October 14, 2025 Meeting - Seattle Community Technology Advisory Board

Topics covered included: Seattle IT Cybersecurity Update

This meeting was held: October 14, 2025; 6:00-7:15 p.m., via Webex and in City Hall Room 370

Attending: s

Board Members: Phillip Meng, Aishah Bomani

Public: Dorene Cornwell, Robert Kruse, Aaron McCloud, Rahim Malik

Staff: Jake Hammock, Brenda Tate, Jon Morrison Winters, Vinh Tang, Cass Magnuski

11 In Attendance

Vinh Tang: Welcome to the October 14 Community Technology Advisory Board meeting. My name is Vinh Tang. to get started, it is unlikely that we will have a quorum tonight. Several board members are out of town. We will still proceed to have our meeting tonight. Since we do not have a quorum, we cannot vote on anything. We cannot take any CTAB business this evening. We will just proceed with the presentation. Cass Magnuski is taking minutes for this evening. Thank you very much. With that, I'll stop talking and defer to our chair, Phillip Meng.to commence as normal.

Phillip Meng: Thanks, Vinh. I'm really quite excited for this meeting, which aligns with Cybersecurity Awareness Month. As Vinh noted, we will keep it short and sweet. I want to start with a round of introductions.

INTRODUCTIONS

Phillip Meng: Given that we won't hold a vote on the minutes or the agenda, we can jump right into our main agenda item today, which is a presentation from Jake Hammock. With that in mind, would you like to introduce the topic of the presentation with a couple of words on what would be helpful from this committee?

SEATTLE IT CYBERSECURITY UPDATE

Jake Hammock: Thanks, everybody, for joining this +month's Community Technology Advisory Board. I have a special presentation on cybersecurity efforts that are mainly applicable to what you can do and how your actions can propagate security for Seattle as a whole.

A little bit about me. I recently joined the City, about four and a half months ago. I have a multi-faceted background. I worked for the federal government. I am an Army veteran with multiple tours. I also worked in the intelligence community for many, many years. I was a cyber national (unintelligible) commander within the US Cyber Com and have worked in all sorts of cyber operations, where I led several units. After my tenure with the federal government, I then moved on and become a (unintelligible) at a Fortune 2000 company, where I worked defense. From there, I came to Seattle. I very much have passion for the cyber community and eco-system and our nonprofit partners. I have a very diverse career in cybersecurity from the offensive side to the defensive side of our operations. I am honored and thrilled to be the Assistant CTO for Security and Infrastructure and Chief Information Security Officer. A little bit about me. And I made a presentation tonight that is inclusive to how you can better prepare yourselves, and to applying cybersecurity trends, tactics, procedures. Some of this information may not be new to you and some of it may.

There is an important point that I will make at the end of it, that even notifying one person can have an extreme impact that will better our City's operations. So, I hope folks will be able to hear me, and that is the purpose of tonight's Cybersecurity Awareness Month briefing for CTAB is to create more of (unintelligible). I will tell you up front that we will not be disclosing any vulnerable system data or infrastructure data, to ensure the integrity of our information systems. I'm sure that there are multiple questions on what we're doing at the City to protect our high level program overviews to be mindful not to expose vulnerabilities so we can better protect our critical applications and core services, public safety technology, so that we can best support our residents here in the greatest City on earth.

Today, I'm going to go through a few frameworks, our home methods and stock protocols, and I'm going to be introducing a few cybersecurity trends that I have been seeing across the years and some novelty trends that are affecting our industry as a whole. We can hold all questions till the end. If you do have a question in the middle of it, by all means. We can make this informative. We can make this engaging. I would rather have questions at the end because we can just go back to the slide.

What are we aligned to? Well, we started One Seattle. That's Mayor Harrell's priority, and anything referencing cybersecurity in our applications we apply to One Seattle. And if you look at the link -- and I will share the slides at the end -- there is a specific section, multiple sections actually, within cybersecurity and how we nest in the matrix within the One Seattle framework. So, how we apply cybersecurity is a multi-faceted topic. We're talking about application firewalls. We are talking information protection, risk management and reporting, cyber insurance policy enforcement. We have compliance control, such as DCI. I'm not going to go into all of these acronyms, but it's very complicated and an ambiguous subject. So, I want to start with our foundational model and what it is. It's no longer optional. It's essential. What we do here with the City is include as much as we can to all departments. There are more than 39 departments within the City. We do our best to strive forward and include cybersecurity in all departments' functionality. From public safety technologies to internal applications, process and payments. I've highlighted some domains for reference here, nested to the One Seattle priority, to communities, we innovate with security, we absolutely ensure that equity is included in any decision we can possibly make so that we provide a transparent atmosphere. In the bottom one, you see opportunities. These are the opportunities that we can improve on as a community, as a City, in a trusted partnership in delivering our secure services to residents. Let's face it, right, we are not in the business of selling cybersecurity. We are in the business of ensuring that all systems are safe and safeguarded. When you hear about security generally in the news, it's not a good thing. So, it's actually great that we are operating with the transparency need to apply these controls, to apply good governance, to apply what we can do to safeguard and ultimately deliver trust to you and residents of this community. So, the opportunities are actually what we're going to expand upon for really the next two to three years, aligned to the IT strategic approach. If you have not already viewed the IT strategic plan, I encourage you to do that. Our cybersecurity operations are also nested under One Seattle, under the IT strategic plan into what we see now.

