NAVIGATING THE NOISE PODCAST EPISODE 8: THE FUTURE OF DIGITAL SECURITY AND BUSINESS

JANUARY 2019

Brian David: Hello, everyone, and welcome to Navigating the Noise. A podcast series brought you to by CHPA, the Corporate Housing Providers Association with support from ASAP, the Association of Serviced Apartment Providers. I'm Brian David Johnson, your futurist and host for the podcast, and I'm joined by ...

Mary Ann: And I'm Mary Ann Passi, the CEO of CHPA.

Brian David: Welcome, everyone, to episode eight of Navigating the Noise, where we're going to look at the future of digital security and business, what you need to know. Now, in true spirit of Navigating the Noise, there's a lot of noise around digital security, cybersecurity. There's a lot of hype. There's a lot of fear-mongering. There's a lot that's going on, and some of it is fear-mongering. Some of it's hype. Some of it is noise, but also, some of it is a reality. Some of it is actually really important, and that's what we're going to focus on today is kind of what you need to know. Again, we're going to follow what we always try to do here on Navigating the Noise is cut through the noise and give you some clarity.

Mary Ann: So, BDJ, along with that, the number one threat that CEOs fear are cyber attacks, so members have always focused on ensuring that the data that they're storing is secure. Now with the advent of GDPR and other regulations, they also need to switch the focus to what data they're even collecting from people that are staying in their units. Most members are navigating this new world of data security by choosing to put data processing and storage in the hands of experts and providing more internal training around awareness, and they're seeing this as a natural extension of their duty of care to their guests and clients.

Brian David: Yeah, so certainly a big, big subject that we're really going to dive into. As we do with all of our episodes, we'll examine this subject from multiple angles, getting different perspectives and ideas about the subject, and we'll also look at how to apply it specifically to the future of corporate housing and longer-term rentals. The podcast is broken up into three segments. First comes the road ahead, where we explore futures research, looking outside the industry to get that bigger picture. To do that, we bring in a guest who is an expert in this area, who works in this area, and people who might be doing some research in this area.

Mary Ann: Then we go to what matters, where James Foice and I ... James with the Association of Serviced Apartment Providers, ASAP. We've gone out to find corporate housing in serviced apartment providers and partners, so global thought leaders in our industry, to bring you the realities of what's important to you and your companies. These are people like you who are taking this information, using it, and putting it into action.

Brian David: Finally, we'll discuss, in section three, pragmatic steps you can take today to prepare for the future in a segment we call Three Things to Do. With that, let's get started.

Brian David: This is section one of the podcast that we call The Road Ahead. As we explore the future of digital security and business, Mary Ann and I are going to look at the road ahead and understand, what do you need to know about this area? Now, these days, there's a lot of noise around digital security and cybersecurity, and a lot of it's really dark. A lot of it really disempowers people, so that's why we really wanted to take this one episode and really focus on, what do you need to know and what do you need to know for your business?

Brian David: Now, this future of digital security and cybersecurity is something that I know a good deal about. One of the things that I do aside from just being a futurist is at Arizona State University I'm the director of something called a threat casting lab. This is where we go and work with government, and military, and private industry, and trade associations to look out into the future 10 years and discover new threats. New threats to economic security, to national security, and then turn around and look backwards and say, "What do we need to do to disrupt, mitigate, and recover from those threats?"

Brian David: We wanted to pull that into this episode and with the spirit of Navigating the Noise. To look at this very large sometimes daunting world, but really give you that idea of, what do you really need to know? Ultimately, what are the three things you need to do to be prepared for tomorrow? To get us started and to really start to push in and understand it more Mary Ann and I have invited a guest onto the show.

Brian David: We want to welcome to the show, Dr. Natalie Vanatta. She is a cyber officer in the US Army focused on defending the nation in the cyber domain. Lieutenant Colonel Vanatta also holds an appointment as an academy professor in the Army Cyber Institute, which is the Army's think tank on all things cyber. Natalie, welcome to the show.

Dr Vanatta: Thank you. I'm super excited to be here today.

Brian David: On this episode, Natalie, Mary Ann and I are talking about the future of digital security and business, and what our listeners really need to know. We want to dive into kind of the reality and certainly, with your background not only in academia but also in the US Army, you certainly have a sort of rich history in this area. As people and businesses start to think about cybersecurity and digital security today, when you talk to people about it, what should they be worried about? How should they think about this type of security?

