CONVERSATIONS
WITH THE ST. LOUIS FED
FEDERAL RESERVE BANK of ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

Cybersecurity: Mission Possible

June 24, 2021

Allen North, Carey Sharp, Nathan Goodson, and Megan Kahlenberg

Carl White: Well, hello, everyone, and welcome to *Conversations with the St. Louis Fed*®. This is Carl White. I am Senior Vice-President responsible for Supervision, Credit, and Learning here at the St. Louis Fed. Today, we're coming together to discuss "Cybersecurity: Mission Possible." So, our presenters will, kind of, clue you in on that title here in a little bit.

On Slide 2, I just want to run over some logistics. So, the best experience is if you're joining us through the webinar and then through the webinar's audio. Some of you who are calling in via phone and then maybe watching the webinar on a screen, you may notice just a slight delay. So, one suggestion is just to download the presentation and then go through it as you hear the speakers advance the slides, and we'll make sure that you know which slide we're on as we go through the presentation. So, on Slide 3, regarding questions, we certainly welcome your questions, and you can ask a question using either the Ask Question button right there in the webinar or you can shoot us an email at conversations@stls.frb.org. And, that's right there on the slide as well.

So, I have a full team of my folks that are going to be presenting today, all from here at the Fed in St. Louis, and let me briefly introduce them to you. Some of these names, I'm sure, are familiar to you all. We have Allen North. Allen is Vice-President over Safety and Soundness here in St. Louis. We also have Carey Sharp. Carey is a Supervisory Examiner in Supervision, Safety, and Soundness IT Unit, Information Technology Unit. And then we also have Nathan Goodson. Nathan is a Supervisory Examiner also in the IT Unit here in St. Louis. And finally, we have Megan Kahlenberg. Megan is a Supervisory Officer in Safety and Soundness.

So, before I turn the call over to our presenters, I do need to cover a few call logistics. First of all, please note that you can access the presentation slides in the webinar tool under Materials, and they will also be uploaded to our Conversations page on our website. Our website is www.supervisionoutreach.org, and you can find a lot of great information there. So, that's—I would recommend you tagging that website for reference purposes.

As always, we do record every session. So, this session, like others, will be recorded, probably up on our site in a day or so, maybe less. So, if you need to go back and revisit the material or maybe you want to share this with some of your staff, your IT staff, or maybe even your directors as well, you certainly can do that. So, once again, go to that website. And finally, a reminder that the opinions expressed in these presentations are statements of the speaker's opinion, they're intended only for informational purposes, and are not formal opinions of—nor binding on—the Federal Reserve Bank of St. Louis or the Federal Reserve System.

Okay. So, we got the legal language out of the way. So, we're ready to get started. We should be on Slide 6 now, which is the meat of the presentation, and I'm going to kick it over to Allen. So, Allen, why don't you take it from here?

Allen North: Sure. Thanks, Carl. Well, good morning, everybody. It may go without saying that cybersecurity and cyber risk is top of mind of everybody, and obviously, we have these quotes from Chair Powell spanning over a couple of years. Interestingly, you know, we're coming out of the pandemic, and it's still top of mind. And, in fact, the pandemic, maybe in some ways, even exacerbated some of these risks in that we've seen more and more attacks on financial institutions, and certainly, we don't see that easing in any way. So, you know, most of the time when I'm talking to the public, whether it be something— Unfortunately, these virtual events, but I actually had a face-to-face panel yesterday with the Kentucky Bankers Association. That was certainly nice to get out and see people in person, but cybersecurity was really a topic of discussion. The FDIC, OCC, and, of course, the Fed, we had some comments to make about that, and certainly, we've seen an increase in cyber events, really, across our district and really nationally.

So, you know, this, as I—one of the other responsibilities I have at the System is I represent us on the System's Risk Council, and that's where we really try to identify all the risks that are facing institutions of all sizes and really throughout all the portfolios that the Federal Reserve has responsibility for. And cybersecurity is the top risk. It just absolutely is the top risk, and it affects everyone the same—in many ways, the same way.

So, in 2019, you know, this isn't really news to anybody, but in 2019, we really took this very serious at the Federal Reserve Bank of St. Louis and said, "Hey. What can we provide to executives that might be helpful?" Because this whole thing seems pretty daunting. And, you think about it, we're—we've gotten into banking, most of us, because we're finance or accounting folks, not IT folks, and we've had to really adjust and certainly evolve and learn along the way. And I think for executives, it becomes increasingly difficult given just the vast information that you have to process and how you actually do, actually, the risk management for your bank. So, and certainly, the importance of cyber—you know, I think all executives are concerned about it, but it's like where do you start?

So, in 2019, we put together a video series called *Cyber Talk*, and that's still out there on our website, by the way. I encourage you to take a look at that if you get a chance. Carey Sharp and Matt Case on our team did those videos, and it was really, kind of, meant to be, kind of, a broad overview on how you might determine how well prepared you are to prevent cyber events.

