Eye on Security Podcast

Protecting Healthcare and Academia Against Cyber Threats

Transcript

Luke McNamara:

Welcome to another episode of The Eye on Security Podcast. I'm your host Luke McNamara. Joining me today for what I think will be a very timely discussion we have Monte Ratzlaff, a System-Wide Cyber Risk Program Director at University of California Office of the President. In his role Monte participates with University of California leaders to establish cyber risk strategic plans and objectives. He also leads the UC Health Chief Information Security Officers from each UC Health location in various information security-related initiatives. In his prior role at UC Davis Health System Monte managed the IT Security Department and also served as the Chief Security Officer. Monte also has over 20 years of experience in cyber security within the finance and healthcare sectors and holds multiple professional designations and has presented at numerous conferences and webinars and it's great to have him here. Monte, how are you today?

Monte Ratzlaff:

Good Luke, how are you?

Luke McNamara:

I'm doing well and I'm looking forward to this discussion and maybe where we can start is I gave a little bit about your background but I'm interested in hearing more about what is your team's mission and focus at the UC and how do you work within the UC community?

Monte Ratzlaff:

So my team is called the Cyber Risk Coordination Center, otherwise known as C3, and our primary goal is really to support the cyber risk reduction efforts and activities programs across UC. Some of those programs are Threat Detection and Identification Program, we support security awareness by coordinating the Security Awareness Workgroup across the system, as well as the Security Awareness Training Program that is mandatory for all faculty and staff across UC, we have a Cyber Champions program that we help support, and these are location-based programs that really are a force multiplier for their different security awareness effort. So Cyber Champions typically are folks who don't necessarily work in technology but they are nonetheless interested in cyber security and want to participate in getting those messages out.

Another effort we do is our biannual Cyber Security Summits. We hold those twice a year and

we just finished our tenth biannual Cyber Security Summit. What we do is bring together speakers from all over the nation in different fields of expertise so these aren't just cyber security experts; sometimes these are legal experts, sometimes these are folks who specialize in medical research, but they all have a spin around cyber security and cyber risk. And our attendees are also diverse coming from privacy, legal, procurement, security obviously, and those folks come together to hear about different ways to protect themselves and protect their organizations. We have participants also from outside of the UC with our partners at the California Community College systems and the California State University systems.

One of our key stakeholder groups is the Cyber Risk Governance Committee. This committee is made up of cyber risk executives from each location of our 10 campuses and these are not necessarily also technology folks but business folks who focus on cyber risk and how it impacts the business because at the end of the day that's really sort of where it hits. And then just 1 other thing I want to touch on is our support of our IT Security Committee, which is a group of CISOs from across all of our locations that come together once a month to talk about different initiatives, efforts, and issues. So that in a nutshell is sort of where we focus our efforts.

Luke McNamara:

It sounds like you have a very holistic view of security and the reduction of cyber risk that you're kind of approaching this and I wonder if you could give folks a sense of – I mean you mentioned quite a very broad set of certainly all the different participants of the UC system, all the different universities and colleges. What are the sorts of assets and users and systems and networks very broadly again because that's a huge category of things that you're charged with helping people secure and protect, but what does that typically look like in terms of the types of things that you're focused on protecting?

Monte Ratzlaff:

Well our primary user base are obviously the staff, the faculty, and the students. You know we do, because we're health systems, we do actually have public users so these would be patients of our different systems that support patient care. The type of assets really is sort of also a broad gamut. We have regulated and unregulated data, we've got protected health information, PHI, we've got payment card data so we have a PCI space, we've got FERPA data, which is student data, and then research data, which you know research can be regulated and it also is vast amounts of non-sensitive, unregulated data that's tied to research that we wouldn't necessarily want to be either disclosed or stolen or lost. So there's a really broad swath there.

The threats that we face are not uncommon to those of really any industry. We definitely get hit with phishing, we have CoinMiner attacks, we have ransomware espionage, we have Nation State threats, and then insider threats. So in some ways we're not that different and in other ways obviously with faculty and students we're not like a bank. So there are some nuances there but for the most part we really run like another organization in terms of paying attention to the threats to our data and our people.

