**Public Sector Future podcast**

**Episode 21**

**Transcript**

**File: Public Sector Future\_EP21-Mary Ann Blair-Carnegie Mellon-Reference.mp3**

**TRT: 34:25**

**Talent:**

**Olivia Neal [host]**

**Mary Ann Blair, CISO for Carnegie Mellon [guest]**

**OLIVIA NEAL:**

Hello and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches in the public sector to deliver better outcomes. I’m your host, Olivia Neal, and together we explore stories from around the world. Throughout the series we discuss technology and trends, as well as the culture aspects of how to make change happen.

I’m joined today by Mary Ann Blair. Mary Ann is the Chief Information Security Officer at Carnegie Mellon University, in the USA. Together with her team, she protects the campus from cyber threats that attack the confidentiality, integrity and availability of information and systems.

As you’ll hear in our discussion, Carnegie Mellon is a global research university, with almost 15,000 students from over 100 countries, and has a particular history in leading cyber security research. This context provides both opportunities, and challenges, for Mary Ann’s role.

Mary Ann, welcome to the show.

**OLIVIA NEAL:** Hello and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches to deliver better outcomes. I’m your host, Olivia Neal and together we explore stories from around the world where public servants have been successful at delivering change.

Today, I’m joined by Mary Ann Blair, the chief information security officer at Carnegie Mellon University in the USA.

Mary Ann, welcome to the show.

**MARY ANN BLAIR:** Thanks, Olivia. It’s wonderful to be here.

**OLIVIA NEAL:** Well, maybe we could start at the top. Could you explain to our audience your role as a chief information and security officer? What are you responsible for?

**MARY ANN BLAIR:** Well, the way I see my role is I’m responsible for collaborating with our global community of faculty, staff, students, alumni, parents, affiliates, as well as internal service providers and external research sponsors, our vendors, our regulators, our sharing communities, professional associations and even law enforcement, to ensure that Carnegie Mellon, its community members, its computing infrastructure, our information assets, our research data, intellectual property is protected from and resilient to threats, whether those are internal, inadvertent threats or external, intentional threats.

Our end goal is to enable and support and actively participate in the University’s mission of transformative teaching and learning, research and entrepreneurship, artistic expression and creativity, and ultimately societal impact through knowledge, transfer and innovation. So it’s a super exciting role in a very vibrant community that is on the leading edge of many disciplines.

**OLIVIA NEAL:** Wow, what a broad ecosystem you’re working within, because I have to admit, when I was first thinking about this space, of course, I was thinking about the students and the faculty and the research. But this much wider perspective that you’ve got is really interesting, thinking about that global community of people engaged in the university in all sorts of different ways, and really interesting set of stakeholders for you to engage with and work with.

**MARY ANN BLAIR:** You know, it really is and the engagement is sort of broad and deep. We’re a global university. We have campuses in Qatar and in Africa and programs in lots of places in the world.

And one of my challenges as part of security operations is to cover 24 by 7, 365 security monitoring, and that can be a challenge in terms of recruiting a workforce, especially when you think about shift work.

[TCR 00:03:10]

To conquer that, we actually engaged with our campus in Doha and we stationed one of our resources on the Doha campus in Qatar.

And so, that was a great approach of partnership and collaboration, where some security monitoring is happening in other parts of the world.So, yeah, so it provides many advantages.

**OLIVIA NEAL:** Yeah. Some real, real opportunities to be taken advantage of there with that global perspective.

And you mentioned that this is a particularly kind of dynamic and interesting environment to be working in, in Carnegie Mellon, to be the CISO there. Could you tell us a little bit about the role of Carnegie Mellon historically in cybersecurity and what role it plays now?

**MARY ANN BLAIR:** Sure. Well, Carnegie Mellon prides itself as being the birthplace of the first computer emergency response team. So back in the late ‘80s, the Morris worm hit the Internet. That was the first major Internet worm. And suddenly, lots of folks were concerned about cyberthreats as a result of this proof of concept.

So at the time, Carnegie Mellon, through its Software Engineering Institute, was world renowned for developing the capability maturity model for software. DARPA, the Defense Advanced Research Projects Agency, in the U.S. here commissioned the SEI to develop a response capability.

So that came to be known as the CERT Coordination Center at Carnegie Mellon. Their responsibility was to research software security, but that obviously branched into lots of other areas in terms of information security response, concerns about incidents, malware detection, malware reverse engineering, and eventually other areas of interest, such as insider threat, forensic examination, monitoring and tools for all those capabilities.

