NAVIGANT

On Healthcare

HEALTHCARE

CYBERSECURITY—CYBERCRIME THREATS AND RISKS TO HEALTHCARE

Announcer: Welcome to Navigant On Healthcare. Offering insights for healthcare leaders striving for success in an evolving industry.

Host: Welcome to Navigant On Healthcare. I'm your host, Alven Weil, and today we're joined by Bob Anderson, managing director of cyber and information security at Navigant. A former FBI executive with 30 years of law enforcement experience, Bob is one of the nation's foremost experts on cybersecurity and national security issues. At Navigant, Bob leads the global cyber and information security practice, responding to more than 600 breeches a year across all industries. Bob, thanks for joining us.

Bob Anderson: Alven, great to be here. Thank you.

Host: Today we're discussing an issue that all industries are coping with, and that's cybersecurity. Now, as I just mentioned, Bob, you were an FBI exec for about two decades. Please tell us a bit more about that role and how cybersecurity threats have advanced during this timeframe.

Bob: Alven, sure thing. My last position in the FBI was the executive assistant director of the cybercriminal response and services branch, and, really, what that means that I was in charge of, is, if you look at it, the FBI is about 35,000 employees. I probably had about 22 to 24,000 of them on my side, and I was in charge of worldwide cyber, worldwide criminal, and all critical incidences regarding international operations.

The one thing that I can tell you in the last four or five years that I was in the FBI and currently in the practice I'm at at Navigant, the cyber landscape and the threats that we saw coming from bad guys while I was in the FBI has monumentally changed. They've become much more sophisticated and much more easy for them to be launched from people that aren't traditionally hackers. I think that's the biggest change I've seen in the last several years due to the dark web and a lot of other things out there that lack of better term, "laymen individuals" in the cyber world can launch attacks nowadays against industries around the world and not necessarily have to be a seasoned hacker like say 10 or 15 years ago.

SPEAKER

BOB ANDERSON
Managing Director
+1.202.481.7306
bob.anderson@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

Host: Specific to healthcare, just about every hospital or physician enterprise, or really any type of provider, now faces cybersecurity threats. Tell us a bit more, Bob, about the major risks, the types of risks they are facing.

Bob: Yeah, healthcare nowadays is a huge target, not just in the United States, but globally. PII and PHI information is extremely valuable to bad guys nowadays and when they're attacking the healthcare industry, really that's what they're seeking. Over the last six or seven months, I've seen a huge steady rise increase in the number of healthcare breaches that we're dealing with at Navigant across the United States.

You know, nowadays when we look at medical devices and we look at the features like wireless connectivity and remote monitoring features that they have on different medical products, nowadays, it really makes them vulnerable to any type of cyberattack or when they interface with data or IT structures that are trying to update their capabilities. That all is a huge risk, nowadays, for healthcare companies.

Host: Bob, you mentioned medical devices and some people will say that's really kind of the next area, the next big cyber security nightmare in healthcare. I think that begs the question, what can be done to protect patients using the devices so that hackers can't, for instance, hack into an insulin pump to administer a fatal dose or hack in and obtain information, sensitive medical records and really hold systems hostage until they pay ransoms?

Bob: Now, that's an absolutely great question, and a lot depends on how the device is actually set up or how the device is being set up to be accessed by the hospital provider to repair, maintain or increase or decrease dosages for the patient. It's a lot like looking at how things are connected to the Internet, or necessarily connected to Bluetooth. The medical field looks at, and it's made huge innovations in the last several years, especially for the patients. They use remote monitoring or near field communication techniques, which allows the device to be implanted in the patient without very invasive procedures to be done every time they need to update the device or check to make sure the device is working well.

And I think that one of the things that really needs to be looked at in the future is how to create less risk for the patient and the industry on the potential points of exposure to that device. And that really revolves around the maintenance and the engineering of it. And I think you're going to see a lot of this come out over the next several years in the healthcare industry -- not only with the advances of how these devices work inside patients, but how we make sure that the engineering and the software that is implanted in these devices are not in any way accessible to bad guys to use for their own means.

