Keith Mattox: Okay, I'm Keith Mattox and I'm speaking with Dave Newell. Dave is the founder of Loptr, LLC. Did I pronounce that correctly Dave?

Dave Newell: Loptr.

KEITH MATTOX: Loptr. A security services company. It's located in western New York. Prior to that, Dave was the Practice Director at CTG Security Solutions. And before that, he was the Principal Consultant and owner of Crave Technologies. Dave, could you take a few minutes please to introduce yourself and talk a bit about your company and your experience in the healthcare security space?

DAVE NEWELL: Sure Keith, and thank you. My name, as you said, is Dave Newell and I am the founder of Loptr LLC, which is a security consulting firm in western New York. And I started the company in 2013, so we've been around for a few years. And we focus primarily on small to mid-size businesses, helping those organizations to create working security programs. And from my standpoint and background, as you mentioned, I had been the director of the security consulting group, that computer task group. And I worked there for about eight-and-a-half years, and I'd been a consultant prior to that. And from a security perspective and an IT perspective, I've got decades of experience. I've been working with HIPAA really since about the time that the HIPAA Security Rule went into effect. I think my first HIPAA project was in 2006. In addition to HIPAA, I've also worked in credit card security, working with the PCI Data Security Standard, and with a variety of other security control frameworks like the NIST Standards and the ISO 27001 certification standard.

KEITH MATTOX: Great. And there is so much going on with security, Dave. What do you check regularly to keep up-to-date with security threats and other information on the security front?

DAVE NEWELL: I'll start by talking about what I do personally. And what actually I do is every morning I spend about half an hour reading through security news. And so what I've done is, along with the rest of my consulting team, we put together a reading list of sources of information, security news. So those come into our tablets and computers every morning and I spend about a half an hour every day reading what's going on in information security. And even then, it's really hard to keep up because there's so much going on in terms of information security. And so one of the things that we look at is... This is actually something that we've shared with our clients. So we share this list of reading sources and we encourage organizations to be able to put together a set of sources that they pay attention to that help. One of the things that we look at too is, one of the tricks is to understand what you need to read. Now, because I deal with a lot of different organizations, I have a lot of different newsfeeds that I pay attention to, but one of the things that's important is to pay attention to... If you're a Windows shop, pay attention to Windows patches. I pay attention to news sources from the government and from a bunch of different security companies as well.

KEITH MATTOX: Great. Yeah, I think that's good advice. So one of those things you've probably read a lot about is ransomware, which clearly it's probably the biggest threat this year and especially with healthcare organizations. They seem to be particularly vulnerable. What can hospitals and clinics, particularly small practices in our membership, do to mitigate this threat, and what are the most important steps to take to guard against this?

DAVE NEWELL: Yeah, that's a good question. And the answer is really when it comes to ransomware that it's a very challenging threat, and it can be very hard for organizations to defend against it. And the reason is that, unlike some of the security threats that we worry about, ransomware can come through a number of different paths. And so one of the things that can happen is, hackers... I tend to just call them bad guys because it's an easy way to understand that these aren't good guys. So bad guys, when they're attacking your organization, can try to break into computer systems and install ransomware or you can be infected by ransomware just by visiting a website that has already been compromised. Or you can get ransomware in a way that I think most of us think about it arriving, which is it arrives in an email. And so in any of those cases, it can come in and hit your organization. But I guess that the point that I want to make about that is, because ransomware can come from a lot of different paths, it's really hard for folks to defend against.

So when we look at how we defend against ransomware, one of the things that happens is, you have to defend... You have to be able to secure the end point. And so when I talk about the end point, I'm talking about the computers or laptops that are where ransomware initially attacks. And so in this case, there are a set of things that we need to do in terms of making sure that our operating systems are patched and up-to-date, removing software that we don't need and patching some of the riskiest software that's out there like Flash and browsers and Adobe products and Java. All of those, while they can be secure, they're also very widely used and they are targeted by bad guys. So one of the things you need to do is to make sure that those are up-to-date. You need to be able to run some kind of anti-virus or anti-malware software. And then the other thing that you need to do is focus on training and make sure that people are on the front lines, that is these people that are receiving emails, understand what to do or what not to do to avoid ransomware. So one of the key focuses for organizations has to be making sure that people understand how ransomware can get into your organization and what you can do to stop it which really comes down to not doing things. Don't click on things. Don't open attachments.

KEITH MATTOX: Yeah, right. I think there's a lot of awareness now about that and it sounds like there's just a lot of the fundamentals that are really necessary to deal with ransomware need to be put into place. Now, you also have been doing a lot of work with hospitals over the years and have done a number of risk assessments for healthcare providers. What are the most important things that smaller practices can do to help keep them safe?

DAVE NEWELL: Well, a few years ago, I was at a conference that NIST and the Office of Civil Rights, which is the division of Health and Human Services that is responsible for HIPAA Security Rule enforcement. So anyway, the HHS, OCR and NIST put together... And NIST I'm sorry is, the National Institute of Standards and Technology. So every year, they put together a symposium where they talk about the state of HIPAA and security and healthcare. And I was at this conference and a person from OCR said that, one of the things that they look at when they're doing a HIPAA audit, one of the things that they look at is your risk analysis. And what they said was that there are no organizations that they have found that have done a good risk analysis that do not use encryption. So the point here is that, you can't be doing a good job of securing healthcare data if you're not using encryption on your desktops and laptops.