Dr Vanatta: Well, they should think about it as every other kind of security. It's there and it has to be everywhere. It has to encompass every piece of your life. Every decision you make, every risk calculus you calculate, cybersecurity and securing that digital domain has got to be part of the conversation each and every day.

Brian David: For you, what you're saying is that when you think about digital security it's really not about digital security. It's just about security, so just like you lock your

door or just like you make sure your windows are locked or you don't walk out onto your front stoop and scream your Social Security number out, that people should really think about that digital isn't something that's over there. It's actually something that really today is a part of everything we do.

Dr Vanatta: Absolutely. It's not just your physical footprint you have to worry about but also your digital footprint, and that every action you do is somehow putting out the ones and zeros, the waveforms out in the world, and has an impact across the cyber and digital domain as much as in the physical domain.

Brian David: So, do you think that most people don't think about it this way? I'm interested, Mary Ann, to see what you think when it comes to industry members as well. Is this something that people are still thinking of is that digital security and cybersecurity is something that's kind of ... It's a high-tech thing that's just kind of over there. Do you think people are thinking about it as ... Kind of as Natalie said, that we need to think about it in every action that we take. Do we think about it on par as locking your door?

Mary Ann: Mm-hmm (affirmative). Mm-hmm (affirmative). Well, I think members for a long time have focused on securely storing the data that they have, but now they've got to look at and they're required to look at the data that they're taking in. I think that it's becoming more prevalent in their business planning, but we've talked a little bit about not if member companies are hacked, but when member companies are hacked, and so putting a plan in place. Natalie, do you have some recommendations on how businesses can address that? How they start even thinking about it if this is not on their radar?

Dr Vanatta: Absolutely. It comes to a change in behavior is really what everybody can do, whether in their organization for work or in their family. There's three really small changes in behavior that people could start doing today if this big problem of cybersecurity seems to be too much, too techy, too geeky. Three little things that they can do today.

Dr Vanatta: The first one is they just need to patch their computers. Computers, I mean tablets, and iPhones, and anything with electrons. You just need to install those security updates because that is going to help defend your footprint and your physical space. It's something to change, right? We learned we brush our teeth twice a day because that helps defend the body and our health. We need to just get in the habit of accepting and installing those patches.

Dr Vanatta: The second really easy change to behavior you have to make is just question when applications and web pages ask for your information. As Brian alluded to earlier, if you randomly get stopped in the street and someone asks you, "What's your favorite color? Where did you meet your spouse?" and, "What was the first car you drove?" You're probably just not going to tell them that. You're just not going to lead with that. If people would just actively think before blinding clicking to allow systems and applications access to all their data, or why does that app even need your GPS coordinates or the ability to see all the

photos you've ever taken on your phone? Think through that before you make a decision.

Dr Vanatta: The third really small behavior change you can make are those passwords. Passwords are scary. They're complex. They're difficult. They're 18 characters. They're uppercase. They're lowercase. They're not the last five you used. It seems overwhelming, but I would say the one small thing you could do is just don't use the same password for everything. Think about the levels of security you're using that password for and maybe it makes sense that the same password you use for your online banking is not the password you want to use for your social media because think about if one of those passwords get compromised, what else can the adversary or criminal get? Just those three little changes to behavior could set the world on fire for us being able to better defend in this domain whether at home or at work.

Brian David: Yeah, I think it's those simple things. I think, Natalie, you make a great point. You wouldn't have the same key for everything, right?

Mary Ann: Right. Right.

Brian David: You wouldn't have the same key because if you lost that key somebody then may have access to everything.

Mary Ann: To everything. Mm-hmm (affirmative).

Brian David: Or, as you said, it's just like brushing your teeth. I love what you said about when somebody walked up to you in the street and started asking you these questions.

Mary Ann: What's your mother's maiden name?

Brian David: You would be suspect-

Mary Ann: That's right. Exactly.

Brian David: ... and say, "I don't think that's a good idea." To try to translate that into the digital domain. I certainly have seen when I do work with people as a futurist that people do think that the digital world is something that's over there and that the physical world is here. I think, Natalie, you make a great point that, especially now in the 21st century, it's all together. Everything is all together.

