Cheryl Dowd (00:00:04):

All righty, there we go.

Leigha Fletcher (00:00:10):

Okay, we're good.

Cheryl Dowd (00:00:11):

Okay, everybody, welcome to our State Authorization Network and WCET webcast. Today, we are very pleased... We can move to the next slide, please. We are very pleased to have part one of our Cybersecurity Webinar Series, and this is the CISA Overview Briefing on the Cybersecurity Threat on Postsecondary Institutions. This is the overview structure, and we will have a part two that is talking about ransomware. You'll see that is June 8th. You can go back to the SAN website, and register for our part two. But part one, we're going to get the big picture.

Cheryl Dowd (00:00:50):

We have just been talking with our presenter who we'll introduce in just a second, but he is willing to take your questions throughout because we want to make this germane to what you need at your institution. So while we normally wait for questions at the end, we are going to accept questions throughout, so start keeping that in mind as we go through the material. Can we go to the next slide, please? I'm Cheryl Dowd. I'm the senior director for policy innovations for the State Authorization Network, SAN. Can we go to the next slide, please?

Cheryl Dowd (00:01:23):

The State Authorization Network is a membership organization that addresses regulatory challenges to improve student protections in digital learning. We do this through analysis, training, collaboration among members, and many resources on the SAN website. SAN was developed by WCET, our partner for this cyber series. WCET is the WICHE Cooperative for Educational Technologies. 11 years ago, WCET created SAN. WCET is also a membership organization, and their focus is addressing post-secondary digital learning practice policy and advocacy to help create quality digital learning opportunities.

Cheryl Dowd (00:02:06):

We're really grateful to be partners with WCET in this work to be able to provide you this cyber series and other policy work that we are able to collaborate. If we go to the next slide, please. As I was mentioning before, we are going to take questions throughout this webinar, so we would ask you use the Q&A box. You'll notice there's both a chat and a Q&A box. Please put the questions for our presenter in the Q&A box. The chat box could be used for something if you're having difficulty with the audio or some other type of technical issue that you would like us to address, but we would appreciate your questions being in the Q&A box.

Cheryl Dowd (00:02:49):

Different from what we sometimes do, we are going to take questions throughout, so you may place your questions in the Q&A box. Kathryn, who I will be introducing more in a minute, she will be monitoring the Q&A as will I, and we will make sure that your questions are addressed. If for some reason we get to the end of today's presentation, and not all questions are answered, if your question

has been put in the Q&A box, we do have the benefit of that being saved for us, and we will communicate with our presenter to get answers to those questions as well.

Cheryl Dowd (00:03:25):

So we can move to the next slide, please. Now, I'm very happy to introduce Kathryn Kerensky. She is part of the SAN team. She is the director, digital learning policy and compliance. She will serve as our moderator today. I'm going to turn this over to Kathryn.

Kathryn Kerensky (00:03:42):

Yes. Thank you, Cheryl. I'm happy to be the moderator for today's webinar. If we go to the next slide, I'll go over to the overview of today's presentation. Today's presentation is going to consist of an overview of the Cybersecurity and Infrastructure Security Agency or CISA and the Cybersecurity Advisor Program, details on the types of cyber threats, the tactics used by ransomware and other malicious actors, and how that could relate to the education sector. As Cheryl mentioned, there'll be questions throughout, but definitely at the end, we'll have some time for questions, so please use the Q&A box for that.

Kathryn Kerensky (00:04:18):

If we go to the next slide, I'm very happy to introduce our presenter today, David Sonheim. Dave currently serves as the supervisor at the regional headquarters for the Cybersecurity and Infrastructure Security Agency Region III Cybersecurity Advisors. The CISA Region VIII Cybersecurity Advisor Program includes promoting cyber resilience and preparedness through public and private sector partnerships through various engagement activities and performing risk and resilience-based assessments. Dave served as the task force cyber commander for the Colorado Department of Transportation Ransomware event in 2018, and shortly after transitioned to full-time employment with the Department of Homeland Security CISA in his current role as the chief of cyber for region eight out of the Denver Federal Center.

Kathryn Kerensky (00:05:06):

For more of Dave's biography, please review the event page on the SAN website. If we move to the next slide, I'm happy to turn it over to Dave to begin his presentation and more on the agencies that he works with. Take it away, Dave.

David Sonheim (00:05:21):

Great. Thank you, Katheryn. I really appreciate the introduction. Welcome, everybody. Thank you so much for joining us today for the first part in the webinar series. Thanks to Cheryl and the group for the invitation. Happy to be here, happy to, unfortunately, talk about something we don't like to talk about, which is the cyber security threat, but the idea is really to help you understand what's happening in the sector, pull the curtain back, help you understand the threats that are out there, and maybe some ways we can get after it to try to defend ourself and be proactive.

David Sonheim (00:05:53):

I know that all of you have a long and a hard passion for promoting technology, enhance learning programs, and so the idea here is to try to help understand the threat, and then try to work to try to defend it. We can move to the next slide. Most people may or may not have heard of CISA, newest agency within the Department of Homeland Security Infrastructure. The cyber security back to 2018 is how we were actually rebranded and created. You may have seen our director, Jen Easterly, on a recent 60 Minutes episode on the Russian-Ukraine threat sphere, and talking about the mission of the agency.

David Sonheim (00:06:35):

We lead the national effort to understand, manage and reduce risk, both cyber and physical, for critical infrastructure across the United States. We connect with stakeholders from industry to government and other resources, really to try to help them connect them with tools, awareness, briefings, anything we can do really on the preparedness side. Obviously, we have some work to do on the incident response side as well, but the idea is really to get on the preparedness side so that we don't end up in those situations, really try to ensure a secure and resilient infrastructure for the American people.

