Merrill Perspectives Podcast

Episode 9: "Cyber Security"

With Candace Browning
Head of BofA Merrill Lynch Global Research

Chris Hyzy, Chief Investment Officer,
Merrill and Bank of America Private Bank

And Stephen Sparkes, Head of Cyber Security Technology,
Bank of America

Brandon McGee, clip #1
"We have a small company and we have maybe 8 to 10 computers. Somebody ended up clicking on some link in an e-mail that he got from somebody that he knew, and it turned out to be ransomware."

Candace Browning: That's Brandon McGee, an accountant in West Valley City, Utah, whose small firm was targeted by a ransomware attack. In this type of attack, a criminal sends a virus to an individual or an organization that shuts their computer system down, and says they'll only unlock it when money or a quote unquote ransom is paid.

Brandon McGee, clip #2
"Up to that point I'd never heard of ransomware. Originally, we thought it was that individual computer, but since it was linked to our server it shut us out of our accounting system. Shortly we had all of our people come in saying they couldn't access the software for sales orders, for invoicing, for those kinds of things."

Candace: Like millions of people around the world. Brandon and his coworkers now have a very personal understanding of how our evermore connected world comes not only with enormous benefits and conveniences, but also with real risks. But just how big a problem is it? And what steps can we take today to better protect our digital lives?

[Theme music]

Candace: You're listening to the ***Merrill Perspectives*** podcast. I'm Candace Browning, Head of BofA Merrill Lynch Global Research; and with me today is Chris Hyzy, Chief Investment Officer, Merrill and Bank of America Private Bank

Chris Hyzy: Hi, Candace

Candace: And Stephen Sparkes, Head of Cyber Security Technology for Bank of America.

Steve Sparkes: Hello, Candace.

Candace: Today we're talking about cybersecurity and the ways that the digitization of our personal information and data are increasingly integral to our lives. We'll explore the many benefits this offers and the risks it presents for individuals and companies.

And we'll offer steps and actions you can take today to help protect yourself and your family.

Steve and Chris, welcome.

And let's just start by looking at some of the numbers. In 2018 as many as 5 billion personal records were exposed due to cyber security breaches. One estimate says there are 480 threats released by cyber criminals every minute and it's estimated that cyber crimes costs a collective $6 trillion per year. ***(Sources: Risk Based Security, 2019; McAfee Labs, Q3 2018; Cyber Security Ventures, 2016.)***

So Steve, let's start with you. Where first are these attacks coming from and how do they affect the majority of people and businesses?

Steve: Well, Candace, they are really four main groups of what we call threat actors. Some of them are less relevant for the individual. Nation states who are generally looking at large scale corporate intelligence; hacktivists, who have got a personal beef against institutions and are looking to deface websites or advertise a particular cause. But then we get to the ones that are likely to affect most of the listeners for this broadcast. And those would be the criminals and the insiders.

Candace: So what's the difference again, between a criminal and an insider?

Steve: So sometimes an insider and a criminal may be one in the same. Criminals are generally external and they're looking for money. An insider maybe one of the people that is employed by a company that's in cahoots with them, or they may have a personal beef against the company, but because of their privileged access, they have access to the company's systems.

Candace: Okay, got it. So Chris, let's talk about technology for a moment. We have voice activated personal digital assistants. We have appliances and industrial machines connected to the Internet. We can shop for socks or medicine or orange juice. And there's this vast trove of data that's captured that's, you know, really transforming the economy. Now, how is this all potentially increasing our cyber security risks?

Chris: If you really think about it, our lives are connected everywhere, as you said, Candace. We estimate that the number of connected devices from 2018 at about 18 billion will almost double by 2025 to about 34 billion connected devices. ***(Source: IoT Analytics, 2018.)***

There are so many benefits to being connected, but risks are out there. The greater the connectivity there is, the higher the cost and the greater likelihood that you face a cyber risk.

Candace: Okay. Well let's delve into that issue of risk a little bit more. So Steve, what do you think are the biggest risks that individuals face on a sort of a day to day basis?

Steve: Building on what Chris said, the access to this incredible trove of resources that individuals want to use, creates a two way pipe. And you should always remember that what you're using to get out to the Internet to surf websites and communicate with others can be used by these criminals to exploit access to you.

Email as a delivery channel for ransomware is absolutely a key risk. Websites with malware that can be downloaded without you knowing it, that could then be exploited remotely by criminals to mine your personal information for outright theft and for creating fake identities. Those are the key risks that I think most people should be aware of and should be concerned about.

Candace: So let's talk about what our defenses are. I mean, after all, we're not completely defenseless. We often read about these big successful hacks, but we really don't hear much about attacks that were prevented.

So Steve, can you just start with the basics? I mean like passwords. I think somebody told me that the most popular password is one, two, three, four, five, and that the second most popular is "password." ***(Source: SplashData, Dec. 2018).*** (Laughter.) That seems kind of amazing.

Steve: Yeah, it is kind of amazing. And I think it does speak to the large-scale problem that a lot of people have. It's a pain in the neck to have different passwords for every website. It's troublesome, but if you don't have a, a meaningful password, a long enough password to make it hard for the criminals to guess it, you will be exploited.

If you've used the same password for all of your websites, you are just asking for trouble. The first time one of those websites gets corrupted, you've just handed over the keys to all of the websites that you use.

So you must have different passwords for different websites. And there are tools available to help you with that. So you can use a password manager. You don't have to remember the quick Brown Fox Jumped Over the Lazy Dog and where you put zeros and ones in the middle of that every time, but you absolutely, as an imperative to mix up your password usage.

Candace: And what are some of the common ways that hackers try to trick us into telling them what our passwords are? And how can we recognize those and prevent them?

Steve: Taking the email example, if you receive an email from a Nigerian prince, most people these days are going to spot that for the fake that it is. But if you get a mail from a friend it's naturally our defenses are a little bit down. But these days because of the viral effect of a lot of these attacks, your friend could have been compromised.

If anything looks suspicious, hover over the sender name. Make sure that it looks credible. Don't click on a link. If something comes from an email address purporting to be a bank, start a fresh browser, go to the website that you know is the valid bank website. Don't click on the link that was sent to you in the email because that has probably been manipulated.

Candace: So besides having multiple passwords, and remembering all of them, what else can one do to protect themselves?

Steve: So Candace, one of the other key things that everyone should do is keep their devices up to date. A tremendous number of the exploits that take place are using old vulnerabilities that the manufacturers have fixed ages ago and they've pushed out updates, but people haven't updated their devices. So whether it's a laptop or phone or a desktop computer, do the updates because that is the one thing that you can personally do to manage your own devices to keep you as safe as possible.

Candace: And what about going to more sort of biometrics rather than remembering a password?

Steve: Absolutely. A good alternative to passwords, wherever it's available, is to use the biometric option. And some manufacturers in particular in the smartphone market have really come up with some extremely good solutions and whether it's a face ID option to be able to unlock a phone just by looking at it. That's really super important. And when you set those up, make sure that you choose the option to say you need to look at the device so it can't be done accidentally when you're just passing.

And where you have the option on a website to sign up for multifactor authentication, or two factor authentication as it's sometimes known, that will send you a text with a pin number to enter on the website; you'd definitely want to sign up for that. That's one of the primary controls that you can use to protect sensitive websites.

Chris: And in some cases there are examples where you're offered an actual question, you know, what is your mother's maiden name? What's your favorite pet's name? Where did you go to school? Be cautious in using standardized questions. There are some websites or other places that will allow you to put your own

question in and that is a little bit more customized to you versus others who may know that typical answers for your favorite dog could be Otis.

Steve: Yeah, absolutely. And there's so much availability through social media. So the chances are everybody knows your mother's maiden name by now, so that is not so secure.

Candace: Let's go back to Brandon McGee and that ransomware attack. It turns out the attackers were asking for $700 to unlock the files and Brandon clearly wrestled with what to do next.

> **Brandon McGee, clip #3**
> There was that scare moment; you kind of panic, going, okay, how am I gonna get my files back? What if we pay the ransom? Is it going to be something like every six months they go, "hey, you know what, we need another thousand dollars"? Is it just going to be a repetitive cycle?

Candace: Brandon's small firm was lucky. Unlike many small companies, they backed up their files every day, so they decided not to pay and were able to restore their systems to where they were before the attack, but it still cost them money.

> **Brandon McGee, clip #4**
> We have beefed up our security. We use a different email server. We were using kind of a freeware email system. We've added a firewall. Instead of using the tape backups now we backup to hard drives. And the computer that brought that in, we ended up having to replace that computer entirely.

Candace: Besides the steps that Brandon just outlined, what else can a small company do? Is there maybe training that they can give their employees?

Chris: Yeah, I would say training for sure is number one in all aspects of it. Also I think companies really need to think about each year changes to their software systems.

Even more important going forward is the vendors you work with as well. Understand exactly what their protection status is and how you work with them. And just make sure that everybody understands it's okay to be skeptical about things that are being sent to you and what's asked of you.