We want to skate slightly into why these areas are important, going back up into the column of thriving, innovation, equity, digital, and AI. Scams are on the rise. We know that. And even last week, you saw a banner on the seattle.gov web site, there was a real (unintelligible) scam in the City. So, as they are increasing, we need to match this level of threat vectors head on in a way that we can mitigate as much as we possibly can. And with good processes, great technology, and even better resources, and our staff, which we are constantly training and (unintelligible). So, we need to protect for small businesses and our commercial partners. to include our nonprofit partners. How we innovate, going to the domain in the middle here, it's one thing to say you need

confidence; it's another to know it exists. So, what we do in inserting trust into all of the IT systems that we have, and that includes (unintelligible) systems, email going in and out of the City, when there is a radio call for a public safety response, all of this data being processed and is stored in multiple areas. Think of servers, computer drives, mobile phones, that need to be processed, and secured for all systems, all devices, all networks, if we are to deliver on that One Seattle promise and our commitment.

And then finally, equity. Something I want to touch on here is that non-English speakers can click on a link. That's generally in our inherent nature, to trust emails, content coming into us, documents. We have an entire nature in humanity to trust one another. And unfortunate as it may be, we have a rise, for one reason or another, we have acts of malice. And it is easy to click on a link, especially if you don't know the language here. So we want to make the point to ensure that all of our recording channels are in multi-(unintelligible), as we comply with our digital accessibility working group, we assure that we maintain our commitment within the April deadline for federal requirements so that all content is accessible to the public. We're going to leave you with a clued in awareness, including multi-lingual reporting channels for anyone in the community, and also with some good practices and how we can better ourselves.

Some of this may be new. Some of this may be old. I'm going to start with the foundation, something I was trained on early in my career is foundations save lives. Another way to put that is complacency kills. That's exactly how I was taught at an early age in my career. You may know this, but actually it is a great refresher. Check the domain when you click on a site. If the protocol was https, look for the 's.' That means it is a secure link. And I always refer folks to always communicate with a secure link. We can go into some of the nuances and what that means, which is (unintelligible) security, But just look for the 's,' and it will make sure to tell you that the site you're communicating with is trustworthy and has a security certificate that has been issued. On the top level domain, you see Seattle.gov. Oftentimes, scammers will use different domains to trick you. We see seattle.com or seattlebillpay.com. It is always mindful to please look at the .gov in the top level domain. And then you have sub-domains right after that. After .gov, you have links to initiative, one of our departments in the City, a project that we're funning that is open. So, I just want to give you a refresher on some domain knowledge that when we look at a URL, this can come in handy, especially if any of your antivirus systems allow malicious links to come through, like in an email, for example. Always QA. Always quality control. You just need a domain to make absolutely sure that your domain is trustworthy. Too often, if you look at the bullet in blue, most domains with domain look-alike, that is a primary threat catcher. That will expose

sensitive data. But we trust the links, right? Let's make absolutely sure that the link we are clicking on is what we should be looking at. The City only uses seattle.gov. I want to make one important distinction that our friends at the Seattle Public Library use .org. Those are the two primary domains for the City of Seattle, Seattle.gov and SPL.org.. And then, any sub-domain after that has implicit trust through the main top level domain. We're going to talk more about some of the social networking fata, and this goes into my introduction here, that all it takes is informing one resident that has a ripple effect, that can positively impact our City. I was able to find that we have about 150 online contacts. We're all residents here. And then one prevents a breach, that's a potential 150 targets saved by telling one person that they propagate through their network. That's over 15,000 people that could be protected through reporting. And I will provide a supplementary handout later. So, the network impact is very, very real. And something I should mention up front is that we have approximately 860,000 residents in the City of Seattle that we serve, and 860,000 reasons why our team, why I, our executive staff, and IT, and our department partners every morning. That's 160,000 reasons why we put our best foot forward to secure your data in our environment to deliver our critical services to you.