David Sonheim (00:07:10):

I think we can move to the next slide. This gives you the vision and mission for CISA. I had it on the first slide, defend today and protect tomorrow. So really, that's the vision and mission across it. CISA really has three strategic priorities or strategic goals, first is defend the civilian executive federal agencies. So typically, we will do that through a binding operational directive or emergency directive. So if a vulnerability hits the streets, we're going to say it's a priority, and federal agencies will be underneath a timeline to get that vulnerability corrected before it has a bigger impact.

David Sonheim (00:07:54):

The next one is really to help manage systemic risk to critical infrastructure, national critical functions. That's really critical infrastructure, state and local government across 16. We'll hit those real quick, but it's really to help prevent a lifeline sector type impact. There's various critical infrastructure that we rely on every day. If that critical infrastructure is impacted by a physical or a cyber threat, then it means a community outage or community problem. That's really trying to look at it from a strategic perspective.

David Sonheim (00:08:25):

Lastly is really to just raise the physical and cybersecurity baseline of all our stakeholders, and the portfolio that we really offer. Everything is no cost to take advantage of it. That can be in assessments. That can be penetration testing. It can be various things, but the idea is to offer those all at no cost. Let folks take advantage of them to proactively do preparedness activities. Defend against the urgent threats today while strengthening critical infrastructure to assess the long-term risk for tomorrow. We can move to the next one.

David Sonheim (00:09:01):

This one on the right side hits the seven organizational focus areas that we really have. Because we're non-regulatory, we don't audit. It's really more of come and build a partnership, and through the partnership, share information, help you improve your posture, gets after the information sharing. Those that may have awareness of Information Sharing Analysis Centers or ISACs, that's really within each one of the sectors that we rely on to know the specifics of the sector, and share that vital threat information to help protect their systems.

David Sonheim (00:09:37):

I talked a little bit on the incident management response side. That can be from a natural disaster. That can be from a cyber threat, various things along that. Always assessing risk, understanding the risk posture, obviously, network defense is in there. We also have a big slice within the emergency communication sector. We can move to the next one. So when I mentioned the 16 critical infrastructure sectors, they're all listed here. What's important to understand is that as part of each one of these 16

sectors, CISA is actually the lead agency for eight of the 16 sectors. You can see the other federal agencies that are the lead for the other ones.

David Sonheim (00:10:18):

These sectors underpin the essential services of our nation's economy, security, and health. Each one of these agencies actually also has, as part of the government apparatus, what we call a Sector Risk Management Agency. That was identified in presidential directive 21. What that means is that Sector Risk Management Agency includes folks from that sector that know the sector the best, connecting with government to try to say, "Here's resources we don't have that we need to help either protect our organization, improve our organization, et cetera."

David Sonheim (00:10:53):

So if you're not familiar with that, I'd encourage you to look at that, because anytime we want to make change through Congress, it has to come up through generally the Sector Risk Management Agency. We can move to the next slide. So as part of our outreach efforts, obviously, we have to be out in those communities. What you can see here is that although CISA has a large precedence in D.C., obviously, we are out in the region, so very similar to FEMA. FEMA has broken up across the same 10 regions. We are very closely partnered with FEMA, but for CISA, here is the breakout.

David Sonheim (00:11:26):

Obviously, I'm located in Denver, Colorado. Then I supervised all the cyber advisors in our six states in the region. Recently, we were able to hire a cyber security advisor for all the states. When I first hired on, I was having to cover three states, and constant travel, and then COVID changed all that. But just to give you an awareness, if you're not on the west side, the United States or in Region VIII, I'm happy to connect you with the cybersecurity advisor or the protective security advisor in your local area. Please, help take advantage of some of the resources we offer.

David Sonheim (00:12:00):

We can move to the next one. So specifically within the portfolio on the cyber side, I mentioned the cyber advisors we have in all of our states. Their mission and their charge is really to get out there and try to promote cyber security, connect them with stakeholders with no cost assessments, no cost resources, webinars, tools, tabletops, all those things. So if those are things that you feel like your organization can benefit from, again, it's no cost. Please just connect with me or your local cyber advisor or protective advisor, and we're more than happy to help come out and try to promote your program.

David Sonheim (00:12:35):

You can see across the wheel there the different areas that we focus on. A lot of that really is that stakeholder partnership, education build, coordinate, provide that awareness, and then, again, connect with resources. We can move to the next one. We can move to the next one. So for today, we're obviously going to focus on the cyber side. We know that cyber can be a challenge for all of us. We know that it's somewhat hard to understand. We know that it can impact us. We know that sometimes it just requires us having endless password lists or having to remember those.

David Sonheim (00:13:10):

Unfortunately, yesterday in the news, there was an article about a college in Illinois. It's Lincoln College. The news article, the title of the article was U.S. College is Shutting Down for Good Following a

Ransomware Attack. Then they said in there that basically they will have to close their doors for good on May 13th. They point to the ransomware attack being one of those key drivers as well as the COVID pressures from enrollment numbers, and not being able to sustain it. We know the threat is real. We know that it's impacting multiple sectors.

David Sonheim (00:13:49):

We know that the higher education sector has been hit extremely, focused on them, obviously, because there's not always the strongest cybersecurity protections in place. We know that education systems have to be open and available. When things are open and available, unfortunately, those cyber threat actors take advantage of that. We can move to the next slide. I know there's a lot on here, some terms you're probably not familiar with. Like I said, this is a perfect opportunity for folks to drop some questions in there.

David Sonheim (00:14:22):

Like I said, it's not about me running through slides. It's about helping to pull out things that matter to you, or concerns you have, or questions you have. Maybe I can help break that down for you. I'll start, and then maybe we'll hit some of the questions as we go here. I know most people in the world of cybersecurity. Hard to understand typically means having multiple passwords, or having to have a password manager. It seems like you always have to reauthenticate and log on. That's what we're after here. We know that cyber problem is complex. Unfortunately, it's not something we can fix overnight.

