ORTHO SCIENCE BYTES TRANSCRIPT

Episode 30: The Evolving Cybersecurity Environment in Laboratories

Tony Casina:

Welcome to Ortho Science BYTES. Ortho is proud to sponsor this podcast as a continuing commitment to advanced patient care from donations to patient transfusions.

I am Tony Casina, and today I am joined by Patty Ryan. As Ortho Clinical Diagnostics Chief Information Security Officer, Patty is responsible for defining the firm's global information security strategy, roadmap and operating infrastructure. Partnering globally with IT, compliance, commercial, regulatory, legal, quality, R&D, and strategic marketing resources, she ensures that all information security controls operate effectively and efficiently, that staff are aware of their responsibility to protect client and proprietary information, and that the security team defines and manages information risk appropriately.

Patty has over 30 years of IT experience, over half of that in information security executive positions. She has worked in financial services, life sciences, such as Johnson & Johnson, and legal. And brings a wide range of experience to ortho. She holds a BA in Economics from Columbia College, Columbia University, and an executive MBA from the Stern School of Business at New York University.

Thank you so much for joining us today, Patty. Okay, let's get started with the first question. Welcome, Patty.

Patty Ryan:

Thank you for having me. I'm excited to have this opportunity to talk shop.

Tony Casina:

Okay, the first question really is about cybersecurity. Cybersecurity is a complex topic, maybe we should start with a definition of what cybersecurity is for our listeners.

Patty Ryan:

Yeah, that probably makes sense. Cybersecurity is all about protecting IT assets. There's something called the CIA triad. So you look at the confidentiality, you look at the integrity, and you look at the availability.

Now, these days, confidentiality is to make sure that only people who have access to either a firewall, or a data set, or a report have that access. So it's need to know and it's least privilege. So they are doing their job with the least amount of system resources at their disposal.

You have availability, which is to make sure the information or the asset is available. You don't want to log into a web server and have something not work. Or think of what happened with the Taylor Swift tickets, the tickets were not available.

And then, it's integrity. You want to make sure that the information is kept at the state it was. So, for example, you don't want someone buying tickets illegally, or changing a data record, or taking a laptop. So really cybersecurity is about looking at IT assets, be them traditional physical laptop servers or right now, more importantly, data, information and making sure that it's protected.

Tony Casina:

Okay thank you, Patty.

What has been the impact of breaches on the healthcare industry from a large scale, economic, personal info, exposure, medical treatment perspective?

Patty Ryan:

The impact has been tremendous, especially with COVID. Obviously, over the last two years, 30 months, the healthcare industry has fought a tremendous battle with this pandemic. As we know, the amount of healthcare workers who were frontline heroes put in day in, day out to try to protect and save individuals.

Unfortunately, many cyber criminals, hackers looked that as an opportunistic way to make some money, or to hold medical care hostage. So it's been breaches, threats of breaches, attacks have had a tremendous issue. Now, IBM Security recently had a survey that said breaches were up 9.4% from 2020 to 2021, but what's more incredible is 41.6% since 2019. So the attacks have been coming very, very significantly across the healthcare industry.

Tony Casina:

Okay, thank you.

Do you have some specific examples of types of breaches that have occurred?

Patty Ryan:

Types of breaches? There's many that happen, but we kind of have been coalescing around two or three specific types. One is called ransomware attacks. I think people have seen that across the news. What that's about is basically hackers encrypting data and holding it hostage for a ransom. That is very complicated on most organizations because it's not just one piece of data. Something like this could traverse an entire network going from your finance systems to your email systems, to your medical data, to your HIPAA data. And, in some cases, affecting point-of-care systems. So there's a wide network here about the interconnected abilities with healthcare.