And so I think, this is kind of a key takeaway. And it's one of the things that I've used in terms of risk analysis just to kind of help to gain an understanding of whether folks are doing enough. I'll look to see whether they are doing encryption. Because it's such a basic building block of security. There are a handful of other things that are just things that you must be doing along with encryption. There is running something for antivirus or anti-malware and keeping your operating systems up-to-date. So we will look at whether all of the systems on your network are running AV and whether all of the systems that are on your network are receiving patches, they're receiving updates to the operating systems.

We also look at Flash and Adobe products and Java, as I mentioned earlier, because those are one of the places that we see attacks the most. So that's kinds of it. There's a set of what I guess we would call table stakes for security programs. So organizations need to have policies and procedures in place. They need to have done some kind of risk analysis. They need to do training and awareness as well. And so if we go into an organization and don't find those things in place, that can be a red flag in terms of HIPAA compliance. And then, I think, a last area that I'll mention is logging. And so one of the things that you need to do for HIPAA, and you need to do this for a lot of regulatory requirements is review your logs and monitor for security incidents. And so when you look at a smaller organization, one of the key things for you to understand is you need to be able to capture information about what's going on in your organization.

KEITH MATTOX: Right. And sort of contrary to that, are there things that you see being done in hospitals or other organizations that you think are misguided or are not a good use of resources for security?

DAVE NEWELL: Yeah. So one of the broad things that we see is that folks tend to confuse information, security and compliance, or risk management and compliance. So there tends to be a confusion that things that we do to determine that we comply with the HIPAA security rule are the same as being secure. And so one of the difficulties here is that there's a lot of things that you need to do to manage risk and not all of them are listed in the HIPAA security rule. So a mistake that we see organizations make is that they focus on just hitting a checklist of, do I have this document? Do I have this document? Do I have this document? Do I have this piece of software? Do I have that piece of hardware? And the thing that happens here is folks focus on having things versus doing things. And so there's a quote that I often refer to from a guy who's been a security expert in the field for a long time, Bruce Schneier, and he said, "Security is a process, not a product." And so this big mistake that we see is that folks tend to think about security and say, "Oh, security is having a firewall or having antivirus software." Where security is really about using those tools, monitoring your environment and making sure that everything that you have is actually working.

KEITH MATTOX: Right. So HIPAA just turned 20 this year. In your view, are healthcare organizations and practices doing what's necessary to protect patient privacy and securing patient healthcare information?

DAVE NEWELL: Well, there's so many organizations out there that it's hard to speak too broadly about it. I think that there are a lot of organizations though that are not doing enough. And part of what we see with HIPAA is that, HIPAA turned 20, but the security rule took 10 years to put in place. So it really wasn't until 2005 that the HIPAA Security Rule was official.

KEITH MATTOX: Effective. Yeah.

DAVE NEWELL: Right. And then if you look back into the late 2000s, a lot of folks like myself would say "HIPAA doesn't really have any teeth." And of course, we're talking about HIPAA Security. They have a Security Rule that didn't have any teeth. There was no enforcement mechanism related to the requirements of the Security Rule. And so it really hasn't been until 2013 and later that that has started to change. And so now what we're seeing is an increased auditing activity and fines and settlements that have been years in the making that are really starting to come out. So we're starting to see increased enforcement and I think that that has caused people to pay attention to security. But when I look at whether organizations are doing enough to protect privacy and secure patient information, which is really kind of this hard to question, I'd say as organizations, I think what we need to do to focus less on compliance and more on managing risk, so that what we're doing is making sure that our security practices are in place. So rather than worrying too much about whether we comply with the HIPAA Security Rule, we need to be going and saying, "Are we doing what we need to do in terms of putting security in place throughout the organization and then monitoring security?"

DAVE NEWELL: And then when it comes to protecting data, actually one of the key things that we need to think about as an organization is, how can we keep data from proliferating throughout our organization? How can we keep it in secure places and to reduce the number of locations where sensitive data like PHI is located, so that we can actually keep it safe?

KEITH MATTOX: Yeah. Also, as you know, there's been a big push by regulators for a nationwide and interoperable health information exchange for health records. What do you think are the biggest challenges in making that reality and still keeping patient information secure and private?

DAVE NEWELL: I think that there are some challenges that are beyond the scope of security when it comes to HIEs and it just has to do with the way that HIEs are handled at the state level and how different health exchanges are from state to state. We actually work with one in New York and have seen some great things done with HIEs. But one of the things that we see, and again this isn't so much a security thing, but consent is a big deal when you're dealing with HIEs. So to be able to share information between different health exchanges, you have to actually... You have to be able to get your patients to agree to share the information. I think that is a big challenge that probably leads us into the discussion of privacy and security because patients need to have confidence in the security of their data before they're willing to consent to any organization sharing it.