So, let me try to set the stage a little bit for our presentation today. The "Mission Possible" title, I thought, was pretty creative. I think, when Carey and Nathan were working through this and we asked them, we said, "Hey, listen. What we think would be helpful is to tell actual stories, actual events that have taken place somewhere in the country, that we can share with our state member bank folks and then talk about, well, how should you have reacted, how—what are the appropriate steps to take?"

And, I think when Carey and Nathan thought through this, they said, "Well, you know, it's really, it's like anything else. There's going to be steps that you've got a mission. That mission is to somehow deal with whatever this incident is." And, I think the whole idea of *Mission Impossible*, it, kind of, came into play. So, I thought it was pretty creative, but really, for the—just so everyone knows, we've had several events within our district and been pretty—I think it indicates the importance and the risk that's there, but just so everyone knows, none of these incidents that we'll talk about today actually occurred in the Eighth District. Carey and Nathan were kind enough to reach out to other folks in the System and come up with some stories to share that would be relevant. So, with that, I'm going to turn it over to you, Carey.

Carey Sharp: Thanks, Allen. Good morning, everyone. On Slide 7 is our agenda, and as Allen said, you know, we picked a theme. Allen came to us and said, "We want to tell some stories." And so, you know, a little bit about myself, I am a military brat, so my dad was in the Air Force, and I heard all the lingo all growing up about missions and debrief. And, I love old TV shows and movies, and *Mission Impossible* comes right to mind. And we have the—you're probably aware of the Internet Movie Database, or IMDB.com. It's a wonderful treasure trove for those of you who like trivia about TV and movies. And so, when we went through and we were thinking about what stories would we tell and how would we leach out some lessons learned that could be applicable to anything of any size and complexity. We went to the Internet Movie Database and I started looking at the old *Mission Impossible* episodes and the titles. These are actual titles, folks: "Takeover," "The Ransom," "Recovery," and "The Bank." We're going to weave these stories together and build upon them, and hopefully, you'll get a lot out of it today.

Then, we'll have a mission debrief and, kind of, what can you do as a bank executive, what questions should you think about, what reports and information should you be reviewing on a regular basis. You know, we took the old *Mission Impossible* title, and we changed—we took out *Im-* because we think cybersecurity is possible. It is possible to protect yourselves. And so, we're going to walk through these four episodes today, and we're going to have a little mission debrief. So, then, finally, we're going to turn it over to Megan Kahlenberg, and she's going to walk us through how and why you should report a cyber incident and how that helps the ecosystem as a whole. So, let's dive in on Slide 8, and we'll talk about our first story.

Before we talk about this story, I thought it'd be interesting to give you a real quick synopsis of what was the actual TV episode about. Well, "Takeover" aired in January of '71, and the synopsis reads, "The *Mission Impossible* team is charged with bringing down a political manipulator who intends to use a group of student protesters with deadly effect to elevate his political puppet to higher office." So, much like a hacker will infiltrate and then elevate their privilege and take over your system, there you go. It's still relevant. These same concepts of crime applied to cyber is still the same old concepts that have been around for centuries.

Well, what is zero-day? Well, let's define what zero-day is. It basically means a previously unknown software vulnerability. So, you have the zero days to fix it. You didn't know it was there. The vendor didn't know it was there, but the hackers did, and they started exploiting it. That is a zero-day vulnerability. Every one of us are exposed to these potential issues. The Fed is not immune to zero-day vulnerabilities. Your bank isn't immune to zero-day vulnerabilities. Even in your personal life, your computers and your phones, they're not immune to zero-day vulnerabilities. It's a part of life. There have been a couple of pretty high-profile zero-day events already this year. You probably heard of the SolarWinds vulnerability. And then, the other one is the Microsoft Exchange Server vulnerability, and that's what we want to talk about during this episode.

On March 2 of this year, Microsoft published information related to the Exchange Server zero-day vulnerability. That the threat hackers were actively exploiting those vulnerabilities—that vulnerability in the wild. It really wasn't just one single vulnerability in Exchange Server. Well, let me back up. What is Exchange Server? That's your email. If you run it on premises, you have a server running the Exchange software, which is Outlook email, if you will.

There were actually four different vulnerabilities that Microsoft was unaware of prior to March 2. There were active hackers exploiting those. It only affected, though, on-premises Exchange Servers. If you were running a hosted Exchange Server, such as Office 365, where Microsoft is managing your email for you, you weren't affected by this, but if you were running your own email in house on Exchange, this was a vulnerability that you needed to address.

And, you know, what is the impact? Well, it could lead to, you know, theft of credentials, theft of your mailbox data—we all know that, you know, there's going to be some sensitive information in your email—and establishing persistence for further exploitation in the environment. And, what I mean by that is, once a bad guy or gal gets into your system, they can sit there and then they can monitor and then they can pivot and elevate their privilege, much like the premise of the old TV show. So, Microsoft actually announced the vulnerability, the zero-day threat, on March 2, and they also, later that same day, published patches to resolve those four different vulnerabilities. Timeliness, timeliness of patch management, application of patches, is going to be the key to success to avoiding the pitfalls of zero-day issues.

