© Andrew Angelov | Dreamstime.com

Cybersecurity Awareness for Healthcare Organizations

This podcast highlights keys to protect your data.

BY JULIE CHUA AND MICHAEL J. SACOPULOS, JD

This article is a transcription of a podcast posted on October 13, 2021 at www.soundpracticepodcast.com/e/cybersecurity-in-healthcare-with-director-julie-chua-from-hhs/.

Mike Sacopulos: *Welcome to the SoundPractice podcast. My guest today is Julie Chua. She is the Director of Governance, Risk Management, and Compliance Division within the United States Department of Health and Human Services, Office of Information Security. Julie is also the Federal Lead for the Implementation of the Cybersecurity Act, Section 405(d). Ms. Chua, thanks for being on SoundPractice.*

Julie Chua: Thanks, Mike. It's great to be here to share our experiences and talk about cybersecurity in healthcare.

MS: *October is National Cybersecurity Awareness Month. In the past five years, cyber has become a major risk for the healthcare sector. Can you talk about the kind of threats that you're seeing daily?*

JC: Sure. I think it is important to know that there are many different threats affecting all industries, including healthcare. Ransomware, which is covered heavily in the media, is the main threat, and a prevalent threat right now. A cyberattack inclusive of a ransomware attack impacts clinical operations, patient care, and, ultimately, patient safety. What you will hear a lot from the government side and also our industry partners is, "Cyber safety is patient safety." It's not solely an IT issue, and it cannot be that IT is the only solution when an organization faces a cyberattack.

To your question about different kinds of threats, there are many. You could see phishing, which is very much connected with ransomware. You could see insider threat, which means you have malicious actors within your organization. You can have unintended malicious actors within your organization, meaning errors. Unintended errors include inadvertent mailing of PHI (protected health information), or PII (your personal identifiable information).

Another thing to remember is that when a cyberattack occurs, it's important for an organization to know everybody's roles and responsibilities during a response. I'm not just talking about the IT shop or the information security professionals doing the response work. What I'm

Continued on page 106

Cybersecurity Awareness (from page 105)

alluding to are contingencies, including paper processes and communication plans. Know your role if you're a physician, a nurse, a hospital administrator, and all the other non-IT and non-InfoSec professionals.

Keep in mind that these threats can come in different ways. You may hear "attack vector," a way that the cyber professionals talk about the different ways that malicious actors get into an organization. That just means it could come from your medical devices. It could come through your email. It could come through your laptops, your personal phones, your other devices, and equipment that are interconnected within your hospital. If you're within a clinic, your billing is interconnected with your fax machine, is interconnected with your hospital EHR, or other service providers.

MS: *For our audience's sake, you're right, we hear most about ransomware. Can you give us some statistics associated? How prevalent is this? Is the problem on the rise?*

JC: To state a few statistics, in 2020, the number of ransomware attempts, and this is just "attempts" against the healthcare industry specifically, rose by 123%. That's huge. Another thing is ransomware attacks and the costs affiliated. It's over $20 billion in downtime, and that is almost double from where we were in 2019. The last statistic that I think the audience will find relevant is in 2020, 92 individual ransomware attacks affected over 600 separate clinics, hospitals, and organizations. That represents more than 18 million patient records.

Three core risks that organizations look at with an attack is loss of revenue, patient care impact, and, of course, ultimately, the patient safety aspect.

Loss of revenue is very connected with patient care impact and patient safety. If you have a down EHR and you don't have any way to perform any of your treatments, you don't have a way to perform any other scheduling, there is a worst-case scenario of diverting care. When you divert care, the result of that down the road is, of course, loss of revenue, because you've transferred the patient to other hospitals within your local environment, within your regional network. And, although you may have insurance coverage or a policy, you still expect some sort of lost revenue and outlay outside of what you've already budgeted or funded for your insurance policy.

One additional thing you will hear from the media: ransomware is becoming increasingly complex. It's twofold, yes. The malicious actors are getting more sophisticated. They are banding together, getting third-party partners to help them with their ransomware activities. Also, on the technical side, they are constantly re-engineering their operation, the way they launch that malware or malicious software into organization environment.

Getting into the human nature and the human aspect of ransomware, where it's as easy as clicking a link. That's why you will also hear that a phishing attack is almost always connected to a ransomware attack, because the phishing is how the ransomware gets into an organization.

MS: *It's with fear that I ask you any more questions after those statistics, but we're going to forge ahead here. Maybe you can help explain why healthcare is being targeted.*

JC: That is another very complex question because there are so many facets to why healthcare is targeted. I'll go through a few things and then expand on a couple, not all of them. One is, in the healthcare industry, we have a huge volume of PHI and PII. Those two types of data are worth a lot of money for attackers and malicious actors.

Another thing to remember with healthcare is that we have become increasingly interconnected using digital technologies, using EHR, and all those interconnected medical devices. That is not abating. We are still looking at emerging technologies, ways that technology can help care delivery, and optimizing treatment of different illnesses and different diseases.