There is a lot happening on this slide. Lets start with some of the new threats that are coming online. I'm curious to know, and maybe we'll have a discussion at the end, but phishing is on the rise, voice impersonation by phoning. We have heard of phishing in the past. Phishing means simply that someone is impersonating a trusted user in order to trick you into exposing sensitive detail to pay a bill, to do something. vishing is on the rise. This is voice AI and it is extremely difficult to detect. We actually just saw this in the City last week. So, if anyone has been exposed to this, you may know how difficult it is to detect with AI. AI has many models that can train and learn how to replicate and use your voice pattern, to include your behavior. I read an exercise recently to prove how easy is was to conduct vishing by replicating our voice. When this happens, there are a few things you can do. We will go into prevention techniques, and you can see them there. We need to encourage more validation mechanisms with our trusted friends, our partners our community members, even the sick, through public safety with vishing on the rise now as a credible threat. Phishing has also changed. You're not going to see typos anymore with AI. So, with large language models, small language models retrieval automation systems in AI logic, we are seeing phishing that looks identical to what we would see from a trusted party, a trusted organization. Maybe it's an insurance company, or a healthcare company that is reaching out, that is attempting to phish or vish you, and this is even more difficult to detect because there are not typos anymore. You could once spot if there is a typo or a character that was misspelled and didn't look right. Now they look incredibly better. So, let's go right back into our validation methods

here. Let's email a verified contact. Let's call the verified numbers. Generally, scams occur by levels of urgency. If someone is attempting to claim that you need to pay this ticket within two hours or there is some consequences associated with it. Oftentimes, that can be portrayed as a scam. With these urgency maneuvers when they start coming in, always call back. Always verify that those are the official channels. If there is urgency, there is a high likelihood, especially with domains, that it is most likely a scam. We will talk about multi-factor authentication later on in the brief. And the last picture on the bottom right is a real scam from Pennsylvania, a pay ow utility scam. You may have seen these in the past in the City. I believe not one city is immune to this particular type of threat, and that's why I brought up the domain security and domain observation at the beginning of the presentation. Make sure to check the domain. Look for that .gov. We are working with Seattle Public Library, or using their services, a .org. So, these scams are very, very real. It is very difficult to detect them. And we, as a City, are doing everything we can to inform you when they are here. You also are telling us where malicious web sites are. We will get into how you can communicate with us, and directly, our team.

Another threat is on the rise. It is QR codes, or QRCs. It is very common, when you see a QR code on a slide presentation -- and I made sure those are not linked to anything -- that we want a standard. We want to take a survey, we want to unintelligible). It's easy. People don't have to type in a URL. With the same approach, hackers also know how to do that. So, unfortunately, they take advantage. But again, going back into simplicity, simplicity is our greatest strength in understanding. And it is also what nefarious actors, malicious actors precisely what they prey upon is not understanding, which is why we elevate simplicity and foundation, QRCs are on the rise, QR codes with malicious data. A couple of things you can do here to prevent this particular scam is 1) (on the far right of the slide) you can see that it looks pretty obvious. Congratulations! You have won. You get a unintelligible). You see the urgency that is applied. You don't know who this person is. Those are generally dead giveaways that it is a scam. When I say scam, there also could be malware involved. Malware is short for malicious software. When we think of viruses or malicious executables, that's what I mean by malware. It's essentially spyware. Anything running on your device that you don't know about or that you did not implicitly authorize. We don't really know what is behind these QRs, but it's a lot most oftentimes. And there are applications in the Google Play store, in the Apple marketplace, where you can have app scanners to verify the link before you actually scan with your camera. I've used a lot of them, and they work really well. I would encourage that if you don't already have one to verify the link before I actually know what I am clicking on. The City of Seattle also uses QR codes for payment. And we do that because of that .gov domain. So, I put the valid City path on there and you see the

slide deck. In order to pay a bill, always go behind that pay wall. Seattle.gov/pay. And you will see all of your payment options across our utility partners, our SDLC, Department of Construction and Inspections, Seattle Police Department, Seattle Municipal Courts. you will see any payment information for how you pay for a particular service behind that pay wall. So, we give you QR codes in bills that we send out across the City. One thing that I wanted to point out. See that banner in the middle of the slide? That was posted on the Seattle.gov web site. If you looked at the web site last week, there was a malicious robo-call happening around town, someone was claiming to be a representative from Seattle Municipal Courts. You had to pay these parking tickets or else. You see the urgency behind that, and with the urgency applied, there was a good chance that it was a scam. Luckily, it was reported so much that we put the banner up immediately. But when that happens, there is very little we can do at the City because we can't control that infrastructure. When that happens, we will do everything in our power to inform you. And this will happen again. This will happen continuously. We will do our best to keep informing, and create the recording channels back into the City so we can propagate and share that message out.

Vinh Tang: Before we move on, that image that you have right there, is this a situation people in a public setting are basically making a huge sticker, a QR code, and then putting that on the City?