You know, one of the questions—and, we'll get into this later in the presentation—but one of the questions that immediately comes to mind, if I was an executive manager: How quickly can we respond to zero-day threats? How do we monitor for these things? How do we monitor the software publishers so that we become aware ASAP so we can take action? Now, the lack of awareness of vulnerabilities obviously can lead to loss of data, loss of access to your systems—we'll talk about that a little bit later—and even loss of money. We have some real monetary losses from zero-day threats. But from a regulatory perspective, here, poor controls can directly impact the support and delivery rating in IT, as well as the management rating and, obviously, the composite rating of IT. The vendor release in the timeliness, that is probably the most paramount thing and the number one thing that you can do to protect yourself against zero-day threats, simply because by nature, the zero-day threat is something you don't have any control of. What you have control of is your responsiveness and your timeliness of that response. So, that's episode one, "Takeover."

I'm going to pass it over to Nathan Goodson, and Nathan is going to talk about our next episode. Nathan?

Nathan Goodson: Thanks, Carey. And if we could advance to the next slide? This next episode is called "The Ransom." It aired on November 5, 1966, and the synopsis of this episode is that you have a guy who has kidnapped the daughter of a friend and he is demanding a ransom. And so, while we don't have a person being kidnapped, in this case, the ransom was the bank's data. So, what led up to how to this happen? The bank's profile is mostly outsourced, core processing, network monitoring, outsourced. But what was in house? Their email server. And what do you think got exploited? The vulnerability that Carey just talked about in the zero-day.

They had an unpatched Microsoft Exchange Server, and that was just the start of it. It was almost this perfect storm. This unpatched Exchange Server allowed them to get in. They were able to use a privileged user account that had no type of multi-factor authentication. Then, they were able to put the ransom on the bank's data. And unfortunately, this institution had no off-network air-gapped data backups. And then, as they were doing their forensic analysis, it was really unclear this network monitoring vendor and how often or how quickly they actually notified the institution, if they had notified them, if they hadn't notified them, and if they did, did bank staff respond in a timely manner?

So, what was the impact of all of this? This institution actually had a multi-day outage. Fortunately, their core system was outsourced. So, they were still able to get access to core data, but anything that was running internally, they had some issues with. And just as a point of reference, this bank is in that $500 million to $700 million range and low risk from an IT standpoint. Ultimately, this organization did pay the ransom, and they used a firm to negotiate, you know, the price that they had to pay. Some other outcomes that came out of this: They quickly transferred their in-house email solution to an outsourced hosted solution, and management also went through the process of starting a comprehensive gap analysis to really see where they had any type of gaps in the current system and where they needed to beef things up going forward.

When we think about it from a URSIT impact standpoint, support and delivery is really the thing that comes to mind first. A lot of these are basic, you know, cyber hygiene type controls to have in place, and it only stresses the importance of being on top of patching your systems, especially when it comes to zero-day patches, you know, using MFA whenever you have a privileged account, the importance of having off-network backup. And, when we think about backups, this actually isn't something new. You know, we've had backup tapes for as long as I can remember, and one of the things that I've always thought about is plan for the worst. And, the worst is complete destruction, and anything—and an event really is always a subset of complete destruction. Ransomware is the same thing. If you have a fire and lose, sort of, your data center, you have to recreate. In the event of a ransomware, we may have to recreate that data. So, we want to make sure that our information is stored in accordance with recovery time objectives.

And, there also is to be said about, you know, the other URSIT ratings as well, management and audit. You know, when you think about this institution, they, after the fact, were going to do a comprehensive gap analysis of where they were at, where they should be. These are things that, you know, have to be done on a periodic basis, and, really, you know, it only stresses the importance of it—of it's not a one and done. It's something we need to keep top of mind. And from an audit standpoint, making sure that audit is really going in there and looking at these controls and seeing how the organization is changing and making sure that our audit program is adjusting accordingly. So, with that, I will turn it back to Carey for episode number three.

Carey Sharp: Thank you, Nathan. Let's go to Slide 10, "Recovery." So, Nathan just talked about ransomware, which is built upon the zero-day threat concept, and he talked about backups. So, we're going to talk about a little bit more about this. And this episode, "Recovery," which aired on March 17, 1968, the episode synopsis reads, "A U.S. bomber crashes behind the Iron Curtain. Its failsafe device, however, failed to self-destruct. A brilliant U.S. scientist who defected to the unnamed country is supervising efforts to take the device apart, which will yield valuable information about the entire U.S. defense system. The *Mission Impossible* team must recover the failsafe device and abduct the scientist." So, how does that relate to cyber? Well, you know, I can stretch anything to make this work.

But the concept here is still ransomware, but it's not your system that's being attacked. It's your service provider. We all have service providers. Everybody on this call, including the Federal Reserve, has critical service providers or vendors that we rely upon for key operational aspects of our businesses. And, you know, one of the things that hopefully all of you are aware of, or most of you are aware of, is that the Federal Reserve, along with the FDIC and the OCC, we recognize the service provider risk and we actively supervise key service providers across the country to help monitor this risk.