Luke McNamara:

Well and I think this is what is particularly fascinating to me and part of why I really wanted to have this discussion because as you mentioned these threats aren't especially new but I think they've come forward to the public consciousness and awareness more than ever before this year and that's really because the twin threats, at least 2 of the threats that organizations like yours face, which is theft of IP/theft of research, the concern around that, and just today there was an article in The Wall Street Journal talking about North Korean threat groups joining Russia and Chinese and Iranian and other entities targeting COVID-19 research and in the middle of the pandemic the continued and growing importance of that data and I think the realization that universities and research institutions kind of sit in the center of this ecosystem between pharmaceutical organizations, public health entities.

So you have all of that, which is again I think coming to the forefront because of the COVID-19 pandemic and then you also have the threat from ransomware, which we've seen grow this year and for universities that are involved in running and maintaining healthcare systems increasingly having to deal with that. So maybe we can tackle the COVID-19 research bit first, but as you're thinking about that and as you're thinking about securing that data how do you think about that? How do you think about the steps that kind of need to go into that as this work is so critical right now?

Monte Ratzlaff:

Well as an academic, medical, research I would say leading in that space we definitely have the COVID-19 research trials, we have vaccine research; there's a lot of things that make us a target. But at the end of the day we have to be prepared for sophisticated, potentially Nation State APTs, who also want to get their hands on the research that we're doing. Their governments may not be able to afford or have the resources to do this research and so they're highly interested in obtaining it. We have to be diligent in detecting and responding and just an overall resilience when it comes to back-ups and basic hygiene and awareness because you know we know that the people are who typically are that first target. They're the way in. We have to look at our threat intelligence around who are these actors, what are their tactics, techniques, and procedures, what are their main focus points on what we're doing. And just that solid defense and being prepared is really key for us. It's – obviously COVID-19 brings that to a finer point but we have to do this every day because of all of the different things that I mentioned prior in terms of our research but particularly because of COVID-19.

Luke McNamara:

And you had mentioned the human component of this and I think another fascinating area and 1 that I'm sure must be a challenge sometimes working within the university space, higher education university is known for being very open environments focused on collaboration, which isn't necessarily something that always goes hand-in-hand with good security practice and hygiene and securing networks and ensuring the right data and research is segmented off, proper security protocols are being followed. How have you found it in terms of working with all these different parts of the UC in having users become educated as to the risks they face? How has that process been in terms of that conversation with them?

Monte Ratzlaff:

Well we've taken an approach years ago with requiring information security awareness. And I think early on it was our first and best effort that has since grown over time, I mentioned our Cyber Champions program, and we recognize that having the click-through slide-show is not always that effective. So we've tried to focus more on getting messages to people in ways that they understand clearly but also are engaged, making it make sense to them. And sometimes that's around including things that help them in their day-to-day practices, staying safe online at home, and so it resonates with them that when you're talking about some of these good habits that helps them protect themselves whether it's their online banking or all the different things we do online with shopping, credit card, et cetera. The good habits translate for both at the organization level and at the home level. We've steered away from the 'thou shalt nots' and really focused on what are the good habits, what are the things that you can do, so it's more of a positive approach because I think that resonates more with people instead of being told what not to do.

Luke McNamara:

Do you think there's also been some impact around the fact that I would imagine there's a lot of folks still working from home that you're working with in terms of users and it seems that in some cases users, individual users, are more aware of cyber security threats because they hear about this a lot more in the news, that sort of message around giving you things that make your day-to-day more secure, is that message do you see translating more in the era of COVID where maybe folks are a little bit more aware of okay now I'm working from home, I need to be more careful about what websites I'm accessing, how I'm securing my personal devices that are on the network? How has that impacted or played into the strategy that you're trying to push?