Jake Hammock: We're not seeing it in the City, but I have seen that in other areas. That's how easy it is to replicate a valid QR code. It's similar to the gas station hat trick, where you put the payment terminal in front and you scan your credit card. It's similar to that.

Vinh Tang: Gas station card skimmers, too.

From Chat: Robert Kruse: Excellent. I attended PACT-hackathon last Thursday at AI House. Eventually that intersects here with Cyber..

Robert Kruse, VenLogic, DigitalTwinsNorthwest.org

Jake Hammock: Right. Same principle. There is definitely a code in your magnetic strip. That's why I would recommend to everyone to have a QR scanner. That application will run immediately before your camera does. If you're running anti-virus on

your mobile device, you can see if it is safe or not. So, be on the lookout when you scan something. We're seeing a resurgence of this particular vector (unintelligible). I can print out 10,000 QR code stickers, place them somewhere and redirect a web site to a malicious site. So, we want to be mindful of that. I'm happy to go back and answer questions.

I want to leave everyone with a few methods. This is one, particularly, that I have used. I like it. It is foundational. And even having been in the industry for more than 15 years, I still use these foundational models, even on my home network and when I am interacting with external networks, to include the City of Seattle. Because I live here, too, right? The HOME is harden, optimize, manage, and ensure. And we can go through each one of those. We won't go through each bullet, to save you time, but harden means we harden with updates. When is the last time that we have done a forced update of all of our applications on our mobile device? A lot of folks don't do it. Another one is if you are using a router from more than five years ago, on your home network, (unintelligible). Hackers love that, because firmware updates are not automatic. They are now when you have Meshnet working or Starlink or WiFi, or Amazon, with their smart system. (unintelligible) is another one. Netgear now includes it. So, if you have a router on your network that is over five years old, that router may not be patched . It's difficult to find out how to do it, because you have to enter your IP address and to the header bar, the URL, and your login to your router, which is not your WiFi login. So it's a process for how to update it. I would encourage everyone here to check the make and model of your router in your home network. You can Google, or prompt to an AI source of your choice, how do I update and patch my router, with your make and model number. And that knowledge base is out there. Those articles are out there. They will guide you into including and inputting the right IP address, your username and password. And I finally encourage everyone upgrade, update, and patch your router.

Going to the 'O' and how we optimize, this is actually going to be a takeaway I would recommend for everyone here. If you would make one small change tonight, let's optimize. How are you authenticating into your device, your mobile phone, and your applications that you use and trust? Banking, healthcare, insurance, critical service that you have for monitoring your family, for example, on the network to ensure their safety. Do you have multi-platform authentication, a means of accessing your laptop, your desktop, your phone, for the applications that you use, such as banking, healthcare, and email? If not, I encourage you to. And I'll tell you why. It is difficult to exploit and hack multi-factor authentication. That's what MFA is. It's a loaded term. It comes from the old

CIA triad, which stands for confidentiality, integrity, and availability of all systems that you have. (unintelligible) preserving the integrity of all data that you have. So, we'[re talking about the three tiers of what multi-factor authentication. It is something you know; something you have; or something you are It's a combination, two of the three, it doesn't matter which, but two of the three. So, with the MFA, do you have a fingerprint bio-reader? You combine that with a pin number or a password or pass key, which could be a hardware USD key that combines authentication within the device. So, it's two layers or more of how to authenticate into a machine, a phone, desktop, your banking application, which most of them now do require MFA To access. Some banking applications (unintelligible). I would encourage you to apply that same rigor into accessing your personal systems. It is much more difficult to exploit when you have multi-factor authentication applied to your accounts. Protect your accounts. It comes in handy. Most exploits come from accounts. It goes a little bit in the HOME framework. Manage your passwords properly. Never reuse the same ones. I know how painful it is to have more than 30 applications for these services that you use, each one requiring a different password. This is why I suggest a password manager. A lot of people use them now. This is not a new concept. But continuously recycle and issue new passwords, beyond the password manager. I highly encourage it. So, you don't have to remember these 30, 40, 50 different passwords, and it can generate new ones without you ever having to remember them again.

Let's go back to the final component of the HOME method of ensure. And ensure goes into the availability line. (unintelligible) When we say media, it can mean two different things. It could mean the style itself. So, let's say I wanted to have a photo in a JPEG and a PNG, two separate files. If one is corrupted, I always can use the second file. Or with documents, you can have a docx file or a PDF, two different media. You also can have two different media by the technologies they are stored on. That could be having one picture stored on my laptop. I have another picture stored on an external hard drive. I'm sure the backups exist (unintelligible); inevitably will fail. They are depreciating assets. We know they will fail over time. We have Moore's Law that tells us that will happen, so we prepare for that. We also live in a natural disaster area. We have earthquakes. We have tsunamis here. Let's ensure that enough data replication exists so that there is no data loss. The continuum of data is ultimately where we all should be. Even with personal photos and personal documents you have on your host systems. I always recommend that you keep that 3,2,1 rule as much as you can. This whole framework is cyclical. Even recently, I took my router as an example. I changed my passwords on too many applications that I personally use, and I deployed pass keys to access several of my systems. So, that's the HOME method. It actually can stop most attacks from happening. You can harden your own network and your environment.

