.

After you make these changes, do you provide that ongoing support and non-judgmental support to get people through what is a frustrating period, as they're learning new technology that, as Ken says we suddenly put a door in the hallway, they used to walk right through, now they've got to use a door.

Ken Montenegro:

Yeah. The other part that I'm going to throw in is, I'll share, in our environment, we're lucky that we've been issuing people hardware tokens, as part of multifactor, where we want people... We're like, "Mo more SMS," because that's an insecure second factor. Use an app, or ideally use a hardware token. We were lucky that the Yubico folks gave us a whole bunch of YubiKeys. We've been rolling out.

It's interesting how the adoption felt so much smoother once we told staff, "Oh, by the way, if you use one of these keys for your personal Facebook account, a) you get to keep it." Once you use CCR, we're never going to ask for this back. This is yours. Oh, by the way, this will totally lock down your Facebook account, some of your banking accounts. You can use it with your own personal stuff. We don't care. We're never going to ask. The other thing is that LastPass, relatively recently, I think started this year, says, if you have a corporate account, they will give you a free family account.

How good that is, I don't know. I use a different password manager for my personal stuff, but still there are these openings where, and thanks, Husain, for that reminder, that invitation to think about this, because so much of our lives are digital, this is actually an opportunity to improve the at home, or the out of work life of some of our staff and actually learn from them as they give us feedback. Thanks, John.

John Greiner:

Sorry. I guess in terms of some of the initiatives that organizations might take on, I don't know if Husain and Ken, if you might talk about what we're suggesting that folks consider?

Husain Rahim:

Yeah. Like John just mentioned before, multifactor authentication, Single Sign-On. One example of multifactor is Okta. It's very important to have multifactor set up. For example, going back to the phishing slide, say, for example, if you

accidentally give out your password and someone now has access to your account. Why multifactor is important because they'll still need that other additional form of security before they could actually get into your account. Whether it's through text messaging, which isn't as safe, but it's still another option. There's text messaging, voice call, or through an app provided service, all that's important, and it helps with tying down the security in case if it ever happens.

Single Sign-On, just like John mentioned earlier, it's an easier way where people aren't writing down their passwords or they're having it saved all over the place. All you need to know is your Single Sign-On password. You log into your account and from there, you can access all your other services, whether it's Office 365, SharePoint legal server that everybody loves to use, it's all under that one umbrella. Just having that one password, which is also tied down with multifactor, really comes into play.

Ken Montenegro:

Yeah. Building on that, I think, Husain, that's so well put, because I know for our users, the sexy thing about moving services to SSO, is, you don't have to open LastPass anymore. It's like, no, there isn't another login. On the back end, we know, on the technology team side, that in a very roundabout, almost covert way, we've implemented second factor, because we know the authoritative source is going to say like, all right, that's a good user, come on in.

But the user doesn't see that, most of the time, which is ideal, because, as I tell our support manager, I'm like, I want our job to be invisible. I want us to be a lubricant that people don't even feel we're there. We're just like, everyone's moving, able to do their work, et cetera, in a way that's smooth.

Anne asks, does that mean password managers aren't needed as much as if you have MFA? I would agree with that statement, that I'm trying to make our LastPass obsolete, where it only exists to share accounts that are not SSO capable. I would say that's an accurate statement. The other thing that I'm going to stress, especially for the HR or the deprovisioning nerds in the audience is, just the beauty of, once you revoke the original token, then suddenly you don't have to turn off 20 different accounts. Let's say in our phone system, we don't have to go like, oh no, I forgot to go into the phone system and turn off this person's account. Now that we're using SSO, we revoke the initial token, and if someone's trying to get into the phone system using that person's account, they can't because that token is not going to be issued again, because the user account doesn't exist. I'm sorry, that probably was a little bit into the weeds but-

John Greiner:

But there are administrative management benefits to some of this. Setting up new users can be quicker, tearing them down, if they're leaving students, obviously volunteers are critical to legal aid. You still need that same level of security for anyone, really, volunteers or staff. Again, there's a silver lining to some of this inconvenience, and some of this expense.

