OPEN NINTH:

CONVERSATIONS BEYOND THE COURTROOM

CYBERSECURITY - SAFETY IN THE DIGITAL AGE

EPISODE 93

FEBRUARY 10, 2020

HOSTED BY: DONALD A. MYERS, JR.

(Music)

NARRATOR: Welcome to another episode of "Open Ninth: Conversations Beyond the Courtroom" in the Ninth Judicial Circuit Court of Florida.

And now here's your host, Chief Judge Don Myers.

CHIEF JUDGE MYERS: Hello, and welcome to Open Ninth. Joining me today is a leading expert on cybersecurity, Mark Lanterman. Mark is the Chief Technology Officer of Computer Forensic Services. But before entering the private sector, he was a member of the United States Secret Service Electronic Crimes Task Force. Mark has 28 years of security and forensic experience, has testified in over 2,000 cases, and has provided training in digital evidence, computer forensics and cybersecurity to the United States Supreme Court.

It's great to have you with us, Mark. Thanks for joining me.

MARK LANTERMAN: Thank you, Your Honor. Great to be here, so thank you.

CHIEF JUDGE MYERS: So I gave to our listeners just a brief thumbnail sketch of your background, but your background is really much bigger than that. And I really thoroughly enjoyed reading and hearing about some of it. So can you just give us some highlights of the places that you serve as a faculty member, the other roles that you serve?

And as I told you before we got started here today, I heard you speaking at the NACM Conference, the National Association for Court Management. Tell us a little bit about some of that background.

MARK LANTERMAN: Yeah, sure. And, you know, I think that education is probably the most important thing that I could do -- that I can give back to the legal community. I'm faculty at the University of St. Thomas law school in Minneapolis, the Mitchell Hamline School

of Law in St. Paul, Minnesota, where I'm based. And I'm also faculty at the National Judicial College as well as the Federal Judicial Center in Washington, D.C.

CHIEF JUDGE MYERS: Those are incredible -- for our listeners, incredible institutions that make so many phenomenal contributions to what we do in the law. So thank you for your service in that way and for the educational focus that you've brought to us.

Tell us a little bit about how it is that you got this connection with the courts.

MARK LANTERMAN: Yeah, that's a good question. I conduct approximately 60 continuing legal education seminars a year, and I think just through word of mouth, you know, from teaching attorneys and law students, word kind of got around. And now I primarily teach judges. So --

CHIEF JUDGE MYERS: Do you have a background in the law; law school education, or --

MARK LANTERMAN: No. No. But I do teach at two law schools. No. I'm a technician by training and education.

CHIEF JUDGE MYERS: All right. And let's start with this overarching topic of cybersecurity. Kind of give us an overview of what that means.

MARK LANTERMAN: You know, cybersecurity is such a broad topic. And I guess my general philosophy is whenever we gain a benefit, whenever we gain a convenience from technology, we always give up a little bit of security, no matter what that is. Whether that's automated products, self-driving cars, insulin pumps, pacemakers, you know, there is always a risk with technology. So I think cybersecurity touches our lives in more ways than I think we can appreciate.

CHIEF JUDGE MYERS: Well, I hope we're going to touch on some of those ways that it impacts us or touches our lives as we go through today.

You're familiar with the court systems, obviously, and there's been a lot in the media as it relates to the court systems and other governmental agencies and cybersecurity issues. We unfortunately hear a lot about ransomware attacks and other things that are impacting the court systems.

But what is the -- what's an organization's greatest cybersecurity risk? What is -- at the foundational level, where are we most vulnerable?

MARK LANTERMAN: Our people. We are the weakest link, not to coin an old TV show. But the fact is, organizations, whether that's a corporation or the courts or a law firm -- we're spending a lot of money on products and technology to prevent and to protect ourselves from these cyber threats.

But the fact is, one untrained employee can result in a devastating cyber event, and all of that money, all of that investment means nothing. All it takes is one employee to click on a link that he or she should not have clicked on and your entire investment in cybersecurity is out the window. So I think that we are the weakest link.

CHIEF JUDGE MYERS: And you talk about individuals and clicking on links. That connects in my mind to this idea of phishing, is that right?