David Sonheim (00:14:57):

We know that software vendors crank out lots of software with lots of vulnerabilities, and then all we do is spend endless hours trying to patch and remediate. We know that phishing attacks seem to never stop. They seem to increase. We know that fraud and malicious activity on systems, which we rely on to deliver for you guys your remote content in order to do that. That impacts all of us across society, so we know the problem is large, and it's wide. As far as the slide goes, and the jargon that's on there, I'll try to break it down real quick.

David Sonheim (00:15:31):

There's three key areas there that we try to associate or try to understand. We talk about the cyber threat or cyber attack. Obviously, the one that gets loss and pressed that everyone's aware of is the ransomware threat. We're going to talk in a second, a little bit more about the ransomware campaigns, but what we're after there is you see some of the terms on the screen. We can use an analogy here. If I was to drive around downtown Denver, and look at graffiti, it really wouldn't mean much to me. But if I was with maybe a highway patrol guy or a Denver police officer, it tells them a lot because they can look at the signature.

David Sonheim (00:16:08):

They can look at the little details. Well, cyber's the same way. Each one of those variants or each one of the threat actors that's doing it, they leave little signatures or fingerprints or those kinds of things behind. We pay attention to those as defenders, because that helps us understand how to defend. It helps us understand what techniques or tactics they typically use. The more we understand the threat actor, we understand their capability. We understand their motivation. We start to get a better idea of what's happening here.

David Sonheim (00:16:39):

So really underneath that ransomware piece, these are the specific variants as well as some of the threat actor groups that we've seen active in the while in the recent time. Like I said, there's more names that I could ever remember, or lists. They seem to change all the time, but the reason you'll see the lingo and the naming is because we're trying to associate that. Typically, those groups can be associated with a country, a nation state. We're going to talk about those down at the bottom, but that's the reason for the terms and the names that are there.

David Sonheim (00:17:17):

Like I said, typically, those associate back to a country of origin, which also helps us understand the motivation. When we say the word malware there in the middle, what we're really saying is a generic term for all malicious type software. Unfortunately, the threat actors are very good at building customized software that's malicious in nature, but it's designed to do a very specific task. So an example of that, Emotet, I think, is listed in there somewhere, or Trickbot, which those are really designed to steal financial-related data. It's going to get in and look for that financial-related data, and steal it.

David Sonheim (00:17:54):

Some other ones we have in there are actually stealing credentials. They're looking for user names and passwords and credentials to gain the initial foothold so that they can escalate, and try to get domain level authority. Another term you'll see on there is the term RAT, which is a Remote Access Trojan. What that basically means is that after the initial access, the attacker has persistent in the environment with a remote ability to conduct operations or to do further-on activity. That's how the jargon and the terms typically look at.

David Sonheim (00:18:27):

Typically, we see this a lot in the business side, the business networks or typical IT networks, but that doesn't mean it's limited to that. We obviously also see it in the industrial control systems, operational technology environments as well, which really gets us very concerned because a lot of those are the safety systems and the fail safes that we use to keep people safe. Lastly, in there, I hit the advanced persistent threat or APT. Typically, you'll hear that type of lingo. What that typically means is this is a nation state, right? So whether that's Russia or China or North Korea, we like to understand when a nation state is doing that.

David Sonheim (00:19:06):

Typically, when we see nation state or APT activity, it's probably not cyber criminal activity from a motivation perspective. It's probably more espionage activity or something along those lines, but just to make sure folks are aware that multiple nation states usually typically have a civilian-based cyber criminal entity that they're connected to. An example would be China. Why do they do that? Well, because they can now have deniability, right? So when something tries to happen, they can stay, "Well, that wasn't us. It was a rogue cyber criminal group."

David Sonheim (00:19:44):

Well, I would find it hard to believe that the threat actor groups, the criminal actor groups in China are doing activities without approval from the government, but hopefully that gives you an idea. Most folks are familiar with the colonial pipeline attack that was done by a group called DarkSide. DarkSide is what

we call a Ransomware as a Service Corporation. When we say that, what we're really saying is that they are such a large entity, that they farm out different parts of the business to different folks, meaning that they could subcontract to somebody just to get the initial access, then somebody else to build the payload, somebody else to do the extraction of the data.

David Sonheim (00:20:22):

What we're trying to paint the picture here is it's extremely hard for us either in state local government, in a critical infrastructure sector, in the education sector for us to really be able to defend ourselves from this kind of high-level activity, whether that be from the nation state, which is our most dangerous course of action, or our cyber criminals, which is more than likely our most likely course of action. Let me see if I can hit some of these questions here. I think the first one is, "Will the CSA visit the institution?" Yes, absolutely.

David Sonheim (00:20:53):

All it requires is a simple email to the region. The regional personnel will usually try to handle that, get it to the current cyber advisor, have a conversation about what activities or what assessments you're looking for, and then you just simply move down that process. So more than happy to provide you the email address, which I can try to drop from the chat before we're done, and to help you connect nationwide across all 10 regions. The next one I see in here is our college requested, submitted the forms for CISA's remote penetration testing service, have not been contacted to schedule the service yet. Any idea with the delay?

David Sonheim (00:21:28):

As you can imagine, we don't have endless workforce, right? So when we're providing no cost services, it's first in and first... Then it comes the time to schedule and then deliver. But if you connect with either me or your local cyber advisor, we can chase down your request. We can reach into headquarters, find out what ticket number was associated, and then try to get with the vulnerability management team to see how long the wait time is, or when you're coming up on the list to be able to have that facilitated. Happy to have you connect with me directly. I'm happy to chase that one down for you.