I just want to... Again, I think we talked about the taking stock, but it really is important to understand if I guessed right, and I think the folks who are on this call know that, but for staff in their offices, they're back in their offices to understand that a lot's changed over the last couple of years. Getting a handle on that, inventorying that, knowing where that data is, having control over that data, that's a big initiative. It's a lot of work, it's laborious, but it really is critical.

It's not quite knowing where all the skeletons are buried, but it is, we need to know it and then we need to have a plan on whether we need to bring it back in-house or make sure it's destroyed, if there's any kind of privileged information that's out there. Again, I don't want to undervalue that need to go back and take stock.

Ken Montenegro:

Yeah. I think that's really one of the key things for me is, I think John, you framed it this way of, the emergent situation, the tragedy of a global pandemic forced us all to become very inventive and resourceful in how we do this work. The fundamental question is as we move out of an emergent situation, into a new state of, I don't know, let's call it normalcy or return to workacy, whatever, something new, to this new phase, is how do we get people all on the same page? With the understanding, particularly for folks who are working on the direct services side, in those initial days, they had clients they still had to see, and there was this whole degree of re-engineering of how this work is done.

How do we create that safe harbor where people can say, oh, by the way, you know what, I know the court says to do, e-filing this way. We didn't have licenses to that tool. IT couldn't get me Acrobat Pro. So, I'm actually using this other tool and I'm saving all my documents to the cloud, because it's safer than the shared computer at home. How do we engage folks with those conversations in a way that isn't about, you're a bad employee or, oh my God, that's risky.

But we could say, oh, hey, let's do something along the lines of harm reduction. I get it, this is where you were, where do we want to be together, and how do we get there, with the understanding that it's also not going to be like, okay, we're back in the office, everything works how we did before the pandemic. I used to do a lot of consulting work and some folks still hit me up for some stuff. In a couple of conversations that I've had, it's interesting that there does

seem to be this undercurrent of, we want to hit the reset switch and we want to go back to how things were before the pandemic.

I don't know if that is a reasonable expectation. Once again, maybe as we're thinking about security, just with how security always shifts, maybe accepting that how we do our work has shifted. But, how do we get people to, this is our new baseline, this is where we want to go from our jump off point and getting there together.

John Greiner:

Well, it's funny because I was just with the session before this, with the panel of judges about the changing hearing practices. The courts have changed. I think our clients' expectations have changed, and I think, at least the newer advocates joining legal aid, their expectations have changed. I don't see how we can go back to where we were. We were already evolving in a direction out of the office, I think, but this has just accelerated it, and I think the stakeholders of legal aid are just not going to allow us to go back to the way things were.

Husain Rahim:

Yeah.

John Greiner:

Sorry, Husain.

Husain Rahim:

Speaking from a help desk point of view, getting back into the office, documentation's very important. You have a lot of people who haven't been in the office for the last two years. If help desk has updated any equipment or updated technologies, I think documentation's very important, because nowadays office is reopening, some offices are starting at 20%, 30% capacity, and working their way up. As you're having users come into the office, it's important that you have that documentation for them, you're not putting too much stress on your IT team. They're not having to go after every user to explain what's new, what's not, which account still works, which doesn't. Having that documentation on hand and just being able to give them out definitely comes in handy on IT side.

John Greiner:

Absolutely. We have just a couple more minutes on this slide, but would one of you like to talk a little bit about more advanced email screening and I think Ken, you were talking about the endpoint detection and response earlier a little bit.

Ken Montenegro:

Yeah. I know that Husain is really going to want to get into the EDR, so I'm not going to steal your fire. Do you want to talk about EDR for a second?

Husain Rahim:

Yeah. The best way to describe EDR is like antivirus on steroids, where it's basically, it's scanning your computers, checking your emails, checking any services that you use. This correlates back to phishing, for example, if you happen to click on a link, EDR would automatically stop you from even accessing that website. It'll throw a message saying, "Hey, this website is not safe, please close your web browser." It's actively scanning your computer.

