Medical Practice Trends Podcast 55

Update on WannaCry Ransomware Work, with guest Mike Meikle of SecureHIM

Dr. Polack: This is Peter J. Polack, M.D., with another Medical Practice Trends podcast. Our guest today is Mike Meikle of SecureHIM. He's the CEO of a security consulting and education company. They provide cybersecurity training for clients on topics such as data privacy and how to minimize the risk of data breaches.

Mike has worked within the information technology and security fields for over 15 years. He speaks nationally on risk management, governance, and security topics. He's presented for Intel, McAfee, Financial Times, HIMSS, and for other Fortune 500 companies.

He's also a published writer with articles that have appeared in *American Medical News, CNBC, CIO Magazine,* and *The Chicago Tribune*. He's a Certified Information Systems Security Professional, Project Management Professional, and Six Sigma Green Belt. Wow!

Welcome, Mike. This is very timely. We're going to be talking about the WannaCry malware. We were just discussing offline that a lot of medical practices don't seem to be aware of this, but it's pretty big news. Can you tell us a little bit about what the WannaCry malware is?

Mike: It's a piece of malicious code that was created based off a vulnerability on Microsoft's 2003 server operating system that was patched by Microsoft back in March. This, of course, has its genesis in something we'll talk about a little bit further down in the program, about the Vault 7 breach.

WannaCry is taking advantage of old Microsoft operating systems on the server side and also if you're still running XP somehow. Basically what it does is it's a piece of ransomware that will take advantage of the exploits afforded to it by the outdated software and then it'll gain access to your systems. Then it will encrypt all your files, and then it'll pop up a screen on your system saying "Hey, your files are encrypted. Please pay $300 in Bitcoin to get the key back so you can open up your files."

Dr. Polack: This really illustrates the importance of not clicking on and opening files if you don't know exactly where they're coming from. That's ransomware, so something happens and generally the files are encrypted or stolen or whatever, and then in order for you to get them back… The whole point of this is for these people to make money.

Who's been impacted by this so far?

Mike: If we take a look globally, they said there were about 200,000 people who've been impacted, which is pretty small, over 150 countries. The biggest ones are China, India, the U.K., and some Asian countries, and of course, the Middle East. The U.S. has been less impacted by a significant margin.

Of course, if you look at the U.K., who's been hammered over there? The NHS, the National Health Service. They had to put patients on diversion. They've had issues with even serving patients because their patient records have been encrypted.

Over in India, telecom firms have been heavily impacted. The same thing in China. A lot of tech firms / telecom firms have been impacted because they're all running this old software and they have not applied the patches that Microsoft had made available back in March.

Dr. Polack: Part of this was related to the stuff that the NSA was holding onto so that they were able to hack into different places. Wasn't there an issue with that?

Mike: That's correct. Basically what happened earlier, I'd say late last year, was that WikiLeaks had publicized the Vault 7 breach, which was basically a huge stack of files and tools built by the CIA and the NSA, the National Security Administration.

The NSA had built these specialized tools to break into computers, and they had some really nice names, like Fine Dining and Eternal Blue. They have all of these cool code names. These tools allowed CIA case officers to gain access to target systems, and they were custom developed by the NSA.

Unfortunately, they were leaked to WikiLeaks, who then made a statement earlier in 2016 that "We have quite a large cache of these tools, and we will be making them public. We are going to contact a couple large firms so that they can get the jump on fixing some of the vulnerabilities, but then we'll publish them to the world."

They did that, and so basically they have weaponized tools out there. This is like the beginning of the atomic age for cyber-hacking. You have nation-state level cyber-security/cyber-hacking tools released into the wild. That's very significant, and it really changes the game. At one time, only nation states or very well-funded hackers could bring up this type of technology. But right now, everybody has access to the NSA tools that created this particular vulnerability and this particular disaster.

Dr. Polack: Security experts say regarding this hacking that there are these gentlemen's agreements between nation states where they acknowledge that this is going on but they may not necessarily do things that'll befall harm to average citizens, like hospitals and things like that, but now you have these rogue players, some of whom may actually be sponsored by some of these nation states, and there are no rules basically at this point.

Mike: No, there aren't. When you release tools of this magnitude and also a list of all the various vendors who have these types of breaches, it's open season. It's pretty crazy.

Dr. Polack: This is all in the category of what's known as phishing.

Mike: That's right.

Dr. Polack: Explain what exactly phishing is, what are some examples of that?

Mike: Phishing is, you see that piece of e-mail, usually that's been targeted for you, and it has a compromised link or document or it has a link that goes to a site that has malware already on it that finds a way around whatever end-point protection you have.

It will compromise your system and then it'll start downloading usually remote-access Trojans and then eventually the ransomware itself will come down, and then it will encrypt not only your local drive but any drive that you are mapped to, like a network shared drive or your Dropbox or anything like that will actually be encrypted.