MARK LANTERMAN: Absolutely. You know, hackers need our help. So hackers try to trick us into clicking on links that then will download malware, or we're opening up attachments that then launch other types of attacks. So almost every single cyber event that our firm has investigated over the past 18 months has all been tied back to email, all tied back to phishing attacks.

CHIEF JUDGE MYERS: Give us an example of the types of cases you've investigated or a specific case where that phishing has led to a data breach of some sort.

MARK LANTERMAN: Sure. I will tell you that in 2019, four of the top ten law firms in Minneapolis retained our company because they were victims of phishing attacks. And what we saw, we saw two separate attacks. The first was an email purportedly from the Clerk of Courts to attorneys saying, Dear Attorney, as a courtesy, the Judge wanted me to reach out to you and let you know that you have failed to complete your eFiling on your case, and if you don't complete eFiling by the end of the business day today, the Judge is going to dismiss your client's case with prejudice. To complete your eFiling, click here.

And so the clerk is not named, the judge is not mentioned by name, the alleged client's not mentioned by name, there's no case caption. It's a very generic email, but sophisticated attorneys are being tricked into clicking on the link and then they're downloading malware, bad software.

The second attack that we saw was an email purportedly from the managing partner to the head of H.R. Hey, Dear H.R., I need all W-2 information for our employees right away. Thank you.

Well, when we receive an email, typically we see the name and H.R. recognizes the name, yep, that's the managing partner. You click reply and attach a spreadsheet that contains W-2 information; names, addresses, Social Security numbers, dates of birth. And they're attaching spreadsheets and hitting send. In these cases, H.R. did not realize that the email address was badguy@hacker.com, or something like that.

So, you know, these attacks are becoming more and more sophisticated, and we need to be very careful. And I guess the best advice that I can give to our listeners today is if you're ever

asked to provide anything of value, whether that's information, whether that's wire transfer instructions, whether that's, you know, making a payment, pick up the phone and verify that it's a valid request. Technology has made our lives very convenient, and sometimes we're not reading those emails as carefully as we should.

CHIEF JUDGE MYERS: I know that we've all been instructed, certainly in our court system, about clicking on links with .exe files. Those are the ones that seem to be carrying many of the viruses or malware or other problems. But I read an incident -- or you spoke of an incident where somebody clicked on a .doc file, a doc, a typical Word file, and still found themselves in a bad way. Tell us about that.

MARK LANTERMAN: Yeah, you know, not clicking on .exe files, that's fine. But the problem is hackers are smart, and hackers know that a lot of antivirus software will block an exe, an executable file, from ever getting to your Inbox. So in order to work around that protection, criminals are becoming much more sophisticated.

And in that case what we dealt with, what our client, which was a city, a municipality -- city employee received an email, the email contained a Microsoft Word attachment, the employee double-clicked on the Word document, saw an error message. But what the employee didn't realize is that this Word document contained what's known as a macro. And a macro is simply a small program inside of a Word document, a small set of instructions inside of the Word document.

And in this case the macro did two things. It was to verify whether or not there was an active Internet connection, and if there was, to connect to, you know, badguy.com and download malware, bad software. And in my case, it downloaded a piece of malware known as Emotet, and Emotet was configured to do two things.

The first thing that it did is it established what's known as a remote desktop session, which means that now the criminal sitting down at his or her computer can see your screen and can control your computer -- could take control of the mouse and keyboard. So this is one of the most dangerous types of breaches.

The second thing that Emotet did was it also installed keylogging software, so everything that the employee was typing -- usernames, passwords, routing numbers, bank account numbers, everything that this employee was typing was being recorded and sent to the bad guys.

CHIEF JUDGE MYERS: So the message out of that is it's -- the document type or the attachment type isn't even necessarily the key. We still need to look further at the sender information. We need to look at the context of the email and the other content to determine whether that's something that's appropriate or safe.

MARK LANTERMAN: Yeah, you're absolutely correct. And I think the point is we can't just limit our suspicion to .exe files. I was able to create a proof of concept in which I was able to launch the same type of attack that we just discussed using not only a Word document but also a pdf file. And, you know, think about it, attorneys live and die with pdf files.

CHIEF JUDGE MYERS: That's absolutely true.

MARK LANTERMAN: And imagine being the recipient of an email with a pdf file marked urgent, and all that you do is double-click on the pdf and now you've been compromised.