This one is protocol. It's getting a little bit deep here within a protocol. It's kind of like you are home in a box. This is a protocol that stuff can happen, and when they do happen, what are you going to do? In the cybersecurity world, we call that the mean time to contain, and the mean time to respond. But rather than go through these highly technical frameworks, let's talk about what happens if you become exploited. If you have data that is exploited, or is compromised, or a hacker has taken control of a system, it's a little overwhelming at first. If it has never happened to you, it's overwhelming. It has happened to me in the past. I've seen it done many times. And when it does happen, this is the protocol that can help guide you forward. It's basic. It was proven. It is effective. It has been known to work. The first one is implement MFA immediately and change your passwords if you have access to the system. When you change your password, hackers don't have access to the account because we've rotated the key. Track it. Document everything. What has to happen? You may be filing an insurance claim. You may be filing a police report. You may be filing a complaint with the FBI Ic3. And I will go into that as the very last thing. Track everything, because local authorities and different agencies are going to need to know exactly what happened so they can eventually prosecute if they can identify who it was that hacked your system (unintelligible) channels. Going back into the first part of our brief here today, contact the official channels. Look for that .gov. Look for the banking information on their official web site, and contact them. Contact your credit bureaus. I believe that it is even free now to implement a credit freeze if you are a victim to cyber exploitation. So, contact your official channels and the official channels of your public safety authorities. This is an interesting one. Recovery takes time. If you have data that was exfiltrated, if you have a system that you can no longer get access to, it's not an immediate effective approach that wishful thinking it away, to say that the system is going to be back online is not how this works. It can take a long time. It can take up to months for a full system containment and recovery. That's why I recommend again, repeat the HOME framework and ensure that the right authorities are notified. They can help you to mitigate this when it does happen. I have a few links here for Seattle support systems, specifically. I also put in the State of Washington consumer protection site to file their reports for any fraudulent practices you might see. But also Ic3. The Federal Bureau of Investigation has the Internet Crime Center. You can file a complaint with the malicious (unintelligible) and track all documents, photographs. The FBI will see this and initiate their preliminary investigation. And then, on the far bottom right, we talk about some recovery timelines with a factor of one. What do you do in the first hour? Secure everything. The first hour is the highest value moment of how you respond. So, secure your accounts. Implement MFA. Contact he official channels and authorities on day one, and on the same day that the event occurs. File your reports. If it is impacting your credit, (unintelligible) your credit. Ensure that your banks provide new cards, new numbers. And that process is

automated nowadays, so one call can take care of most of that. In your first week, secure all of your accounts. If one account was compromised, it's a pretty good idea to implement the same security controls from the HOME framework all of your other accounts. So, if you use one banking provider over here, let's ensure that the same security is provided over here. Rotate your passwords. Change the way you authenticate. It's a good idea to propagate that even to your own HOME network. Maybe you need to change your router password, or your WiFi password. Even though it was a separate application, it is a good idea and good practice to implement the HOME framework again to all of your systems, then you contain and you control. And the first month is monitored, because there may be active law enforcement investigation that is occurring. Monitor what happens and always be in contact with the appropriate authorities.

This one is a bit different. You're going to mention your nonprofit partners. and WAPAC at the State and State agencies has partnered with a wonderful initiative out of UC Berkeley, which is the center for long-term cybersecurity. I want to read a brief here that is very impactful. So, we have the start-up founders, which is wonderful, and the same logic on the fly. We absolutely want to lean in with our community partners and see our resiliency through. In Washington State, the majority of public services are delivered by nonprofit organizations. For State and local government grants and contracts. And nonprofits are the second most (unintelligible) sector for cyber attacks.(unintelligible) trying to disrupt operations, interrupt the central services in our community, Seattle, and so US Berkeley recognized this particular problem, partnered with WaTech in our State, and are closing the resource gap by offering *pro bono* services to nonprofits here in the community. I have attached a survey link. I encourage everyone to take it. You don't have to be a nonprofit or register as a 501(c)3 at all to take the survey. I encourage you to take it and provide that feedback to US Berkeley so they can start modeling what they can do to provide these *pro bono* and affordable services to our nonprofit partners. That 15-minute survey is going to help cybersecurity unmet challenges (unintelligible) our Washington and local Seattle nonprofits and inform recommendations to me and my State counterparts.

