BALENTINE

Cybersecurity & Wealth Management

In today's digital age, cybersecurity is no longer just an IT issue—it's a critical aspect of wealth management. At Balentine, protecting client data is a top priority – and it requires coordinated efforts between the firm, employees, and clients. Recently, CEO Adrian Cronje moderated a conversation with Chief Compliance Officer Mike Pearson and Director of Information Technology Dre Forbes to explore how the firm addresses evolving cyber threats. Read the transcript below.

Adrian Cronje, CEO: Good afternoon everybody, and thank you for joining us today on the session around cybersecurity and related fraud. Not everybody's favorite topic, but I can assure you as CEO that the management team at Balentine is laser-focused on this topic all day and night. As you gentlemen both know, joining us today is our Chief Compliance Officer, Michael Pearson, and our Director of Information Technology, Dre Forbes. Gentlemen, thank you both for your time today. I think we're all looking forward to hearing from you about how you stay abreast around this issue and to team up to keep the data at Balentine safe. Well, we are going to talk about, and the session is going to unfold as follows. I'm going to ask Dre to set the stage on this area around cybersecurity. He will then go on to talk about what we're doing from both a hardware and a software perspective about how we lock down our data.

Mike is then going to talk a little bit about the SEC, who regulates Balentine, and what the hot-button issues are for them as they look to us to discharge our fiduciary duty in this regard. And he'll talk a little bit more about policies and procedures around how we train our people. So much of today's takeaway is not just what is out there technology-wise, but how people interact with the data and how we interact with our clients. And we're going to end off the session offering a few suggestions for you all about what steps you can take to make sure that your own personal data at home is as safe and secure as it is at Balentine. There is only so much we can do at our firm to control this issue. A lot of it really lies in the hands of you. And we'll finally end off with what the future looks like. And spoiler alert, it's not as doom and gloom as it might seem, right? So Dre, why don't you start, I mean, you've been in several industries prior to joining Balentine. Part of your day job is to stay abreast of changes in hardware and software. Set the stage for us, first of all, and then talk a little bit about how we handle hardware and software issues to protect client data.

Dre Forbes, Director of Information Technology: Thank you, Adrian. So when I think about cybersecurity as a whole, the whole industry itself is crazy because it was founded because of cybersecurity criminals. It's driven by what cybersecurity criminals do. And we're at the mercy a lot of times of cybersecurity criminals because no matter how future-thinking and future-proof, we try to make it. If you build it, they will come. They'll try to knock it down. So we want to make sure that all the threats that have existed for ages now, such as phishing, such as ransomware, such as data breaches, that we're protected from that, from a standpoint now where things are at, but thinking about the future and how they're going to employ AI in different methods in order to try to get data from us. And these threats come from everywhere. They come from inside. They come from regular cybersecurity criminals, and sometimes they're the big leagues - people paid for by other nation's governments in order to corrupt Americans' institutional financials.

Cronje: Sounds like a multidimensional game of chess.

Forbes: Yeah.

Cronje: Sounds exhausting.

Forbes: It is. It can be.

Cronje: Well, let's talk around hardware, right? So many of us at Balentine are traveling, using laptops and using phones. Talk a little bit about the steps that we have taken around device management and interaction with data to protect it.

Forbes: So one of the popular terms in industry right now, MDM, which is mobile device management. And all that means is that all our devices we have them set up, so it's monitored as far as access to data.

So if somebody were to lose a phone with critical client or company data on it, we can lock that device down instantly, we can remote wipe it to make sure the devices are protected. Likewise, with laptops, we do the same thing. We also make sure that our folks are getting on the VPN. So from end-to-end, the data that's going through is encrypted.

Cronje: What is a VPN?

Forbes: A VPN is a virtual network essentially that encrypts the data as it's going from your computer and to our hub here and on time. So it makes sure that everyone stays protected while they're surfing the net.

Cronje: And what about the use of different wifis? It's probably not a good idea to be doing email at Starbucks.

Forbes: You know how easy it is for me to tell my phone to use the code name Starbucks as a wifi hotspot, and anyone then joins it and now all their data is flowing back and forth between my phone to go to the internet. And so if I'm a bad guy, I can take all that data and I'm good to go. Now, VPNs do help in that because they're going to encrypt that data as it's flowing through. But you still want to be careful because there are ways to get around that.

Cronje: What about from a software standpoint and access to the data? What steps do we take there?