And I'll tell you that in this case that we just discussed, I took that Word document and I ran it through every single commercially available antivirus and antimalware application. Not one of them caught it. Not one.

CHIEF JUDGE MYERS: Great. Wonderful. I mean, I -- you're absolutely correct, we live and die in this industry, in the legal industry, by the attachment of documents and the movement of those documents back and forth. And it seems like such a tremendous risk.

And I know as a court system, we make a sincere and really robust effort to prevent those types of downloads or things from even entering our system. So great examples and a lot of dos and don'ts for us to keep in mind.

Now, I'm a Starbucks fan. I don't know if you are as well, or some similar coffee shop. But I frequently will sit in a Starbucks with my laptop accessing the free Wi-Fi in Starbucks. Have I done something foolish?

MARK LANTERMAN: Well, respectfully, yes. You know, as I mentioned earlier, whenever we gain convenience, we always give up a little bit of security. And while public Wi-Fi is really convenient, there are serious risks. And what you need -- and not to just pick on Starbucks, but if you think about it, every judicial conference I've attended, they offer free Wi-Fi to their attendees. You know, every CLE I've attended, free Wi-Fi. Every time I go to a hotel, here -- you know, as a guest of our hotel, here's Wi-Fi.

Stay off of public Wi-Fi. No good can come from you attaching to any public Wi-Fi. Because the fact is, there are techniques that hackers can use that -- in a public setting, on a network that you do not control, they are -- they have techniques that allow them to capture the traffic going between your computer and whatever websites or whatever services you're using and can collect that information. And I have been able to prevent SSL encryption from ever occurring, which means I can now read your passwords. So if you're at Starbucks and you're logging into your court email account, I now have your username and password and I don't care if it's 30 characters long, I have it.

CHIEF JUDGE MYERS: Just scary stuff. Now, I do have that phone that's a hotspot. You're telling me that's a way to interpose a layer of security over those types of communications?

MARK LANTERMAN: Yeah, absolutely. You know, the two ways to protect yourself -- and you just mentioned the first, tether to your hotspot. Use your phone as a hotspot. That is your network. If someone else connects to it, you're going to be notified of that. That is far safer -- you know, public Wi-Fi is an attractive target.

If you think about it, let's say if you're going to a sporting event and the arena has public Wi-Fi; if I'm a hacker, I now have 17,000 potential victims that I can grab passwords from. If you're on your hotspot, that's a lot of work for me and I only have one potential target, so you're no longer low-hanging fruit.

The other way to protect yourself is to go onto the App Store, whether that's Apple's App Store or Google's App Store, and download something that's known as a VPN, a virtual private network. What this offers is encryption for all of your traffic even if you're on a public Wi-Fi. So that means that that's actually one way that you could protect yourself if you had to use Starbucks public Wi-Fi. And it's relatively inexpensive. I think it's about five to seven dollars a month, but the benefit is tremendous.

CHIEF JUDGE MYERS: Huge. That makes sense.

We mentioned at the opening of our time together this idea of ransomware. Let's talk about that because it really is in the news a fair bit here in Florida in particular it seems. What is ransomware?

MARK LANTERMAN: So -- well, from its name, basically it's the kidnapping of our data. And what criminals are doing -- you know, criminals are entrepreneurs. And what they do is intended to make money for them. It's their job, and it's their job to be good at what they do.

So, again, hackers need to trick us. Typically an employee within our organization will be sent an email. Because they're tricked, they're clicking on a link, it's downloading malware, bad software, and it's then encrypting -- it's encrypting the data on that system and all of the data connected to the network that that employee can attach to. So basically you're now without any of your data. And, you know, if you're a court, if you are a hospital or a small business, this can be devastating. And criminals will then demand payment.

You know, this past summer I was in Florida and I saw that a city in North Florida had been attacked with ransomware and the city paid a $600,000 ransom. And frankly, this gets me upset because all that these payments are doing is funding cyberterrorism. Do not pay the ransom. It's going to be painful. You're going to have to work closely with your IT Department to get back up and running. But the fact is, if you make that payment, you're funding cyberterrorism and you're marked as an easy victim and the criminals will be back.