From Chat: Phillip Meng: 10/14/2025 6:46 PM •
berkeley.qualtrics.com/jfe/form/SV_37BdFA0V4bHZyNE

I just want to say thank you again, for taking the time. If you take the survey, I appreciate it. And I'm very grateful for Washington State's CTO and the Chief

Technology Officer, the Chief Information Officer, and Chief Information Security Officer for partnering with the City of Seattle and to allow us to partner more with our nonprofits.

Aaron McCloud: I was just wondering if you could share that link in the chat?

Jake Hammock: I'm not on there, but I believe we should. Good call. Actually, I was thinking about doing that. We're going to send the slides out. There are a lot of links in there that I would like you to have access to. But yes, I believe you should do that.

From Chat: Aaron McCloud: 10/14/2025 6:46 PM •
https://berkeley.qualtrics.com/jfe/form/SV_37BdFA0V4bHZyNE

It's here.

Dorene Cornwell: My question was going to be the same. Is there a way to get those links. Because there is a ton of useful information. Actually, I do have a question. I work a lot around people who are really new to computing. And they do things that make me a little nervous, like they can't remember their main email password, so they just leave their machine permanently logged in without two-factor authentication. And some of them are kind of susceptible to scams. My basic question is are you presenting this in different communities? Because there are some communities where half the room will have no idea about some of these issues, even like what is a router. How much are you presenting this in the community?

Jake Hammock: Starting now, starting here. Though I am briefing other areas within the City and City departments that do propagate within the community. I believe it was three or four weekends ago, I delivered a presentation to the (unintelligible) Communication Services Group, where we actually talked about MFA and delivering on essentially ham radio systems and how you can secure them. This is a very complex problem, too. You brought up a good point, though. To do our job effectively in secure systems, we lose people when we start chatting about these nuanced technologies and products and makes and model numbers. That's an IT thing. That paradigm is switching more rapidly than we anticipated with AI. Now AI systems are becoming embedded into machines, which is augmenting our security work even more. That's why you have screens that time out now. And organizations set their own separate policies. It is never

a good idea to leave a terminal open, a machine or operating system that is continuously open. We always want to put some kind of three minute, five minute, or ten minute warning, so it locks up and times out, and only the authorized user can authenticate, based on that two-factor authentication. But that is difficult when organizations don't have those policies configured. It is also time-consuming, right? We have to maintain them. We can roll over passwords. I'll tell you one amazing trick that I have seen across the years that work very well. And that's password-less. Many organizations now are already in a password-less environment, with MFAs, like Windows 11, for example. I believe that Apple has a similar feature, where it is fully password-less. There is no need to put in these long, 16-digit passwords and rotate them every 120, 90, 60 days. We now can authenticate with Q forms where the credential is stored actually on the machine and not on a separate server. So, we're actually moving over all. Is the security becoming democratized and decentralized to the end user? More so than it was 18 years ago, when it was heavily centralized in credential management. (unintelligible) were stored. But we're actually moving that data and security to the edge and closer to you. We are also going to store at the machine -- the laptop, desktop, phone, whatever you are working on -- those credentials will be stored there, as well. But the goal is to get more out into the community, Dorene, to actually share this message. It is greatly important because it impacts more than just the organization. It impacts the entirety of the City. It tends to propagate, so we do want to do a better job of getting out there more.

Dorene Cornwell: Yes. These are brand new users, and in sort of a home environment where there are all kinds of things that come into the picture, but thank you.

Jake Hammock: You are most welcome.

Phillip Meng: Help me understand what the scope of the information security for Seattle. Of course, that is to provide a source of truth when these scams come around. How much communication or outreach do you all do?

Jake Hammock: It is through either this forum or for a digital engagement team that we have now. And chatting with Jon Morrison Winters, who is on the call, we need to deliver this message in different channels more so than a once a month briefing, for example. I'll tell you about another one that we have. I believe this is on a resource handout that I will deliver after the brief. We have our vulnerability disclosure program

for the City, and it's one of the premiere programs that other cities have already modeled off of. Let's say you are a security person or a computer science student, and you see a vulnerability in our web site, or application, or server environment that should not be there. You can report that to us and we will fix it. As a matter of fact, we remediated a fantastic one that was submitted to us. Other cities, to include Chicago, Boston, San Francisco, and Los Angeles, have already replicated our disclosure program. It has been that effective. And to your question, Phillip, we should be getting out there more and partnering with other departments. That's how we've been channeling security, through for example, FDCI, SHR and others. We need to do a better job of interfacing directly with the community. And I do have plans for that. Actually, next year, we are going to include some events for Q2. I'm planning right now, in partnership with my boss, the CTO (Chief Technology Officer) Rob Lloyd.

Phillip Meng: Do you have a sense of how many folks are affected by scams related to these services?

