Barclay Damon Live Presents: The Cyber Sip Podcast™
Episode 22: "Four Best Tips to Improve Cyber Security, with Bill Prohn"

Speakers: **Kevin Szczepanski**, Barclay Damon,
Bill Prohn, Director of Information Technology for Dopkins and Company/Managing Director, Dopkins System Consultants

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Bill Prohn is an accountant by trade, but today he is the director of information technology for Dopkins and Company, one of Western New York's finest accounting firms. He is also the managing director of Dopkins System Consultants, an affiliate that focuses on all things technology. Bill Prohn joins us this morning on Cyber Sip. Welcome, Bill.

[Bill]: Morning, Kevin. Thank you for having me.

[Kevin]: I wanted to ask you about something that we spoke about during one of our recent conversations. Not only are you an accountant and the IT director and the managing director of Dopkin System Consultant, you are what…I can't remember if you call it that or I called it: "a cyber evangelist." What is a cyber evangelist and why is it so important to be one in this day and age?

[Bill]: Sure. So I got started in this business 35 years ago when the personal computer was in its infancy and our clients were asking, how do I use technology? So my initial response was to our clients' needs, and at the time I was evangelizing for "you should use a computer," don't use a pencil and paper.

[Kevin]: Right.

[Bill]: And as that… when Windows came out, how do I do that? Should I do this? When networking happened, when the Internet happened, all those things were to try and introduce this new concept in the world and what its efficiency was, what its capability was. And about a dozen years ago, that kind of shifted to security. Now, everything was computerized. Everything. I think we were successful, not just me, but the industry—in evangelizing and getting people to automate, as was, you know, was the term in the olden days. Now, how do I secure that? And I see it as a huge need because everything else fails if your security is not there, if your computer has ransomware or your data is breached, all bets are off. So it's really kind of the last thing we are talking about, or at least the most recent thing we're talking about. But it underpins everything that went before it. So all of your technology and all of your advancements and all of your efficiencies can be felled by one bad email.

[Kevin]: Right. I think that leads naturally into our main topic of today. So we are on the cusp of October. I don't know if you can believe it. I can't…it's flown by, but every October is Cybersecurity Awareness Month and this year the Cybersecurity Infrastructure Security Agency, or CISA, has gone back to the drawing board and come up with a very, I think, unique theme for the world of cyber. And it is "See Yourself in Cyber." And the idea, I think, is that cybersecurity can be, needs to be, is often made to be very complex, difficult for the average business owner or employee to understand. But it's ultimately about people. So if we keep it simple, we can create a culture of cybersecurity and maintain good,

strong cyber hygiene in our organizations. So with that, CISA has come up with four keys to seeing yourself in cyber, and I think they really do help us all to keep it simple. It's a good refresher for those of us who are sitting here in 2022 thinking, what do I do? So let's take our remaining time and run through that list; there are four items on the list, and the first one is enable MFA. What is MFA and what does it mean to enable it?

[Bill]: Sure. So MFA stands for multi-factor authentication. So there's three things there, or two things, right? Authentication is how does a system—a computer, an Internet website, an email account—know who is connecting? Okay, so your authentication is usually your username. You're going to authenticate. So now, how do you prove to that system who you are? Well, the most common thing is a password. People have a password. You're used to that. I log in, put in my email address. Put in my password. That password is your first factor of authentication and there you can actually have zero-factor authentication. I guess you could log into something and it doesn't ask you who you are. You just put in...you just go in. But then there's no way to know, is this you? Is this your bank account that you're accessing? Is this your email account that you're accessing? So the password is a way to prove that. So in multi-factor authentication, there's basically three different ways you can authenticate. The first is something that you know, right? So a password. So tell me, prove to me who you are because only you will know this secret, right? That's the concept. The second factor would be something that you have. A key, for example, to get into a lock would be something you have or a token. You're probably familiar with online banking, at least business banking—is not very common with personal banking yet. But for business banking, the bank gives you a little token, a little thing that every 30 seconds it spins a number. And you, when you log in, you put in your username, your password, and then it asks you for this little code. So that's something you have. If you lose that thing, you can't get in, right? So you have to have it in your possession. The third type of factor would be biometrics, something that you are. So in science fiction, it's a thumbprint, a retinal scan. In one of the episodes of Star Trek, which is now, what, 50 years ago, all of the officers had to authenticate to the computer and they spoke and the computer said, recognizing voice. So biometric authentication has been around for a long, long, long, long time. So the idea is the more things you have to present to prove who you are, the safer your data is. So you could have 30-factor authentication if you wanted. It's just really, really impractical. So two is better than one. Three is better than two. So multi-factor authentication is more than one.