Another thing to highlight is healthcare staff and employees. They are a wide variety of professionals. It is very hard to educate each type of role and each type of professional about cyber hygiene and cyber safety. They need to understand their roles have an impact on cybersecurity within their specific organization.

Three core risks that organizations look at with an attack is loss of revenue, patient care impact, and, of course, ultimately, the patient safety aspect.—Chua

One additional item on the technology side where those connected devices exist: largely, they are legacy devices. That's another term you will hear, meaning, they're either outdated, they are not supported by certain protection, and that makes it even more of a likely and easy attack for malicious actors.

In healthcare, there is an innate nature of sharing information, the need to share information, and that is becoming a weakness to a certain extent in the cyberspace. We are very trusting in terms of who is asking information, why they are asking information about a patient, about a patient record, about a treatment, etc. The first thing that comes to mind is, "How do I help this person or how do I share that important information about somebody's care?"

The cybersecurity aspect of it is last on anybody's mind. I know this for a fact because physicians say that, nurses say that, front office in a clinic say that, because, "Oh, they're asking about Mr. So-and-so's patient records." Of course, they have a need for it, why else would they ask? I emphasize this point because that is the main way that ransomware gets into our environment. I say that because of the phishing aspect, and I've been saying phishing.

Let me describe phishing in case

Continued on page 108

Cybersecurity Awareness *(from page 106)*

everyone is not aware of this. Phishing is just a way for a malicious actor to ask for information, seemingly coming from a trusted source. Concrete example: It could be an email that says, "I am from HD or HR department, and I need the patient information of Mr. X, Patient Y, and Mrs. Z." Without anything else in that email, you are already trusting that "Oh, it's my HR."

Another situation is, "It's my billing company," or another situation is "My accreditation." That is a common one that I've heard as an example of, "If it's my accreditation courses, yes of course, I will immediately act upon those requests."

Those are a few of the things in terms of the human nature of things in cyber, the awareness piece of cybersecurity, and why healthcare is such an easy target, and why we are targeted.

MS: *Let's talk a little bit about how HHS is helping the healthcare sector. Can you give an overview of what the 405(d) Program is and how you're supporting the healthcare sector in cyber?*

JC: That's a great question, Mike. Thank you for asking that. Essentially, this work on the 405(d) Program, it's a public–private partnership. This means government and private sector stakeholders together are working to share expertise, best practices, perspectives, and they all come to consensus on what is applicable to the entire healthcare industry based on their own experiences and what works.

This effort, like you said in the beginning of our conversation is out of a key piece of legislation. There's a Section 405(d) specifically for aligning health industry security approaches. What does that mean? We have a group of healthcare and cyber professionals. We have chief information officers, chief information security officers.

In addition, and this is where the strength of this group comes from—we have physicians, nurse practitioners, hospital administrators, chief medical officers, those who are not really in the cyberspace, but that non-cyber background lends expertise into the conversation. We're not just putting out mitigating practices or recommendations that are not practical from a clinical operation sense and the patient and care delivery aspect.

I emphasize this because this is an opportunity for those who are not in the cyberspace, but who are concerned about the impact of a cyberattack when it comes to your clinical operation and patient care.

Phishing is just a way for a malicious actor to ask for information, seemingly coming from a trusted source.—Chua

MS: *Great. What is HICP and what information can we find in it?*

JC: Sure. With the group that I just talked about, Cornerstone Publications produce a source called the *Health Industry Cybersecurity Practices*. Appropriately, our acronym is HICP. It's kind of funny that that turned out that way, but it's affectionately called the HICP. It's meant to raise awareness. It has vetted cybersecurity practices.

The key takeaway is the publication is meant for a variety of stakeholders. You can be a board of directors within a healthcare organization. You could be a hospital administrator. You could be a CIO, or SSO. You could be a nurse. You can find yourself in this publication and take away actionable information as you try to do your role in cyber safety. You can also use it as a resource to teach and educate your stakeholders, your employees, your team.

More specifically, this publication includes two technical volumes. One is for small organizations, and one is for medium and large organizations. The technical volumes really get into the weeds of implementing some of the cyber practices. But I would like to highlight the small organization technical volume.

It includes language like, "if you have a service provider, these are the things you should know about what their practices are." These are the things you should ask your service provider. "Are they doing these things within their networks, within their environment, within your EHR?" We recognize that for the small organization, you don't necessarily have a dedicated information technology or information security team, and you are relying on that third-party service provider.