David Sonheim (00:22:07):

For the others on the call, we offer various services. The remote pen test is one of them. When you submit the request form, it's good to make sure you bug them until they give you a ticket number. Then you can go back and chase the ticket number and see how long. I know that there is some backlog in trying to get those delivered. I know that they're bringing an additional workforce on to try to handle some of those. I think the next one I see in here is GDPR data, privacy laws, help reduce the risk of cyber attacks. Are we behind in this regulation in the U.S.? I think that's a whole separate conversation.

David Sonheim (00:22:45):

I don't know that I can give a quick answer to that one. The aspect I will give you, which may not be exactly what your question is, is on the cyber side, regulations like GDPR do a lot of good things on privacy, but actually hinder us from trying to chase and resolve a cyber incident. Meaning that now I've got a regulatory component for me to get the forensic evidence I need to degrade and disrupt the cyber activity, and so just a little interesting twist on that, but maybe I can come back to that one. At the end, we can talk a little more about it.

David Sonheim (00:23:17):

I think that's the only one, let's see, that I see in the question. So if I missed one, hit me on chat, or stop me, and let me know. We can move to the next slide. This chart really is try to help you understand what we call the threat spectrum on the cyber side, anything from hacktivism all the way to warfare, which is really the nation state cyber actors and everything in between. If you look at the text that I have on both sides, you'll see that I break it out into cyber criminal groups or Ransomware as a Service groups versus the nation state or the persistent threats, and that matches the chart in the middle.

David Sonheim (00:23:54):

At the top, I have an equation. As a cyber defender, I care about capability, motivation, and intent. We talked about on the previous slide why I care about the name and the variant and the group. It's back to that fingerprinting. It's back to that, "What signature do they leave behind? What is the file extension they use to encrypt?" When they encrypt, it creates a file extension. That tells me a lot of information I need to try to help restore, identify, and when I look at it forensically, so hopefully that brings it to light. Then on the chart, I have capability, motivation, and intent.

David Sonheim (00:24:31):

I'm trying to foot stomp this for you just from a general understanding. Although from the general user perspective, it all seems like cyber noise. When we try to peel the layers back on our side, that's what we're after, right? Is this a simple trying to steal data, or do a data breach for financial gain, or is there something more involved in here? Is this a nation state persistent campaign to try to get usernames and passwords and credentials for follow-on activity? Those kinds of activities are really what start to get us very concerned.

David Sonheim (00:25:05):

Although an immediate action of a cyber fraud is a bad deal and could cause financial loss, unfortunately, we are looking at the bigger picture of what is the tendency. If it's going to be hitting one state, more like it's going to be hitting 50 states. If it's going to hit one water sector, it's going to be across the entire water sector, so hopefully that helps. I think we're good on this slide. If there's no questions, we're going to move to the next one. This is just another way to look at the previous chart as well. It talks about specifically a nation state, what is their motivation all the way down the line.

David Sonheim (00:25:44):

We know that cyber criminals are always motivated by profit. So what does that mean? That means that they are going to find a way to do cyber activity and malicious cyber activity, and find an immediate way to monetize it into payment. We know that the sector or the industry has absolutely erupted in the last few years. We know they're highly profitable. We know that they have the ability to get in there, and lock up sensitive data, and take down critical systems. We are absolutely trying to get after that as much as we can. A lot of that is the preparedness like we're doing today, and the awareness and the training that goes with it.

David Sonheim (00:26:19):

Typically, when we look at the big four from a threat perspective, we're talking about Russia, China, Iran, and North Korea. We all have a general idea of the TTPs or MOs they follow. Obviously on the Russia side, they're always geopolitical and motivated trying to extend their national power. They do have a financial piece of trying to generate financial benefit on their part. The scary part, which we've seen in

Ukraine, is really that destructive and destroyer piece. Those of you that pay attention a little bit to the industry know that.

David Sonheim (00:26:53):

With the Ukraine threat, 2015, 2016, Russia took down Ukraine's power grid. That got a lot, folks, in the U.S. very excited, very quickly, not only on their capability to do it, but the impact that it had, and the precision that they used during those attacks. When we talk about China, and we know that you're in the education sector, and we know that you do a lot of research and development and those kinds of things as part of university functions. We know those are typically global programs. China's main aspect of their activity is always going to be that espionage, stealing secrets, stealing technology.

David Sonheim (00:27:31):

It really is part of their national strategic plan. They do not disguise that in any way, and they will boast of it every opportunity they have. They want to be a world leader, and there are no rules in order for them to get there. We also know that they take advantage from the financial side as well. We know that they also have affiliate cyber criminal groups that the government will deny are directly connected. But again, I highly doubt that those groups will do the activity knowing that they would have fallout from the government. Iran, Iran has very specific an eye for an eye mentality, a lot of disruptive and destructive.

David Sonheim (00:28:08):

If you've heard of some of the attacks to Saudi Aramco, where they did a destroyer activity, the idea there is they were in there doing malicious activity, and then launched a destructive malware to cover their tracks, so that couldn't be attributed back to them, which is concerning. North Korea, obviously financially motivated. They actually fund their government through their cyber operations. Again, this helps paint the picture for who we're dealing with here and the threat picture. We can move to the next slide.

David Sonheim (00:28:38):

We're going to hit the ransomware threat here real quick. I think folks are pretty familiar with it. We know that we talked about the colonial pipeline. We know that it's hit healthcare in the middle of a COVID crisis. The idea here, there is nothing they will not attack. There are no rules. They will try to make themselves be some kind of a cyber Robinhood that they're really there to stop the bureaucracy, but that's not necessarily what we've seen in reality.