Host: What can providers do to protect themselves from these types of threats, and on top of that, in doing so in planning who should be involved within provider settings to prepare for the threats?

Bob: Absolutely, great question. The one thing, and the biggest thing in my opinion, especially proactively, you need to have a plan. The company or the corporate environment nowadays needs to have a breach response plan and a plan that in detail looks at different aspects of what the threats are to the current environment. And they need to have a plan and they need to train for that plan. The first time that you're looking at your breach response plan should not be when your company's either attacked by a malicious malware or has some type of ransomware attack in it.

The other thing, especially in the medical industry, which I'm seeing nowadays, is really look at their infrastructure. A lot of the breaches that we respond to, and a current practice at Navigant, the infrastructures are extremely outdated. A lot of them stem from the early 90s and they're Windows-based. A lot of these industry infrastructures are wide open and susceptible to a variety of breaches and ransomware attacks, and I think looking at those two things really hard helps reduce the risks of the company.

The other thing I think that companies need to do is know who their insurer is, know what the carrier will provide for and will not. And also have met, talked to, and are very comfortable with a forensic and IR company like Navigant that can respond back out and help the client, whether it's proactively or reactively and then the last thing that I would say is train your employees. One of the biggest offenses nowadays is not from a malicious insider, or somebody that's actually trying to hurt the company, it's from good employees that have been there a long time, that maybe not have had the amount of training that they need in today's cyber landscape.

They click on something wrong, or they reply to an email, or they click on some social media content and without knowing it at all, they've opened that company up to some type of potential cyber breach. They're the things that I would highly recommend to anyone running private sector healthcare companies currently.

Host: The million-dollar, or you could say multi-million-dollar question: should hospitals pay up with it comes to ransomware, or is it really more complicated than that?

Bob: It's a very complicated answer and I'll tell you, when I was in the FBI we always advocated not to pay the ransom, in most cases. Out here, the reality of most of the clients that we deal with -- and we always make this to be a client-based decision, we don't decide for them -- is to pay the ransom. It's not because they want to, but because, in a lot of cases, the clients have either not had the infrastructure or the revenue to hire and make sure they maintain backup systems, redundancy or segmented data. Really, this is much more than a business interruption. It's a business crisis.

What I say most of the time when I talk to clients, that it's 100 times cheaper to proactively look at potentially what could be damaging to the company if we do get hit with a ransomware attack prior to doing it,, because nowadays because the way ransomware attacks actually work, they're very sophisticated and in most cases you're never going to be able to break the code. Without the backup systems or potential redundancy of the data that the company has, they almost have no choice.

Host: What's next? Are there any new advancements, for example, that you can expect to help offset cybercrime? Whether it's in healthcare, or otherwise?

Bob: Well, I will tell you the one thing that I think, and it's very cheap to do, but I think it's one of the best things to do for any company, is training your employees of the current cyber threat and constantly evaluating where your company sits at risk. Those things can be done with very little revenue expended by the company, but it allows them to understand where they sit on the risk continuum.

I will tell you the bad guys don't have boardrooms. They don't work under a constitution. They don't slow down. They are constantly revising and refining their threats to corporate America. While they're meeting and moving at the speed of light, sometimes, because of the way we work in corporate America and everybody functions under some type of chain of command, we move slightly slower, and that gives the bad guys a huge advantage.

The two things I would really, really stress is train your employees and constantly evaluate where your company is on the risk continuum of the current modern day cyber threats. If you do those two things, you'll reduce the risk to your company monumentally.

Host: Some excellent insights, Bob. Thanks so much for sharing them, and that's it for the day. Be sure to check in with us regularly for new episodes of the Navigant On Healthcare podcast series by visiting navigant.com/healthcarepodcast. Thank you for joining, and take care everybody.

Announcer: That concludes today's episode. Be sure to check in with us for future installments of the Navigant On Healthcare podcast series on navigant.com/healthcarepodcast. Navigant On Healthcare is a podcast series produced by Navigant's healthcare practice. If you enjoyed this episode, please share it with friends and colleagues on social media. Learn more at navigant.com.