Forbes: So this is one of the few areas in cybersecurity that AI is actually really helpful because not only is it monitoring and bringing all the data in one place and we can easily see it, but it also does things like look for behavioral patterns. So if someone's doing something that's out of the ordinary that, hey, you're accessing this system and you regularly don't access it or you wouldn't need to based on your access management, it'll give us a notification - say, "Hey, this person is accessing this file, doesn't need to especially click this link and shouldn't have." So those notifications save us a lot of time in hunting to find abnormalities. And we'd have had to sift through tons of pages of data to find.

Cronje: So monitoring the data, using AI predictably to detect threats.

Forbes: Yes.

Cronje: Michael, let's turn our attention to your seat as Chief Compliance Officer. So the SEC regulates Balentine as a fiduciary. Tell us about some of the hot-button issues that they are looking for to ensure that firms are chinning the bar in this regard.

Mike Pearson, Chief Compliance Officer: Sure. So as you mentioned, we take our fiduciary responsibility for not only investments but in financial planning and estate planning. But an extension of that and an important extension is what we're doing - some of the things that Dre mentioned. We've got a cybersecurity and fraud framework that we've put together, and we'll cover a little bit of those things that we put in place. The one thing I did want to ground us in is that the cyber-related fraud incidents

are growing at a tremendously rabid pace. And I think it's threefold. I think it's to what? To add on to what Dre mentioned, the fraudsters and the scamsters, it's their full-time job. This is what they do for a living. They're becoming more sophisticated. They're becoming more aggressive. And I think secondly, the reason for that is everyone is using personal devices, technology applications to run their daily lives in a normal way. However, there's a lot of personal and financial information that those scamsters are after. And then thirdly is the flip side to Adrian, to what Dre mentioned about AI is I have the perspective that AI can also be used in a more nefarious way, meaning that there's something called DeepFakes as an example. I don't know if some people are out there, but voiceovers, voiceovers of a client. One of the things that we do to protect our clients, particularly when it comes to third-party movements of funds when assets are being moved out for whether it's buying a separate property, moving assets, we ask the clients to verbally confirm after they sent us the request so that we can confirm A, it's them that we're speaking to. Secondly, that it is the information and confirming that that's exactly what they want to do. And that helps mitigate any risks of any fraudulent takeovers, such as sometimes what happens is these fraudsters take over their personal email address, and that's how most people communicate.

And incidentally, we actually stopped a fraud recently here where a well-known client sent in a request to make a payment and said, please contact me at this particular number as we've trained our employees that when you do call back from one of these verbal confirmations: (A) confirm who they are, get some demographics about, it's the person you're speaking to. And then she was trained that we're not supposed to call them back on a number that's not in our official record keeping system. So the fraudster said, call me at this other number, which happened to be their number. And she felt uncomfortable with it, did exactly as Dre and I teach, raise your hand, come to us if it feels uncomfortable. And we stopped it and the client was incredibly thankful.

Cronje: I'm sure they were. And even if that comes at the inconvenience and disruption of taking an extra step, it takes a village. And so it's not just what we're doing with hardware and software and policies and procedures, it's Balentine. It's how we interact with data. Dre, you've often told me that this issue is a people issue. Is there anything else that you think you want to expand upon what Mike said in terms of how we train our people to be situationally aware around these threats?

Forbes: Yeah, I think one of the statistics that always dumbfounds me but makes sense when I really think about it is that 95% cybersecurity incidents are caused by human error. Someone not paying attention, someone clicking on a link they shouldn't have. So we try our best in that. As you know with technology, you can control that with people, not so much. So we try our best to provide as much training as we can - ongoing quarterly, we have tech sessions where they have to get training, but in addition to that, we have constant phishing tests that are out there and make sure people are on their A game. If they fail one of these, they got to go do some stuff they don't want to do, which is take more training. So we just want to make sure that our people have the best training and representative disposal in order to combat cybersecurity.

Cronje: So this is not a one-and-done exercise. It's continual improvement. I guess one of our fundamentals, a Balentine way is to be a continuous lifelong learner. And issues around cybersecurity is no different.

It sounds to me like texting might be bad for my health.

Pearson: Yeah, well, it depends on what you're putting in there. But yeah, texting is something that people need to be very careful about how some of that stuff, Dre is not encrypted all the time. And again, like we mentioned, those fraudsters really have an ability to get into that stuff, which are pretty amazing.

Forbes: The government recently released a statement saying that our texts that weren't encrypted we're being intercepted by China. So we have to be very careful because if it's intercepted by China and you think that's the only person that can intercept it, then you're mistaken. So encryption and calls and just verification is the best way to make sure you stay protected.