If you have a VPN going, it adds a second even more secure tunnel connection between your whole network and your computer in the office, stopping anyone from interfering through that. EDR works with multiple layers, and depending on which service you're using, you're just adding more and more layers of protection to, not just your home network, but also when you're remoting into the office network as well.

John Greiner:

That layered approach is, again, instead of building castle walls, which maybe worked when we were all in an office, but now the castle is everywhere. Essentially, EDR creates those layers of security with your laptop or your tablet and some of the platforms, even with your cell phone. Anne has a question about, if someone loses their cell phone, which might have passwords saved in the iPhone password manager that's included with the iCloud, and maybe also has an MFA app, like Authy on it, what to do? Maybe also what to do ahead of that, perhaps. What would you do to manage that potential risk? Because it's a common issue.

Ken Montenegro:

For me, this ties to, and then I'd love to hear what Husain has to say about this question. For me, we've actually suggested that our folks with their second factor app actually use Authy, because Authy is cloud-based and redundant across devices. It has a very good end device enrollment security process. We don't have to worry about people backing up their codes.

But the other thing that we do is, and particularly, let's say for our VPN, which by the way, shout out to the Just-Tech people who helped us figure out how to do it right, where the password manager at CCR, we're telling people to save up their backup codes. Usually, when you set up a second factor for access, you're given a number of backup codes in case you lose, let's say the Google authenticator app, Microsoft authenticator, et cetera. In case you lose the

phone or the device that you can use a backup code to get in, re-associate another device and then things are all back to normal.

I like Authy for that. The other thing is, yeah, within the question that Kyle presented earlier, the second part that I failed to address or mention was the difference between a local password manager, like what Anne is mentioning or a cloud password manager. Cloud password manager has the benefit that your passwords are backed up to that cloud. It has the detriment that were that password manager vendor to be compromised, they have all your keys.

I think that it's a calculus of what is the right tool for the environment. But for me, with direct answering to Anne's question, is, a) before the phone is lost, move to a password cloud manager and make sure that all staff are using the same password manager. Because in an organization it's very unlikely that everyone has an iCloud account, which will be where they're saving-

John Greiner:

There might be some Android users out there. But I would say, again, any devices that... If you can get your staff, whether they're personally on devices or not to encrypt their cell phones because Android and Apple allow you to encrypt, to make sure that there's a pin code set with a maximum number of tries, so it gets erased.

This goes to the second part of Anne's question, can someone else get in? But also knowing what people... Getting people to feel comfortable saying, "Hey, I lost my phone." "Great, thank you so much for telling me. Let's work to secure the accounts and figure out what we can do to help secure your data too." You want to work together with them, but it might be revoking, like Apple, for instance, there's so many devices that are authorized for iCloud. You can revoke that access so that if they did figure out the pin, let's say you put in six 7s or something as your passcode, which hopefully no one would ever do, and they guessed the passcode or they use some other expensive, if it's a government agency or some sort of wealthy group that can crack the iPhone. You can still revoke access to your iCloud account.

Similarly, like with Authy, you can revoke access too. The more you know, the sooner you know, the more you can do. But obviously, at the front end, if you can make sure that you're setting these devices up, so that they're a little more secure, like with encryption and pin codes, you're definitely better off. It protects their, as Ken and Husain both said, it protects their personal data too, and their information that's equally important to them.

Husain Rahim:

Yeah. I was also going to mention, in the case with a lot of clients that we provide, we use the service called Okta, which is a single sign-on service. From the management console, we're able to revoke and kill any of those

authentication apps that you might have running. For example, Anne mentioned, if she had authenticator app, that's spitting out a code, we could kill it from the management console.

We usually have to do that when we have users moving over to a new phone, where we'll revoke all their old multifactor access and then set it up for their new phone. In the case that Kyle was mentioning, do we usually use YuniKeys or stick with apps? I've noticed a handful of people use either/or. In our case, for example, Just-Tech, we usually stick with apps because you're able to manage it from a console, or you could always deactivate it. Even if you lose the phone, someone gets in and they try that code, it's no longer working because we had already deactivated the access.