Brian David: I want to move on now to tomorrow, as I know, Natalie, you do work with the Army Cyber Institute. You actually look out into the future and looking at the future of possible threats not only to the United States Army and the United States, in general, but also, thinking about business, thinking about economies, thinking about things like that. As you look out into the future when it comes to this cybersecurity and business, where do you see things going? How should

people be thinking about prepping for the future? Aside from those three simple things you just gave us, what are some other areas that they should be keeping an eye on?

Dr Vanatta: Great question. If I could truly answer that well, well, I'd be walking down the corner and buying a Mega Millions ticket, right? Because I would understand the future exactly. I'd say the future of cybersecurity is really not scary. I spend so much time watching the media and folks writing and trying to scare everyone like, "Oh, no. The world is ending." It's not. The future of cybersecurity is full of opportunities and really challenges because it parallels where technology is evolving. That new, interesting gadget, or gizmo, or system that we're going to want to bring into our work environment or bring into our home and make it part of our lives, cybersecurity has a hand in that because we're going to have to figure out how to protect and defend that.

Dr Vanatta: Really, to understand this future of cyber it's hand-in-hand with how technology and society is going to evolve. The challenge is going to be standing up with those scientists and researchers and figuring out, "Hey, this is a really great idea. This is cutting edge. This is what the world needs," but let's not forget about, how do we secure it? How do we secure that system or that gadget? How do we secure how it's connected to the larger world and how do we secure that data that it's going to either produce or consume?

Brian David: Yeah, that's one of the things that the work that I do on the engineering side, that's one of the things that we see that's quite prevalent as you look out at these devices. Devices that people might bring into their homes or devices that people might bring into their businesses that generally people aren't thinking about security first. People are thinking about efficiencies..

Mary Ann: Like smart speakers?

Brian David: Smart speakers. Ease of use and all these different ... Smart thermometers.

Mary Ann: Right.

Brian David: They're thinking about, "How can I just make it work?" Because it's new. Very rarely do they think about security first.

Mary Ann: Right. Right.

Brian David: But I think Natalie makes a great point. We need to take a step back and say, "Well, wait a minute. You're bringing something into a living space." You would also, let's think about security and the security of those people and the security of the data that's moving back and forth in the care of those people who are in that space. I think it's a really great point that as we think about the future and also when it comes to business, as you bring these devices into your business both physically and even from a digital standpoint, are you taking a moment and

thinking about, "What's the security? Why do people need to know a certain thing? Why does this need to be connected? What happens if this is hacked?" Having a plan for that, I think is really, really an excellent point.

Brian David: Natalie, when you're thinking about these future areas, are there anything that when it comes to how businesses could collaborate ... You had mentioned before that people need to kind of stand up with those engineers, with those researchers, with those businesses. Is there a role that maybe businesses could play? I mean, certainly, we all know that there's a role that the United States Army can play and that the government can play, but is there a role that you see that private industry could really take some steps to make us more secure?

Dr Vanatta: Oh, absolutely. Right? As we look at what's the next gen, the next cool thing that we want to build or that business needs, obviously, you have a vote. You can vote not to pay for it, right? The supply and demand curve by saying, "Well, you did not consider security in this aspect. You didn't build in this and you can't show to me how secure this is or how you're going to protect my data or how you're going to ensure that if something happened to this device that not everything else that's connected to it in my business is now going to suffer from it."

Dr Vanatta: In the end product, absolutely. You can vote by not supporting it. But I would say having an honest conversation with cybersecurity researchers to understand what your business platform, what your business needs would be very helpful. I find even in the Army, as we try to talk to commanders that are used to infantry formations or armor formations, so they have a bunch of tanks, understanding how they operate, how they do business, what their expectations are make it much easier to help figure out how we protect and defend from a cybersecurity perspective.

Dr Vanatta: If that conversation is not happening between the cybersecurity research community with academics and your business sector, then that's why the products and the ideas that are designed are not going to have security baked in. Not because we wouldn't want to, but we just don't understand who to talk to and how to even start this conversation.

Brian David: Yeah, so private industry has a role to play, number one, with the dollar, right?

Mary Ann: Mm-hmm (affirmative).

Brian David: Number one with what you buy. As you say, vote with your wallet and to say, "No, we want this to be secure and we're not going to bring it in unless it is, but it's a great point. Number two, to say, "Well, no, you have a role to play as private industry to stand up and say, 'We want this. This is how our business works. This is what we need to get done.'" We still need to have ROI. We still need to make business. It's a business, for heaven sakes, but at the same time, more and more security gets put at the forefront.

