BNY Mellon
Perspectives

Strengthening Cyber Resilience

APRIL 2020

Jeff Lunglhofer, Chief Information Security Officer
Maria-Kristina Hayden, Head of Cybersecurity Wargames and Awareness

Brenda Tsai (00:01):

Through times of calm and crisis, BNY Mellon's perspective has made us the trusted steward of the financial system. To help our clients make stronger decisions, our experts explore the many angles of the financial markets, investing and business. Welcome to BNY Mellon *Perspectives*.

Brenda Tsai (00:24):

Hello, I'm Brenda Tsai, Chief Marketing Officer of BNY Mellon and just a quick note before we start. We're launching this podcast at an unprecedented time where working remotely has become our new normal, so we're recording this podcast from our homes. Thank you for joining us from yours. We're here with two of the firm's leading experts to discuss some of the challenges around cybersecurity and the pandemic COVID-19. I'm joined by Jeff Lunglholfer and Maria Hayden. Jeff is BNY Mellon's Chief Information Security Officer and Maria is our head of Cybersecurity Wargames and Awareness. Jeff, Maria, thanks for joining us today.

Jeff Lunglhofer (01:07):

Thanks so much for having us, Brenda.

Maria Hayden (01:08):

Thank you.

Brenda Tsai (01:10):

Jeff, my first question is for you. Since the coronavirus became a true global pandemic, a large percentage of the global workforce is now working from home. How has this opened up new avenues for cybercriminals? What are you seeing?

Jeff Lunglhofer (01:26):

That's a great question, Brenda. A work from home workforce is a completely different dynamic when it comes to cybersecurity. We used to have people sitting in their offices, talking to each other on the phone, sitting in, right next to each other, having ad hoc conversations and today

we've got everybody sitting behind computers at home.

Brenda Tsai (01:45):

Yes, it's the new, not so normal.

Jeff Lunglhofer (01:47):

What that means is that the attackers have changed how they approach our employees and how they try and steal information. That's been a real challenge cross-industry.

Brenda Tsai (01:58):

Are you seeing new angles of attack?

Jeff Lunglhofer (01:58):

One of the attacks that we are seeing is an increase in phishing and other attacks on employees. Those can include COVID-19 related emails that contain malicious links to websites, malware and other things. That is people using this crisis to try and get people to click on those emails, to try and get people to click on those websites. It's become much, much easier to get people's attention with a flashy headline, a flashy subject line in an email or even a direct phone call to somebody saying, "Hey, I'm Jeff from our marketing department and I really need a piece of information to help me get my job done." How do you know that that's really Jeff. How do you know that it's really Brenda or really Maria on the other end of that line? Do you know them personally?

Brenda Tsai (02:45):

I hadn't heard that one before.

Jeff Lunglhofer (02:47):

These are questions that we really have to ask ourselves and it's really important that everybody understand, our adversaries know that we are changing the way we work. They're exploiting that. They're using the changes in the way we operate every single day to look for new ways to gain access to our information, and that's something that everyone needs to be aware of and vigilant for 24 hours a day.

Brenda Tsai (03:10):

Wow. It's a different world. Given what's happening right now, how are you thinking about our BNY Mellon overall cybersecurity strategies?

Jeff Lunglhofer (03:19):

BNY Mellon considers cybersecurity to be one of our number one focus areas. We take cybersecurity very seriously at Bank of New York Mellon. Everything we do is intended to protect our clients and to protect our core business and all of the information and assets that we have under custody and under management. All of our training awareness and our whole cybersecurity operation is designed to protect our client's information and to keep everyone safe. We invest heavily in cybersecurity across the board.

Brenda Tsai (03:49):

That's right, like at CTOC. Can you explain to our listeners what that is?

Jeff Lunglhofer (03:54):

We've recently invested in a cyber technology operations center at 240 Greenwich Street to help bring together all of our businesses, all of our operations, staff, technology and cybersecurity in one location so we can protect our clients better. That's just one great example of how we're investing in cybersecurity globally.

Brenda Tsai (04:11):

Thanks Jeff. Maria, now you're the head of our cybersecurity wargames and awareness. Tell us a little bit about your day to day.

Maria Hayden (04:19):

Certainly. So, I think that we could spend this entire session describing in detail the robust cybersecurity program that we have, the technology, the tools that we use and our to follow the sun model of global teams. But one thing I'm really proud of with this program is our emphasis on educating the human as well. The human side of cybersecurity.

Brenda Tsai (04:43):

Yes, I agree. The human side of tech is critical.

Maria Hayden (04:47):

We focus on empowering global staff with tools that they can use day in and day out to make better security decisions in their day jobs. One of the ways that we do that is to maintain but not only maintain, also rehearse extensive business recovery plans as well as cyber incident response plans. What this allows us to do is not just document best practices and plans for recovery, but also to have dress rehearsals where we can play through fictitious incidents that allow us to test those plans.

Brenda Tsai (05:21):

It's great to see this effort devoted to keeping our information safe and secure. Maria, you're in charge of conducting Wargames. Can you tell us a little bit more about them?