David Sonheim (00:29:10):

We can move to the next slide. We know it's a problem. We know we've seen endless highlights from it, endless news stories. We know that multiple higher ed, and we're going to hit some of those instances here in a second. Just for folks to truly understand, and we do talk a little bit about it in the future slides how they do this activity, but we know it's custom-designed malware that's designed to specifically encrypt sensitive data. We know that threat hackers have adapted their techniques that they use to do this.

David Sonheim (00:29:45):

It started off where they would just encrypt the data. What we've seen recently is they want an additional lever that they can pull to get the ransomware payment, so they're going to steal the data first. The reason they're stealing the data first is now they have... Once they lock up your data, and you

don't want to pay the ransom, now they have another way to try to motivate you by saying they are going to release highly sensitive or personal identical information or health sensitive information. And if you don't pay, then we're going to release it.

David Sonheim (00:30:16):

That's their additional motivation. They'll also do a denial of service attack against... Maybe if you're a business with their revenue generating website, they'll try to stop your ability to generate revenue as part of their additional tactics. We know that, like I said, there's nothing. There's no low bar. They won't go under. We know that they will go after the most critical thing you have. So if you're talking about how to defend it or how to work it, I would say if we put together a tabletop exercise, we would get after the most critical system you depend on.

David Sonheim (00:30:48):

For you, folks, I think it's that distance learning, that learning management system, those distance learning systems. I know a lot of vendors provide those, and so what are their critical systems? What is the IT systems that hold those things together that deliver those? What are they doing to help secure those or provide redundancy so that if they are having an event, we can continue to deliver that content? We can move on to the next slide. Here's the one specific on the education sector. Here are some statistics, some data, some trends that we've seen in 2021.

David Sonheim (00:31:26):

I'm going to get into it here in a couple slides, but CISA as an organization takes on various sectors as we call a sprint, or we do a deep dive, or we try to make a significant improvement. As we saw, a lot of these higher education institutions and K12 for that matter start to be impacted by cyber attacks. CISA took it on as an initiative to try to understand what was going on, and then render some services in regard to try to help improve the posture. Those are what's coming up in a couple slides here. This one gives you the facts and trends.

David Sonheim (00:32:03):

We know that it increased, it's on here, at 100%. We know it's probably higher than 100%, but there's the article in the reference that does it. There's a strict number there of 1681 higher ed and 84 ransomware attacks just in 2021. Those are only the ones that were reported, so there's probably more than that that were not formally reported. Here are some statistics around how and why these threat actors have a tendency to go after higher ed. This one lacks basic email security configuration. How do we know the threat actors start their work? They started through a phishing campaign trying to gain credentials, trying to gain a foothold.

David Sonheim (00:32:42):

We know that statistically about 66% of universities lack that sophistication in their email to get rid of that spam or that malspam that comes in, try to stop a phishing activity from actually doing its work. The next one is 38% of universities that were analyzed had an unsecure open database. We know that obviously, availability is king in education sector. If folks can't get to our resources or our tools, we know that we can't do our work. So the other side of that coin is by having it available and not putting security controls in place, you're making yourself a target unfortunately for the cyber actor.

David Sonheim (00:33:23):

It gives you a statistics there about targeting on K12, talking about paid a $10,000 Bitcoin ransom after a cyber attack in Massachusetts, and they're not alone, many across the United States. On average, from a cost perspective, folks that are aware of cyber insurance or liability insurance around this, an average cost there about two and a half million to remediate it. So even though the ransomware actor only wants a million, the conversation gets to, "Why would I spend 2.73 internally? Why would I not just pay the million dollar ransomware?"

David Sonheim (00:34:00):

Well, first of all, it's a cyber criminal gang or a nation state type actor in some instances. The idea is you want to contribute to that. Even though it may cost you more money, the idea is remediate yourself and make yourself better. I think Atlanta is a good example of that. I think they... It was something like they paid five to seven times what they could have paid in the ransom in order to recover from it. I think we can move on to the next one. Here are specific ones that I pulled out from the data, other organizations that have been through it, and actually paid the ransom or did not pay the ransom.

David Sonheim (00:34:43):

University of California, it looks like they paid the ransom. I don't have a lot of detail on exactly what they got back and didn't get back. University of Colorado and Regis University, obviously being in Colorado, I've got some firsthand knowledge in that. I can't disclose a lot of the details behind that one, but in general, University of Colorado had an event. They were able to restore from backup, and not actually have to pay the ransom. Regis did end up paying the ransom. A significant thing on the Regis one is that threat actor, that was not random. They waited till the day of school starting or right before school starting to put as much impact and strain on them as they possibly could, as they were trying to start a new school year, in the hopes to really extract the payment, and do as much damage as they possibly could.

David Sonheim (00:35:37):

On the guard side of the house, we have a very close relationship with Regis University. We've done several cyber security workshops with Regis, and it was unfortunate to see them fall victim to this one. Typically on there, the statistic we have on there, education organizations recovered 68% of their data after paying the ransom. How does this really work? Well, when you get infected, you're going to have a ransomware note from an authority perspective. We don't see it as a cyber crime, unless you have a ransomware note.

David Sonheim (00:36:09):

When you do have a ransomware note, that gives the authorities a lot of detailed information they need. At that point in time, if you have cyber insurance, they're going to hire a broker that's actually going to negotiate with the cyber threat actor. The cyber threat actor typically will provide an example description key, because obviously, you wouldn't pay the ransom. If you didn't have an insurance, it would actually decrypt. Some agencies go through that. The issue is the amount of data that's been encrypted. The decryption key only works so fast.

David Sonheim (00:36:44):

It's not like it unencrypts as quickly as it encrypted. So even though they have the decryption key, that doesn't mean they 100% get it back. That means that they have to go through a laborious time consuming, manpower intensive process to attempt to decrypt, and sometimes things don't work right.