Jake Hammock: I don't have a general number from GAO, the General Accounting Office. I don't have a localized number for residents of Seattle. It's a good question. I imagine that the data is all over the place and very hard to measure. We see a scam. It's typical to capture the data as reported. Federal agencies don't oftentimes share their reporting methods with our local civic (unintelligible). It's only if it is reported to us that we know it and we try to capture that data internally is recorded to try to measure those trends. Good question, though. I would like to remind you of the vectors of what we are seeing in other municipalities, including the City of Seattle. More so than what is our overall trend. Maybe next year we can have some more empirical data.

The final slide here is going to be the challenge. I offer everyone on the call, and there is going to be a recording of the call, to implement MFA on one account. You may have it on your laptop, your desktop. But do you have MFA on any of your critical accounts that you use? Banks oftentimes require it so that is most likely done for you at this stage. But what about your insurance applications? Life insurance, health insurance? Your mobile apps on your phone, have you enabled MFA on those accounts? What about your network account. Do you have Google Home or Amazon or Alexis? Have you enabled MFA to access these services? I encourage, at least tonight, one small move can have an extreme positive propagation for our community. To enable MFA, Multi-Factor Authentication, on just one account. And then, before Friday, can you teach someone in your network of approximately 150 plus or minus folks, about the key

verification method? Especially for what is on the rise. Can you share it with someone. There is a way to verify malicious QR codes. We actually need to look at verified domains. This is how you do it. Maybe you will find an app in your app store of choice that can scan, show exactly what you need, and prove that the QR code is indeed valid and trustworthy and not somebody putting a sticker over a parking meter and attempting to evade your trust. If each person before Friday -- that's three days -- if one person can let this message propagate. The resource is there. CISA, the Cybersecurity Information Security Agency, have a pretty good Secure Our World, which is a very user-friendly, compatible download kit. Again, the links will land in the chat, but when you get the slides, click on the links. But this user-friendly, downloadable kit can help you to secure your systems. I highly encourage you to check that out. Our lovely friends over at the State are also hosting their event, if you are interested in attending the Washington State Cybersecurity Awareness Month events. (unintelligible) is doing something very similar in town here, so you can do that. And then, if you have any web site that you suspect is malicious, you can report that to your provider of choice. So, a lot of folks don't know that. If you have an Alexis site that you visit and there are ads popping up that make you think that clearly something is wrong or attempting to get money out of you, or is a cloned domain that doesn't match .gov, for example, in Seattle, report it to Google. Google takes that incredibly seriously with their security partners and they investigate (unintelligible) with probably the fastest response times I've seen. Safari has something similar. I believe that Bing does something similar with Edge. Look for these in your browser of choice and report those to the providers so they can take them down, because that is truly doing your part to help us secure our City and protect our resources.

I just want to say thank you to everyone listening. I know I went a little bit over, but I'm very grateful for the presentation. So, with that, I will open it up to questions.

Phillip Meng: Feel free to raise your hand or just speak up. I want to start this by saying thanks for coming here and having this presentation. Just as you were speaking, I was thinking about the texts or emails I have gotten, and I have gotten quite a few that revolve around parking tickets, or that revolve around other kinds of City or State services. It goes to show how common this issue is, because it's kind of a ripe target for a scammer. These are services that everyone interacts with, and therefore are potentially applicable to everyone. One question for you: When and organization, or even if just we were to ask, what are some resources that we could share with the community or share with our organizations? Do you have handouts, or other collateral? That would be great to share.

Jake Hammock: Absolutely. It's being reviewed right now, but I do have Help The (unintelligible). If you report a scam and your utility bill with Seattle City Light, this is the link you should click on. If Seattle Public Utilities has a water-based scam or water bill pay scam, this is the link to click on. If it is essential fraud or identity fraud, for example, Seattle Police Department has two separate links that you can click on. If you need to get hold of our team separately, there could actually be a threat to a City of Seattle information system or you are seeing a City service that has been spoofed or impersonated or replicated to the wrong domain contact us. We want you to contact us. Please contact us and send us a note, and that will be at the email address of security@seattle.gov. Actually, this collateral sheet medium that we will repropagate to Phillip Meng and send it out to you. It's a two and a half page resource guide that complements this brief on who do you contact and when, and how to apply the right contact medium, because it can be a little confusing. You have 16 different channels to contact; what is the right resource guidance that will put me in front of the right agency at the right time? Because events like this can happen. So, I will get this out.

Dorene Cornwell: As long as no one else has a question, I have a couple more. One is I love the idea of having handouts, but like a one-page handout about how to detect fraudulent QR codes would be extremely valuable. I will say that as a visually impaired person who is around a lot of people worse off than I am, where we hate QR codes in the first place because we don't always have access to what the link is doing. And so having some tips that will respond to accessibility tools as a big design aspect. You're allowed to say, wait, that might not be out there yet. But that's a big design aspect. Just a one-pager about QR codes.