Second thing would be someone stealing credentials, so phishing. Now either sending an email that says, "Hey, you won the lottery." Or, "Hey, your password needs to be changed." Or, "Hey, I am your boss and you need to fill out this form for me that gives me your confidential information." Those types of phishing attacks are quite prevalent these days because it's a way to social engineer someone remotely. And if you think of the amount of information that's on the internet about an individual, or a company, it's quite easy for someone to get a recent replica, or enough data to fool another individual.

Finally, we don't have as many of it, but in some cases it's something being stolen, your mobile phone, your laptop with data, sensitive data on it, or access to sensitive data. While they're not as common these days, it's still a method in which cybercriminals do take advantage of where data is.

Tony Casina:

Okay, thank you.

So what is the impact of these breaches for the laboratory, or the hospital when it comes to, for example, blood donors, or patient data from your perspective?

Patty Ryan:

The impact is really because the data is interconnected. Twenty-six thousand on average Internet of Things assets -be it a point of care, be it a firewall, be it an email server- are across the hospital space. Every single one of those tends to have a connection to another device, what happens if, let's say, an email system is under attack from ransomware because you don't want that particular tech spreading into critical care infrastructure, the hospital may shut down the entire network. What does that mean? That means maybe critical surgeries aren't going to happen. Maybe that means someone can't pay the hospital bill. Maybe that means that there is an impact to a point-of-care device, be it a heart machine, a lung machine.

The fact that everything is, right now, Internet of Things buzzword is quite incredible because you have now hospital systems that are struggling to protect their patients' lives are also now looking at the fact that the attack surface, or how hackers will attack them, is tremendously large and, in a lot of cases, diverse. It takes a lot of effort and time to have systems in the hospitals secured, and people don't realize that just because it's, let's say, something that's on a corporate structure could directly affect the patient care.

Mortality rates right now are increasing. I read somewhere over the last month or so that hospitals that are under ransomware attacks have a 57% higher mortality rate just because of the fact that everything is so interconnected and people in the hospital systems don't really realize how that happens.

Tony Casina:

Okay, thank you.

So with these increasing occurrences in future threats, how have regulatory agencies become involved in cybersecurity?

Patty Ryan:

Oh, there's been a tremendous effort by regulatory agents such as the FDA. They have brought in experts in cyber, starting in about 2018, just to look at how to integrate security formally into pre-market and post-market mandates. So they have taken into account this whole idea of interconnected devices, point-of-care devices, and that large attack surface that I talked about. It's something that I found to be quite incredible is how quickly they have decided to make a medical device cybersecurity requirements to be just the same as it would be, let's say, a critical firewall or an asset.

Before, earlier on, the FDA and other regulatory bodies really weren't thinking of cybersecurity in a medical device. It was a black box. No one would think of hacking a blood analyzer, or heart machine. Well, that is obviously something that's changed over time, and COVID was the perfect example of a lot of that.

So what we're seeing is the stringent rules upfront that you have to show the FDA in order to be able to get approval to market a device is becoming standard with every other asset you've got in a traditional sense. You have to patch them. You have to understand the threats and protect against them. You have to be able to detect and protect the devices. You have to be. And our customers are seeing that and asking for the same things. It's becoming a tremendous focus of the FDA, and that has had

other regulatory agencies around the world look at the same level. So it's as if there's nothing special. Right now, you have to treat cybersecurity from the beginning as part of your design with every single medical asset.

Tony Casina:

Very good. Thank you. That certainly covers the next question. I was going to ask about was medical devices and the responsibility of the manufacturer. Obviously, there's quite an emphasis from the regulatory agencies these days on this whole cybersecurity aspect of bringing a device to market.

Antivirus programs are offered often with these products. So are they effective in securing against cybersecurity attacks?

Patty Ryan:

Well, they're better than nothing. I do think most antivirus programs are what we call passive. So you have to understand how a threat, or an attack is going to work. And then, you can adjust that particular antivirus technology to detect or block. But that's time for which you're vulnerable.