So even though they paid, and they're showing you there are only about 68% less than 70% actually truly restore. So if folks think, "We'll just spend more on cyber insurance, and not do proactive cyber defense, and implement controls," that's probably an upside down way to think about it.

David Sonheim (00:37:22):

Only 11%, if we look at it on the flip side of that equation, actually got all their data back. There's a story I tell sometimes about a medical facility here in Colorado that went through this event, and absolutely had all the backups, were doing all the right things. When it came time to pay, the reality was the time that it would take the personnel, that it would take et cetera to do the recovery, it was just an upside down financial equation, which is part of the reason why they had to pay. I think we can move to the next one.

David Sonheim (00:37:57):

I see some things in the chat, but I'm not seeing them necessarily. To keep password secure, there are some utilities out there, some password keepers out there that you can use, LastPass and some of the other ones. We can move to the next slide as well. They're out there available. It's hard for me to advocate for one vendor versus the other one. I would definitely say some type of an automated password keeper is a good solution. I would definitely say look at maybe CNET or maybe some of the other articles that are online to try to understand which one give you the better value based on the investment you have to make.

David Sonheim (00:38:36):

I would say at the end of the day, moving to multifactor authentication, moving across all your social media accounts, across all your banking accounts, et cetera, where you can't just get in with a username and password, you have to get in with a code. You have to get in with some other way to identify your identity. Then you get an alert if someone is trying to get in your Amazon account with just a password, and constantly trying to get that second code, and then you're getting a notification from them. I would say it's a password keeper along with trying to do a multifactor. Hopefully I hit that question.

David Sonheim (00:39:12):

What this slide is designed to do is to pull the curtain back, and help you understand, from a cyber defender perspective, what we call the Cyber Kill Chain. They want to gain an initial foothold. They want to do their infection. They want to run their exploit. They like to escalate their credentials to try to gain full domain admin, and then possibly exfil sensitive data or possibly lock. What this helps try to do is try to break down that kill chain. Typically, that reconnaissance phase, threat actors will spend a significant amount of time in the reconnaissance phase. They will sometimes sub that out to a specific organization that is hyperly focused on that. They'll know who registered your domain.

David Sonheim (00:39:54):

They will do research on your website. They will know who the key players are, who the C-suite players are. They'll know who pays invoices. They will... It will almost scare you the level of detail. I think I may hit it on a follow-on slide, but I'll hit it here as well. If you don't think they're looking at all your social media and your LinkedIn and all those things as part of that equation, that is absolutely how they are crafting their phishing messages. They know who the key players are. They know who the folks who have access are, and they are absolutely going after those folks.

David Sonheim (00:40:24):

They are planning out their entire activity they're going to do. They're not going to spend more time than needed to go after an organization that they know they're not going to have successful with. In that reconnaissance phase, that is what they are doing. So with that in mind, I know that we like to put everyone's contact information out there on the web. I know that water sector is one of the ones that is just tough, because I think there's a few water laws that mandate the waterboard be open on a public internet page.

David Sonheim (00:40:56):

Well, you're just giving an attacker far more information than you ever should, right? But that law was probably written in the '50s or '60s, so it hasn't adjusted, but what I'm getting after here is try to do what you can to have a generic email, have a generic group. Don't provide people's detailed contact details exactly to them. Try to give a layer or two distance behind that, so try to slow the attacker down or not make it too easy for them to do the research. MITRE, if you're familiar with, MITRE is a pseudo government type organization. Research organization puts out lots of best practices. They actually created what we call MITRE ATT&CK.

David Sonheim (00:41:35):

MITRE ATT&CK is actually an acronym. It's techniques and tactics. So the idea is as we move down this kill chain, as a defender, if I understand the attack cycle the attacker is doing, it gives me the opportunity to detect them, and then disrupt their cyber kill chain to try to preserve my environment. That's really what this one is trying to show you. When we specifically talk about ransomware, we know they follow a certain methodology regardless of the type of actor or the threat country. We know they typically do the same kinds of things.

David Sonheim (00:42:06):

The idea is you put lots of sensors on the wire, gather that information, correlate it where we see different logs, or maybe somebody's trying to brute force into something that triggers an alert. Somebody's getting access to something they shouldn't have access to. All those things help bring the picture to us so that we can gain awareness of this activity, and try to shut it down as quickly as we can. Disrupt and deny and degrade, we try to use those three Ds typically in the cyber defense world, disrupt, detect, deny. Deny the adversary presence. That's typically how we try to do that.

David Sonheim (00:42:40):

On the left part, they show you the kill chain from reconnaissance to initial access, execution, persistence. A lot of that persistence activity is they'll actually set up a way for them to remotely access without the entity knowing for them to do the follow-on activity. Sometimes we call those C2 beacons or command and control beacons. If you heard about the solar winds incident, that was the thing that was concerning on that one is a nation state activity had persistence and remote access into lots of government networks, which was obviously very concerning. Hopefully that gives you an idea.

David Sonheim (00:43:17):

It maybe pulls the curtain back on how we look at it from a cyber defender, understand how they do their activities. The more from a red team perspective we understand what the adversary is doing, the better we can do on the defense side. Now, I think we can move to the next slide. Let's see. I think I see a question in there. Let me see if I can hit it. Like other crimes, does there tend to be some direct

connection to the target organization member or former member community, for instance? Do you have an advice on how institutions or others can have trust yet monitor, but adjacent to their own communities? I think that's a good question.

David Sonheim (00:43:56):

At the higher level there to understand, am I the only target? Is this part of a bigger campaign? Is it because they were going after something, and they stumbled upon something else? I think all those things are part of the threat picture that we look at. I'd say it's always in your best interest. You can't always control the second and third order agencies you do business with or have connections with, but you should be able to control to some degree, and your IT professionals, and your cyber defenders should be able to control what we call the cyber barrier around you.

