HIMSS Cybersecurity Forum

Healthcare Cybersecurity: The Ransomware Epidemic

Audio Transcript

Salwa Rafee: Security is the responsibility of every single person in any organization, from the CEO to the very much smallest end user. Everybody is responsible, everybody has access to IT systems, and anybody can fall a victim to a phishing attack.

Mary Ann Borer: Hi, I'm Mary Ann Borer with HIMSS. Today I'm joined by Salwa Rafee, Global Managing Director, Healthcare Security at Accenture. We'll be talking about the ransomware epidemic in healthcare. And before we start, I'd like to say thank you to Accenture for sponsoring this podcast. Now, Salwa, thanks for joining us today.

Salwa Rafee: Thank you, Mary Ann and good morning, good afternoon to everybody out there.

Mary Ann Borer: Could you please tell us a little bit about your background and what you do for Accenture?

Salwa Rafee: Of course. So, I'm the Global Managing Director for Accenture Security focused on healthcare. So the industry is very important to us, and we have vertical expertise in each one of the main infrastructure critical industries. So I take care of our clients who are the payers, providers, and public health systems around the world. And Mary Ann, you were asking about my background. I'm a Biomedical Engineer by training, and I have spent over 25 years in healthcare IT. So, between security and IT, and digital healthcare transformation, this is what I focus on and this is how Accenture security is differentiated with.

Mary Ann Borer: Fantastic. Now, Salwa, what would you say makes healthcare so vulnerable to ransomware attacks?

Salwa Rafee: Oh, there are many reasons, Mary Ann, and, you know, the healthcare industry is one of the most vulnerable ones when it comes to cyber-attacks. There are so many reasons for it. You know, the industry is a slow adopter of IT. There are lots of legacy infrastructure, legacy networking systems and legacy software in the infrastructure in the organizations. And we see that with all of our clients worldwide. The spending as well on cybersecurity and IT is not comparable to what we see. For example, in the financial sector. If you want to get really a good benchmarking, financial services spends on average, 15 to 20% of their IT budget on healthcare. Healthcare spends 3 to 5%. So, we end up with tons of legacy infrastructure that does not cope with the sophisticated cyber-attacks that we have.

You know, the third most important factor is also the value of healthcare data that is almost 10 to 20% more than any data like credit card data or even, you know, in other industries. Typically a health record has tons of sensitive information about the patient, about their diagnosis, prognosis, treatment plans, but also about their genomics and family history data that is so valuable that cannot be changed, as opposed to your bank account or your credit card number. So these have higher price when they are sold on the dark web, and this is the much sought after data from the hacker's perspective.

Mary Ann Borer: Well, that makes a lot of sense. Now, what can the industry do to improve their security?

Salwa Rafee: Yeah, it is a journey as I always say that cybersecurity is a journey. It cannot happen in a day or a week or even a year to reach. We are working with our clients so that they can progress very positively on the cybersecurity maturity journey. And it starts with, you know, looking at first one is a cybersecurity hygiene. A basic hygiene will go a long way against phishing attacks. As an example, having a cybersecurity strategy is critical for every organization, and that should be tailored and customized to their size, to their budget, to their needs, and also to their attack service. Usually what we see that, you know, in the world and the domain of IoT and the IoMT, which is the Internet of Medical Things, with all of the medical devices, all of the electronic medical record systems, the tools that are being implemented in a hospital or a payer organization, and also the sheer volume of vendors, contractors, and partners working in any given organization, you can see how this is all a very high risk situation here.

So starting with a good strategy would go a long way for us and that's what we are trying to help our clients with. And it goes all the way with an assessment to look at the vulnerabilities of any organization. There is a roadmap that each organization should have so that they can keep progressing and keep maturing. Resiliency is number one objective that we would see in our industry.

Mary Ann Borer: Yes, that's so important, of course, to have that buy-in at every level of the organization. So who would you say has the responsibility for making those changes to an organization's security?

Salwa Rafee: It really, it's a great question, by the way, because security is the responsibility of every single person in any organization from the CEO to the very much smallest end user. Everybody is responsible, everybody has access to IT systems, and anybody can fall a victim to a phishing attack. And that's actually what the bad actors are using. A simple phishing attack or even a brute force would expose the organization infrastructure and would have access to the credentials that would enable them, you know, all of the full control of the patient data. And sometimes we see the data exfiltration or ransomware attacks happening so much often in our industry.

Mary Ann Borer: Of course. Now, what is it exactly that ransomware attackers are usually after?

Salwa Rafee: They are after the data itself. So they can do many things with their, once they have control of an organization, they can do data exfiltration, so stealing all of the very sensitive information. And so this is a financial incentive for them to have all of these data sell it on the dark web. They can also demand a ransom from the hospital or the insurance company to regain access of their organization. And what we see is that everybody wants to get back to business as soon as possible. So recovery time is critical for them to resume services to the patients. So they can pay the ransom, which is typically millions of dollars of damage to the hospital. And also they are going after the reputation of any organization.

There is a mandate of disclosure that if there is an exposure or exploitation of medical data, they have to report it to the government.

And so there is a damage with the reputation and the branding. On top of that, there are lawsuits. The patients can sue their treating physicians or a hospital or a claim information system that, you know, their data has been exposed. So it is damage on all aspects and, you know, only the bad actors and the hackers can gain from that. If you look at it from a national security perspective, if you know, a country or a state actor really wanted to damage a certain country, and we see that different actors are targeting the US healthcare system, they can paralyze the entire society. If we can't operate, if ambulance systems cannot navigate to serve the citizens, if hospitals are not open to serve and provide services to patients, this can completely paralyze our infrastructure.

Mary Ann Borer: Yes, it's easy to see that that can go really all through a society. So, how can the larger security community help to protect against these kind of attacks?

Salwa Rafee: Yeah, there are many things that they can do. And really it is collaboration, collaboration to share threat intelligence, collaboration to build the resilience of our systems. Having an incident, an integrated incident response plan is really mandatory. What do we do when we are breached, is it has to be well practiced, well designed so that it becomes a muscle memory. We don't have to think about that because everything is engaged and practiced several times per week, per month, per year. The main thing is, you know, everybody can be hacked. Every single organization can be hacked. The main thing is how resilient we are to withstand these kinds of cyber-attacks and get back to business and have data backups, have resiliency to open the doors and do the forensic analysis of any attack. And then we can give back to business to open doors again, to serve our patients, to building the resiliency is number one. And the most important thing for any hospital executives, for the industry stakeholders and frankly government entities and people, you know, companies like us who can help and support building this resiliency and the strategy and the incident response plan with our clients. This is our mandate as well.

Mary Ann Borer: Fantastic. Now, Salwa, where can listeners go if they'd like to learn more?

Salwa Rafee: Yes, so we have many assets that we are sharing with our clients and the society at large. You know, on of course, LinkedIn, great resources there. There is Accenture security for healthcare. We are publishing many points of views, many assets, contact information and actually hotlines. If any organization is being attacked or suspect that there is bad actors in their systems or they see their data exfiltrated or being sold on the dark web, they can call us and it's a hotline that they can reach our resources, we will be first to engage with them and help them get back to business to protect the patient data.

Mary Ann Borer: Well, Salwa, thank you so much for joining us today, and thank you for sharing your insights. And special thanks to Accenture for sponsoring this podcast. Have a fantastic rest of your day.

Salwa Rafee: Thank you very much for the opportunity.