I think it's better to having nothing. But what I consider to be far more important is the ability to take advantage of machine learning, or artificial intelligence. So you're using the next generation antivirus products. Looking at ways to have a pattern developed organically that the device software understands what's normal activity and what's not normal activity.

So, let's say, a device all of a sudden is trying to connect to something external to the network, an IP address, or a internet address, they have never done that before. And let's say it's in a country that this particular hospital has no reason to connect to. Well then, you want something to be able to say, "Wait a minute, that's not part of my pattern," and stop it, or at least alert.

So what I'm seeing is that well, antivirus is a good, older fashioned way to make sure that you've got these protected, the next generation devices, or technologies such as those with artificial intelligence and machine learning, are the ones that are going to help real-time protect medical devices and assets. And it's something that I think is essential because of how significant, and complicated and quickly changing the attacks landscapes are.

Tony Casina:

Since antivirus programs alone are not as effective, what solutions beyond the artificial intelligence and machine learning can be offered that are more effective in preventing these attacks?

Patty Ryan:

Yes, it's preventing, but it's also making it incredibly complicated, the attack, to be successful. And also, being able to learn as soon as possible that something malicious, or suspicious could be happening. So you're really looking at defense in depth. You're not looking at one component, let's say, a medical device and not thinking about the rest of that network. You want to isolate critical systems. You want to put firewalls in place. You want to put network traffic monitors. You want to limit, by privilege, who has access to different network segments or assets. You want to be vigilant on that access because if someone changes jobs, or leaves, you want to make sure that they add access to suspended or changed appropriately. It's really about defense and depth. That's a concept from information security from years ago.

Think of a medieval castle. You had the moat, you had the bridge, you had the outer circle, you had had the inner circle. Well, it's the same typical type of thing. You want to look at every single area of a network, or where your data is and see how can you effectively isolate it, not to prevent it from being used effectively. It's really about just trying to make sure that only the people who can have access, have access. And if anyone is trying to do something malicious, or suspicious have to go through multiple different channels. In some cases that just makes the hacker, or the cybercriminal just give up and go to an easier target. You also then, have all these different points to understand when something suspicious or malicious is happening so you can react quickly.

Tony Casina:

Thank you. That whole defensive approach is an interesting concept.

Well, to close out this interesting conversation, can you convey how cybersecurity has changed over the last few years?

Patty Ryan:

Well, cybersecurity necessarily hasn't changed. It's, in my opinion, the vast amount of IT assets, or technology being leveraged every day, every individual in every situation. It's made more examples of what could be broken into, what could be hacked, what could be stolen.

It's also the fact that different technologies haven't necessarily worked together all the time. So you have to merge divergent technologies like an Android phone, and a Linux server, and a special type of firewall and a point-of-care device, and how do you make sure you understand the nuances and subtleties of every single one of those and how they can be exploited. It's that order of magnitude that I think has been more of an issue because just the threats are everywhere now. It's the same basic principles to protect the environment, just a lot more of them to do.

Tony Casina:

Okay, thank you. Sounds like a complex and expensive approach to this cybersecurity issue and one that will certainly continue on to the future.

Patty, I really want to thank you for taking the time with us today and giving us your experiences and insights on this fascinating topic.

Patty Ryan:

Thank you very much.

Tony Casina:

It's been a pleasure to talk with you, Patty. And, again, thank you so much for your time today on this podcast.

I hope you all enjoyed this podcast episode about cybersecurity and its potential impact on the healthcare industry. Make sure to review the sections within the podcast description for any reading materials that we've suggested.

Based on today's podcast, I'll leave you with our pop quiz: ”What are specific examples of types of cybersecurity breaches?” You can always go back and listen again. Thank you for listening. Please subscribe to Ortho Science BYTES, our monthly podcast, where there will be discussions on more complex questions we face every day in our labs. Brought to you by Ortho Clinical Diagnostics, pioneering advances in diagnostics for 80 years. Because Every Test Is A Life. Take care, stay healthy and safe.