[Kevin]: Right. So a password in combination with something that you have or that you are.

[Bill]: Correct. Or you could theoretically have a thumbprint and a key. Okay. Those are two-factor...password. I don't need password at all, but that only really works if you're physically present to, like a bank vault or something like that. Right.

[Kevin]: Right.

[Bill]: So in the cyber world, in the Internet, online password is the most common because it's the most easily transmissible.

[Kevin]: Right. And this may be a topic for another time, but I think we're moving in the direction of eliminating passwords. It's going to be biometrics or tokens or keys. So step one to keeping it simple is enabling multi-factor authentication. Step two is using not any old password, but using strong passwords. And this is a topic that comes up very often with our clients. What is a "strong password" and why is it so important?

[Bill]: So what is a strong password? I think there's two things that make a strong password. Number one, it's easy for you to remember. If you can't remember it, you've got to write it down. If you write it down, it's not strong anymore because anybody who comes across that piece of paper knows your password. So it's got to be easy for you to remember. And secondly, it's got to be hard for somebody else to

guess. So "password" is not a really good password because everyone guesses that first. Right. Your daughter's name and birth date. Not very good password because some...anybody who knows you even in passing or has been to your Facebook account can probably guess that. So what do you need to be a strong password? It's got to be easy to remember. So historically what we've had is things like capital Q number six, lowercase R, exclamation point. Okay, I've already forgotten what that was, and I'm not even through reciting it.

[Kevin]: So that's not a good one.

[Bill]: Not a good one. Although that is what almost everybody has today. It's got to be, quote, random. That means that means a computer that what that does, it makes it hard for somebody to guess because that's utterly random, but it makes it really hard for you to remember which is a problem. So the easiest thing is a long password that is easy for you to remember. "Now is the time for all good men to come to the aid of their country." Okay, that's really, really, really, really too long. But the concept is, take a phrase from your...a song or a poem or a book that you like, that you remember, that you always like. Maybe not one that you like so much that you've talked about a lot on Facebook.

[Kevin]: Right.

[Bill]: Pick something or look around the room and say, Door. Carpet. Telephone. Easy to remember. Door, carpet, telephone. And that's your password, right? And nobody's going to guess that in a million years.

[Kevin]: Right. And as well, Bill, without revealing secrets, if you have a password that you remember and you're comfortable doing this, you can then mix in capital letters, only you know which of those letters is going to be capitalized. Or maybe you use a symbol to substitute for a certain letter that can make...the combination of length large and small cap, large and small letters and symbols can make it almost, I would say, practically impossible to guess. Right?

[Bill]: Right. The thing to keep in mind is it's not a person typically at the other end, the hacker is not usually a person sitting there trying to guess what your password might be. It's a computer that is hammering away six or seven or 10 times a second, putting in password combinations, trying to access your account. So, capital P at sign dollar sign dollar sign w zero RG is no more safe than the word "password" because that's assumed to be another password. So the computer has millions of...try...of things that it knows are going to guess and sticks them in. And you know, within two seconds, it's tried 20 times.

[Kevin]: Right. So. All right. So already we have number one, multi-factor authentication. Number two, use of strong passwords. And if your organization does those two things alone, you're already significantly more secure than you were when you weren't doing so. But there are two more items in the list. Next one, tip number three on the chart of Keeping it Simple for Cybersecurity Awareness Month is recognize and report phishing. And that sounds like a great tip, but if you don't know what "phishing" means, you're not going to be able to do it. So tell us, Bill, what is phishing and how do you recognize it?