Cronje: Michael, some of our clients still like to text.

Forbes: Yes.

Cronje: What do you have to say on this subject?

Pearson: Well, I would encourage them that they find and change their behavior on sending a more secure method, which is actually sent through emails. And maybe I'm aging myself, but pick up the phone sometimes.

Cronje: What's the telephone?

Pearson: Picking up the phone sometimes is one of the best ways to get a clear message across and being careful about what you're sharing. One of the things I mentioned too is sharing information in a secure way. There's ways that Dre and I have created to share information with us that is in a secure portal. So when you're thinking about sharing information like your tax information or your estate planning documents, documents that have personally identifiable information that can be taken advantage of - using those secure methods so that they're maintained and encrypted.

Cronje: Well, that's been very helpful. And Mike, what I took away from the example that you gave of how our policies and procedures have helped us intercept a potential breach is the realization that it really does take a village. It's not just what we do at Balentine to secure data. It's not just what we do at Balentine to train our people. It is how we interact with our clients and our clients' potential vulnerabilities that we can't control.

So I'd like to ask each of you to give some practical examples of what our clients can do to secure their own situation so that they don't unintentionally become compromised and jeopardize the system. Dre, starting with you.

Forbes: Yeah. So we've talked about passwords before, and we have our own password manager here, but I think clients should take advantage of that because you don't want to use the same password in every different platform.

Cronje: Are you saying Adrian 1, 2, 3 doesn't cut it anymore?

Forbes: Not anymore. Unfortunately. Back in the 1980s, it may have been fine, but nowadays, it's the first thing they'll try.

Cronje: It's such a pain to change the password – remember so many passwords. How does a password manager look?

Forbes: Well, it's simple. You simply go to the website and most password managers will automatically offer you to create a password and save it for you so you never have to think about it again. Apple even has one built into their devices now where it will do passkey and I'll talk about that a little later. But also the normal passwords for you, it'll set it up, it'll store it. And so if you're in any of your devices, you're anywhere you're at, you can pull it up, look at it if you need to copy and paste it and get into the site. In

addition to that, we also have to put other layers in there. And I like to use the word layers because just like with a cake, the more layers the better.

Cronje: Yeah.

Forbes: So with passwords, I look at that making your password complex, using as a password manager as additive. When you add another layer there, some other device you have to go to, some other metric they have to abide by. Now you're doing multiplicative and your protection is now to the umpteenth. And lastly, wifis, we talked about it earlier, but just want to reiterate that just because you see something that says Starbucks at Starbucks doesn't mean it's actually Starbucks.

Cronje: Right?

Forbes: You want to also verify that you're using the correct wifi from where you're at. You can ask the front and they'll tell you. And if you add another layer to that, as we say, we love layers, it's VPN, you can pay for your own VPN - four bucks a month - and add another layer of protection for yourself no matter what network you're on.

Cronje: So what does VPN stand for?

Forbes: Virtual private network. Essentially, it just allows you to communicate with your home hub and make sure an end-to-end security. So any of the data that's flowing through is encrypted, can't just be taken down and used for whatever malicious people have.

Cronje: So I'm hearing password management, multifactor authentication, use wifis carefully and consider the use of a VPN.

Forbes: There you go.

Cronje: Michael, what about from your perspective? What are some of the things that our clients can do to secure their own situation?

Pearson: Yeah, I think two things that come to mind. One is frequent monitoring of your financial applications. They're easily readily available. It's easy to catch things that are unusual or things that might be fraud. By monitoring those patterns, you can then raise your hand and say that this is an fraudulent activity and that it's something that you can resolve pretty quickly. So I think doing that and getting it closer to the time of the act will help potentially regain some of the lost assets as well.

Cronje: You talked to me about Cybersecurity insurance the other day.

Pearson: Yes.

Cronje: What do you mean by that?

Pearson: Yeah, so as business owners, and I know many of our clients are business owners, I think it's incredibly important risk management to have a cybersecurity policy. And what that does is that not only protects you from certain cybersecurity incidents like a ransomware or a data breach, whether it's internally or externally, that could provide additional compensation for that. And I think actually more importantly, many of them offer services to help you work through that issue to notify clients how to go about maybe identifying opportunities in your current system. Do you be able to stop those things from happening again?

Forbes: I know ours gives us a break as far as cost goes if we are following the proper procedures. Training, making sure all our employees are trained and using the right tools. And the more we have in place as far as stop gates, the better discount we get.