Monte Ratzlaff:

I don't know if being at home or even COVID has been in and of itself increased awareness or increased vigilance, but we certainly have focused on sending out those messages to make people aware that this is a threat. We are seeing fishing emails directly targeting COVID-19, not necessarily in the sense of trying to perform espionage, but just the normal tactics of a fisher to say, "Here's the latest and greatest thing that I think you'll click on if I make it sound interesting or compelling." And so we've definitely made a concerted effort to get those messages out there to say, "Here's what we're seeing and here's what it might look like or here's what we're seeing across the world even if we haven't seen it yet," and just trying to get those messages out as best we can because you know it is a different world. With almost all of our organization working from home it's unprecedented and so we've got to continue that diligence and that messaging and we have to rely on people to resonate with those messages and pick up on themselves following those good habits.

Luke McNamara:

Beyond just security practices and security hygiene have you seen a shift or a change over the years particularly amongst researchers that are working on the types of data you mentioned before, either data that's controlled or regulated in some way and is sensitive or even data

that's sensitive but maybe doesn't have particular controls around it? Do you see more of an awareness on behalf of researchers that there are entities that want to target that data, that want to steal that data, that they are at risk from?

Monte Ratzlaff:

We've seen a heightened sense of awareness from the researchers who are directly involved in COVID-19 research. I think the broader research community we still have a challenge in getting those messages to them. I think where a lot of universities face those challenges is engaging with the research community. The researchers have a great deal of pressure to get their grants, get their contracts, and fulfill those grants and contracts with their work and do it in such a way that's effective and productive. And we as a security community have not done a great job at getting those messages to the researchers in compelling ways because I think historically we've been seen as a barrier, we've been seen as a roadblock, and we've got to do much better at providing the resources that fit the researchers' needs and then messaging them to let them know that we've got those resources. So it's not 1 of those things where if you build it they will come; you've got to build it, you've got to make it easy, and then you've got to let them know that it's there and I think we're working on that at UC. There's some things actually we're doing right now to address that very issue. We've got a ways to go.

Luke McNamara:

Yeah. It seems like a constant challenge in security and I think that approach of making them aware of how you're there to help them and you're not just there to be a roadblock and tell them you can't do something, you can't plug this in, you can't access this with this system. That seems like it would go a lot further in helping build those bonds that overall you need to to grow their awareness and their understanding of you're there to kind of protect them and their systems and the research they're doing.

Monte Ratzlaff:

Yeah and it's not a new thing for security to be perceived as a roadblock. I think that's still something that we still have challenges with in just general organizational environments where the average end user sees sometimes security as a barrier and we're still not that good about making security be sort of invisible where it's just part of your routine that it's just secure and we still have that challenge. So we certainly haven't achieved perfection there and with research it's probably even more of a challenge.

Luke McNamara:

I want to switch gears a little bit and talk about the threat also from ransomware that we've seen this year. In particular obviously it's something that is disruptive that has the ability to impact and increasingly the concern is the impact of healthcare facilities, healthcare providers, and for organizations like the UC that are involved in running health centers some of the concerns around not just again theft of data, theft of research, but maintaining uptime of critical systems. How has the state of ransomware attacks that we've seen this year impacted how the UC system is thinking about security in particular of healthcare centers?

Monte Ratzlaff:

I think at universities and really other organizations we have to know our environment. That's 1 of the key things that we've learned recently. It's not that we didn't know that before but we saw how critical it is to understand what is on your network, where is the data, what is the data, and knowing that is the first step because you can't secure it, you can't back it up, you can't make it resilient if you don't even know that it's there. And so that's – to me having that solid understanding is sort of the first starting point. The normal hygiene that we've heard for a while now isn't different. It's still practical, which is you've got to back-up your systems, you've got to back-up your data, but you've got to also make those back-ups secure that in the case of a ransomware that those back-ups themselves don't become ransomed.