[Bill]: Okay. So phishing is typically an email, but it could be a voice mail. It could be a text message that is coming from somebody who isn't what it reports purports to be. Right. So, 20 years ago, you know, it's now a joke. "I'm a Nigerian prince and I've inherited $1,000,000. And if you send me $20,000, I'll make sure you get a million" sort of thing. And it was easily recognizable by the fact that it was written typically in broken English, and it just became so widespread that it was a joke. And people are saying, that's not real, right? That's not what we typically see today. What we typically see today is a text message that comes to you from your boss saying, I'm out of town, but I really want...when I get back, I want to recognize a half a dozen people in our company for their really good work. And I want to give them each a gift card. So go to Tops and buy a half a dozen $100 gift cards. Put it on your credit

card and I will pay you back when I get back to the office. Right. And so the first is, okay, I'm going to help out the boss and I'm going to do that. Well, it's not from the boss. So a "phish" is any attempt by somebody to trick you into doing something because you believe they're somebody else. Okay, well, the biggest concern about phishing is if I can trick you into telling me your password, because now I can do whatever. I don't need you anymore. I can do whatever I want.

[Kevin]: But nobody is going to give their password up voluntarily. How do you get tricked into giving up your password?

[Bill]: Oh, sure. An email that comes from the IT department that says your mailbox is full. If you don't log into your mailbox and delete some of the items, we're going to turn off access to your account. Click here to log in and delete items. Okay? So you click on it and it says enter your username, enter your password and then nothing. And then you go, uh oh, I bet you that wasn't real because it didn't log me into my email, etc. So how, how can you address that? Well, you should know...in your business, you should have a protocol for how IT interacts with people. Right? If here in our firm we don't have a quote IT department, we have three people. So if the email comes from me, well, it's more likely real than if it comes from IT. And our people know that. So they know that you can't trick me by pretending you're IT. So but typically what happens with a phish is there's a sense of urgency. In that message, it will say you need to do this right away. Right. Because I'm your boss and I want this right away or we're going to shut off your email account if you don't do this. So it gets you in a panic to want to...I got to do this and you stop thinking you start acting. And that's a big and that's a big problem. Right. So and in typically there's also some penalty involved, right? It'll say if you don't do this something bad will happen. So again, tries to get you to react and stop thinking.

[Kevin]: There's a sense of urgency. You're asked for sensitive information. You don't normally share with others, like a password, and there's some urgency to it. If you don't do this, I will be upset. You will lose your access. Anything that gets you to stop thinking and just react, right. So the tip we're—before we move to tip number four, I want to stay on tip number 3, because it's recognized and report phishing. A lot of us experience these things and we say, oh, I see that that's fake, delete it and move on. But that's not really helping the organization you're within. If you experience a phishing attack and you don't tell your director of IT, they can't do anything to share the word with other members of the organization. So talk about that a little bit. How should I report something like this if I experience it?

[Bill]: Sure. So it's a little, I guess, ostentatious on your part to think that somebody is trying to hack into you personally. Right.

[Kevin]: Right, right.

[Bill]: It's probably not even the case that they're hacking into your business in general. It's just a random attack. So what we see is, we'll see 100 emails come in all at once to 100 different people, all exactly the same. The only thing that's different is who it was addressed to. And they're all of the same phishing attack. And as you said, you know, half a dozen people might recognize, oh, I see that—I'm going to delete that. I'm not going to fall for it. But if you've got 500 employees, there's another 494 who maybe aren't as swift and picked up on that. So it gives the IT department an opportunity to warn others if it's a particularly malicious problem. And another example of a phish might be it has an attachment, UPS sending you a receipt for your recent purchase of $12,000. Right. I didn't do that and click on the thing. And what that really is, is ransomware, right? So there's a really immediate threat that if it's reported, the IT department could go and enter the email system and retrieve all those emails and get them out of people's mailboxes before they have a chance to read them.

[Kevin]: Right. So critically important not just to know what phishing is and recognize it when it happens,

but to report it to the director of IT or the information security professionals in your organization. All right. So we've got one more tip for keeping it simple for Cybersecurity Awareness Month, and that is, Bill, update your software. What is that? Why is it important?

[Bill]: So there's two things related to update your software. One is you should be on the most current version of whatever software you're running, whether that's Windows or your spreadsheet or your word processing or whatever that happens to be. We're an accounting firm and we've implemented, you know, hundreds and hundreds of accounting systems. And our clients take the approach, well accounting hasn't changed in 500 years. Nothing wrong with my 25-year-old accounting system...