Mary Ann: Mm-hmm (affirmative), and then both educating and collaborating around that. Those points of security, what needs to be secure, because there's a lot of personal identifiable information in the industry, in our industry that gets transferred as part of any move in or relocation and housing experience.

Brian David: Yeah, that's a great point, Mary Ann. I think one of the things, to Natalie's point, a lot of them may not know. A security researcher, a cyber researcher may not know, "Oh, we need to protect this," or, "Here's why we need to protect this and not this." I mean, again, in the spirit of Navigating the Noise, there is so much noise and so much fear-mongering, and so much ... This is so big that you can't do anything about it, which disempowers everybody and it's awful. What we're trying to do is say, "Well, no, you could stand up and say, 'Well, no, as a part of my business, here are the things that I need to protect. Here are the things that this is my duty of care when it comes to data. This is what we need to protect.'" To then go back to not only industry but also cyber researchers and say, "This is what we want," and if you do this it's good for business. It's not only-

Mary Ann: Absolutely.

Brian David: Security is good for business.

Mary Ann: Right.

Brian David: Yeah. Well, Natalie, fascinating, fascinating perspective. I really appreciate you taking the time to come on the show and share with us not only what we should be considering today. Everybody remember those three simple steps from Natalie that you can take today just to make yourself more secure, but also, kind of pushing the industry. As somebody who is deeply, deeply embedded in this world of cybersecurity and, certainly, national security of saying, "I think private industry has a role to play to step up to understand that security's important," but then also to reach out to other sectors and say, "Here is how we can make things more secure and make everybody more secure."

Mary Ann: Right.

Brian David: Natalie, we really appreciate you coming on the show. Thank you so much.

Brian David: Welcome, everyone to the What Matters section of the podcast, where we take the broad futures that Mary Ann and I have just explored and figure out what matters to CHPA and ASAP members, as well as the corporate and long-term housing rental industry. Today, on the podcast, we're looking at the future of digital security and business, and more specifically, what you need to know. Mary Ann, who's our first guest today?

Mary Ann: Well, with us is Bob Siegel. As the President and Founder of Privacy Ref, he started Privacy Ref in 2012. Bob took his experience as a senior manager of

worldwide privacy and compliance at Staples, Inc and applied that to assisting companies implement and maintain strong privacy programs. Bob has worked with many different organizations dealing with programs of all sizes and regulatory needs. Bob's also led a webinar for CHPA member companies about GDPR recently that's available for viewing. Thanks for joining us today, Bob.

Bob Siegel: Glad to be here. Thanks for the opportunity.

Brian David: Bob, as I said, we're talking about the future of digital security and business, so as you look into the future of digital and cybersecurity, what does that future look like? How do you see things?

Bob Siegel: I actually see things becoming a little bit more dangerous, a little bit more risky. As new technologies get rolled out we're finding that there's less and less time being spent on security. It's one of the last things that get added on. It seems to be that there's a real push for time to market, get these new technologies out, this new software out, new hardware out, and that leaves these new technologies vulnerable to hackers and others who would want to steal your personal information, for example.

Bob Siegel: It means that businesses have to be more vigilant about what they're doing to protect that information and be very selective in the type of technologies that they do implement. I always advise my clients that they should be looking at new technologies, but they shouldn't necessarily be the first to grab something that's innovative because of that risk.

Brian David: That's a great point that you bring up, Bob, and this echoes really what our expert had said at the top of the show. Dr. Vanatta had said that, yeah, you are beginning to see that the level of security and often times security is not even a second or third concern. What she was advocating for is just like you said, that people need to really think of physical security and really also understand that digital security is kind of a similar thing. Right? We all lock our doors. We need to start thinking, especially when it comes to business, about that in a different way.

Brian David: Let me ask you, why do you think in business that people really separate those worlds? It seems like today, in the 21st century, you would really understand that people's data and your digital footprint is really as meaningful as your physical footprint and your sort of physical being. Are you seeing people that there's still a gap with some folks?

Bob Siegel: Absolutely. I think it's understandable. As things innovated, let's go way back to the early and mid-20th century, change wasn't happening that quickly. People had time to bring in a new technology. Let's say a car from a horse-drawn carriage. They had time to adopt to it, figure out what needed to change, how they could use it, where the risks were, where the dangers were in operating a car. Now, by the time I get my Amazon Echo installed there's Echo Plus and Echo

Spot and so on and so on, so I don't have the chance to understand what the risks are and what the best practices are for using that technology. Instead, it starts to proliferate.