Now, back to ransomware, you know, Nathan just told us, you know, the story, but yet, here it is again. This time, though, it doesn't affect just one bank. It affects a multitude of institutions, and that is the key risk that service providers present to the financial sector. It is the concept of risk to more than just one institution.

So, last year, we had one of our significant core banking providers experience a ransomware attack. It affected core banking services. It affected Internet banking services and various other ancillary services. Everything went dark. And by that, what I mean is these were all—if you were running their software in house, it didn't affect you, because this is a service bureau situation. The data center was attacked. The data center went offline. And so when I say it went dark, you at the bank, you don't have any access to your core information unless you stored something offline on premises. So, you know, that's something that might keep you awake at night.

But, to get into a little bit about what happened, the attack began about a week prior to the provider becoming aware of the intrusion, and that is just classic Hacker 101. They gain access. They lie in wait. They surveil the system and the landscape, and then they pivot and elevate their privileges. So, once the provider took the affected—so, they recognized a week after—you know, post-mortem, you can look back and say, "Okay. We see a week prior to us becoming aware was when the infection started." So, once they noticed this, they took the data center offline on a Friday afternoon. So, it didn't affect the full day Friday, but you weren't able to close out Friday. You weren't able to close your book on Friday. By the close of business the following Monday, approximately 89% of all affected services had been restored to normal operations. And then, so, you had 11% left, and mostly, this was Internet banking and a few ancillary services, very limited on the core side. But by the—so, that was on a Monday. Wednesday, a week later, was when they finally restored everything back to operating—operational positions.

The problem was the data center was backed up by another data center, and Nathan mentioned how important backups are. This is what happened. The primary data center was infected. Then, they also—the hacker was able to traverse to the backup data center and corrupt it as well. So, there was a lot of data restoration that had to occur, and it wasn't the flip a switch and go to the backup site. The backup site was down too. So, you think about total downtime in business days from inception to final restoration was nearly eight business days for all services. Now, granted, you know, the lion's share of the services were restored in less than a business day, but still, that's a huge impact to not just the bank, but the bank's customers. And, it's not just a bank. It's many banks.

So, how did it happen, though, you know? That's one of the things that you always want to, you know, after the fact you look at, well how did this happen? Well, there's a lot of moving parts here. This particular service provider had undergone a sea change in key management positions, in executive management. This is a global company with numerous IT environment complexities. They had acquired a lot of different companies, and there were some legacy systems that they didn't have a clear understanding of their IT asset inventory. Those of you who know me, who I've talked to in the past, that is probably my number one thing that I always talk to you about is you have to understand what's connected to your systems, what hardware is running. You have to understand what software is running in your environment, and you have to understand this is what I want to run. They had business continuity flaws, obviously, and then, you had some endpoint protection issues. But because ultimately, what happened was human error. It was phishing—phishing and, we believe, some spear phishing, which is targeted towards certain individuals within the organization. You click on the wrong thing; you let the bad guy in. He doesn't do anything right away. He lies in wait. He surveils the system, and then, there you go. It's takeover time.

So, from a regulatory perspective, you know, we're looking at third-party risk management here. So, how can you, as a banker, you know, how do you understand their controls? We'll get into that a little bit later in the presentation, but one of the things that we want to emphasize is keeping that ongoing, open dialogue with your key risk—your key critical service providers. That's going to be huge, and also, you know, understanding that regulators go out and they examine on your behalf actually. It is very self-serving from the Fed System's perspective, as well as the other regulators, but we're looking at the risk the service provider presents to their client financial institution. That's you. So, if you're not aware of the program that we do, we also have an opportunity where you can receive the regulatory reports that we publish if you're a client as of the date of the examination. You can contact your portfolio examiner. You can contact Nathan or myself, pretty much anybody, to receive those, to start the process to get access to those reports. But the service provider, it's not just one institution that's affected. It's a multitude of institutions that can be affected. So, with that, I'm going to pass it back to Nathan to talk about the people aspect of cybersecurity. Nathan?

Nathan Goodson: Thanks, Carey. And if we could advance to the next slide? Our last episode here is called "The Bank [a Data Loss Story]," and this one aired in 1967. And the synopsis is, "Belzig, head of a bank in East Berlin, tricks unwary people anxious to escape to the West that he can help them. Instead, he steals their money and kills them." So, in our case, we have a loan officer who is taking information, customer information, and forwarding it to a personal email account. This activity was not discovered until this individual left the organization and actually went to another financial institution. While the number of customers impacted was low, it does set the stage for a very interesting conversation when you think of having to tell the customers that your information was taken or there was a breach of your information.