[Kevin]: Right.

[Bill]: Well, except that in this day and age, people want their email or their invoice emailed to them. Well, email wasn't even thought of when your accounting system was created. So you've created some sort of workarounds and those workarounds potentially cause issues. So you should, whenever possible, get the newest version of a system, not just because of its features that you're looking for, but because security controls have been built in over time, as things have been discovered. The second and the much more common thing is patching the software that you have, right? So you got an application, let's say Microsoft Windows version 10 and you're running it on your computer. It is the current version. Well, 11 is now out, but 10 is still the current version. And... but Microsoft finds something wrong and they issue a fix or a patch that happens at least every month. So the second Tuesday in every month is Patch Tuesday and Microsoft releases. Here's all the things that need to be fixed. So some of them are critical, identified as critical. Some of them are so critical. And we've seen this this year that there's been an announcement from CISA or even from the White House to patch your email system immediately. There is a threat going around sort of thing. So the problem with patching is, first of all, it might take an hour every month for every computer to get updated. And people don't want to do that.

[Kevin]: Right, right, right.

[Bill]: The second Tuesday of every month, people go, I'm just not coming to work today because I'm going to have to sit and wait my computer updates so it's unpopular and people don't want to do it. The other issue is, in combination with my first point, if you're running an old accounting system and you patch your current windows, it might break your old accounting system because it's changing something that that system doesn't understand. So while you want to be current and you want to be patched, it's not as easy as just do it. You might have to test that, try it out, make sure you don't break something before you release that to the rest of your organization.

[Kevin]: Well, what's wrong with saying, hey, look, I know it's Patch Tuesday, but we've got a lot of work going on here. We've got a quarterly deadline for IRS filings. We're not going to be able to get to this patching right away. Let's do it next week.

[Bill]: So typically what happens is Microsoft, through whatever means, will find out that there's a bug or a vulnerability in their system, let's say, and they keep that a secret right up until—because if they announce, by the way, I've left the back door wide open...

[Kevin]: Right. The threat actor knows.

[Bill]: The threat actor knows. So it's a secret right up until the point where they release the patch. Okay. The back door has been open for the last month, but I'm locking it now, right? So at that moment, the clock really starts to tick because all the bad people who didn't know about this vulnerability now do, and will potentially start trying to break in. So you need to patch as soon as possible because they've made that notice public.

[Kevin]: If I leave my back door open overnight and I don't realize it, and no one else does either, I may survive. But if I go around the neighborhood and tell everyone, just so you know, I'm leaving my back door open for the next week, I'm going to be vulnerable. And that's the whole point about patching right away. All right. So the four tips for Keeping it Simple for Cybersecurity Awareness Month are: enable MFA, use strong passwords, recognize and report phishing, and finally, update your software. Before we close, Bill, I want to ask you this question. I think many may wonder, okay, Kevin, Bill, these are four tips. To some they may sound straightforward, to some they may be hearing them for the first time. If I do these four things, how much stronger and safer is my system really going to be? Is this going to make a difference in the security of my network?

[Bill]: Absolutely. If you're not doing these things and you start doing these things, your security goes up exponentially. And the main reason is that most attacks are utterly random. They're just drive-by attacks. And so if I can guess your password is "password" and break in, I can do whatever I want. If it takes me four tries to guess you're password, I'm going to move on. I'm going to go to somebody else who hasn't done these things and guessed that their password is "password."

[Kevin]: Yeah, I know it's hard to quantify, but I think you're 50% safer if you take these four simple steps and they're not difficult to do... it'sreally fairly easy to do it. Well, Bill Prohn, thank you so much for coming on the Cyber Sip podcast to talk about these four Tips for Keeping It Simple Cybersecurity Awareness Month. Have a great Cybersecurity Awareness Month. October is upon us and I hope you'll come back and we'll talk about some more of these topics in more detail later on.

[Bill]: Thanks, Kevin. I appreciate it. It's been a fun trip and it's easy to stay safe online.

[Kevin]: Yes. No, it is. So thanks again, Bill, and thanks to all of you. We'll be back with another episode.

[Kevin]: The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers: