THE Patti Brennan SHOW

Ep20: Cyber Security

July 19, 2019

PATTI BRENNAN: Hi, everyone. Welcome back to the "Patti Brennan Show." Whether you have $20 or 20 million, this show is for those of you who want to protect, grow, and use your assets to live your very best lives. Boy, protection is what it's all about. Today, we're going to be talking about how to protect everything in your life.

Joining me today is Vince Kailis. Vince is our Chief Operating Officer. I will also tell you, he is our resident geek. This guy knows anything and everything that has to do with computers, operations, etc. He's really, really good as it relates to cyber security because, frankly, we have to be really, really paranoid about all of this stuff.

Vince, welcome to the show.

VINCE KAILIS: Thanks for having me today, Patti.

PATTI: Absolutely. I'm really looking forward to this. You've got a wealth of information, lots of wisdom. I think that as we were talking about, some of the statistics that you shared with me were really alarming.

For example, I didn't realize University of Maryland came out with a study. "There's a hacker attack every 39 seconds." They're constantly barraging all of us, trying to get at our sensitive information, etc.

Since 2013, there are almost four million records stolen from breaches every single day.

VINCE: Every day.

PATTI: Every day, Vince. Literally, these hackers have gotten so good that they're getting this information at the rate of four million per day. Think about it, guys, 300 million Americans. How long is it going to take for them to get to every American and their computer?

We have to be extremely vigilant. That's what we're really going to be talking about today. The cost of this is tremendous. What I thought was really fascinating is, of course, they're going after small businesses.

You told me that 95 percent of the breaches, in terms of corporate breaches, came from only three industries in 2016, government, retail, and technology. You have a story about a government breach or a government phishing scheme that just blew me away.

VINCE: There was a scary one that came out a few years ago. It was during the last presidential election cycle in 2016. John Podesta's emails were hacked.

PATTI: Now, John Podesta is who?

VINCE: We were talking about way high up in politics, people on the Clinton campaign. His emails were compromised in what's called a phishing attack, which we'll get into in a couple minutes, probably, to make sure that the listeners really understand what phishing is and what the types of phishing they should be looking out for.

His team got an email that his Gmail account had been tapped. They had gotten this nice little email from the Gmail team that said, "John, your email was hacked. We stopped the attempt in the Ukraine, but you're going to need to reset your password. Click this link to reset it now."

PATTI: Wow.

VINCE: To make matters worse, the Clinton campaign security team emailed his team that, "Hey, it looks like his email was hacked. Go to Google and have him reset his password." They didn't do that. They actually clicked the link that was in the email.

Even the security team thought it was a legitimate email, but their way of getting to it was very different than what was in the email. The link took him to a site that captured his username, his password, and all his emails were stolen.

PATTI: Wow. That is amazing.

VINCE: Subsequently, ended up on WikiLeaks.

PATTI: Wow. That is amazing. Let's talk about this thing called phishing. By the way folks, it is not spelled F I S H I N G, it's P H. Where did the name come from, Vince, phishing?

VINCE: Yes. What us nerds have ways of renaming things, like putting P H instead of F in things. It's just phishing is a method to get your confidential, sensitive data through emails or through a website. It's just like regular fishing if you think about it.

I'm going to put some bait on a hook, I'm going to take the line and I'm going to cast it out there, and I'm going to hope to catch a fish. I'm going to hope somebody nibbles on that little piece.

Sometimes that bait is, "Hey, this Nigerian prince really has this money for you," and sometimes it's things like, "Hey, we know what you've been doing on your computer, and to keep us from disclosing it, click this link."

PATTI: That is really interesting. That's a form of that ransomware, right?

VINCE: Absolutely.

PATTI: The goal of phishing is two fold, from what I understand, from what you've taught me. Number one is to get our personal information, whether it be our social security numbers, our credit card information, etc., or to load malware onto our computers, where there's significant damage that could be done as a result of the malware, right?

VINCE: Absolutely. Sometimes, they're not even looking initially for your social security number or your passport ID. All they want is your username and password. If you look at some of the common mistakes people make, they use the same username and password on things.

Once they have one username and password, they can put it into a system that tries to log into hundreds of different sites.

If they get a hit, they're near your bank account, they're into your kid's 529 account, or they're into a different email that you have. Now they have two email addresses and potentially even more compromising data.

PATTI: That's really interesting. A couple years ago, with the Experian situation, where millions and millions of Americans' personal information got stolen. The more information that is out there the more likely that somebody is going to attempt at least attack you, get additional information and steal from you.

VINCE: Absolutely.

PATTI: Tell me more about this URL masking – using different characters in the address, how does that work? How can our listeners prevent a situation when they're on their computer?

VINCE: An example that we gave of the Podesta email, it was the Google email team. It was Google Mail team as opposed to "google.com" with a link to how you get your Gmail.

PATTI: It sounds so reasonable. Google Mail team, your emails been hacked. It seems reasonable. Right?

VINCE: Yeah. Some of the newer ones – your Microsoft account is about to expire or has been compromised, reset your Office 365 password, that's a common one going around right now. There's been a huge uptick of those.

How about this one? We failed to deliver your package today, click this link in the "UPS thing" to set a new time to have your package redelivered. The link actually isn't UPS, it's "ups.ru" which is a Russian site. That takes you to a different site. You put in your information about your email address, and whatever, to reschedule the delivery, and you're not even on "ups.com."

PATTI: Wow. The hacker also knows when you're not going to be home.

VINCE: That's the next piece of it.

PATTI: Wow, It's amazing. The information, it's not just the random and get your credit card information anymore. It's that kind of stuff. You've got to be extra careful.

When we heard about this, we literally put those cameras all around our house. It was really cheap. You get them on the Internet, they record, you put the little warning there so that it...So far it's been a good deterrent but you don't realize who is getting access to this information and what they could be taking.

VINCE: Sure. Can be social media combined with the hacking efforts, put those two things together. They know you're on vacation that week. That's the week they'll hit in your house.

PATTI: Tell me more about this social engineering, Vince. I thought that was really interesting when you were talking about it?

VINCE: There's a couple funny stories that go along with this, we'll go with the funny one to start. There was one I think was three or four years ago that came out, it was on Facebook and on a couple other sites. It said, "If you want to know what your adult film stars name would be, it's your street you grew up on plus the name of your first pet."

If everybody thinks about that for a second like, "Oh, yeah, that's clever. That could have been my adult stars name." But really what they were doing was they were capturing two of your security answers to security questions. If they had one piece or two pieces – username or password, they couldn't get past the security question, now they have to have those.

There have been a couple of those viral things that have gone around on Facebook and a few other places, where they were capturing these extra security credentials.

PATTI: You think about Facebook and some of those other, Instagram, etc. My kids are posting that stuff all the time, thinking it's just random and not a big deal, it's our dog Bentley. I mean, even on our website here, we've got Bentley. It is interesting. I'm not using Bentley as security password. I thought this was a fascinating tip.

We had a client who we were talking about all of this. She said, "When they ask those

security questions, I don't answer the question – I give something random." For example, "What was your first dog's name?" She'll put in a month, February. You wouldn't name your dog February, it's a random word. She knows the answer, and that's not on Facebook or any other social engineering.

As you think about your security questions, make it completely unrelated to the question itself, so that it's a word that only you will remember. I thought that was a really interesting tip that can prevent that.

VINCE: Another one of our clients had brought up a really great one at an event too. We had a cyber security event where we had a specialist come out and talk about how to protect yourself. Our clients seemed to love that one. They had some really unique ways of protecting things. One was the password was a phrase. It was the first letter of each word in a phrase that he would remember.

The capital would be the words that were supposed to be capitalized in that sentence. If it was America, it would be an A or the first letter, the, that would be capitalized. He only took the first letter of each of those. It was easy for him to remember what the phrase was but to anybody looking at it, it'd be a random string of letters.

PATTI: I've used that many times. As you know, in our industry, I've got 50 different websites. We have to change them every six weeks. They can't be anything related to anything that we've done the last three years.

I don't know about you guys but I am not that smart when it comes to remembering my passwords period, much less what did I do for the last three years. Phrases are a really good way of figuring a different way of providing that kind of security.

When you think about this, what are the top subjects? What are the ones that are really popular right now? You mentioned Microsoft.

VINCE: Things going around right now, Netflix is a big one. Your account has expired, to continue viewing this great selection of movies click here and put your credit card info back in. It's a fake website. That one's up this year 25 percent more than it was last year.

PATTI: What's really scary about this – this is what we did with our seminars, we brought it up on the screen. The email has Netflix's logo. It looks exactly like Netflix, what you would expect from Netflix with all the same colors, etc. You'd have to really do what we're teaching everyone today and right click on that email address to make sure that it is legit Netflix.

VINCE: That's a really good point. You went through the exercise of bringing it up on a screen and showing the clients what was wrong with each of those emails or what was right and how to do it. If you're not sure, ask somebody.

You held that seminar for people. It was great to inform them of that. If you don't have access to go to a seminar where somebody can teach you that stuff, ask somebody. Ask your kids that are under 13. They'll tell you exactly how to do it.

PATTI: Right. We got to hope that our kids under 13 know how to do it and know they're being taught about it too. They're probably as vulnerable as anybody out there. They're probably not thinking about it as much as we're thinking about it.

Even more so, because of the information, you really want to protect your kids. There's some nutbags out there. God forbid they get access to your kids, their information, their Facebook, when are they traveling, when are they home, etc. You want to make sure that you're paying attention to this stuff and teaching your kids. What else is popular?

VINCE: It's actually funny how the things come in waves. They discover a flaw in security somewhere, and they'll send out a ton around that area. UBS was surprising. That went up in the fourth quarter of 3,000 percent as an email subject.

PATTI: UPS?

VINCE: UBS.

PATTI: UBS, the financial services company.

VINCE: The financial services company went up 3,000 percent in the number of tax. During that same time period, then ones from the previous year that were really high up on the list, Bank of America, Wells Fargo, both dropped off. People got onto it that, "Hey, it's one of those Wells Fargo scam things, emails going around." They caught onto it. They switched and they started going after UBS.

PATTI: You know, Vince, as matter of fact, I've got to tell you. About a month ago, my son Jack got a text message. The text message said, "Wells Fargo HTTP," which has made him think that's the URL Wells Fargo, "Your account has been locked. Click on this link to unlock your Wells Fargo account."

Fortunately, Jack is very much aware. He texted me. He said, "Mom, what's going on with my account at Wells Fargo?" He was wondering, he said, "Do I even have an account?" I said, "No, you don't even have an account. That is a phishing scheme, completely ignore it, and block it for future texting." Those are the kinds of things that you really want to be aware of.

You're going to get these. Vince, like you said – I love the metaphor – they're casting the line. They're saying, "How many people are going to nibble on it?"

You and I both know this. I'm shocked at the people, really smart people. We're all just so damn busy, "OK, let me just get this thing done. I'll just click here and fix my username and password."

We've had clients who are really high level, C-level executives, and they got scammed. We had another client who called us in a panic because their computer was frozen due to ransomware. They just didn't realize what they were doing. This was, unfortunately, people who are getting older, etc. Their cognitive problem solving often declines.

That's what we've learned from the prior podcast with the MIT work and the AgeLab. She was so panicked that she ran to the store and got the $8,000 worth of the debit cards and gave it to them to unlock her computer. When she told us about it, it was too late. They had already cashed that money.

Interestingly enough, with the ransomware, they will unlock the computer. They know if they don't unlock the computer, nobody will pay the money. They want the money more than anything else.

VINCE: They're also looking at especially these large publicly trading companies. What's the value of our stock if people find out this happened? How much is it going to cost us to put security in place to make sure it doesn't happen? Sometimes it's just cheaper for them to, "Here we go".

PATTI: Right. Exactly.

VINCE: Here's the 25 bitcoins that you wanted to unlock our data. Thanks.

PATTI: It's amazing. I know we spend a lot of money on security, on systems like 2FA, encrypted servers, and firewalls. For the listeners who are tuning in today, what should they be thinking about? It's one thing if you're an SEC firm. We're even over and above what the SEC requires. We're doing everything that Europe requires because we want to be ahead of the pack.