David Sonheim (00:44:33):

So from a external perspective, your external presence, your external entrance, and entrance nodes, your firewall, your what we call a DMZ, those are things we should be able to control. The idea is to gain as much awareness around that. As a person in the organization who's dependent on those services, it's good for you to go ask those questions. What happens when this happens? How are you defending this? How are those things working so that you can understand it? As far as advice, I'd say there's lots. I would say in the cyber industry, generally, there are so many resources. There are so many best practice guides. There are so many cybersecurity frameworks.

David Sonheim (00:45:13):

What we are really trying to do with all those efforts is work on that preparedness piece. I would say there are always plentiful resources when we talk about, "How do you implement a best practice for this activity? How do you do a best practice for this activity?" If you're familiar with NIST, National Institute Standards Technology, they actually have very specific guidelines across all those spaces, whether that be cloud infrastructure, on-prem infrastructure, password management, multifactor. They have lots of fantastic resources that provide a best practice in class.

David Sonheim (00:45:47):

Let's see if I can hit the next one. Your point about contact info. Higher education tends to pull all kinds of staff and faculty names and contact information to public websites. At my organization, we removed the employee directory from the public website to make it easy. I mean, that's an exact thing. It's unfortunate because when webpages started, it was to share information, and get contact information, and get all those things out there. Unfortunately, we're seeing that the threat actors just see that as a easy reconnaissance ground.

David Sonheim (00:46:17):

You might want to build the slide. You might want to hit next one more time on the slide to let it build. Not sure if there's a build on here. There we go. You can probably build it. I'm not sure if there's another build on this one or not. There we go. Build maybe one more time. There might be another build on this one. Sorry. I'll let you know when you stop advancing. You can keep going. Maybe one more time. More than one more time. This is really showing... I got this deck from somebody else that built the slides. I wasn't realizing all these built, but keep going.

David Sonheim (00:47:02):

I think one more maybe, and it'll show the full slide. There we go. Actually, what happens if you hit back one time? Nevermind. Sorry. Hit for... There you go. Just leave it right here. It's good. To hit the question there, like I said, websites were designed to try to share that information, and provide it publicly awareness. Unfortunately, it's just too easy ground for them to do their reconnaissance. I think the methodology set in there, and taking the employee directory off of there, creating the generic accounts or the generic phone number, et cetera, those are the things that unfortunately you have to do in this day and age to try to protect your organization.

David Sonheim (00:47:43):

Just think about it from an attacker perspective. If you're looking around in your website, and you're saying, "I want to do malicious activity. What information did I just glean that I could use for evil activities?" So, anything along those lines, you can do, like I said, to try to give yourself a little bit of standoff from the threat actor where they're having to work harder. They may move on to somebody else who's not doing those activities. I don't want to say the best course of action is to use the bear in the woods scenario, where I just got to be faster than the guy behind me.

David Sonheim (00:48:14):

But the idea is take care of your own environment, have folks who are in the industry take a look at it. See what information is out there that shouldn't be out there. That goes also to the web application side, which I'll hit here in a second. But a lot of times when folks serve up web applications, they don't think about it from a cyber perspective. There's an entire framework that we call OWASP Top 10, which is an open source. How do you protect web applications from a cross-site scripting attack, or other types of attacks that are typical when a web application allows an input on a screen, and the attacker tricks it with a wrong value, but it actually, from a programming perspective, lets them move on to the next step?

David Sonheim (00:48:56):

Those are the things that we get very concerned about. We know that they always like to do a method of infection, kind of the previous slide that was building for us was showing us the various ways that they start their activity or begin the infection. We know that a lot of that comes from the phishing activities. We know that they try to send you a link, which is actually not the real website, but a compromised website. Another piece on the phishing piece, which we call maladvertising or malvertising, which is really tricking you into thinking it's Amazon when it's not really Amazon, part of that includes an exploit kit, a download of some type of messaging, credential stealing, or possibly access to remote systems.

David Sonheim (00:49:40):

I think we can... Let me look at this slide real quick. Here are some specific challenges that we pulled out to higher education. We know that the sheer volume of digital assets that are shared and managed increased what we call your span of threat, meaning that you've got a large threat landscape for them to go after. They can choose many ways to come after it. So again, maybe think at it from an attacker's perspective. We know that your student population ranges from non-US students, which means that we don't know their country of origin, or where they're coming from, or what their motivations may be.

David Sonheim (00:50:23):

A lot of times, we know that students are using their own, bring your own device type idea to our campuses, and plugging into a public wifi or a community wifi. We know that they're probably not connecting one device, but they're probably connecting three or four devices. All of these things just expand that threshold, that attack surface that we're trying to shut down. With all the... Everybody can connect their microwave and their refrigerator and their doorbell to the internet. We're just giving too many things and attack surface.

David Sonheim (00:50:57):

We know that on the education side, like I said, it's just difficult to not only secure it, but have those topnotch cybersecurity professionals to train and retain in order to try to implement innovative and creative ways while we cannot implement our ability to deliver curriculum, but still have some controls in place, and ability to monitor when someone's doing something they shouldn't be doing. I know we're getting a little tight on time. Let's move up a couple slides. The one I'm looking for is the recommendation slide.

David Sonheim (00:51:43):

This one right here. The previous slides, we moved through just based on time. Really, it was an effort that CISA went after, and I talked a little bit about it before, where we took a sampling of higher education facilities. We did some deep analysis to understand their cyber threats. We looked at them from the external perspective where we can scan the ports and protocols they use, and did some analysis across them to say, "What are some common things we saw?" What we saw is things that we typically see in a similar type sector, right?