And if you think about the lack of skills in cyber security in and of itself, they estimate that there's one to 2 million of a job gap already in that field. Estimated to go to three and a half million in just a few short years. ***(Source: World Economic Forum, 2018.)*** As that continues, the training is gonna have to go up exponentially.

Candace: So we're going to see a lot of growth in jobs available in cyber security going forward.

Chris: Significantly.

Candace: So Steve, if I'm a small business owner, how should I train my employees to be aware of these risks?

Steve: So there are a couple of different security training companies that you could contact. And one of the things that they will offer is phishing training where they will send you fake mails and test your employee's ability to detect them and hopefully they catch them. And if not, you'll be able to identify the kinds of tricks that your particular population will fall for.

And the other path that I highly recommend is to talk to the auditors, if you have an audit firm that will provide best practices around financial processes for releasing funds. Because they've seen it all, and can help you train your staff to look out for these particular exploits that are a rife in cyber security.

Candace: Okay. So we've been talking a lot about companies. Let's talk a little bit more about individual people. And one of the statistics I thought was particularly interesting is that the most common form of stolen personal information is actually electronic health records. Now you may wonder, is it really valuable for a cyber thief to know that I had a sprained wrist or that I went to the doctor for a checkup back in April? So what's the risk there?

Here to help explain is Robert Lord, Co-founder and President of Protenus, a firm that helps hospitals protect medical records.

> **Robert Lord, clip #1**
> Think about what's in an electronic health record. You've got everything from your demographic information to your address to billing information, financial information, insurance. You've got your entire family history, historical addresses, historical diagnoses, any types of sensitive information.

Candace: It sounds like once a cyber criminal has all of this very personal information, they could easily build a false identity using far more detailed information about someone than a normal identity theft.

So we do know that there are some companies like Protenus that are applying artificial intelligence or AI to sift through the millions of data inputs in these systems to find problems.

> **Robert Lord, clip #2**

> The reality is that the digitization of medical records is absolutely essential for the next wave of advances in health care. And we calculate probably roughly 10 million or so accesses to patient data a day in your average, large healthcare system. Even a very diligent reviewer can only review in the thousands of these records, whereas AI is able to cover tens of millions or billions in a second.

Candace: So, Chris, clearly there is a role for artificial intelligence in all of this. What else are you seeing in terms of new solutions and technology being deployed to help us protect our data?

Chris: Some of the new technologies out there are actually not new in and of themselves. They're actually older technologies that have been around for decades, one of which is secure ID. And secure ID is a way to create a digital password every few seconds. So a hacker or a criminal or someone trying to get into a system has a very difficult time latching onto one particular password.

Secondly, it would be blockchain, which still is in its infancy as it relates to where it's used but not in its infancy in terms of its potential. And then third, as Steve mentioned before, it is about bio-metrics.

Steve: I think it comes down to making you a harder target than the next guy. Just to be blunt around the challenges, the criminals are always going to go after the weakest link and if you're vulnerable they will find that weakness and exploit it. If you take reasonable precautions, you can make it too expensive for them to justify going after you as an individual.

Candace: Okay. So let's switch gears a little bit and talk about the effects on the economy and companies in particular. I saw that the FBI estimated that one form of cyber crime, which is business email compromise, has actually cost companies more than 12 and a half billion dollars in just the last five years. ***(Source: Federal Bureau of Investigation, July 2018.)***

So what do you think are some of the effects on the economy of those kinds of huge numbers? And is it changing the way that companies are actually doing business?

Chris: When you just break it down simply, when you're spending dollars, resources, energy, people, skills, et cetera, to protect things, you're taking what could have been dollars being put to direct economic activity to use outside the system.

Once you bring it outside the system, clearly productivity can have the potential to go down in the broader economy. That's in the short term. However if you're protecting against something happening, you don't have to pay the costs later. So I think that balances out.

But in terms of just general economics, the clear economic benefit is the potential of three and a half million jobs in the cyber space. ***(Source: World Economic Forum, 2018.)*** And that ultimately leads to better income growth and economic activity.

Steve: And I think you see that in the cyber security technology industry as a market. It's a very immature space. It's still a relatively new field. There are a tremendous number of small companies growing to address specific threats. So there's an explosion in the cyber security ecosystem, which is somewhat offsetting the drag from the extra precautions that people need to make.

Chris: In terms of other sectors, we all talk about the technology sector. We talk about healthcare, but what's not talked about enough is the utility system, as well as the industrial sector.

Transportation, if you thwart transportation in a local municipality, in a state, in a city, or across the nation, you shut down the economy. It's the same thing with the utility system. If you don't get access to water and it's not a natural disaster, but it's an actual attack on the utility system, you don't have electricity. Those are areas that I believe you'll see the greatest outgrowth in capital intensity to build the systems needed to protect against attacks.