Bob Siegel: I go to a hotel room now, for example, or rental unit, and I walk in and there is an Amazon Echo device sitting there. Now, if I'm not familiar with that device I don't know what risks are. I don't know how to use it. I don't know if somebody can hack in and use the camera on the Echo Spot to see what I'm doing in that rental unit. We just don't have the time that we used to have to adopt and understand these new technologies before we start using them.

Mary Ann: Well, Bob, how would you recommend that people could educate themselves on what the risks are and how not to open themselves up to risk?

Bob Siegel: Well, with all these new technologies you can't assume and no one can assume that they know everything. There's a lot of experts out there. There's a lot of articles that purport to be experts out there. You need to find a trusted advisor. Someone who could help you navigate what those risks are before you go and implement them. Implement those devices, I should say. Reading the articles on the internet, for example, I never would suggest is a good source unless you have a reliable author, reliable journalist you're using because a lot of those articles are there to help support and sell those technologies and they ignore what the risks are. You need to find someone who can help you through, how you can navigate through it.

Bob Siegel: The other is, don't necessarily rely on those key vendors that you're outsourcing your work towards either because, again, they're selling product. They're trying to get you to work with them and to offload some of your work to them, which is good to you from one perspective, but from the other perspective, you don't know what steps they're taking to protect your information.

Bob Siegel: The recent introduction of the General Data Protection Regulation in Europe has a great model for when you're bringing vendors onboard and what types of things you should require them to do and what types of things you should limit them from doing. I'd advocate putting some sort data processing agreement in place along those lines. The things that are changing with the new California law that's been put in place from a privacy perspective, as those things get sorted out that's going to help improve privacy here in the US as well.

Bob Siegel: From a business standpoint, buyer beware. Get someone you can trust to help look at these different alternatives and different technologies to identify the risks and understand how they apply to your own business.

Brian David: You make a great point there, Bob. One of the things that we'll make sure to do on the website is make sure that we get some links to those different areas that you've mentioned because I do agree there. A lot of people are putting in a lot of time and they're very important, and they also can have a big impact on your

business depending upon where you're doing that business as well. You also make a great point that making sure that when it comes to digital security and cybersecurity that you have the appropriate level of a solution.

Brian David: Let's not use an M1 tank to get rid of your ant problem, right? We have to make sure that it's not out-sized, as you're right, but then on the flip side is don't be kind of overwhelmed by the noise. Don't be overwhelmed by and disempowered by people telling you, "Oh, you can't understand this. You can't understand this." That really ultimately you can because you can understand business, and just as you can understand your physical security there's steps that you can take when it comes to your cybersecurity.

Brian David: But I'm going to call you out, Bob, and push you a little bit further if you could. I want you to be our trusted advisor. Today on Navigating the Noise, you are our trusted advisor. Pick any area you want. Again, I leave it up to you. What should businesses and what should business people do today as they start to prepare for that tomorrow? What are the possible threats? What are some areas that you're ... right now that are really kind of topical for you as you're thinking about, as your advising and you're thinking about where things could go for the future? What's top of mind for you?

Bob Siegel: What I find myself doing fairly frequently is that our clients are developing or having developed for them innovative technologies to differentiate them from their competition. One of the things that I always stress for them to do is to think about how that personal information they're collecting with those new applications, with those new technologies about how someone might want to misuse them. What are all the risks that they can identify beforehand? Who is going to be the perpetrator of that risk? Is it someone internal? Is it someone external? Then what they can do to put controls in place to avoid those risks, to mitigate those risks.

Bob Siegel: The point of it is it then brings privacy, which is really where I focus on, to the forefront of developing an application and establishing a business practice. It allows you to then work with the security team to put their controls in place that will effectively prevent misuse of the data. Privacy and security have to work hand-in-hand. I always joke, I grew up in New York City, I'm a paranoid New Yorker. That's a good thing to be in privacy and security because you think about all the things that could possibly go wrong and try to find a way to avoid them. Hope that helps.

Brian David: That's certainly putting ... I don't know about being a paranoid New Yorker, but I think the idea of putting ... Yeah, thinking of security and taking that moment to take a step back and, like you said, ask that question about security, about privacy, about data, or maybe even the duty of care when it comes to people's data. I think that's something, especially for this industry, you could start to think about, "Well, you could duty of care for a person, sort of being in a property, but what does that mean for their data?" I think there might be some very nice kind of parallel models to at least give people a place to start.