[TCR 00:05:24]

At Carnegie Mellon, in addition to the CERT and the Software Engineering Institute, our CyLab Institute is a multidisciplinary home for research in cybersecurity education. We deliver products and services that span the gamut: incident response of course, software security, insider threat I’ve mentioned, but resilience management, vulnerability management, usable security and privacy, which is very interesting.

From where we sit as the operational arm of the university’s cyber response, we partner as much as we can with our researchers to investigate problem and solution spaces and then integrate their research results into our operation.

And so, this sort of bridges theory and practice and kind of cycles back through. When we have a problem of interest, we may reach out to our researchers to study that on our behalf, and then we incorporate the learnings, and they of course share their research results to everyone. And so, we all improve as a result. So that’s how we kind of take advantage of our unique position at a world-renowned research university.

**OLIVIA NEAL:** Well, that’s a fascinating opportunity to be able to have that so directly linked between the operational steps that you’re taking on a day-to-day basis, to be able to put those in a bigger picture and give them as challenges and opportunities for research and then feedback in the work that happens.

I also wonder whether most CISOs are operating in organizations where they are probably the person who knows the most about cybersecurity in that organization, . You have this opportunity, but maybe also a pressure of all of these people who have got great expertise in your area as well to help inform and shape how you’re moving forward. I’m interested in how you go about setting your priorities in your role.

**MARY ANN BLAIR:**

Well, certainly having the subject matter experts at hand will help in the priority setting process. Because, as you’re rolling out your program, you may be challenged. There may be criticisms. And so, there’s that constant dialog back and forth, right, how we need to shape our security agenda.

But I may also have a bit of a unique role because I also started the program back in 2004. So I’m kind of the longest running CISO that I’m aware of, right? I’ve had the benefit of both sort of conceiving the need for an office and then also building it, and watching how we’ve changed on the priority setting process over time.

[TCR 00:08:12]

So initially, it was sort of a crisis management approach at first, right, where are we bleeding or likely to bleed? And that’s where we sort of started with good incident response strategy.

At that time, the first state breach notification laws in the U.S., right, the need to tell customers if their data had been breached proactively, that was first coming into vogue, as well as some of the first security safeguards rules. So we started there and basically said, well, let’s find where all of the concerning data is and remove it from lots of systems that don’t need to have that data.

So we started with reducing the risk footprint, but also making sure we had good incident response strategies because you couldn’t start off preventing everything.

So from there, we moved on to more policy and training and guidance. And because we were starting out, we had many possible targets. we chose to grow organically by actively responding to community inquiries and the business drivers. And so, we used what people were asking for to begin to build our document and our guidance repository.

We used crisis that was happening at other institutions to raise the bar for us. So in a strategy that I called prep and step, we first did our homework to understand how we would combat the same threat that was being experienced other places. And when compliance requirements came along, we sort of had our strategy built in advance so we could quickly deliver.

Workforce development was a priority throughout. As concerns grew about cybersecurity, the workforce was not prepared for all of the demand. And so, hiring, good people, smart people, people who could do what I cannot do was very, very important. we emphasized workforce certifications for our individuals so that we could take on more and more.

from incident response, the next priority that we chose was detection. First, you want to be able to respond quickly and then you move to how can I detect more quickly to limit the impact? And then eventually, over the years, more and more prevention was able to occur.

So this in a way, was sort of building the program backwards. We started again with response and then move to detection. And then as the community became more ready to absorb the preventive controls, higher ed is sort of unique of industries, right, academic freedom, openness, inviting folks into your network for collaboration. I mean these were the hallmarks of higher ed.

So beginning to understand how we needed to lock things down, those were some cultural barriers that we worked on over time.

We’re unique in the sense of being not one industry, but many industries. So many different compliances sort of cross roads in a university setting. we obviously have privacy requirementswe handle credit cards,. we recruit from around the world, so the EU statutes apply for us. We have health care within our organization,. We give loans to students and financial aid, so the financial safeguards apply. And in doing research for the federal government, there are various requirements there.

So we, in terms of priority setting, realized that we could not sort of develop multiple compliance plans. We instead focused on developing an overarching framework in higher ed, again we have multiple lines of business. And so we consolidated into one overarching design that met the needs of all of those different business drivers. And those continue to evolve and as they evolve, they continue to set our priorities.