Cronje: So purchasing that insurance, not just a risk management measure, it will help business owners put the right policies and procedures in place.

Pearson: Yeah, exactly.

Cronje: So we've talked a lot about where we've come from, what we are doing today. I want to ask you to opine on what the future looks like, each of you, both in terms of technology and also in terms of regulation on this issue of cybersecurity and related fraud. So Dre, look two, three years ahead, what does the future hold in store for this? Because you told us that the outset, this is not going away. It's a multidimensional game of chess that we play all day and night.

Forbes: So piggybacking off of chess, I love that because if we think about it, you have cyber criminals employing AI in order to attack, and we're on the defense, and now we're using AI in order to play defense. So you're going to essentially have a game of Terminator where we're going back and forth between two different AIs fighting each other for supremacy, and then what we are going to do is hope that the investment that we put in the technology to protect our clients is going to be the winner and we're going to do our best to make sure all that information stays in there. But the good thing is, at the outset of this, it looked very grim, but just like they make deepfake videos, now they're making software to detect deepfakes. So for every ying there's a yang.

And so we're with, cause like I said, the industry of cybersecurity is led by and driven by cybersecurity criminals. So whatever they do, we're reacting to and we're making measures in order to protect them and safeguard our clients and ourselves against. In addition to that, they got cool things for passwords. Now where we're leaning more on things like biometrics. For instance, I talked about Passkey earlier, which is pretty awesome because what it does is instead of having to enter your password when you go to a site, it'll ping you on your personal device and say, Hey, you're trying to log into Google, Adrian, let me see your face ID so I can confirm it is actually Adrian. And then once it confronts it, you sends a signal to Google server which then lets you in, so you don't have to remember a password. And it authenticates using biometrics, which is infinitely harder to hack than a simple password or text code you might get.

So those things, as we move forward soon we'll have a chip in our eye that lets us get in anywhere we need to go. And it seems scary, but let me ask you this. If you never have to enter a password again in your life, you may be like, okay, I'm going to get a chip my eye. But the future is bright because we're employing technology to protect us as bunch of cyber criminals are trying. I think as long as we stay on the right path and we keep our clients and ourselves' best security steps in mind will be fine.

Cronje: Well, I'm looking forward to the chip that opens the front door here at Balentine, so I don't have to use all my multifactor authentication and passwords.

Forbes: There you go.

Cronje: Let's hope that the good side wins out. Michael, what about from a regulatory standpoint? What does the future hold?

Pearson: Yeah, I think the most important thing is what we've talked about is our risk management framework, which doesn't just include cybersecurity or compliance related matters, but staying abreast of all the different things that are happening in the industry. So one of the things that we do, we've

engaged a third party expert that helps us analyze, identify, notify us of threats that they're seeing out there in the industry. We can learn from that, do an internal assessment as to whether we have some vulnerabilities, and then we also engage them to do an assessment of our framework of all the different educational things that Dre's talked about, the measures we've put in place, are there any gaps? Are they seeing anything in the industry - because they are experts. That's what they do for a living and sharing that knowledge with us so that we can have the mindset of continuous improvement to make sure that we're going where the puck is instead of waiting around to see where the puck goes.

Cronje: I think that's all very well said, gentlemen. Thank you so much for your time and for your expertise and for working so hard at this critically important facet of what we do at Balentine. And we hope that you took several things away from our session today. Firstly, all the steps we take at our firm to discharge our fiduciary duty, to make sure that the data that we have on you is safe and secure. That's not just around device management. It's not just around software architecture, it's around policies and procedures and what our regulator is demanding from firms like Balentine. I hope you take comfort that we acknowledge that this is vastly, in fact, you said 95% of the time, a people problem. And so we are continually training our people to stay abreast of emerging threats. And finally, we hope you took some practical steps away from today's sessions that you can implement in a low-lift way in your life to secure your data on your end.

Because one of the messages Dre and Michael and I wanted to get across is it really does take a village. And so we will unashamedly apologize if it's inconvenient to receive a phone call so that we can positively identify you when moving money. And we will positively apologize if our relationship managers are asking you to download your information at a secure link that will expire. Those are some of the examples of the extra steps that we can take together in order to risk manage cybersecurity and related fraud. Dre and Michael will be available at any time if you would like to touch on any of these subjects, especially if you want to apply it to your individual business. And if you'd like to have a conversation with them, please reach out to your relationship manager and I know that they will make that happen as quickly as possible. In the meantime, thank you very much for the trust that you place in our team. We hope you found this session to be useful.