Bob Siegel: Yeah, I would first recommend that people don't think about owning the personal information they collect. Businesses should think of themselves as stewards of the information they collect and that the individual who they got the information from is the actual owner. They're just a caretaker and need to provide the due diligence to make sure that information isn't lost, isn't leaked to anyone else.

Mary Ann: Bob, I was just going to say, your recommendation to find a trusted expert, that's what most member companies are doing. As they're trying to navigate the new world of data security, they're choosing to put data processing and storage in the hands of experts and also providing more internal training to their employees and their staff to be good stewards of the data, as you just mentioned.

Bob Siegel: Yeah, and that's a challenge in itself. If you think about the individuals you have as members of your organization, they're going to range in certainly age and generation, but also in cultural background. Protecting information privacy is very cultural and it's very age specific. For example, I have a niece who's in her 20s who posts stuff on Facebook, which my sister used to write in her diary and my mother won't even talk about. It makes Thanksgiving dinners really interesting. You've got to get all those people from those different generations, different cultures abdicating or deprecating what they think of from a privacy perspective and adopting your organizational morals from protecting information. That's a tough, tough row to hoe.

Brian David: Definitely. Well, Bob Siegel, we want to thank you for coming on the podcast today. We really appreciate it. I think you're perspectives and advice are going to be really, really helpful for the listeners, but first and foremost, we want to thank you for coming on the podcast and joining us today.

Bob Siegel: Thanks again. Really enjoyed it.

Mary Ann: Thank you, Bob.

Brian David: Mary Ann, as we're looking out to the future of digital security and business, who's the next guest you found for us?

Mary Ann: We have Aaron Turner. Aaron is Chief Technology Officer of BridgeStreet Global Hospitality. Prior to coming to BridgeStreet, he was COO and CTO of Branch Out, a provider of digital commerce solutions to Fortune 100 companies. While there, he was accountable for delivering $100 million in revenue through their commerce operations, and before that, he led marketing operations and technology for the enterprise marketing division of eBay. Welcome, Aaron.

Aaron Turner: Thank you. Thanks for having me.

Brian David: Yeah, welcome to the show. As I mentioned, Aaron, on this episode we are looking at the future of digital security, cybersecurity in business and also what people really need to know. Right? Because there's a lot of noise around this subject, and that's one of the things we try to do here on Navigating the Noise is get people to be able to navigate that and figure out, what do they need to be concerned of?

Brian David: The first question that Mary Ann and I wanted to ask you is, what are you doing today around digital security and cybersecurity? What are the things that you're focusing on?

Aaron Turner: At BridgeStreet we have a pretty robust cybersecurity and data security program. It's broken down into five parts where we focus on business processes, our product and services and the information that they collect. The flow of information is the third part. We have a whole section dedicated on outsource services, and then last is access to information. That's our five-part strategy to data security and cybersecurity.

Brian David: How did you get to that? I think for a lot of companies and for a lot of organizations out there, most people look at digital security and cybersecurity as something that's sort of very separate or almost too big to understand. How did you get to those five areas? What was that process like?

Aaron Turner: Yeah. We took a look from the ground up. We looked at all of the data that we were collecting, including TII data, including PCI data. All of the data needed to fulfill a guest reservation within our space and we took a look at all the business processes that are needed to generate that reservation and all of the guest interaction. Then we looked at the products and services that need put all that data together that actually collected the data, and then how that information is sent to either third parties or even within different systems within the BridgeStreet ecosystem. Then we looked finally at the people who had access to that information all along the guest journey, but it really started with how we collect the guest information and the confidential information and made sure we had a good understanding of the people, processes, and technology associated with that.

Brian David: Yeah, and that's really helpful because I think following that data, following the kind of flow and that information flow, I think, can be really helpful for folks. Because just in running your business you need to have an understanding of that, but being able to put the security and privacy lens on top of that, I think could be a really helpful first step for people just to kind of analyze how they're doing business today so that they can make sure they're securing themselves for tomorrow.

Mary Ann: I have a question for you, Aaron, that's along the same lines, but a little bit down the road. Member companies are talking about continually needing to invest to stay ahead of the curve. Investing in software, and firewalls, and encryption. Do you have any recommendations on how they do so? Because

they're hearing investing in this is really expensive, so do you have any recommendations on how they can kind of stay ahead of what they need to be protecting?