[TCR 00:12:35]

pr

**OLIVIA NEAL:** Wow, there’s so much to unpack in the answer. I think, the final piece that you were talking about, having one overarching compliance framework which really pulls together these different industry requirements, different global requirements, which must be continually developing, and something that is an evergreen document, it’s a really, really big piece.

And then I found really interesting what you were talking about on the theme of usable security, so really understanding what are the business drivers, where are the inquiries coming from – and making security something which reaches its intended outcome, but doesn’t get in the way of the things that people are trying to do on a day-to-day basis.

And the example of, well, how do you manage academic freedom and collaboration, which is such an integral part of what academics do, alongside the need to protect and secure data, really interesting challenges for you and the team to move forward on over –over a period of many years.

[00:13:35]

**MARY ANN BLAIR:** It’s certainly taken time to sort of integrate all of that and come to the point where you understand that security in some ways, in our environment, you know, we consider it to be a risk management. It’s not risk elimination, it’s risk management because with any great endeavor or any innovation, you’re going to run some risk. There are unknown unknowns. And for us, we want folks to sort of understand what the potential risks may be, not to slow or stop, but to have mitigations in place that allow that innovation to move forward.

So we talk a lot about the upside of risk. In some ways, I want my work of my ISO office to be able to help folks take more risk, be more comfortable with taking risk as they explore those innovations. And so, when folks would say, “ – you’re from security, you put the no in innovation,” and I say, “Absolutely, K-N-O-W, know is what we put in innovation.”

And what we’re helping our researchers and our entrepreneurs and hopefully what we aim to do is to say, you may not have thought about this, but let’s think about it so we can avoid it happening even as you’re moving forward. Let’s make sure you’ve got good backups in place so that you don’t lose that research result. Or, consider if somebody changed your research data and you suffered a loss of integrity in your research data, and now you’ve lost time and you’ve lost certainty and you can no longer publish.

So these are areas that we want to change the dialog that security has with the business and make sure we’re speaking in the language of the business, in the incentives of – our community members, and that we kind of create that partnership.

people say that security is a team sport. you’ve got to know what position you’re playing so we’re a preferred supplier, we’re not the office that you try to avoid.

[00:15:55]

**OLIVIA NEAL:** Hearing you talk in this way about the role of security, it’s just it makes me so joyful.

So we’ve talked to a good number of people working in governments or public sector environments or in education environments over the past year. And one of the constant themes where people who were trying to move forward with making change happen in their organization is often a real cultural barrier actually around risk.

And that pushback between what is the right level of risk to take has often not quite found the right balance, and I think that there are functions and people within organizations who are often brought up as being these real either blockers or enablers for looking at a transformation in an organization. And normally these two groups are the legal team and the security team.

And I think when you can have somebody who talks like you do around the upside of risk and risk management rather than risk elimination, that just empowers the whole organization to move forward.

And so, as you’ve been moving forward on this journey and you’ve been a CISO at Carnegie Mellon, since 2004, what lessons have you learned on the way? Is there anything that you would have done earlier if you’d known what you know now, or what would you recommend to other people who are going on this journey as well?

[TCR 00:21:04]

**MARY ANN BLAIR:** To see it as a community and a community effort, is – a lesson that I’ve learned is very important. Stamina.

**MARY ANN BLAIR:** These are gifts to have and necessities I think for a CISO in order to – not become frustrated. Perhaps sometimes, the pace of change is too slow and then suddenly, it turns on a dime and folks demand progress in very short amounts of time.

my role can also be to level those curves out a little bit more. And for that to happen, you need to be engaged with your business leaders, with your customers, with the researchers.

You know, we talked about our researchers. And, that can be intimidating to have subject matter experts as your customer group. But I think when you engage with folks and you share sort of how perhaps those research findings aren’t going to translate directly or immediately into changes in practice. How do I help connect the dots so that researchers understand that it will take time for the market to respond, but that’s no reason not to deliver the results? And so that we as a community can sort of address what we’re hearing from audit or regulators even, so our researchers will go to our regulators here in the States to explain why guidelines and standards need to change, because research shows that it’s not effective. So we’ve had that kind of dialog.

So that’s a great lesson to understand how lots of different things work, so you could take advantage and orchestrate how those different things work.

The more that you engage and take the position of the learner, the better your message becomes,. And perhaps you’re actually able to accelerate the pace of change because you’ve developed a better messaging and a better strategy because you’ve had that dialog.