Folks, those of you who are listening, it's so hard to be...Let me put it this differently. Don't be too confident as it relates to this. A little, maybe a lot of paranoia is a very good thing, because it'll force you to be that much more vigilant.

VINCE: Well put.

PATTI: What exactly would you say should the listener be considering doing, etc., in terms of protecting themselves?

VINCE: The biggest thing whenever I read and research anything about cyber security make sure all

our systems are ahead of the curve, make sure our procedures are lined up, is to really make sure that you're following basic password security protocol.

Password1 with a capital P is not safe, nor is writing your really good password down on a Post it note. When they interview cyber security experts and they say, "What are the top reasons?" They interview 50 people. They come back and they say, "Here's the top things." 30 out of the 50 will say something password related.

PATTI: Let me play devil's advocate here and push back a little bit. What's the big deal with writing it on a Post it note? Who's going to steal that? Who's going to use that? Is it somebody that knows you? Tell me more about that.

VINCE: A lot of the stuff does come internally. We do background checks and all sorts of things on employees. If you're working for a call center, for example, and you have your password, there you go. You just have access to someone's internal systems and they're going to be the one that's blamed for it because it was their username or password that logged in to get client data.

It's not necessarily that it's the person you trust right next to you. In large companies, where it's written down in places, they hire outside people for cleaning, they hire outside people for IT support. All those sort of things that happen, that Post it is just sitting around.

Again, they're going to use that same username and password. They're going to bump it into a bunch of other systems and see what else they can get into.

PATTI: That's exactly right, and it's so hard to track it. It's so hard to catch these people. That's the hardest thing about all of this. How do you catch them? How do you know where the original source was? That's what the regulators and the law enforcement are really dealing with.

I remember that, frankly, I talked in a prior podcast, this happened to my mom. You know what? They went to the police. The police said, "You know what? Where you're down here, in Florida, they are literally, unfortunately, going after the elderly. You can stand in line with the other 300 people that have been in this week that also got raided."

It's a big issue, very difficult for law enforcement to go back to the original source. The most important thing is, you think about your health, prevention is key, Same thing with your money, prevention, make sure nobody can get access to it.

VINCE: Probably the second most important thing, after we talk about the password stuff, is to make sure any site that offers what is called two factor authentication is in place. If they offer it, take them up on it.

Two factor authentication is really simple. You put in your username and your password to get in. Then you get a text message to your phone or a phone call to your home or an email that has an additional security piece that you have to then enter in that site to actually access it.

The idea is that it's something you know and something you have. You know your username and password, and you have your phone. This way, if somebody does capture your username and password, they don't have your phone to get that other piece of the ID to get in.

Enable that whenever possible. Don't overthink it. The institutions that have put those things in, "Oh, it's so much harder for me." You can't underestimate the level that people will go through to get this information that are out there.

PATTI: Would it be safe to say, Vince, that if you get an email and it's basically telling you something, as legit as it might look, don't click on the link in the email. If there is a username or password, or something that you need to do, even if you see an advertisement.

I know I get advertisements all the time through email just because I was at the store, they got my email, and now I'm getting all these ads. Don't click on that link because it may not be going to Talbots, or whatever store that you were at recently.

Go out of your email and go in through the regular way that you would normally go through the website. That way, you know you're in the legit website. Also look at the extensions, right?

VINCE: Yes, absolutely.

PATTI: Let's tell people, how do you do that?

VINCE: When you get a link in an email, it's usually underlined or in blue. If you right click on that and you hit "properties," it'll be in that drop down that appears when you right click on it. In some emails, depending on what company you're using for your email, you could simply hover over it and it will give you the actual URL it's going to, the website it's going to. Look at those.

Again, as you said earlier and you were showing in that presentation you gave, they're really close. It's like Amazon spelled with two Os, Amazoon, or Google with three Os. They're so close that when you first look at them, you go, "Oh, that's it. That's legitimate."

PATTI: Right because you want to get it done and you want to get it taken care of. Again, I'm at the point where I'm not clicking on any links. I'm going out and going directly to the site, and that way I know I'm safe.

Again, as I said before, I don't know that we ever know that we're truly safe. You can also right click on the email address as well, right?

VINCE: That's correct. That's called spoofing, where you get an email. Let's just say I got an email from you that says, "Hey, Vince. Give me a call about a bank deposit and I go, "OK, hold on one second. What do you need, Patti? I email back and you say, "Can you just withdraw $10,000 and send it?" No, don't ever do that. Call the person.

They spoof the email address so it looks like it's coming from that person. As you just said, right clicking on that and going to properties will actually tell you the email address it's coming from. Some of the really good ones are very good at spoofing.

Even when you click on it, it says the email address. You have to actually dig deeper. Again, that's the ask your 13 year old or your resident nerd in the office, that'd be me, "Hey, who did this really come from?"

PATTI: You know what is really interesting about all this, Vince? I feel like we are going to go backward. Here we are in this digital age and I'm at the point where when you get an email like that, I'm going to say, "Pick up the phone. Call the company. Verify that they actually sent that," because that's really the only way you're going to really, really truly know.

VINCE: Yeah. When it comes to transacting money, when it comes to paying for things online and you're going off of an email without actually talking to somebody, that's not a bad thing to do.

PATTI: Right.

VINCE: Pick up the phone.

PATTI: Pick up the phone. Just make sure. I think it was really interesting, we were talking about this. If there was an industry that our kids should be thinking about going into...

VINCE: [whispers] Cyber security.

PATTI: Cyber security, guys. Think about it. This statistic is fascinating. Approximately six trillion dollars is expected to be spent globally on cyber security by the year 2021. Wow, that's an amazing amount of money and again, it's constant. It's like medicine. It's always changing. These guys are getting smarter and smarter and we just have to be that much more aware.

VINCE: It's stuff that we don't even understand yet. We just had one that we were talking about this morning about Huawei and the whole Android that Google is not going to allow them to use the operating system.

People are looking that going, "I don't even understand how they would use that as an attack form, let alone why they would stop them when it's all this money involved. There has to be something there, though."

That's an industry that is just growing and growing and growing. If you go to any site that handles cyber security or computer technology around security and go to their website, you will always find job postings.

PATTI: You know what's really interesting? Getting back to that cell phone thing, you think about it. I think the big risk is it's a Chinese owned company and the worry with the government is they have the technology if they have access to Google and they're able to access somebody's search history.

They're going to get a lot of information just from the manufactured phone and that's going directly to China. I guess our government doesn't want that.

VINCE: Again, even more so with the infrastructure of the 5G networks.

PATTI: Which is also an interesting thing. Is the infrastructure strong enough? Does it have the firewalls? Is it safe? Be wary before you go 100 percent into 5G. Make sure that the world is prepared for that.

VINCE: You're saying buy a flip phone?

PATTI: Oh yeah, yeah, yeah. I think I'm done with phones period. You know what? Let's talk to each other. How's that for a concept?

VINCE: I like that.

PATTI: Vince, you have been terrific. Let's think about the takeaways for our listeners today.

What I heard from you, what I hear from you every single day, is do not underestimate the enemy. These people are getting smarter and smarter and they're coming after us. Passwords, don't use passwords that are not random.

They can figure it out and they can get into multiple sites all at the same time. Don't write them down. Don't put them on a post it note. Last but not least, read your emails carefully. Right click on the email address. Hover over any kind of a link, or better yet, don't even go to the link.

Don't click on the link from the email. Go out of email and go to the website itself to figure out what might be going on. Plan B, pick up the phone.

Vince Kailis, thank you so much for joining me today. This was terrific, relevant, and important information to protect our listeners from attacks that are happening, literally, every 39 seconds.

Thanks to all of you for joining us today. I hope you found this interesting and helpful to you.

Please, if you want more information, like we said, I have a resident geek right here on staff. If you want to talk to Vince about your computers and maybe the different ways you can protect yourself, different software that can be used to protect your computer, give us a call. Go to the website, put in your information, and we can give you a call and give you some of these tips on a personal level.

In the meantime, I am Patti Brennan. Thank you so much for joining us today. We'll see you in the next episode. Take care now.