It's very damaging. It's also very prevalent. Healthcare has had a huge uptick in malware. It's something that especially healthcare providers really have to be very careful with.

Dr. Polack: What are some basic rules that you would tell employees? If they see an attachment and it looks like it's coming from a friend of theirs, what rules should you have in place that you would recommend?

Mike: Basically, you should always train your employees on how to spot phishing e-mails. If you look at the e-mail address of the sender, is it coming from a recognized sender? Looking at spelling mistakes in the e-mail. Also if there are links that you're supposed to click on and they say "Please click on this link," normally that is a phishing e-mail. And if you have questions about it, please don't click on the link; call the company that supposedly sent you the e-mail and ask them.

People get upset that they see lawsuit documents coming at them via e-mail or something from the IRS or something from another government agency. Nine times out of ten, that's a phishing e-mail. They try to look very official when they send these documents to you.

The first step is you have to educate your employees because a phishing e-mail and a phishing campaign, if done well, can easily bypass most of the security controls you have in place in your organization. That includes end-point anti-malware and various other intrusion detection and prevention services you may have in place because you're giving it access internally. It can really damage your environment if you're not careful.

Dr. Polack: Why are these things so hard to keep patched? These are patches for the software, correct? This is something that you have to continually keep on top of, and the typical doctor or medical practice can't do this, so what are tools or services that medical practices can use to stay on top of this?

Mike: For a small- to medium-sized practice, it's always good to work with a third party to put together an agreement for an actual service to maintain your infrastructure. People will say if you put everything in the cloud then, of course, you're not going to have any of these problems. That's not true. You still have many localized end points in your environment – medical devices in particular – that you're going to have to manage. What you want to do is work with a third-party provider to help you patch and keep your environment up-to-date.

Also, you want to work with someone who can sit down and come in every six months or so and educate your staff and employees about the latest threats and what they can do to prevent them getting a foothold into your practice and also just giving them general information on how to protect themselves in that type of high-risk environment.

Also, have online training available and then every month, bring out an update on the security situation and what they see and what's maybe targeting your particular industry because a lot of doctors and also other health care providers are just unaware of the risk that's out there.

Dr. Polack: That's for sure. Let me ask you this: if your systems have been accessed and this information has been accessed and either encrypted or stolen or locked up, is this classified as a breach?

Mike: According to Health and Human Services / Office of Civil Rights, yes, you should be reporting successful ransomware attacks on your enterprise. That's their latest statement within the last few months.

Now, does that mean they're going to penalize you? Most likely not. This is like if you do have a successful ransomware attack and you sweep it under the rug and then you do have a real data breach –

a significant one – further down the road and they come in and start doing their audit and they find out you had a ransomware attack and you haven't told them, that's not going to look too favorably on your situation.

It already shows that you weren't really protecting your environment particularly well, and so they're going to be much more suspicious of your protestations of misunderstanding the situation. You've already had a warning shot over the bow. They're going to not look at you particularly favorably.

So yes, it is considered a breach – not as serious as say, the records have been stolen, but it is something to consider.

Dr. Polack: In your experience, has this been a common thing here in the U.S.?

Mike: Yes, very much so. Healthcare has seen a 90% increase in ransomware over the last two years. Remember, medical records are worth about $50 to $90 on the black market each, because you can make multiple people out of them. You can use it to fabricate other medical records. You could do Medicare and Medicaid fraud. You can do prescription drug fraud.

They're very, very valuable because they contain pretty much everything you would need to create a fictitious person or persons. It's pretty crazy.

Dr. Polack: Has this occurred with actual medical devices?

Mike: Yes. Just very recently, this week, Bayer medical devices for radiology were compromised. Many medical devices still use embedded Windows XP or older Windows 2003 Server versions or just older Windows versions that can't be patched or told that they can't be patched, even though the FDA has put out many memos saying, "Patch your stuff. We're not going to make you re-apply for your certification, so just patch your stuff." That's what they say.

Dr. Polack: That's pretty scary.

Mike: It's very scary.

Dr. Polack: You've actually been working on something that would be a great resource – and we can probably put a link here with the podcast for this – "Navigating the Medical Device Cyber-Breach Jungle" – as well as other resources.

Mike: That's correct. Collaboration is ongoing. This is something that I believe all physicians should be concerned about and also the book should be very interesting for them, not only from a medical device perspective but in general, some security tips and solutions for small- to medium-sized practices.

Dr. Polack: That's great. Mike, any last words, final thoughts on this? Nothing has happened at your practice, so what are your next actions before anything happens?

Mike: First is to do a risk assessment of your environment. Basically have someone come in – a third party – review your infrastructure, your environment, and find out where the riskiest areas are and then address them, because if you don't know what you don't know, you can't act on it.

Dr. Polack: Very good. Mike, thanks very much. Appreciate it.

Mike: Thank you, Dr. Polack.