The other one that comes to mind is, at two different times this year, I have been notified of data breaches. One of them is from a large City landlord full of vulnerable, not sophisticated users. And then, another one is a different place. I looked at the one from the landlord, and I thought I wonder if I need to pay attention to this or not. And I've gotten some weird phone calls and some other things from my bank where, if I dispute a transaction, one time they called me and said, "Do you order from this clothing company?' I said nope, they never have anything in my size. But that effect can last for a long time. Do you have any tips for just staying sane while you are having to deal with these dubious calls?

Jake Hammock: Yes. You mean a robo-call, right? This is how hackers ultimately exploit systems that are difficult for you to control. And it is precisely why the Federal Communications Commission enacted their reporting channels. I will put this into the collateral document to share out. To prevent that is inherently difficult because if you were to receive a scam call, you have no idea how they got your number. I get a lot every day. We can play the whack-a-mole game. Likely your phone settings will filter this a bit better than that in the last few years. I have seen the feature in most phones and models. Another defense layer to recommend is we are all familiar with anti-virus. We do have some level of anti-virus protection on our laptops, but we also forget that phones are computers, right? There are CPA chips in there. So, I would recommend to include an anti-virus app on your mobile device. There is an anti-virus flavor of choice; there are hundreds out there, and they all proceed a little differently. Look at the reviews in your app store. Does it work? Does it not? But I would recommend to put an anti-virus agent and scanner on your device because you can also filter spam and robo-calls out within registry that have already been reported to these services that will auto-block. We can't detect and mitigate scammers from calling you. Your data somehow became exposed and we see it all the time with supply vs. vendors that we cross our information with and they have a data exposure incident. Most often we will never know exactly why. We just know that our data is out there. And when that happens, I recommend to go right back into the HOME method and apply those four habits. Change all my passwords as data was exposed. I am also not exempt. A supplier that I work with exposed my data and I went right back to the HOME method. It won't change all of my accounts. I can't change my number because I'm used to that and have been emphatic for years, but my anti-virus service now is on lookout for the City as it was already reported. Because the phone is not going to pick that up. They are not necessarily in the security business. I recommend you have an app that can help.

Dorene Cornwell: Thank you. That's really helpful.

Jake Hammock: You're very welcome.

Phillip Meng: I think that is one thing that would be really helpful in community messaging. I think that a lot of us know that when you see a scam message about, say, City utilities or something, we know to ignore it. But it is hard to know either what is next or when to be concerned and need to take protective action. Maybe that is something that this kind of collateral can help with.

From Chat: Phillip Meng 10/14/2025 7:07 PM • security@seattle.gov

Jake Hammock: Yes. The one page that I have shows QR codes. I will work on that and do what I can to propagate that message board. We made it with that potentially on our security web site going up next year. When we more like this on the rise, we need to communicate that outward. And at the same time, be mindful. Do we have the right technologies to mitigate? Because some scams, like robo-calls for example, we can't entirely mitigate all of that. It's from the supplier, the FCC it's on the Federal Communications Commission on tower registry through carriers. And they're not accepting all of this either, but there is a one-pager that we sponsor (unintelligible). There is the HOME method. I have a sticker on my refrigerator about this. I'm going to use this now. But just call and we will have more resources soon.

Aaron McCloud: I guess I just have two thoughts or comments. The first one is have you thought of getting in touch with the apartment buildings and the community centers or sort of social hubs to distribute this kind of information?

Phillip Meng: SPL (public libraries), Seattle Housing Authority?

Dorene Cornwell: Yes, definitely, the Digital Navigation Program at SHA. That would be really helpful. And other low-income housing providers are going to have a lot of the same considerations.

Aaron McCloud: My second thought is, if I want to get in touch with you guys, will you share your email information in the chat?

Jake Hammock: Yes. The email is security@seattle.gov. That will take your email right up to us. Also, if you check out our cybersecurity page at https://www.seattle.gov/tech/data-privacy/information-security .

Aaron McCloud: Okay. Thank you.

Jake Hammock: You're welcome. It includes our vulnerability disclosure program, which is also posted on the web site.

Phillip Meng: Folks, I'm sending that link into the chat. Any other questions? If not, once again, thanks for joining us. We will move to the last agenda item for today, public comment.

PUBLIC COMMENT

Phillip Meng: Is there anything that folks want to share? If not, just one item from my end. Due to the holiday next month, I just wanted to let you all know that we are looking at some options to reschedule the board meeting for November. It falls on November 11, Veteran's Day. You will get an update on when the new date and time has been established. All right, with that, once again, thank you for joining the October meeting. We will see you next month.

ADJOURNMENT