John Greiner:

Yeah. There's a platform from Duo. There are a few platforms that allow you to do managed across the organization, MFA and single sign-on. Okta has a really nice program for smaller nonprofits, in terms of their community donations, that's good to consider.

The other thing is, again, SMS, if you don't have any other second factor, certainly SMS is better than nothing. It's a start. I know we're getting close to time here. In three minutes if we can get through this, I want to mention some resources and I really appreciate all the questions coming in. Please keep sending the questions. We'll try to follow up after and answer them, even at the end of the session. Some low hanging fruit. What most organizations could do now without major project?

Husain Rahim:

In this case, as the first point says, keeping everything up-to-date. I mentioned this before on an earlier slide, if you have old equipment, this also ties into the second bullet point, don't have old equipment sitting around, being used. Get a shredding company, shred any hard drives, anything that you're not using. Keeping all your equipment up-to-date in the office, but also at home. Remember, you have users that are using their personal computer, personal devices, make sure that they're running either a VPN, they have the EDR installed on their personal devices and make sure that they're keeping up-to-date.

In our case, we use a remote service with ConnectWise, where we're able to push out updates automatically without even needing to touch the user's computer. We're just in the background pushing out updates. That's important to keep everything up-to-date in the office and at home as well.

John Greiner:

Ken, anything you'd like to add?

Ken Montenegro:

Yeah. I think it's interesting just to think like that. That is super best practice, Husain, where I think we've come to the point where it's super cheap. We do it, at my previous employer, Legal Aid in Los Angeles, good folks there. We were always big on patching because for me, I was like, this is the cheapest thing that I could do, and I can do in bulk and I can deploy software and it saves so much time, and it makes everything more secure.

The part that I really do want to highlight, and it's coming back to the idea of creating a safe harbor is, once again, creating space for honest conversations to happen, where people can say, "Yeah, by the way, I've been using my Dropbox." Because I didn't have time to learn how to use the VPN correctly or because the SharePoint library I was supposed to have access to, isn't letting me in, or whatever is happening.

John Greiner:

Or I use this e-signature platform because the firm was slow in getting e-signatures going. So, I've got like 10 documents that were signed from that platform.

Ken Montenegro:

Yeah, exactly. Other platform that nobody else has heard of. But by the way, it's what someone told me to use, and now that we have-

John Greiner:

It's with my personal account. Now, if I leave... Yep.

Ken Montenegro:

Yeah. I think just going on in that vein, John, just the store photos, documents on firm systems, like the Lens SharePoint is there are so many camera apps that do document scanning that a lot of people use because people at home, staff at home, not just people, staff at home may not have a flatbed scanner or any other type of scanner.

Once again, what we're trying to do is how do we applaud the resourcefulness of staff, but also make sure that we're enforcing security practices? Having those conversations that are like, yeah, I know you're using Lens, but let's make sure Lens is not saving them into your personal OneDrive.

John Greiner:

Yeah. Using it properly. Microsoft Lens is free with your SharePoint, but it does let you store to multiple locations. It's the right tool, it could get it to the right place, if you do that training and presentation support.

I wanted to share a few resources. Fortinet is a security firm and they just have a really nice plain language, top 20 attacks, common attacks. We got into just a few of them, but I think most or all of them we've seen. It's worth understanding because not only does Fortinet talk about what those cyber-attacks look like, but they talk about approaches to try to mitigate those risks. Then the FBI just released its 2021 cyber-attacks report. If you have a little time to just browse through it, I think again, it's worthwhile.

It might be something you'll use when you're talking with colleagues or board members or funders. Then as Ken mentioned, the LSNTAP security tool kit is live and available for you to use for more information on most of the topics we talked about. If you see a need or gap through LSNTAP, we can continue to try to improve that tool. Really encourage folks to take a look there.

At that, we are, I guess at time. We will, again, look at any questions you put in the chat and try to make sure that we address them in the next hour or two. Thank you, Ken, and thank you Husain very much for working on this.

Ken Montenegro:

Thank you everyone. Especially, you, John and Husain.

John Greiner:

Thanks for attending. Take care.