Maria Hayden (05:31):

Sure, so wargames are one of the many tools that we have in our toolkit when it comes to employee awareness, cybersecurity awareness in particular. So, in addition to written awareness and in person presentations, we also conduct these wargames. They are our favorite way to practice response plans. They are essentially internal cyber exercises that help strengthen our response muscle memory. So, we of course run deeply technical wargames for our technology teams, but we also facilitate many wargames a year that are less technical and actually bring both business teams and technology teams together to mimic a real world cyber attack and play through their response in a multiple hour session. And I think it's really unique that at BNY Mellon, this program is run entirely internally, meaning that we're able to deeply customize our scenarios to the key risks that face each participating group. They're a lot of fun and there's a lot of learning that comes out of each one.

Brenda Tsai (06:41):

That is impressive. So as I think about all of our listeners who are at home and aren't able to have their own wargames, what steps should they be taking to protect the company's technology and information? Jeff, let's get your thoughts first.

Jeff Lunglhofer (06:55):

Let's talk about cyber hygiene. Cyber hygiene is one of the most important things when you're trying to run a secure infrastructure. We need to ask ourselves the key questions. Have all of our corporate devices been fully patched? Are we running antivirus and do we have the right levels of controls deployed across our ecosystem?

Brenda Tsai (07:14):

Do you have a checklist for our listeners?

Jeff Lunglhofer (07:16):

Some of the most important but simple things that you can do. One, make absolutely sure that every system has received all critical security patches. Two, make sure that you have antivirus deployed on every single endpoint that's out there, every laptop, every device that people are using across your ecosystem, make sure you have antivirus installed and that it's fully updated. And the last thing is look at how employees, particularly now, are accessing corporate services remotely. Are they using secure channels? Are you using the right levels of encryption? Are people choosing and using good passwords or better yet, are employees required to use multifactor authentication before they gain access to corporate services? Those are some of the very simple but important things that we can do to protect our ecosystem in these troubling times.

Brenda Tsai (08:11):

We all need to do our part. Maria, what are some of your recommendations for our listeners?

Maria Hayden (08:17):

When people ask what bothers me, what keeps me up at night, one of the things that continually comes to mind is the fact that year after year we still must list phishing and spear phishing as some of the top cyber attack vectors globally.

Brenda Tsai (08:33):

Yeah. For those unfamiliar with cyber terms phishing and spear fishing, can you quickly define those for us?

Maria Hayden (08:39):

Absolutely. Phishing and spear fishing are both types of social engineering, so essentially social engineering is any attempt to manipulate someone for information or for access. So phishing uses any kind of communication channel. It could be email, could be a phone call, a social media message or a text message to entice someone to divulge information or to get them to perform an action that is somehow helpful to an attacker. Very often phishing attacks are achieved by casting a very wide net, so for instance, sending the same message to hundreds of

thousands of people whereas spear fishing is a more targeted approach. Instead of fishing with a net, someone is fishing with a spear, if you will, and targeting a specific set of people or it could be one individual. And to do that, they use highly customized messages that they think the person or the small group will respond to.

Jeff Lunglhofer (09:39):

And just to interject here, we are seeing an advance and more sophisticated types of attacks using phishing and spear phishing as Maria just mentioned. We're seeing multiple companies being targeted simultaneously by spear phishing attacks to make it appear as though two executives are communicating with each other. That is a real step up in terms of the type of attacks that we're seeing in that every financial institution and in fact every business should be aware of. It's a really significant problem that we all need to track.

Brenda Tsai (10:07):

Given what's at stake, who should be taking the lead here? Should governments and the private sector partner up more closely together?

Jeff Lunglhofer (10:14):

I don't think it's as simple as who should take the lead. Everyone needs to work together to confront the cybersecurity threats that we face today. There's no way any individual company, any individual government, business or even individual person can possibly combat the myriad of cyber criminals that are out there trying to do us harm. What we've found at BNY Mellon is working closely with the government, working closely with our peer institutions, working closely with our clients and our staff is the right mix and the right way to approach dealing with cyber threats. I would say one of our most important resources are our people. They can report and identify when they're subject to cybersecurity attacks, when they get those malicious phone calls, when they get those malicious emails. They are the first ones to tell us about it most of the time. That enables us to react and work with our peer institutions to rapidly contain any cyber threats that we may encounter.

Brenda Tsai (11:10):

Any last thoughts you'd share with our listeners?

Jeff Lunglhofer (11:12):

I would leave all of our listeners with simple advice, focus on cyber hygiene and stay vigilant. This situation is evolving and it's going to continue to evolve over the next several weeks, possibly several months. We are going to have to work together to stay ahead of cyber threats and to make sure we keep our businesses fully functional and fully afloat at the same time. That is a difficult challenge, but we can get through it together.

Maria Hayden (11:36):

Couldn't have said it better myself.

Brenda Tsai (11:38):

Great. Well thank you both. Clearly cybersecurity is critical, especially in these times. It was very

helpful to get your insights on what we can do to remain vigilant. Jeff, Maria, thanks for joining us today and thanks for listening to Perspectives where we'll continue to look at critical topics from every angle.

Brenda Tsai (12:01):

Be sure to download and subscribe to future episodes available on bnymellon.com and all other major podcast platforms. Stay safe. Stay well.