So, how did this happen? When we think about some of these basic cyber fundamental controls, this institution didn't have data loss prevention, and they also allowed employees to have access to personal email accounts on their work devices. So, those two things right there, if implemented, probably would have helped prevent this situation. As we talk about the impact and the resolution, having to, sort of, get that conversation to the customer that, "Hey. Your information has been taken," and then, of course, now we have to pursue, sort of, legal action against this employee and—this former employee. So, this one was actually still pending, but only I think to reiterate the importance of having cyber controls, but also the human error—humans are a big weak link and can be a big weak link in your protection of information.

And, it really can be hard to prevent, because we, as humans, we process, we transfer information. We know so much, and it's so easy now to print something off. We can take a picture with a smart phone. When you think about, you know, the remote environments that we've been working in the last, you know, 12 to 15 months, a lot of these controls had to be modified, because now we're giving people access to do things at their house. I think back; I worked in a bank when I was in high school and when I was in college, and, you know, we had no remote access to the network and no, sort of, remote access to the core system. But now, 20 years later, that's completely changed.

And so, this episode, while less about, you know, a cyber incident and more, kind of, an insider threat, again, I think it just demonstrates that importance of why we have to have the appropriate controls in place to monitor what people are doing on our network, what they're doing with our customer data that we are protecting, and making sure that we've restricted access to that data appropriately or we've restricted access or their ability to access things like social media or personal email accounts. So, when you look back at a lot of the threats that have happened, you know, over the last couple of years, a lot of it really can be attributed to human error, and, you know, it only stresses the importance of why we train, why we put through—why we test people to keep them on top. Because, all it takes is one little click, and we could be in a very interesting situation. And, of course, you know, you think about the last year, people working from home who are easily distracted, and that is, sort of, a great thing for someone that's trying to take advantage from that human element. So, those are our four episodes.

If we could advance to the next slide? Let's do our mission debriefs. So, these mission debriefs, questions to consider, these are questions that we really wanted to target toward executives, you know, people in that upper level that maybe aren't necessarily in the day-to-day management of the IT environment, things that you can go back today and ask those IT management individuals, "Hey. What are our answers to some of these?" So, we'll quickly go through these eight or so questions.

The first one is who is aware of independent technical testing engagements? So, when we think about the human element, making sure that people are aware of what's going on and trained appropriately, we thought about who actually knows when we're going to do a vulnerability test or a social engineering test. And I think, in this case, an event will probably likely happen when you least expect it. So, doing tests when very few people know can really mimic a real-life event, and I think, when you think about the ransomware episode and, sort of, the ambiguity that we saw with the network monitoring vendor notifying the bank and not really knowing how that actually played out, things like period vulnerability—or penetration tests, vulnerability scanning, social engineering tests, can really help gauge that reaction in that time from when something started to how quickly we can pick it up.

We also think about incident response. I think we're all familiar with, you know, testing our exact recovery plan or business continuity plan, but now more than ever, you know, incident response is such a strategic thing when you think about responding to a cyber incident. And, it's not one where we need to wait until the incident happens to figure out what we're going to do. We need to be able to test. We need to be able to pull out a playbook, run through it through various scenarios so that, when and if something happens, we can respond quickly and timely.

One of the other questions that I think will—that you should be thinking about is what are the special requirements/clauses that may come with our cyber insurance policies when we need to file a claim? So, what made us think about this question was actually one that I've asked in the past around wire transfers, and most insurance policies that cover wire transfers usually have some caveats in them that say you need this type of control or we need to know what controls you have in place. And unfortunately, there was an incident years ago, a bank in Florida, that did not follow their controls, and they had a wire transfer problem and the insurance company did not pay. And so, this is just something, as you're looking into or maybe you already have cyber policies to really understand what the expectations are within those policies for you as an institution. What type of controls do you have in place?

Multi-factor authentication, we talked about that earlier, the importance for privileged users. Again, this is just another layer of control that can really help prevent someone who may have gotten in from causing more harm to the organization. When you think about assessing ransomware risks, you can use a number of frameworks. I know there is a ransomware self-assessment tool that came out last year. Of course, any of the cyber frameworks can help you, sort of, assess where you're at from the ransomware standpoint.

Carey talked about earlier the deployment of critical security patches, especially if you have a zero-day, and really understanding what are processes for that, how do we get notified, how quickly are we deploying, and do we have awareness of that? Because, in the instance of the ransomware, the Microsoft Exchange, they knew they had an unpatched system, and they were in the process. But unfortunately, time was not on their side. And then, again, the importance of data backups. Do we have a backup that is off our network? Old-school way is a physical tape, and, you know, the institution I worked for, we took those tapes every night. They went to the police station. I grew up in a very small town, but that was our data, and it was away from the bank. And, that's just something that is so important when you think about the instance of do I pay a ransom, do I not pay a ransom? If I have my data and I can quickly recover, maybe I don't need to pay a ransom because I can get my data back and be up and running.

