Entering the Cybersecurity Field with Dr. Michael Hart

CyberAware Podcast: Season 2, Episode 10

Nathan: Welcome back everybody to the final episode of the CyberAware Podcast, Season Two. My name's Nathan Sloneker, your resident expert on all things cybersecurity here at Minnesota State University, Mankato. And today I am joined as always –

Ham: Dude, Nathan, it's so good to be back in the studio once again, as always. It's such a pleasure to be here. Today we have yet another extended episode, another great thing you love to see from the CyberAware Podcast. Today's special guest is Dr. Michael Hart, assistant professor in the Department of Computer Information Science at Minnesota State University, Mankato. What a great dude to have on the show today.

Nathan: I am excited for everyone to get into this episode and listen to what he has to share with us.

Ham: So if you guys are interested in careers in cybersecurity, Nathan and Dr. Hart will walk you through what's out there for jobs and where to get started. Learn about roles like cybersecurity engineers, cyber crime investigators, ethical hackers, and more. So sit back, relax, and enjoy the show.

Nathan: Welcome back everybody. This episode, we're going to be talking about the cyber security field in general, including things like career paths, resources, and certificates. And today I'm joined by Michael Hart. Welcome Michael.

Michael Hart: Hey, thank you for having me today, Nathan. Appreciate it.

Nathan: Happy you're able to join us here. So I guess just a good start, if you could just tell us a bit about yourself and what cybersecurity means to you.

Michael Hart: Alright. Well, thank you so much. I'm michael Hart from the College of Science, Engineering, and Techonlogy at Minnesota State University, Mankato and it's just a blessing to be in the department. So in our computer information systems area, we have a lot of different degrees. Anything from computer science to management information systems, health informatics, data science. So a lot of good areas to go into. And so I get to teach in some of those areas, you know, information security is definitely a big passion of mine and I teach our information security courses at Minnesota State, along with Dr. Christopher Veltos. So, always was honored to teach in cybersecurity.

I have an extensive background in IT. Been in the field for many, many years since the nineties. My first job, I started with just an internet service provider and I worked with one of the most exhaustive and extensive ISP's in the world. I was mischievous at a young age and so I did a lot of fun little hacking things as a young kid in computer science and IT. And so it was always fun to deal with different types of bot chats and hotlines and we had all kinds of ICS communication channels back then, but we also had a lot of different areas where you could download security tools and security hacks and this and that. And so working with an

ISP and having to deal with a lot of different types of attacks and then being a young student and trying to learn as much as I could and soak it in and being mischievous just allowed me to kind of go in a lot of different areas of this discipline and domain.

Nathan: The amount of jobs – there's, there's so many potential jobs that someone can get into. You got cybersecurity technicians or specialists, you've got cybersecurity consultants, analysts, penetration testers, architects, engineers, managers, cybercrime investigators. The list just goes on and on and on and on. Figure out what you like doing and I guarantee there's a job for you out there in the field. And you said you do consulting. Would you mind explaining for our listeners here exactly what that means?

Michael Hart: Well, consulting a lot of times just means that you're helping out others that have a specific need. And sometimes it's too expensive, right, to have a specific individual such as a threat hunter, for example. It's just, it's too much money and you may only need their services for a couple hours a week. You don't need somebody full-time that's benefitted. And so it gives an organization the ability to actually meet that need with just a few hours a week, rather than having a full-time employee.

Nathan: Outsourcing, yep. What made you, not even just cybersecurity, but you know, IT in general, what made you want to go into this field in the first place?

Michael Hart: Well, really, I attribute that to my, to my dad. I grew up with a data center in my basement of my house. I had it right there. So I got to deal with a lot of equipment just right there at home and having a dad that really is good in computer science and math was a huge benefit to me. I took classes early on. I went postsecondary to college early and right away just fell in love with this area.

Nathan: So where did you end up going to college then if you knew you were wanting to get into this out of the bat?

Michael Hart: Well, the first college I went to is just a technical college or community college I guess you could say. So my first degree is actually just a networking degree, computer and device networking. Back then, it was a little more traditional. So we did everything from voice to telecom. But networking was a big first step. And one of the first certifications that I got was the Cisco Certified Network Associate, the CCNA. And then I went on to the CCNP and so on and so forth. So getting that networking background helped a lot and it's always good to start somewhere. There's a lot of different avenues you can take but networking was mine.