Aaron Turner: I do. I mean, there are a lot of companies out there in the cybersecurity space that you can outsource a lot of your security to. Things like directory monitoring, log monitoring, software packages, web application monitors, spam filtering. I mean, if you take a look at the regulations and requirements, whether it be SOC 2 Type 2, whether it's PCI, they kind of lay out all of the requirements and there are service providers out there that really focus in on meeting expectations when it comes to regulations out in the marketplace.

Brian David: So really finding that outsource or finding that trusted partner, that person that you can kind of trust and making sure that ... We've had some other conversations in this episode about making sure that the solution fits the problem. That you kind of understand what the problem might be first, like you said, understanding and analyzing your business processes around data. Yeah, and then finding somebody who can give you the right solution to that.

Brian David: I wanted to take another step kind of even down a little bit deeper. It's a conversation that we've had on the podcast and we've been talking about around the notion of duty of care. How do you see the protection of client data as an extension of duty of care? Do you see that connection?

Aaron Turner: Oh, absolutely. I mean, when you look at duty of care, a lot of people just focus on the quality of the buildings, the quality of the accommodations or emergency management services, things like that. We focus on multiple parts of the duty of care. Certainly, protecting customer data, guest data, client data is part of duty of care. If that data is shared outside the appropriate people then that creates a lot of risk for an individual guest in their personal life. It creates a lot of distraction and legal implications with the employer of that guest, if it happens to be a corporate traveler, and it creates a lot of anxiety for business travelers just in general, so it's absolutely part of our duty of care program at BridgeStreet.

Brian David: Yeah, and our conversations that Mary Ann and I have been having and also in our conversations with guests that has kept coming up. I think it could be for, certainly people in this industry, a good framework. I think a lot of people understand duty of care, as you say, in the physical world, but how ... Just take that same approach, that same way of thinking and maybe just copy/paste. Put in digital. Right? Just say, "Okay. Well, what does that look like?" I think it can be a helpful framework for people just when they're trying to get their heads around what they should do. I think it's a good approach.

Brian David: The final question we have for you is about the future. You've obviously done a lot of work in this area throughout your career. As you said, you've kind of got a comprehensive approach and a pretty sophisticated approach to what you're doing today. I've got to ask you, Aaron, so what's your plan for the future? What

do you think you'll be doing? What do you think the industry should be doing? What are the things that people should be thinking about as they're thinking about what to do in the future?

Aaron Turner: Well, as technology becomes more available to folks, to the broader ecosystem and it gets more complex from a technology standpoint and a business process standpoint, we need to really ... Everyone needs to understand all of the business processes, all of the flows, and we need to make sure that all of the touch points, the touch data that needs to be secure, we need to make sure that they're locked down and protected. I think we owe it to our guests. I think we owe it to our clients. Things like making sure that data's being transmitted over secure channels, like TLS 1.2, making sure data's encrypted at rest, making sure that if someone's logging into a system to make a booking or looking at reservations, making sure there's multiple authentication methods, so it's just not a username and password. These are all things that are table stakes today in some industries that this industry really needs to focus on and adopt.

Aaron Turner: As far as the future goes, it's really evolving as the people trying to exploit this information evolve, we need to evolve at a faster pace. Whether that's building deeper knowledge with our internal teammates or if that's outsourcing best in class providers to provide that information where there may be gaps, all of that's going to be required to kind of stay ahead of the bad guys.

Brian David: Well, and that's, I think, a very sober and very pointed, I think, piece of advice there, Aaron. I think people do need to understand, well, certainly, that this is important. That you need to view your physical and your digital security in very similar ways, but the fact that this is not a one and done thing. This is something that it is new, it is emergent. It is something that you're not going to fix by doing it once a year. That you kind of create this culture of security, this culture of way of thinking about security and approaching it.

Mary Ann: Awareness of it.

Brian David: Yeah.

Mary Ann: Awareness of all of it. Mm-hmm (affirmative).

Brian David: Yeah, and being able to really make that a part of the organization. That you don't have to spend all your time on it, but if you make it a part of that awareness I think it's a ... I think it might be a little bit of a bitter pill to swallow because you can't just fix it. You can't just swipe or pay somebody and be all done. This is now a reality. Just like physical security has been a reality in this industry for a long time, digital security is here to stay and it needs to become a part of that awareness and of that culture.