So I would give the advice of understanding the business that you’re in, understanding the risk tolerance of the organization you’re in, within that business context. Reach out to your customers with the kind of humility you need to take feedback and adjust to that. And then certainly develop your own network across your peers, your peer group outside of your peer group as well, because, you know, higher ed can learn from other industries and higher ed can inform other industries in terms of their cyber journey. We’ve engaged a lot with law enforcement, and I’ve seen that over this 20-year period sort of change and become a very fruitful partnership.

Treat yourself well and treat your team well. Hire well, retain good talent, and just remember what the mission is.

**OLIVIA NEAL:** There’s a lot of very tangible, practical advice for people there. And there was one piece in there which I just wanted to get back to, which I thought was really interesting, thinking about where your subject matter experts, where your researchers are and being really at the cutting edge of knowing what’s going on and being ahead of the regulators sometimes and having a role and saying that these are the types of things that we need to be thinking about now and need to come up in regulation and compliance.

And then you have to be able to have the products and the software available to you. So it’s that marketplace has to all be in sync and moving along together in order for this kind of ecosystem to work and flourish.

[TCR 00:21:11]

**MARY ANN BLAIR:** It’s quite an ecosystem and we’re all ort of codependent, right? The marketplace needs to hire, people who hopefully have come through an organization like Carnegie Mellon,

Our researchers are sort of testing product and strategy. In our case, our CyLab organization, they work directly with corporate sponsors on areas of research and concern. And so, there’s just this constant flux that then ends up in product that I’m looking to buy.

So yes, in this space, we’ve had researchers and faculty members do a stint, let’s say, at the FTC, where so now they’re responsible for, let’s perhaps say, some, technology at a government agency. And in that interaction, they’re transferring knowledge and helping folks see. And now I see that, you know, NIST has changed its guidelines. And you start to see how all of these connections over time, eventually get us all in a better place.

And so, it’s great to have the experience of being able to contribute. Whether that’s directly or indirectly, I feel like that’s a victory for us all.

**OLIVIA NEAL:** and in your previous answer, your peer network and how important that is to grow that and have the opportunity to get insights from others based within the higher education area, but also outside of that as well.

And I wondered from that group and those conversations you’ve had, is there anybody or any organization who particularly inspires you with the work that they’re doing?

[TCR 00:27:45]

**MARY ANN BLAIR:** every organization can be inspiring in a specific thing, and we’re constantly leapfrogging each other.

I think we’re also participating in information sharing and analysis centers. And in the case of – of higher ed, that’s the REN-ISAC. This is an opportunity for us to, in a safe place, share real-time intelligence, attacks that may be happening on our network with our peers. And in any given day, any one of those institutions is my absolute hero because they just shared an indicator that will stop my institution from being the next victim. So that’s super exciting.

When I talk to our law enforcement partners, I’m inspired by their commitment to the cyber-threat and their willingness to share information and to take information in and run programs, like the CISO program that the FBI runs out of Quantico, so that you understand better as a CISO how important it is to share information with law enforcement and what they do with it and how that finds its way back to protecting us.

And I’m inspired, honestly, by my team, the members of my team and of the organization at large. Their dedication to the task, their willingness to continually improve themselves, to research and develop their own networks and bring that back, their dedication, I find that probably the most inspiring of all.

**OLIVIA NEAL:** I think that’s a wonderful place to wrap this conversation up. It’s been just really fascinating learning about the breadth of the role that you have, the insights that you get, working in this very unique environment, having access to deep subject matter experts and where that can take you, and the steps that you’ve been taking over, gosh, almost the last 20 years in this role. So thank you so much, Mary Ann, for spending time with us today and sharing your lessons.

**MARY ANN BLAIR:** Olivia Thank you. It’s been wonderful.

**OLIVIA NEAL:** Thank you to our guest, Mary Ann Blair, and thank you to you for joining me today on Public Sector Future. Our goal is for you to learn something new and to be inspired to think differently about your journey. If you’re interested in learning more about opportunities for digital approaches in Education, check out our recent episode with Stefannia Gianinni, the UN’s top official in Education.

If you enjoy today’s episode and want to help other people find it, please share, rate and review the show. It really does help people discover new shows like this one. Check out our show page for links to all of what we discussed today. And visit us at wwps.microsoft.com. Please do reach out send us your questions and your feedback. You can find me on Twitter @LivNeal or on LinkedIn, or you can email us at [ask-ps@microsoft.com](mailto:ask-ps@microsoft.com). Thank you and see you next time.

END