You've got to be able to test the recovery from those back-ups. Having the back-ups but not knowing if they're going to work when you need them is not the full picture. You've got to be able to test the recovery and then that response is so critical as well. So having your instant response plan in place, training your team, testing the plan is really key because when you're in the incident that's not when you want to find out that your instant response plan has holes or your team doesn't know how to proceed or isn't sure who's in charge. It becomes chaotic even more when you're dealing with already a chaotic situation.

Luke McNamara:

You're describing how you have to think about this from a broader strategy, having your incident response playbook, and I'm curious with this activity that we've seen this year where so many of these groups are incorporating data theft and then leaking that data as another way to extort victims how has that changed how you think about responding to these sorts of threats given that you now have to be concerned with maybe PII, PHI being leaked out? Has that changed how you think about responding to these sorts of campaigns?

Monte Ratzlaff:

It's definitely a challenge. Even if you've done all of your good homework, you've got solid back-ups, you've got your incident response plan ready to go, the disclosure extortion tactic is still problematic because that data is now no longer in your control and even if you can recover the bad guy has your data. And even if that data's not necessarily regulated it could still be proprietary, sensitive in some way, and so it's definitely a larger threat than just the typical ransomware where you can recover and you can move on. For us it definitely brings into questions of precedent, it brings into concerns of some of the new guidance around paying a ransom and not paying it to a country that is sanctioned, so there's new things that are coming out that we have to pay attention to. I don't know if there is a silver bullet to solve this new threat. We have to just continue to do our best at being resilient against those attacks.

Once that data is out there even if a threat actor says, "If you pay the ransom I'll destroy the data," I don't know that I would feel a whole lot of assurance that that threat actor is going to keep their word. So it really comes down to being as resilient as you can to avoid it in the first place because I think once it's out there I'm not sure you can do a whole lot about it.

Luke McNamara:

And have you found there to be benefit to the sort of work that you and your team have been doing for a while around bringing in these other stakeholders, bringing in people that are focused around the sort of business process, not just engaging with the IT security folks, but all these other groups that have to have some sort of seat at the table or stakeholders to when an incident like this happens and you have to engage coms and these other groups have you found that the work that you've done helping educate them, helping them be aware of these sorts of emerging and trending threats, that that's been useful when you have to deal with these sorts of incidents or when these things come down the road?

Monte Ratzlaff:

I think the most useful is the fact that if something like this does happen it isn't a surprise. It also allows the other potential impacted stakeholders to take the information and to identify if there's anything similar happening in their space. So leveraging that threat intelligence, leveraging the awareness of what might be live in the wild at the moment, and then sort of doing that in a concerted way across our system is really why we even have the Threat Detection and Identification Program is for visibility, for sharing information, and for being able to answer those questions of did that happen to us and I think that's where it comes in handy.

Luke McNamara:

I think most of the examples we have seen to-date with ransomware impacting hospitals have been mostly in the IT network and business systems being impacted. Of course that can have cascading impacts, but I'm curious what you think about threats to biomedical devices and potentially that to become another front in the sort of concerns and risks that organizations involved in healthcare have to think about where the most critical, life-giving systems could be impacted as we go forward in some of this sort of activity?

Monte Ratzlaff:

So for us biomedical devices, and this is true for any healthcare environment, hospital environment, biomedical devices have been around for a very long time, even before this thing called an IT department. And so we're just now, even though we've had that legacy, we're just now starting to get good at identifying the devices on the network. We have newer emerging technology that has these libraries to be able to fingerprint if you will medical devices on the network so that IT and security folks can even know where they're at. That's sort of the first step in protecting as I mentioned before is knowing where it's at and what it's doing.

The devices themselves another challenge is they're legacy devices; they're running outdated code. And being able to secure that or patch that is sometimes just not practical. These devices are often costly to replace and so the budget's not there to just rip and replace. When you're talking about let's say a CT machine that costs millions of dollars and it's running an outdated set of code that's not something you just pull out and put a new one in. And so we have those challenges across all of healthcare really.

