(SOUNDBITE OF MUSIC)

KATE BASTINELLI, HOST:

Welcome to Perspectives. I'm Kate Bastinelli from the Greater New York Hospital Association and this is the first podcast and our three-part series on hospital cybersecurity threats. I'm joined by my GNYHA colleagues Jenna Mandel-Ricci and Zeynep Sumer King. We started recording this series in late 2019 with the goal of exploring the key roles involved in hospital cybersecurity. Zeynep, who is a critical member of our cyber team, was involved in our initial recordings.

ZEYNEP SUMER KING:

Over the last few years, we've provided cybersecurity programming, technical support, and education to our members. Our approach has always been to work in a multidisciplinary manner, urging hospitals to think beyond information technology. One of our goals is to offer our members of space to exchange information, so we saw this podcast series as a way to highlight the need for this approach to cybersecurity. We began planning by reaching out to a few key members at the forefront of cybersecurity planning and response, not just within their hospitals but also at a State and national level.

BASTINELLI:

And then COVID-19 happened.

JENNA MANDEL-RICCI:

While the critical focus of our member hospitals is taking care of patients, COVID-19 brought its own cybersecurity challenges. Huge increases in the use of telehealth, and large portions of staff working from home created new demands on IT and introduced new cybersecurity vulnerabilities. Hospitals in New York saw an unfortunate bump in the number of scams and ransomware attempts with hackers trying to take advantage of thinned resources. To counter these threats, our hospitals and health systems once again had to bring many different stakeholders to the table.

BASTINELLI:

That's Jenna, who headed up GNYHA's COVID-19 response. So, we went back to the drawing board. The first two episodes will cover the cyberworld pre-COVID.

SUMER KING:

These interviews are still relevant, maybe even more so in a way. The principles that govern cybersecurity preparedness, response, and cyber hygiene remain the same during the pandemic as they were pre-pandemic. The first two episodes will discuss the need for inventory management, adequate risk

assessments, encryption, and educating your staff on cyber pitfalls. And the third will cover the changes to the threat landscape during and after the pandemic's peak in New York City.

BASTINELLI:

In today's episode, Zeynep interviews Kris Kusche, the Vice President and Chief Information Security Officer at Albany Medical Center. Let's get started.

SUMER KING:

So Chris, can you just introduce yourself and tell us a little bit about Albany Medical Center?

KRISTOPHER KUSCHE:

Sure, so I started Albany Med back in 1993 as the biomedical engineer for the organization. At that time, cybersecurity really wasn't a topic, it wasn't really an industry at the time, very little being done within health care. When HIPAA came around that changed a lot of things for health care and in the hospitals across the country, and in 2004 I was made the information security officer and at that time that was purely around HIPAA. The organization's grown. We have an academic medical center; we have a college—Albany Medical College—we've now affiliated with two other hospitals. We also are pending another hospital affiliated with the organization and our system is continuing to grow throughout the upstate region.

SUMER KING:

That's a lot of change. There's also been a lot of change in the outside world outside of Albany Medical Center. We've moved much further away from HIPAA being the only concern or priority as it pertains to cybersecurity. What are your greatest worries, currently, related to hospital cybersecurity and for your whole health system?

KUSCHE:

I think the real issues are the things that are evolving, the things that we don't know about. We know about a lot of things, but there's always a change in the cybersecurity landscape. As the technology changes, so do you do threats in the vulnerabilities to that technology. Whether it is the traditional IT technologies, your computers, your end-use devices, or it's the other hospital equipment that is becoming much more prevalent in our hospitals now, at least that the provider level, are medical devices. Medical devices are starting to outpace traditional IT devices two to one. So, my hospital, my main medical center has about 10,000 IT devices. We have about 20,000+ medical devices and at least half of those are on our network.

SUMER KING:

So does that change how you strategically approach cybersecurity? How has it evolved over time?

KUSCHE:

I think it changes in a couple of different ways. It changes not only what you need to do technology-wise, but it means a change at the organization level, at the people level, at the process level, because now you're not just talking about traditional IT staff, you're talking about your biomedical engineers and those folks that are now key to more than half of your inventory. The problem that we have is that we have two different types of educational and experiential sets of people, right? The biomeds and the IT folks, and I represent both. So, I have a lucky world I guess, in that I see both worlds and I have some control over both worlds, and it really requires that we bring the skill sets of both into some type of blend and I'm not advocating that we eliminate one or the other or we consume one or the other. I don't think that's necessary for that blending to occur, but there is an overlap of the skill sets that needs to happen and get brought together in order to effectively manage not only our IT devices but now that emerging class of not only biomedical devices but IOT devices, the Internet of Things devices.

SUMER KING:

Okay so, what does that looks like in a hospital or health system where they are not lucky enough to have one person who can cover both the cybersecurity side of things and biomedical engineering? What are some best practices around coordinating or mixing those skill sets as you said?