DAVE NEWELL: But one of the things that you will see there is that kind of moves towards a place where one of two things that's gonna happen. Either we're gonna be moving data into large data stores where we've combined the data together and it becomes a very attractive target, or we're going to be keeping this data out in different locations and making connections from one place to another, so that as organizations are sharing health records, they are able to make a connection from one place to another to bring together a virtual health record. And in either case, there are security challenges. In one case, it's how do we protect a lot of data that's combined together? And the other one is; how do we ensure that we have security as we allow organizations from one place to another or individuals from one place to another to connect? When you think about it from the individual's perspective, we're even talking about how do we make sure that things are secure as we allow patients to participate in healthcare and gain access to their own healthcare.

KEITH MATTOX: So, clearly as well, organizations are moving away from data centers to Cloud service providers like Azure, AWS and Google, however there's still a lot of responsibility resting with the customers to ensure that they're configuring their systems properly as they integrate into the Cloud. What is your approach, your company's approach to keeping customers secure and providing a consistent level of security? And do you in fact have customers that are moving or looking into moving into the Cloud away from the data centers?

DAVE NEWELL: Yeah. Let me tackle that in two ways. First of all, I'll talk about what we do as an organization and as I mentioned, we started our company in 2013, so we've only been around for a few years. And what was exciting about that opportunity for us as we started a new company was that we realized that we could do most of the work that we would need to do as a service provider within the Cloud. So if you were to visit our office, you would find that we have a firewall that protects our office and we do not have any servers at all. All of our servers are in the Cloud. And what we recognized was that there was an opportunity for us to do that. Of course, we're also a security company, so security was really important to us.

And what happened was there was a shift in paradigm for us; we had to go from building a set of servers altogether and securing them and putting security around them, to understanding the different Cloud providers that we use, understanding how they do security, and making sure that those controls were in place. We also had to understand that they don't take care of all security. We actually have a responsibility whenever we're using a Cloud service to make sure that we secure the configurative services as well. So it's not like when I go to AWS or Google or Azure, as I'm putting my own data into the Cloud, I have to make sure I retain responsibility for my half of the deal when I'm going out and securing the organization.

But having done that, when we look at our clients, we definitely think that there is an opportunity for our organizations to be using the Cloud and actually to gain security benefits from doing so. And we think that, especially for small and medium-sized healthcare organizations, there is a great deal of value in moving services into the Cloud. You have to be careful when you select your vendor. You have to understand how your IT staff and the folks who support your organization will interact in the Cloud instead. But what we find is that Cloud service providers can do a great job of securing data once you understand what your role is and what their role is and you make sure that you take care of the compliance aspects like business associate agreements, the Cloud can actually be a great resource.

KEITH MATTOX: Right. So what have you found to be the most effective way to articulate the business value of security and privacy to management?

DAVE NEWELL: Well, one of the things that we did recently is we put together what we call "a 60-second assessment" and our idea was to go in and say, "If you didn't have a lot of time or a lot of time and money and you needed to go in and get a quick understanding of the security of your organization, how would you do that?" And there's one question in that 60-second assessment that is my favorite question. So I say, "If I only had time to ask one question, what would it be?" And I think that when we look at understanding the business value of security to management, we can kind of think about this one question. And so the one question is this. And usually what I'm doing is, I'm actually talking to executives in an organization or the senior management in healthcare organization.

And so I say, "Go back and ask your IT people, ask whoever it is that manages your firewall and your network. Ask them this one question." And the one question is, how many connections did we have from Russia yesterday? How many connections over the network did we have from Russia the day before today? And so the point of asking this question is to help you to understand whether you can know. Because for most of us in healthcare in the United States, we do not really need network connections from Russia. We just don't have that many patients who are in Russia and connecting into our network. And so if you looked at that and said, "Well, you know what? I don't actually provide healthcare to anybody in Russia. There shouldn't be any Russian connections."

And so you look at it and say, "It's pretty clear that the goal should be nobody from Russia is connecting to my network," but what you'll find in a lot of cases is that you actually can't get a good answer. So what I really look at is to say, "Go in and ask people." Because if you go in and say, "Hey, are people connecting to our network from Russia?" And the answer is, "I don't know." Then you know you've got an immediate problem. You do not know if bad guys are connecting into your network from Russia. Even if you get a response that goes like this, "Well, I can find out for you." And it takes you a day or a week to find out who connected to your network from Russia, you still have a problem because you need to know right now who is attacking your network, who might already be in your network.

So the key thing that I look at is ask organizations to think about that question. Do we know if people from Russia... And I might be unfairly picking on the Russians. But there might be other hackers out there from other countries. But if you don't know what foreign countries are connecting into your network, then you know you've got a problem. Ask yourself that and if the answer is, "We do not know who's connecting to our network," then it's pretty clear that you're not getting enough value out of your information security.

KEITH MATTOX: That's great. Okay, well, thank you very much, Dave, and we appreciate your time and look forward to talking with you again.

DAVE NEWELL: Thanks, Keith. It's a pleasure talking to you.