The good news is manufacturers are starting to get better at security. It's been a long fight and

a lot of really smart people working with the manufacturers on how they can better secure their devices from the beginning, but we're going to be in a mixed environment with these new devices and legacy devices for some time to come. So again you've got to focus on that inventory, know what's out there, know where it is, bring in that ability to monitor for threats, and network segmentation is really an important aspect of protecting those devices from the rest of your network, protecting them specifically because of those different threats. Biomedical devices are not something that you can just scan with a vulnerability scanner. Oftentimes you'll knock them offline or you'll render them useless and you have to restart them and it's a very disruptive thing in a hospital. And so it's a delicate piece of equipment but you've got to protect it, you've got to segment it, you've got to be able to know what's going on in those environments to have the assurance that you're going to need to keep those types of devices secure. They're not laptops. These are very different types of devices and you have to treat them as such.

Luke McNamara:

It seems hearing you describe that in some ways it reminds me of the sort of defense in-depth strategies that you see others in other parts of operational technology or cyber-physical systems security focused around. Are there areas where lessons learned from securing properly segmenting IT and OT networks, where those can be increasingly brought to bear in the security of biomedical devices?

Monte Ratzlaff:

Certainly. It's a very similar approach when you're talking about OT SCADA systems and such. They're very similar where they're not just a laptop; they're running outdated code. They do very critical things. They're not necessarily hooked up to a patient but they're still in charge of different things like keeping the refrigerant at the right temperature for medications or keeping things running in the building; those are obviously very critical things. So there are definitely lessons learned and similarities between those 2 types of environments and 1 can learn from the other.

Luke McNamara:

So with all of these different security threats and challenges that you have to face and contend with, everything that we've talked about today and I'm sure a lot more we didn't have time to discuss, I don't know how I could sleep at night if I had your role and the challenges you have to deal with, but I'm curious any sort of closing thoughts or predictions you have around some of the things that the healthcare space, the academic research space will have to contend with going forward in the future?

Monte Ratzlaff:

I think that due to the pandemic I wouldn't be surprised if we see more around insider threats. You know we've got the potential for espionage; we've got potentially disgruntled employees. It's not just UC; I'm speaking across the nation. When we're talking about the pandemic and its impacts on the economy folks might be scared, they might be fearful, they might be upset, and sometimes that motivates people to do things they wouldn't normally do. And I think there's

potentially a sense of this psychological anonymity. You're sitting in your house, you're not sitting in an office, there's no one there to make you feel in-check, and so there's that psychological aspect of if nobody's watching me maybe I can get away with something. And so I just wouldn't be surprised to see a potential uptick in insider threats.

I also think ransomware and espionage by Nation States could be something that we see more frequently. We're definitely seeing a lot of it but I think as we talk about changes with COVID-19 vaccines and research there's definitely going to be a focus on that from the Nation States. And I think lastly phishing isn't going away. We're going to continue to see better phishing, we're going to see different tactics, we're going to see the phone and text messaging rise in phishing. The bad actors are going to find a way. As we get better at defenses they're going to get better at finding ways around those defenses.

Luke McNamara:

Yeah, all good points. Certainly the point you made around espionage activity and ransomware I would very firmly agree with. And I always wonder and the question for both those types of threats, both those types of motivations is always beyond what network defenders are doing to counter those threats, beyond what others are doing to disrupt those threats, how will governments respond? Will we see some sort of law enforcement response to something like ransomware, particularly now that it's impacting hospitals to a much greater degree? Will we see increased diplomatic even response to things like the targeting of critical research like the COVID-19 vaccine and treatments? And I think those will be interesting things to look for if that shapes adversary activity at all or if we still continue to see many of the same groups and actors that have been carrying out these campaigns continue doing so. But I think certainly at least for the near future those will both remain 2 big threats that organizations will have to continue with. Monte, thanks for your time, your very generous with it, and thanks for the insight into the types of threats that organizations like yours are contending with and dealing with and securing against.

Monte Ratzlaff:

Luke, it's been a pleasure chatting with you. Thanks for having me.