Brian David: Aaron, I want to thank you for coming on the podcast today. Your insights and your points, I think, are really, really important and really added to our broader conversation of where we were going. Thank you so much for joining us.

Aaron Turner: Thanks for the invite. I appreciate it.

Mary Ann: Thanks, Aaron.

Brian David: Okay, everybody, we've come to section three of the podcast. Three Things to Do. This is where Mary Ann and I look through the episode and really kind of think about, what are three things you could do, three pragmatic things you could do today to begin to prepare for tomorrow? On this show, this one was a bit of a tough one. It could be a bit of a scary one, I think, for some folks. We were looking at the future of digital security in business, but more specifically, what you need to know. What do you need to know as a business so that it isn't completely overwhelming?

Brian David: As we dive right in, Mary Ann, I think number one of the three things to do, and I think you won't disagree with me at all on this one, it comes from Natalie, Lieutenant Colonel Vanatta, that the one thing that you can do is do the three simple things. I think she did a great job with that one saying you've got to patch your computer, you've got to question why people are asking for access to your data and what they're going to do with your data, and by all means, don't use the same password everywhere. If you can do those three simple things ... Certainly, if you can do them as a person, if you can do them as a family, you will certainly be more secure and you can start to apply them to your business as well. Make sure you're taking those three simple steps. I think that really will actually just take you so much further and get you prepared.

Mary Ann: Agreed.

Brian David: Okay, so that's number one. Do the three things. Second is prioritize. The second thing you can do is prioritize security. What mean by that is as you're going through and thinking about security, make sure it's top of mind. As we talked about on the show, this is not a one and done. This is not something you can just take care of. Just like physical security is always a concern, that digital security is always going to be a concern as well. When it comes to digital security, make sure you're prioritizing it.

Mary Ann: I really like the point that one of our guest speakers made that you're stewards of the data, not owners of this personal data so go ahead and have a plan in place. It's a when and not an if that you're going to have a breach. Have a plan in place. Your response is quick and decisive. Share that plan with both internally within your teams and also externally to your customer and clients so they are confident in your role in the duty of care process for their employees.

Brian David: You know, Mary Ann, I think one of the ideas that came out that I really liked and we've talked about this before and it's come up is duty of care. That as you're prioritizing you may ask, "Okay. How do we prioritize and what do we do?" All right, well, there's a simple way. Most everybody in this industry understands the concept of duty of care in the physical world, so just apply that to the digital world. Prioritize that and think about what those implications ... I think if you just start there then you're going to be worlds ahead.

Brian David: A third thing that you can do is collaborate. Again, this came up multiple times in the podcast.

Mary Ann: It did.

Brian David: We're always for a big a collaboration, so collaborate. This problem, the problem of digital and cybersecurity is so big and so new, but it's surmountable when you can collaborate. That could be with a trusted advisor. It could be with other people in the industry. It could be with researchers or universities, giving them an understanding of your business because you understand your business and what you need to do, what requirements you might need for security as well. Collaboration can really help you.

Mary Ann: I want to touch on the hiring expertise part of that collaborative opportunity. Finding a trusted expert to help your company navigate it I think is critically important, and I think it was Bob that said be vigilant and selective not only in the new technology that you're choosing and implementing within your company but also in the partners that you choose to collaborate with.

Brian David: Yeah, understanding those partners. I think that's so important. Understanding what they're doing because often times your partners or the people who are involved in your network if they're a weak link they make you a weak link because you're kind of depending on them. Understanding that, especially when you collaborate, that's a good caution. Those are your three things to do.

Brian David: Number one, do the three simple things. Just do them. Just do them and you'll be more secure. Do the three simple things. Prioritize. Prioritize security and collaborate. Collaborate with others. I think that hopefully, as you look at this episode and you think about the future of digital security in business, what you need to know, I think if you do those three things today you're going to be a lot better off.

Brian David: Mary Ann, why don't you take us to the exit?

Mary Ann: Okay. Well, thank you, everyone, for listening to Navigating the Noise podcast brought to you by CHPA and ASAP. Reach out to us, please, and let us know what else you'd like to hear, what else you'd like to ask BDJ or just to help me personally stump the futurist by emailing me at map@chpaonline.org. You can

also follow us on Twitter, @CHPAonline or visit our website, www.chpaonline.org.

Brian David: Thanks, everybody, for joining us here on Navigating the Noise brought to you by CHPA and ASAP. We'll talk to you again soon.