(SOUNDBITE OF MUSIC)

KATE BASTINELLI, HOST:

Welcome to Perspectives. I'm Kate Bastinelli from the Greater New York Hospital Association and today I interview Tom Mustac, Senior Director of Security at the Mount Sinai Health System. Tom's work connects the operational, biomedical side of the business to IT, networking, and cyber-security. I asked Tom for his perspective on cybersecurity in this post-COVID environment.

Thank you for speaking with us today, Tom. What are your greatest worries related to cybersecurity for your health system and for health care institutions in general?

DR. TOMISLAV MUSTAC:

I'd say the speed at which we can react to situations. The bad guys never rest and we're truly outnumbered by them, and an interesting quote I heard the other day was someone said, "industry competes while bad guys to collaborate." That's very true, they do work together. They share are a lot of the codes, a lot of the vulnerabilities that we see hitting us are reused or repurposed from previous attacks, previous other industries, and they seem to work well and share information. Maybe even quicker than industry does in some cases, and in the cybersecurity space all it takes is one entry point to sink the ship so it's important that we can react quickly enter very cognizant of our environment at all times.

BASTINELLI:

That's a really interesting quote. How can we, as a healthcare ecosystem, learn to better collaborate where appropriate rather than compete to our own detriment?

MUSTAC:

I would say that one of the most important things is to develop our critical relationships before we need them—that's both internally within our organizations and outside across industry. There are a lot of organizations that many of us are involved in, like the healthcare-ISAC, InfraGard, CISA, and there's a lot of good information shared. But they need to, or we all need to, dig in deep and not only take information away from these organizations but bring them to the table so that we can share our concerns and what we're seeing so that we can all be smarter and able to react quicker.

BASTINELLI:

How has Mount Sinai's understanding of cybersecurity threats changed over the last five months? And how has that translated to how you approach this issue internally?

MUSTAC:

They are very aware of the issues in the cyber landscape and they have a robust process and broad systems to stay on top of things. So, the biggest changes are that the frequency of attacks across industries are changing, the intensity of them, there's no cost of entry for people to attack other enterprises. There's plenty of free tools out there and we're seeing now that we're getting new manufacturers as well for equipment. The COVID crisis brought in a need for additional equipment, right. There was a lot of news coverage on ventilators which brought companies like Ford Motor Company and Tesla to the table to produce ventilators and it's not a space that they've ever truly operated in. So, because of the expediency and how quickly they're bringing these things to market, it does make everybody worried about how they're going to integrate and how those devices going to be protected.

BASTINELLI:

So how can organizations keep up with the evolving changes in the threat landscaped?

MUSTAC:

I would say communication and collaboration are the most important things between your team's internally. Make sure that your teams are interacting, that they know all the components of your organization—who does what where—and that will start them thinking about how they can support each other, and they'll understand when there is a crisis, they'll already know who to go to when they need that support.

BASTINELLI:

I would imagine that's also been important in your response to the COVID-19 pandemic. Let's turn to that since that has consumed us all for the first part of this year. What has been the most challenging aspect of responding to the COVID-19 emergency and at the same time maintaining cybersecurity at your institution? Were their specific cyber threats that were unique to this emergency?

MUSTAC:

I would say that the biggest threats were the massive amounts of change being introduced to organizations. Because of the influx, large influx of patients, we need a lot more equipment from the existing manufacturers that we've been dealing with and we're comfortable with, and then on top of that we're also getting equipment from new manufacturers that are new in the space. We've also seen a rapid expansion of telemedicine, a rapid expansion and facilities in the number of beds, the introduction of more remote video monitoring and other technologies to limit the patient contact and staff exposure. So, in summary, just a massive amount of change in a very short period of time and we also changed how we operate. Most of us went into long periods of working remotely and working different hours that we normally work with and anyone that wasn't comfortable with remote technologies like Zoom and Skype instantly became an overnight expert and we're living on these technologies today.

BASTINELLI:

If you could advise a group of hospital CEOs of one thing they could do to better secure their facilities, what would it be?

MUSTAC:

The most important thing, as they said earlier, is the communication. Not only establishing the relationships needed inside the organization but also outside with industry groups and especially the manufacturers of equipment. There's been a lot of discussion over the years about what needs to be done. We've all heard about manufacturers being reluctant to get into the discussion of cybersecurity because some of this equipment has been developed a long time ago. They're using, some of them are using outdated operating systems. Some of them have outdated firmware and it was never the expectation that people would be interested in harming others with medical equipment. Well, fast forward to today, the world has changed, and we do need to secure these things that we are going back to repave old roads and we need the engagement of the manufacturers in the discussion to make sure that we can properly secure them and do it in an efficient way. I would also say that you shouldn't waiver from your side of security principles during the crisis. As we've seen during the COVID ramp-up that we went through with adding so much more equipment and different equipment and operating new spaces, it's important that in spite of all the pressure we're getting to make things happen extremely quickly, we don't cut corners, we don't disable controls, we don't cripple things in order to get them up and running. It's just as important to get them up and running efficiently and safely as it is to do it quickly.

BASTINELLI:

What can health systems do to ensure that in the event of an emergency they don't, as you said, waiver from their cybersecurity principles? What are some plans we can put into place now to address the demands for expediency in event of an emergency?

MUSTAC:

I would say that it's very important to remember the lessons and experiences that we have been going through over the past couple of months. We know the requests that we received. We know how we responded to them. We know the issues that popped up along the way they were unanticipated and forever we have been doing desktop exercises and planning and preparing for emergencies, but we also need to make sure now that we take those lessons learned, reapply them back into our plans and our playbooks and that we continue to be resilient so that we not only have a plan A, but also Plan B, a plan C, or a plan D. I think the ventilator issues that continuously comes up in the press was a great example. When we couldn't get ventilators anymore, we saw a new manufacturers pop-up. We also saw new clinical methods where ventilators were being shared. So, those are just some examples of how we need to continually keep our eyes open, be aware of the landscape, be aware of all of our resources and the collaborations that we built, so that we can continuously adapt as we go through an emergency and keep leading back into it so that we can continue to grow and expand.

Thank you for joining us on the three-part deep dive into hospital cybersecurity. Until next time, this has been Perspectives.

(SOUNDBITE OF MUSIC)