Audit coverage is also another thing to think about and how it's evolving. When I think about the last, you know, 15 years I've been with the Fed, IT environments have changed so much. The institution that I worked for, we processed in house, and it was a mainframe, a massive, sort of, single-pocket proof machine, no Internet connectivity when I started, and they had just gotten tele-terminals. Fast-forward 20 years, an IT environment looks very different, and as that evolves, we need to make sure that our audit coverage is evolving as well. There’s always those basic elements that we’re going to review and make sure we have controls in place, but I think things that you can do, making sure you understand the work that is being contracted. I always suggest looking at the work papers and knowing that we contracted for X, we actually got X.

And then, the last thing, again, how are we maturing our cybersecurity posture? I mentioned earlier not treating assessments as a one and done. These things are living and breathing. Environments are changing all the time, and these are really tools to help us prepare for if a cyber scenario would play out at our organizations. And, the other thing to think about, minimal baseline expectations are just that, minimal baseline expectations, but the world continues to evolve, and the threat vectors continue to evolve, and I think your posture, your maturity also has to evolve as well. What may have worked okay a couple years ago, may not might be the best posture to have now. And fortunately, you know, technology has unlocked so much, and costs, I think, you know, has come down a little bit and made some things a little bit more affordable for smaller community banking organizations. Obviously, outsourcing is also a way to take census of things like really enhanced network monitoring.

So, I’m going to stop there with the mission debrief and turn it over to Carey to see if he has anything that he would like to add.

Carey Sharp: Thanks, Nathan. I would just add that, you know, when it comes to FFIEC guidance, if your goal is to comply with FFIEC guidance, in my opinion, I think you’ve lost the cyber war. Like Nathan said in some of his last comments there, minimal or baseline expectations, they are just that, minimal and baseline. The threat actors out there today are rather sophisticated. You may have heard of cybercrime as a service. That’s an actual thing, where you don’t have to be a hacker, per se. You can rent or buy software toolkits to infiltrate systems and then exfiltrate data or to drop in ransomware payloads. So, it’s, kind of, it’s a little bit of a scary world out there sometimes, and we’ll talk a little bit more on the next slide.

We’ll go ahead and advance to Slide 13. We’ll talk about some of the things that you can do to review, to educate yourself, but also just to stay apprised of what’s going on in your environment and in the world of cyber and IT, in general.

It’s information. It’s all about getting the right information and having it at your disposal, and this list here is not meant to be exhaustive. It’s to get you started. I want to take a step back here and think about, you know, one of the things that you do day in, day out that you’re probably pretty good at is making credit decisions. You know, we don’t have a lot of credit problems out there in the system right now, and so, you know, when you sit down to make a credit decision, you want to understand all the different aspects of that borrower’s business and/or their personal situation. That’s just good credit risk management. Hint here, cyber is really no different in this regard. We don’t expect you all to become IT experts. You have people on staff or you have service providers to be that expert. We want you to be knowledgeable enough to ask good questions.

So, you know, patch management status reports, very high level, we're not expecting you to get into the weeds on any of that. You know, if your staff should be providing you with graphical representations and/or percentages, I see a lot of network health reports out there at different banks, and they have a percentage of the whole environment, say 94% of the environment is patched. Well, that's great; 94% usually gets you an A in school, right? Is that a good number? These are the types of questions to ask when you review a report like that. Is this where we want to be? Why or why not? What's our risk tolerance here? Patch reports are always a point in time, and so, timing can skew those numbers sometimes. But if you're asking those questions, that keeps people on their toes to ensure that, hey, somebody else is watching. And that's a good thing.

Disaster recovery or incident response testing results, Nathan talked about that on the previous slide. Read them. You know, more often, if something goes wrong during a disaster recovery test, that's oftentimes where we learn the most. We learn that, oh, we need to update a script or we need to update a process or a procedure. Be sure that those lessons learned, if there are any, are reflected in that test. That's a great question to ask. Technical testing, penetration, vulnerability, social engineering, Nathan touched on that on the last slide as well. Look at it. When you're reading those, they can get really technical really, really fast. Look at the high-risk ones. Ask the questions about why is this high-risk if you don't understand why it's high-risk. That's really all we're asking here is keeping that awareness up.

Audit is always a key. This is one thing that I want you to think about. If your IT audit comes back clean, but your examination isn't clean, that should be a cause for concern. You're paying money for the audit. Especially, the majority of our community banks outsource the IT audit function. If that IT auditor comes back and tells you everything is great, and an examiner comes in and says here's a pocketful of MRAs, that's a mismatch, and that should be—we should be commenting on audit. That's another discussion for another day, but you should be asking those questions of Mr. and Mrs. Auditor: Why did you not find these things? Because, you know how long we're there. We're only there in your institution for a handful of days.

Cyber assessments, you probably have all heard of the CAT, the cyber assessment tool, from the FFIEC. It's been around for a number of years now. That's one way to accomplish this. It's just like any other risk assessment. We, kind of, have that annual expectation of completion, but also, look back and see where you were. You know, in August of 2019, the FFIEC had a press release titled "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness." It was a statement about encouraging controlled framework adoption, and Allen talked about the *Cyber Talk* video series that's out there on our website.