CHIEF JUDGE MYERS: I read a statistic recently that only in one of five cases when the ransomware is paid is the data actually restored. That there are many occasions apparently where, having a paid a ransom, folks still don't get their data or access back.

MARK LANTERMAN: Yeah. I think that that is an accurate statistic. You know, sometimes the data will be unlocked. But, you know, we had a case in which a city was hit with ransomware, they were contacted by the hackers after a newspaper article ran. The hackers demanded payment of the ransom. The city paid the ransom. And it turned out that these

hackers were simply impersonating the real hackers, and they kind of intercepted that ransom payment, which I thought was kind of clever.

So, you know, there is significant risk. And I guess -- and I don't want to seem too critical. But if an organization finds itself in a position where they don't have a choice but to pay that ransom, they need to fire their IT Department, because IT -- we as IT professionals, we need to be prepared to recover from these types of attacks, we need to be backing up our data regularly, and we need to verify that our backups work.

I can't tell you how often I'm involved in a project and IT will say, oh, no problems, everything's backed up, only to find out that their backups were never good to begin with.

CHIEF JUDGE MYERS: What -- tell us a little bit about an interesting case or two that you've worked on. You've already shared some of those, obviously. But I -- my experience in listening to you, you're a fabulous storyteller and I love to hear your recount of some of these things that have occurred. So tell us a story about one of those.

MARK LANTERMAN: Sure. You know, I recently worked on a fairly tragic case. A woman was diagnosed as being cancer-free. Turned out that she was not. There was litigation involved, and it turned out during the deposition of a nurse that the radiologist had ordered the nurse to go find a clean mammogram and put the plaintiff's name on it. So her mammogram was misread. She actually did have breast cancer. But the radiologist ordered the assistant to find a clean film and simply put the plaintiff's name on that film. During the deposition of the nurse, she broke down in a Perry Mason kind of moment and apologized. She said, you know, I haven't slept in weeks, this is horrible.

And in that case, the hospital was ordered to produce the patient's -- all of the patient's medical records in its original electronic format. And the hospital came back with an affidavit

from an expert saying, in order to produce these records, it's going to cost over $3,000,000 because we have to hire programmers to extract the medical records from our database.

And yet when I did a review of the medical record vendor's website, they advertised their product as, doctors, hospitals, you can access patient records in real-time from anywhere on earth from any computer with an Internet connection. And I could not reconcile, you know, does it take months and millions of dollars to access someone's medical record or is -- can it be done instantly. So what we're seeing is an increase in parties relying on arguments of proportionality that are -- I would argue they're intended to mislead the court.

CHIEF JUDGE MYERS: Fascinating. I want to go to a place that I don't understand, so I'm a little off my reservation here. But this idea of the dark web, what in the world is that?

MARK LANTERMAN: Sure. That's a great question. You know, we -- some of us have heard of it. There's a little bit of mystery surrounding it. But the technology behind the dark web was created by the United States Navy in an effort to anonymize or hide or become invisible on the Internet. So it's a cloaking device. I think of it as a Romulan cloaking device.

And this technology has leaked, so now everyone has access to it, including criminals. And so, you know, the -- it's estimated that Google only indexes approximately 14 percent of the Internet. So think about it. Everything that you can find using Google, if you mash that all together it's only about 14 percent of what's out there. So there's a much larger, much darker portion of the Internet out there.

You need a special browser to get online. Google does not go on the dark web. It cannot access it. And the way it works essentially is the way that the regular Internet works; if I go to judge.org, judge.org will have a record of my what's known as an IP address. Think of it as like your home address or your office address. There's a record that I visited that website.

When you use the dark web, my Internet connection will bounce through 5, 10, 15, 20 different countries before it winds up on judge.org. And because of that, it is -- I don't want to say it's impossible, but it's virtually impossible to investigate cases proactively involving dark web technology because of the challenges associated with serving subpoenas on Internet service providers in Russia, China, the Ukraine, Mexico, Canada, and, you know, every hop of my Internet connection will require law enforcement to send another subpoena, and most countries will not comply. So that tends to shut down law enforcement investigations pretty quickly, and certainly civil investigations.

CHIEF JUDGE MYERS: And are there websites on the dark web that advertise services or products or things that obviously your typical Internet user would not be accessing but other folks might?