MS: *Super. For purposes of our audience, I will be providing in the show notes a link as to how people can sign up for or have access to the HICP [Link: https://www.hhs.gov/about/news/2021/12/01/hhs-launches-website-405d-aligning-health-care-industry-security-approaches-program.html]. Let's move on to 405(d).*

JC: Sure. Many of the resources and products that we produce are really aimed for those who don't have the necessary resources to produce these things themselves. Also, they don't have the expertise to produce these cybersecurity materials. Materials could run the gamut of posters, infographics, and tips about everyday things that you can do... ways to start being more cyber safe, to start understanding what a phishing email looks like, and how to spot suspicious emails. It also provides tips like, "Do you know how to report a suspicious email, a potential incident, a potential breach and so forth?"

We are also holding and hosting webinars. We also produce different types of newsletters. This is a wealth of information, not just from HHS, but more so from our industry partners who are willing to share their experiences within their organization, their lessons learned.

Continued on page 110

Cybersecurity Awareness (from page 108)

Let's say they have become a victim, unfortunately, of a cyberattack and what that entails. There is a whole set of resources that I think your audience will be able to take and use within their organization.

MS: *How could a member of the audience find those resources?*

JC: We are very active on social media. We are in LinkedIn, Twitter, Facebook, Instagram, and they can follow us at Ask 405d. It is @ A-S-K405d.

MS: *Super. I think that will be helpful. Now, earlier you had spoken about cyber issues being really a part of enterprise risk management. Maybe you could elaborate a little bit more on that and tell us why we should think of cyber or include that in enterprise risk management.*

JC: I'm glad that you circled back on that because this is really a very important concept to advocate for, and to emphasize: why cybersecurity is very important and the impact of cyberattacks to patient safety.

I want to reiterate the core or key business risks or areas that I mentioned earlier: patient safety, loss of revenue, and patient data. Enterprise risk management, or ERM, is that practice of looking at your core risks as interrelated risks. It also gives you a chance to tie these risks to your mission and business impact. That's the loss of revenue that we've been talking about and how you are able to respond to a cyberattack in concert with how you are responding on the clinical operations and care delivery aspect of that cyberattack.

For example, a cyberattack can give you an opportunity to realize that there are certain medical and patient safety decisions. There are certain ethical decisions during the downtime and after the cyberattack. This could run the gamut of redirecting patients, causing interruptions in treatments that are often lifesaving, and calculations of dosages and regimens. Then also thinking about, do you have the proper contact information for your patient or the caregiver?

If you will notice, many of these things that I mentioned that could be from a cyberattack are more so from an emergency management perspective, a clinical perspective, a care delivery perspective, and contingency planning. Therefore, it is so important that cybersecurity risks are seen in conjunction, in relation to all the other risks that can affect a healthcare facility, healthcare organization, a one-physician clinic, a rural organization, all those types of healthcare providers and healthcare facilities. We should all think about these things, from an enterprise perspective.

I cannot state that enough as a very important concept. I am quite surprised that this is still a novel issue, novel topic, when we bring this up. The common questions are, "How do I do that?" And my very short response is, "You are not realizing you already do that with your other response activities," with other hazards like a hurricane, a power outage, or any other disaster.

MS: *Could you provide some tips for our listeners that they can enact right now to help protect their organization from cyber threats? Any tips for our audience today?*

JC: Sure. If you are a leader—in terms of a board of director, for example, or a CIO, a CFO, a COO—have these conversations in your meetings. Question if you don't have your chief information security officer in those meetings, and question "Why we are not, at this point in time, having those conversations at an enterprise level, in budget discussions, investment discussions?"

A quick tip that is more concrete is knowing how to identify and report email phishing attempts. This is very basic, but it is very important, because that is one of the first lines of defense. If your employees and your team members don't know how to report and don't know how to spot a phishing email, it's an easy way in. Also, never provide sensitive information. If it is an emergency and if you don't know who the source is asking for that information, always verify that the requester is who they say they are. Also, just report it if you're suspicious about an email.

Next, protect patient data. Always know and ensure that you are using encryption and know what your policies are for implementing encryption. Also, be aware that there are a lot of human nature, social engineering techniques that I mentioned earlier that ask you to email patient information. That still goes into the email phishing kind of scenario.

> **When you're accessing your organization's network, first thing I would say is to know your policies.—Chua**

Be smart when working remotely. We are finding ourselves more virtual, more remote. So, when you're accessing your organization's network, first thing I would say is know your policies. Do you have a virtual private network (VPN)? Are you accessing through public Wi-Fi? That is a no-no, in my opinion, and it's just not the best practice. It really comes down to knowing what your organization says about accessing information outside of the network. Hopefully, those top tips are very clear and actionable for everyone. **PM**

Resources mentioned by Director Chua may be found at https://healthcyber.mitre.org/wp-content/uploads/2021/03/405d-One-Pager.pdf.

Ms. Chua is Director of Governance, Risk Management, and Compliance Division within the United States Department of Health and Human Services, Office of Information Security, Washington, DC.

Mr. Sacopulos is CEO, Medical Risk Institute, and host of the SoundPractice podcast. email: msacopulos@physicianleaders.org; website: www.soundpracticepodcast.com.