Candace: So Chris, clearly there's a huge amount of growth in the whole cyber security space. Are there investment opportunities?

Chris: Yes, there, there are clear investment opportunities. There's a number of different companies out there in the software world directly in the cyber secure space. There's larger companies that have major units that are growing much faster than their other units that are also very much connected into the cyber arena.

You will see on average a handful of companies coming public in the next 10 years per year that have some exposure to this space. Last but not least, when you think about the exchange traded fund market, also known as ETFs, there are a few ETFs out there that have a basket of companies directly involved in the cybersecurity space.

Candace: So Steve, we talked earlier about some steps that individuals and families can take to protect themselves. What are other actions that they should consider?

Steve: I think some other general best practices are to avoid posting too much information on social media. I think there's a clear personal risk if any members of your household are tweeting about how excited they are about your upcoming vacation, where your house is going to be empty for an extended period. That's a clear signal that that's a great address for a criminal to put on their to do list.

I think it's also important to be mindful of using public WiFi. If you're in a coffee shop or in an airport or in a general public environment where you're connecting to a network that you're not responsible for, there's real risk there.

If you put in your banking credentials while you're in a coffee shop, there's a decent chance that somebody else is going to be able to record that information.

Candace: Well great. Well we've covered a lot of ground here today. I guess I'm going to put one last question to both Chris and Steve, which is what are the most important takeaways for our listeners?

Chris: I think backing up your information frequently, call it every day, whether you're a company, an individual, an agency, etcetera, is highly important. Number one. Number two, how you back up that data is increasingly becoming important. Instead of doing it on the network itself, having an external drive, if you can, is extremely important. It's hardware and that can be taken off the network itself.

Steve: Yeah, Chris I think nailed it. Taking a regular backup, it sounds like it's technically complicated, but you spend the hour and a half, two hours, whatever it's gonna take to do it the first time. And then most of them you can just set it up and it will run automatically. And I think keeping your environment up-to-date and not using the passwords across multiple sites would be my key takeaways.

Candace: Well, Steve and Chris, thank you so much for your insights today. It's been, I think, a fascinating and really informative conversation.

You've been listening to ***Merrill Perspectives***. I'm Candace Browning, head of BofA Merrill Lynch Global Research.

My co-hosts have been Chris Hyzy, Chief Investment Officer, Merrill and Bank of America Private Bank and Steve Sparks, head of Cyber Security Technology, Bank of America.

We hope these episodes inspire you to see your financial life in a new light.

What would you like the power to do?

You can subscribe on Apple podcasts, Google podcasts, Stitcher, or Spotify or wherever you get your podcasts.

And while you're there, be sure to check out some of Bank of America's other original podcasts such as ***The World To Come*** where we explore life in the future by talking with the visionaries of today. And ***That Made All The Difference*** where we talk to people who have made a positive impact on the world, about the moments that changed the course of their lives.

For more insights into how we can help you pursue your financial goals, go to Merrill.com.

Thanks again for joining us.

This podcast was published on October 9, 2019.

Any opinions or other information correspond to the date of this recording and are subject to change. The views expressed are not necessarily those of Bank of America Private Bank or Merrill. The information contained in this podcast does not constitute research or any recommendation from any Bank of America Private Bank or Merrill Lynch, Pierce, Fenner & Smith entity to the listener.

The information is general in nature and is not intended to provide personal investment advice. The information does not take into account the specific investment objectives, financial situation and particular needs of any specific person who may receive it. Investors should understand that statements regarding future prospects may not be realized.

BofA Merrill Lynch Global Research is research produced by BofA Securities, Inc. ("BofAS") and/or one or more of its affiliates. BofAS is a registered broker-dealer, Member SIPC, and wholly owned subsidiary of Bank of America Corporation.

The Chief Investment Office, which provides investment strategies, due diligence, portfolio construction guidance and wealth management solutions for Global Wealth & Investment Management ("GWIM") clients, is part of the Investment Solutions Group ("ISG") of GWIM, a division of Bank of America Corporation.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill") makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation ("BofA Corp."). MLPF&S is a registered broker-dealer, Member SIPC, and a wholly-owned subsidiary of BofA Corp.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC and a wholly owned subsidiary of BofA Corp.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value

This podcast should not be copied, distributed, published or reproduced, in whole or in part. Neither Bank of America Private Bank or Merrill nor any of its affiliates makes any representation or warranty, as to the accuracy or completeness of the statements or any information contained in this podcast and any liability therefore (including in respect of direct, indirect or consequential loss or damage) is expressly disclaimed.