MARK LANTERMAN: You know, absolutely. You know, I think of the dark web as kind of Deadwood, South Dakota, in the year 1850. There's no sheriff in town, I'm going to do whatever I want, I can buy and sell literally anything. You can buy and sell anything on the Internet, including people. Almost all of our human trafficking cases involve the dark web in one way or the other.

We've had cases involving -- you know, we just did an interview on Dateline. We had an individual go on the dark web and try to hire a hitman to murder his wife. He paid the hitman thousands of dollars. Turned out that the hitman was a scam. So I guess the takeaway is, if you hire a hitman, get references. You know, check the Better Business Bureau for your hitman before you pay him.

And so, you know, we see -- well, so dark web, it's buyer beware. But you can -- you know, you can buy anything, whether that's guns, drugs, stolen products, iPhones that fell off the

back of the truck and, you know, Tony Soprano picked it up. You know, you can buy -- you know, it is a massive market of trade for anything that you could want.

CHIEF JUDGE MYERS: Fascinating. I want to come a little closer to home, and in fact in our homes, and talk some about the Internet of things. First of all, again, orient us to that idea.

MARK LANTERMAN: So the Internet of things is the topic that keeps me up at night. And it better start keeping our viewers and our listeners up at night, and the courts up at night. If you think about it now, everything is getting connected to networks. Everything is getting connected to the Internet, whether that's our cars or our printers, laptops, cellphones. Our TV sets that we have in our courts that are connected to the Internet and have cameras and microphones -- think about these TV sets that are in our conference rooms where we have our private conversations. These devices have microphones, cameras and an Internet connection. Again, what could go wrong?

So whenever we gain convenience from technology, we give up a little bit of security. And what we're finding is that manufacturers and engineers were so busy designing great, great, cool technology, both commercially and for personal home use, but were not even thinking about the security impact that it has. You know, we're inviting security cameras, nanny cameras into our homes, but we as consumers, we don't bother to read the owner's manual and, you know, the default usernames and passwords for these devices are easy to find. And now we have, you know, hackers that are watching us in our homes using the security cameras that we installed.

You know, we see hackers committing burglaries because we wanted the convenience of an Internet-connected garage door opener or, you know, someone playing with our thermostat because we wanted the convenience of a Nest thermostat. So we need to balance the

convenience with the risk. You know, is it worth the risk to have a Nest thermostat? Well, you know, probably. But is it worth the risk to have an Internet-connected pacemaker? I'm not so sure about that. So we need to balance the risk.

CHIEF JUDGE MYERS: I'm really concerned now about my refrigerator which I know is connected to the Internet and tells us when we're out of eggs or we need to buy eggs and sends us messages about the foods and things that we've taken out or need to be replacing inside of the refrigerator.

MARK LANTERMAN: Well, I wanted to remind you, it appears that you need milk and eggs.

CHIEF JUDGE MYERS: Great. Is that on the dark web or did you just have a direct connection to my refrigerator?

MARK LANTERMAN: A direct connection. I keep an eye on your groceries.

CHIEF JUDGE MYERS: All right. Mr. Lanterman, what a fabulous conversation. And I really do feel like we could probably talk for hours about these issues. But I want to thank you so much for joining us, for the insights that you've given to us, and for the warnings that you've given to us. We're grateful for your contribution to the courts, to the law.

And I'm interested and I'm going to follow you. Do you have a Twitter handle or an Instagram or Facebook account where you post some about the stories and cases and things that you get involved in?

MARK LANTERMAN: Yeah. You know, I often keep in touch with my friends using LinkedIn. I'm a little leery of some of the other services. But, you know, I think it's safe to say I'll be coming to a town near you, so --

CHIEF JUDGE MYERS: All right. Well, it was a test question, actually. I just wanted to see how far out there you were willing to put yourself in order for the chance to connect.

So thank you very much, Mark. We appreciate it.

MARK LANTERMAN: Thank you, Chief. Take care. Have a good day.

NARRATOR: You've been listening to "Open Ninth: Conversations Beyond the Courtroom" brought to you by Chief Judge Donald A. Myers, Jr., and the Ninth Judicial Circuit Court of Florida. For more information about the Ninth Judicial Circuit Court, follow us on Twitter, Facebook, Instagram and LinkedIn.

(Music)