Nathan: I mean, IT in general is such a vast field, and cybersecurity even more so. It incorporates so many different aspects of IT in general. As an assistant professor here, what would you say are the top classes that you'd recommend for someone to take if they want to get into it?

Michael Hart: That's a good question. I think, in general, anything in science, technology, engineering and math, in the stem area, is a good place to start. We really emphasize math a lot because you got to have the math, math, math. And now, if you're going to do proofs and theories and become a cryptographer, yes, you know, you're going to have to be very heavy

in math. But there's a whole lot of other areas too. You can take a governance class. Governance, security really relies heavily upon policies, risk management, laws, precedence. And so, you can start with the governance program. You know, you can start with the business program. On the management side, you know, being a risk manager. A lot of project management emphasis there. So a lot of different avenues again on the education side that you can start. But generally speaking, a lot of high schools now, you know, they have a CS One, a computer science one course. That's a really good course to take. Just some type of computer course early on in your career. There's also some really good programs, which I know we'll probably talk a little bit later about as well but, CyberPatriot is a K through 12. CyberPatriot is a youth cyber league and there's a lot of courses in K through 12. You just take that first CyberPatriot course that really gets your foot into the door and in cybersecurity.

Nathan: I personally didn't take too many technology courses in high school. I had a buddy of mine, like you brought up CyberPatriot, he ended up doing that and went to all the, I guess, tournaments they have for that and whatnot. He said he really enjoyed that. And that's kind of what got him kicked started in cybersecurity. MIS is also a really good program for students here if they want to go into cybersecurity. It's so ingrained with the business side of things. You know, cybersecurity and technology and business all go hand in hand. So, I personally am just CIT major, but I know that for students here MIS is one of the probably the ones you should go for if you're looking to get into cybersecurity at Mankato. I'm actually going for CIT as my major, but for my minor I'm going for criminal justice. And that ties in and I have a bunch of other peers in my program as well. One of them was automotive technology. The other one is going for graphic design. One of them is doing a math minor but you know, it's such a broad field to get into. And these little niche minors that you can also get your foot in the door in some areas as well.

Michael Hart: Yeah, Nathan, you're right on the money there. A lot of students don't realize all the pathways into information security. And it really doesn't matter which degree, you know, you start with. If you have a passion for it, then you can build upon any degree in this field, in this discipline. I talk about law and governance just because there's so many individuals we need on that side, on the jurisdiction side. A big need there right now. We're dealing a lot with ransomware. Ransomware is one of the hottest topics right now in our discipline. And I've been speaking a lot on ransomware in some of my speeches. And, you know, with ransomware, a lot of it is sense and respond. There is a psychological aspect to it. There's multiple human discipline degrees that could lead to your ability to sense and respond to a situation like we see with ransomware, where you kind of have to sense and respond to the perpetrator. Their mental state is a big dimension of handling those types of incidents appropriately, and you'd never know it. We often say that in the onion of our discipline, technology is the easy part, people is the difficult part, right? You just don't know, you can't predict the person's side of it. So you have to have those skillsets.

Nathan: It's not just technical skills, even when you're hiring people, you know, networking is a big thing. And for most jobs, you're hiring someone based on who they are and everything's going to be trained. I feel like a lot of people always want these hard set skills when really it's, if you have a good work ethic and you know what you're talking about, a lot of the things they're just willing to train you. They're going to train you from scratch, and that's what I was talking about with some of our past guests as well, is how that's what they look for in hiring people in their sort of fields. With ransomware as well, how the mindset of like threat actors plays into their attacks. Actually, for one of our episodes, we ended up

doing ransomware. There's ransomware negotiators and types of insurance and there's whole policies that so many people wouldn't even think that existed for these sort of attacks.

Michael Hart: My first week of lectures in our introductory information security course at Minnesota State University, Mankato is insurance. Insurance is a big part of our discipline and that's one of the most difficult parts of selling information security to our superiors is – Hey, you're paying for insurance. It might happen. It might not.

Nathan: Fair enough. I feel like even companies nowadays, they don't put enough stress on how important cybersecurity is. It's the backbone, especially for how much technology runs the world nowadays. Everything uses technology. I'd be surprised to find a business or an organization that doesn't utilize technology in some way, especially the big name ones. It's everywhere. And it's only getting bigger and it's only getting more advanced, more specialized as we continue moving forward with attacks and offense and defense. Everyone's evolving.