We talk a lot about that in that series, and we use the Center for Internet Security's Critical Security Controls as an example. You know, a control framework isn't going to—isn't a panacea, never think that, but it's a way to think technically and strategically about controls that make sense for your complexity and your environment. And it can serve you with technical gap analysis, and from that, you can identify a strategic plan and/or a tactical plan to implement controls. Cybersecurity assessments, they are very important, I believe, to increasing your cyber maturity posture.

Gramm-Leach-Bliley, it's been around, what, 20 years now? GLBA is one of our very few actual regulations in the realm of IT and cyber. It's an annual thing, risk assessment, reporting, training, the whole nine yards. Be familiar with those. You should be, because you receive them every year at the board. So, vendor management, ongoing reports, we talked about that during the episode—oh, what was the name of it—"Recovery," the service provider episode. Yeah. We have those. We have those available. There was—they are something you have to ask for today. Fairly soon, there will be more of an automated push, and that automated push you can sign up for. If you're not sure what that is or how to do that, contact your portfolio examiner. He or she can give you the information on how to get signed up for receiving those reports or receiving the notification of those reports are ready for you.

So, we've thrown a lot at you, talked about some stories. Nathan talked about questions to consider. I talked about, you know, the information to review. I'm going to turn it over now to Megan Kahlenberg, and she's going to walk us through, if you have an incident, what do you and when do you do it and why it's important. So, on Slide 14, I'm going to turn it over now to Megan. Megan?

Megan Kahlenberg: Thank you, Carey. So, yes, how can we help? Carey mentioned this a bit earlier, but please use us as resources, especially Nathan Goodson and Carey Sharp, who you heard from earlier. Any of us on this call are happy to answer any questions any time. So, why should you report an incident? Well, one, because it is a regulatory requirement, and, two, because sharing is caring. Right? Knowing what cyber threats are facing your institution allows us to offer better guidance in mitigating those risks and alert other bankers. So, please let us know immediately.

How do you go about reporting an incident? It's simply by contacting your central point of contact. So, you heard Carey mention portfolio examiners. It's one and the same. That examiner you're talking to each quarter who's asking you about any changes in your balance sheet, that is your central point of contact, and they are the best person to start with. But honestly, you could contact any examiner at the St. Louis Fed to report an incident, and we will get it to the right place. The only information we need you to provide is the date the event occurred and a brief description of the incident. So, please include any information about impacted customers or actions you've taken to date.

All right. Next slide, please. The last thing we will hit on before we move into questions is references. We wanted to provide a few links to information we use and reference as examiners. The first is the CIS Controls, so the Center for Internet Security, which lists out actions you can take to protect both your bank and data from cyberattacks. The next link is the National Institute of Standards and Technology, which provides information regarding a cybersecurity framework. And, the last two links are specific to examiners, but you have access to them. The first is the FFIEC IT Examination Handbook, which lists out questions we typically ask when we review IT and how we assess cybersecurity preparedness. You heard Carey mention that earlier as well, so that link is included for you to use going forward. The last one is the Supervisory Letter 05-23, which covers the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. So, hopefully, this presentation was beneficial for you all. I'm going to turn it back over to Carl so we can cover some of the questions we received.

Carl White: Great, thanks, Meg, and thanks, Carey and Nathan, as well. We're also going to send you a link to the *Cyber Talk* series. So, for those that haven't had the opportunity to look at that, that's another great resource. So, we'll make sure we get that information to you as well. So, we only have just five or six more minutes here. So, we do have—we have received a few questions, and, Nathan and Carey, I think we've covered most of these. But, let's—maybe you can provide a little bit more detail. So, the first question goes back to cybersecurity insurance. So, what about if a bank—what's your thought on a bank accepting the risk, meaning self-insuring, rather than adding whatever it may be that the cybersecurity insurance policy may be asking for additional information? This one was about multi-factor authentication. But what's your thought about self-insurance versus cyber insurance?

Nathan Goodson: Yeah. Thanks, Carl. I'll take that. This is Nathan. So, I think it goes back to the conversation that we had earlier in that, you know, your insurance company may start requiring certain things. Some of those may be easy. Some of those may not be so easy. And so, this question about do we self-insure, do we not, really, I think, comes down to a risk management decision. I think things that I think about, data breaches can be very costly. And so, if you're a small organization and you get hit with a ransomware and that's several million dollars, that may have a significant impact to the bank's earnings. So, I think there's a lot of factors that you have to consider in to determine what works for your institution. I don't think you'll find anywhere that says cyber insurance is required, but again, we talked about how the IT environment and really just the world in general has changed so much. And so, insurance, to me, is a way to protect yourself, and it's a way to, kind of, transfer some of that risk. And so, what that right balance is is really up to management, and, you know, they know the institution the best and they have that risk appetite.

Carl White: Carey, anything you want to add to that?