David Sonheim (00:52:14):

Folks are standing up on demand remote learning environment, standing up remote work environments, standing up collaboration tools. When we do that quickly, because of obviously COVID threat, there was lots of vulnerabilities that were there. Lots of things were not secured as they should have been if they would've been deployed in a normal production cycle. The data that I provided in those slides, which I think Cheryl's going to share with you, really gets after the statistical facts and figures that go along to support the assumptions and the recommendations that we are making here, that in general, education needs to treat themselves, unfortunately, more like a business or more like a financial institution from the sense of really paying attention to...

David Sonheim (00:52:57):

I cannot have a disruption from a ransomware attack or a malware attack. Therefore, we've got to implement security controls so that we can assure the delivery of these resources. If we don't do it, we're giving the cyber attacker too many opportunities to stop our activities, or impact our ability to deliver that. We give you some simple things here, practices that we can do to defend against ransomware, improve our vulnerability management, understand what risks we have, get the patches patched in a timely manner, risky services that we have out there or maybe legacy services that we know are filled with vulnerabilities.

David Sonheim (00:53:32):

We've got to be able to do an assessment of those, and shut it down, and then updating operating systems and software. We know that that's always a painful process, but the idea is those latest software patches really provide us a better level of protection. We can move to the next slide. This one

gets after why are education facilities targeted? This is from our director. We know that ransomware attacks on businesses, large and scale, [inaudible 00:53:59] is follow the money. We know that they are all after turning it into a monetary enhancement for them to do the activities.

David Sonheim (00:54:06):

Statistics below basically show average ransomware page and the demand, meaning that we don't always pay the actor what they want. That's part of what those brokers do. I think we can move on to the next one. This one gets after, "How are you targeted from social network and media to job postings?" All those things, unfortunately, are everything the attacker looks at to try to gain a foothold. The next slide, I think, talks about some phishing activity. This one here is really pulling apart what are the different pieces in an email that comes in that I need to pay attention to.

David Sonheim (00:54:40):

We know that we get more email than we can even look at. The idea is the threat actor is banking on you not paying attention, not hovering over the link to find that it's not really going to Bank of America, but it's really going to a website they control. This gives you some of the ideas of a thing within a standard email to look across or scan across, or teach yourself to quickly scan across, to try to pick up on this activity, to try to shut it down. Keep in mind that there are lots of email protection solutions out there that universities more likely are employing. We call one of those a gateway, where it's going to filter out all this spam.

David Sonheim (00:55:16):

It's going to try to look at the links. It's going to try to not allow you to go to those malicious links, all those kinds of things. Let's move to the... There's two examples there, which I think we can move past. Just a general public service announcement, do your part. Be cyber smart. We rely on everyone paying attention to this, sharing knowledge, sharing best practices in order to try to get after it. Let's see here. Cheryl or Kathryn, you might want to drive here. I'm not sure if you want me to hit a specific slide, or you want to try to give some time for questions, or how you want to do it.

Cheryl Dowd (00:55:54):

Well, I think we can... Let's try to wrap it up. Unfortunately, we are running short on time. The good news is that we have Dave back with us in a little less than a month. Perhaps we'll chat about this, and we'll see if we can hit some of these other pieces that were part of Dave's thoughts for this week, because he's hit on some other things that were important for our members. Dave, if that's okay with you, we'll circle back.

David Sonheim (00:56:23):

Well, let's just do questions if you have time for a couple quick questions, or however you think is the best use of the time.

Cheryl Dowd (00:56:30):

Right. I'm looking at the question and answers. They're asking about the slide deck. Yes, like our other webinars, we will be posting it to the website. It'll be on both the SAN and WCET websites in a few days. We want to get a transcript for this webinar, and also be able to upload the slides. You will see that shortly. So thank you for prompting us to address that as well. We'll take one question here, and then

I'm going to close us out. An example of the balance between privacy and security of the European union today, no one wants to see...

Cheryl Dowd (00:57:06):

Douglas, thank you so much for sharing this. This is for folks that would like to look in the chat, and you'll see some information that's being shared there for folks. Also, Leigha, will you please go towards Dave's last slide so that we can share his contact information? You just went by it. There we go. Back up a little bit. There we go. Here, you can find Dave's contact information. We will be posting this entire slide deck on the SAN website and WCET website, so you'll have access to this as well. Could you move to the next slide, please? Actually, two slides forward.

Cheryl Dowd (00:57:55):

We're coming to the end here. I just want to take this time to ask you all to make good use of the SAN website. You can find a number of resources there. We certainly try to reach out to those that are new to the idea of out-of-state activity compliance, and give them beginner resources. Could you go to the next slide, please? You'll also find from the homepage that you can reach these nine tiles that are landing pages about certain key areas of out-of-state activity compliance.

Cheryl Dowd (00:58:21):

Could you go to the next slide, please? We do have some upcoming events. Both SAN and WCET have upcoming events. We have part two of this cybersecurity webinar. You can find this information on the SAN website. There will be an advanced topics workshop. It'll be virtual in September. We will have that registration open in the next week or two. Then also in October is the WCET 34th annual meeting. For SAN members, SAN coordinators will meet at the beginning of that meeting, and then there will be three days of the WCET annual meeting.

Cheryl Dowd (00:58:53):

Could you move forward to the next slide, please? Thank you very much, Dave, for being with us, and to our attendees for being here. I also want to thank our colleagues at WCET. SAN and WCET work together to bring this to you today. We're very pleased that you could attend. You can look for this information. Dave has several resources that you're going to want to go through by reviewing this slide deck. It's very key content for you. We look forward to having Dave back in June.

Cheryl Dowd (00:59:25):

I also want to thank Kathryn for moderating, and for Leigha for managing the administrative side. Of course, we have Rachel here for support. The entire SAN team is here to support this webinar today. Thanks, everyone, and we will be talking with you shortly.

David Sonheim (00:59:49):

Thank you.

Cheryl Dowd (00:59:59):

Recording can be stopped.