KUSCHE:

Number one is always leadership. Leadership is key to establishing the relationships and establishing the agreements on how you're going to handle those types of devices. I think the way we approach it is that regardless of whether it's a biomed device or a traditional IT device, the rules of the game apply to both. So, the same set of rules have to apply to the entirety of your inventory regardless of where they sit managerially. So, however a hospital decides to break that leadership role up, to break the managerial role up, to break the cost base up, however you break it up in an organization, it's really key that the same rules apply across the board, because otherwise you're going to have a fractured system. You'll have devices that are handled differently than our traditional IT space, and quite frankly our IT folks are experts at cybersecurity. They have that core set of competencies, and our biomeds are expert at patient safety for medical devices and understanding how devices are used within the health care setting, that's their expertise. So, you really have to have that melding from a leadership perspective and again it doesn't mean that you have to combine departments, but you have to have leadership that agrees how you're going to handle all the devices across the medical center or across the hospital.

SUMER KING:

That’s easier said than done.

KUSCHE:

It is, it is.

SUMER KING:

But really, really important. So obviously medical devices are of huge importance for a health system. What are some other concerns though? What are your other priorities as the CISO for your health system that, so to speak, keep you up at night?

KUSCHE:

Medical devices are absolutely, and IOT devices, I think are the emerging threat that's out there, are the emerging vulnerability that we are facing in health care. And the reason that's the case is because they're a little different technology-wise then traditional desktops, laptops, printers, things like that. They're designed differently. They don't typically speak the same type of communication languages that our traditional IT devices speak, and because of that our traditional IT toolsets can't visualize, can't manage medical devices like we can a traditional IT device. So, it's really causing the need for an emerging toolset to look at how medical devices are presenced on your network. How are they acting? Who are they talking to? What are they running protocol-wise? What are they running application wise? Are they doing to the right and normal things that you would expect a device to do? As an example, if I have an infusion pump on my network and I see that it's talking to you what country outside of the United States we have a problem, probably, we have a problem and we know what a device should act like and the emerging industry that's coming out right now is really about anomaly detection. So, we need those types of tool sets to manage and visualize our medical devices in a way that is just not capable right now with traditional IT tool sets.

SUMER KING:

You mentioned leadership earlier and there's obviously hospital leadership and then there's other departments outside of IT and even biomedical engineering that will, in the event of a threat or an attack, become involved. If you could advise a group of hospital CEOs and also maybe other leaders of one thing they could do better to secure their facilities what would that be? What's the one in silver bullet, greatest bang for your buck?

KUSCHE:

Alright, so, technically, I'll talk about the technical piece. Honestly, I believe the most impressive and impactful technology that anybody can put in place right now based on the vulnerabilities and threats for us, it was multi-factor authentication. Hands-down, across-the-board, multi-factor authentication has the capability of stopping email compromises dead in their tracks. For the most part. From a non-technical perspective, I think the biggest thing that our leadership can do in the health care industry is make sure that there's an awareness and I speak of it in a little different sense because I grew up in the JCO world. I grew up in the Joint Commission World, in that, you know, I grew up in health care ever since I was a 22-year-old kid starting out in health care and Joint Commission and that process, that culture of safety, that DNA. It's almost like DNA that The Joint Commission kind of becomes in your health care life. If we can get security, cyber security to be that DNA, another strand DNA that runs through, so that it doesn't always become a special request, it doesn't always become, "hey, I got WannaCry and need money," or "hey, I've got this cyber threat going on and I need money or I need you to do something," if we could get to the point

where our organizations just consider cybersecurity as another strand of DNA that has to be done, I think that would be, that would be such a great, I don't know if its an end goal, but I think that would be such a substantial milestone that we could achieve is an industry.

SUMER KING:

Yeah, just an innate part of doing health care business in the world.

KUSCHE:

That’s right.

SUMER KING:

That’s great advice. So, that's all within the hospital, but obviously in the event of an attack there are external entities that would become involved. How can your external partners, law enforcement; FDA; us, Greater New York Hospital Association; federal agencies; and others most effectively support you both as you prepare and in the event of an attack?

KUSCHE:

So, let me break it down. I think you'll find the law enforcement agencies, again above I would say at the state level, at the federal level, are all very engaged, are all willing to engage if you ask them to. You know they can bring resources and they can bring competencies and intelligence that you may not otherwise be able to get. So, I think of establishing a relationship with your, especially with your local FBI organization is key for any organization. From an industry perspective, whether it’s the FDA, whether it's any of the other industry organizations or social groups, whatever it may be, I think we need to push as an industry. We need to push for standardization of cyber security requirements and specifications, and there is a push now in the country with the FDA, at the at the federal level, to get more standardized understandings with our vendors and with our organizations, our provider organizations, of what is it that a medical device needs from a base level of security? What are the things that we don't have control over as a user that we rely on our manufacturers and our government organizations, our regulatory bodies to enforce and ensure? And when we have a lack of those things or where there's a gap, then it's up to the providers to have to implement all of these security measures and in mitigating strategies and what have you. So, if we could move that ball to really look at our medical devices as something different, as something that's susceptible and vulnerable to the same threats that our computers are, and that's a big ask, and the reason it's a big ask is because look at the life cycle of a medical device compared to a traditional desktop. Most people are flipping desktops 3 to 5 years. A traditional medical device, an IV pump 7 to 10 years, maybe more depending on your ability to replace. So, we need to leverage all of our power as providers, as industry colleagues, to really push that meter to a point where we're comfortable and where we’re at least getting a basic level of protection.

BASTINELLI:

In the next episode, Jenna will interview Dr. Mark Jarrett, Senior Vice President and Chief Quality Officer and Associate Chief Medical Officer at Northwell Health. Until then, this has been Perspectives.

(SOUNDBITE OF MUSIC)