Carey Sharp: No. I'd echo what you said as far as it's a risk management decision on behalf of the institution, and that's how we would look at it. You know, it's, you know, if you're talking about multi-factor authentication on devices, yeah, we're going to look at that, you know, from a, you know, privileged user access, remote access, and other things where it might be appropriate, but that's a different issue from cyber insurance, though. Yeah, it's a risk management decision at the end of the day. We don't require that you carry cyber insurance. I think it's a risk-reward. It's a cost issue, and those are things that management has to balance. It's a difficult decision. I don't envy you there.

Allen North: Hey, Carey. This is Allen. I might even jump in here and just add that, you know, I think this is like any other policy that the bank might obtain. You really need to read through it and understand what you're buying and what you're paying for. I think you brought that out in one of the stories, but understanding what those exclusions might be probably are about as important as anything else.

Carl White: All right. Thanks. So, Carey, this is something, actually, we were all talking about just a couple of days ago. What can we do to ensure that our service providers, vendors, have adequate controls to protect our data? That's a big question, right?

Carey Sharp: It's a huge question. You know, my specific responsibilities at the St. Louis Fed are to oversee our service provider portfolio. And so, this is very near and dear to my heart of what I do day in and day out, and it is challenging, because, ultimately, you can't transfer the risk, cyber or otherwise, to your service provider. You still own the risk as a financial institution. You need to be, you know—you have contracts. The contracts should have service level agreements, and those service level agreements, oftentimes, for critical services there are going to be uptime requirements. Be sure you're monitoring those. That's a part of the strong third-party risk management program is monitoring those measurable SLAs.

As far as, you know, assuring adequate controls, does the vendor provide you access to—you should have the right to audit clause, perhaps, but at a minimum, you should be getting SSAE 16, which is a control attestation type of report. SOC 1, SOC 2, again, these are control-type reports from your IT service provider. Accessing those regulatory reports that I mentioned earlier in one of the episodes. And, at the end of the day, you really—what you're going to do is you want to match your ongoing monitoring to the level of risk presented by that service provider. So, it goes back to your third-party risk management program, and it goes back to your risk assessment. And so, does your risk assessment present that this vendor or service provider has an elevated amount of risk to your operations as an institution, and, therefore, you act accordingly with different monitoring activities. So, you know, when core providers—you know, if you're a service institution from a core perspective, those providers are going to have disaster recovery tests and failover tests. Participate in those. Be active. If you're not, ask to participate. You learn a lot through those things. Connectivity back to the service provider is paramount to access, so accessing your core data. So, there's a lot of different things you can do. At the end of the day, it's about risk management, appropriately managing risk based upon the risk presented by that service provider, based upon what they do for you.

Carl White: All right, thanks. Thanks, Carey. Okay. We're going to have to wrap up. Thanks for the questions you have submitted. If we missed a question, we may reach out and forward that on to the CPC or maybe have Nathan and Carey take a look at it, but if you still have questions, please, like Meg and others said, reach out to us. We're here to help, and any of these individuals—you might not want to call me. I'm not an IT expert. I'll probably just refer you to one of these folks, but any of us can certainly get you an answer to your question.

So, before I wrap up, I did, kind of, jot down some key takeaways, and this is certainly not an exhaustive list, but I was just, kind of, taking notes as Carey and Nathan went through the presentation. But I would definitely refer to Slide 12 and 13, the questions to consider and the items to review, but just some key takeaways that I wrote down. Timeliness of vendor patches is critical. You may want to consider a comprehensive gap analysis. Basic cyber hygiene, I think that's just a real critical theme. Off-network backups, prepare for the worst. Understand what's connected to your systems. Keep an open dialogue with your key vendors and service providers, and Carey just mentioned that again about, you know, engaging with them. And then, last, your people, train, train, train. You know, we go through tests here at the Fed constantly, whether it's phishing, whether it's other things to protect our data. So, I just can't emphasize that enough.

All right. So, we need to wrap up. So, I know we're running over just a couple minutes, so thanks for bearing with us. But thanks for your questions and thanks for joining us today. First of all, thanks to our presenters. Thanks to Allen, Carey, Nathan, Meg. Many of these folks you know. If you don't, these are people you should know, especially if you're in the IT space. So, thanks to all of them for their work on today's session. As I said at the beginning, all sessions are archived on our website, supervisionoutreach.org, so you can review those materials. You can listen to our session again, forward this on to other staff, forward it on to your board. It's there to help.

So, finally, *Conversations with the St. Louis Fed*® is a program of the Federal Reserve Bank of St. Louis. It's intended only for informational purposes. The views are not formal opinions of—nor binding on—the Federal Reserve Bank of St. Louis or the Federal Reserve System.

This *Conversations with the St. Louis Fed*® session is eligible for continuing education units. So, all you need to do, first of all, is you need to make sure you're registered for the session. That's the easy part. Secondly, you need to complete the last section of the online survey, which is going to be sent out any minute now. So, we do look at all those surveys. It helps us improve our events. So, if you have a minute, please take that survey. Thank you so much for joining us today, and we'll talk to you next time.

(END OF RECORDING)