Michael Hart: Yeah, absolutely. It's really important I think as well – big data has been a tremendous advocate for information security, because as data has become more pertinent to firm survival and to our competitive advantage in organizations, its protection has become even more critical. Also, you know, the ethical, you know, aspect with artificial intelligence and machine learning. Some of the more dynamic aspects of what we're seeing in organizations and how we're predicting things has tremendously increased the need for security as well and the ethics behind it. Because we really don't know how ethical we can be with ones and zeros at the end of the day. It's very difficult to predict robotically what those ones and zeros can turn into given any type of backdoor trap, any algorithm manipulation.

So there's a lot of opportunities in these areas and going beyond the traditional law and precedent and some of those old adage areas, students should really look for these new technologies and the trending areas such as artificial intelligence and big data if they want to get into this discipline as well, because there's going to be some key areas of need in the career paths in those areas that traditional computer scientists and IT individuals like myself that just didn't have an introduction to in our early education. So this gives students a tremendous advantage over us older professionals.

Nathan: You're talking about machine learning and AI. How everything's moving towards more automation and in certain fields, you know, we're always talking about the job deficit in cybersecurity. And as you stated earlier, a lot of that's found in the public sector. They're hurting for workers that are able to help them out with security, protection, all that sort of thing. That's a big topic that is going around nowadays and how public can compete with private sector when it comes to cybersecurity jobs. ML and AI, all moving towards automation. Do you think the field itself is going to get more specialized as we continue moving forward? I mean, it already is, but it's going to be crazy to see new technologies emerging and just how specialized each job can actually get.

Michael Hart: It definitely is going to continue to become more specialized. Computer science as a discipline was one of the traditional areas. But prior to computer science, you know, you had math degrees. So you have math degrees, now you have computer science degrees. Now out of computer science, you know, you have IT degrees, MIS degrees, data

science degrees, cybersecurity degrees now, which is even a greater microcosm of a macrocosm. So we're seeing degrees become more specialized and we're seeing the same thing in our discipline career wise. Prior, we had an information security analyst. Now we have incident analyst. So just once again, a microcosm of a macrocosm. Now we have specific incident analysts. And we have pen testers, we have threat hunters. These are very specialized areas now of our field, specialized careers. And by the way, pen testers and threat hunters, you know, that sounds very promiscuous in some ways, but what it is is it allows us to become very good in a specific area of the discipline and nonetheless, just because we're specialized, doesn't mean we're not gonna have people that need to have more of the general skillsets either.

Really, it depends on the company size. The smaller the company, the more skillsets you need to have in a broad array of information security. So when I work with smaller organizations and consult with them, sometimes there's one information security professional, if that. And sometimes there's just the system administrator that does the networking, that does the IPS, the IDS, so on and so forth, the networking, and the systems in the virtual machines. So I think the organizational size has a lot to do with it too, just so far as how specialized you become. But I think over time, absolutely we're going to become more specialized. So far as the artificial intelligence, will automation draw some positions? Potentially, but often automation also creates positions. And as we get better at certain things, maybe we'll see additional positions that we didn't have elsewhere, just because of specialization.

Nathan: Okay. Some of the more mundane tasks, that might be what becomes automated. The daily in and out sort of things. Even with tools we have right now, for instance Defender ATP, or that security center software in general might already ping these sort of things that you don't need to go hunting for. Already kind of do some of these automated tasks for you. So, looking down the road, jobs might become more specialized in that sort of sense. And the more mundane tasks are just going to be handled by machines and stuff. In one of our last episodes with our guests, we talked about what the future of cybersecurity may look like. It's crazy just seeing how, moving forward, the types of technologies that are arising and what comes with that. I was reading recently – I think it's the national security council, they release a report like every four years hinting at what they think the future may look like. And they read a lot into how technology is going to play into politics going into the future on a world stage, geopolitical stage. Whoever has the most technology is going to be kind of the major players in the world. And it's even leading into tech companies. And these big, big corporations are actually going to have a big say with what goes on in the future because they're going to be the ones who are dealing with all this technology, from a private side standpoint as well.

Michael Hart: Yeah, that is a very good point. If you look at what's come up in the news a lot in politics, we've seen a lot of politics around social media and some of these big outlets, because it's so powerful to use these platforms for political purposes. So I think that it's very important to recognize that and be cognizant of the general direction and influence of big tech and those firms. And so you make a very good point.

Nathan: I wouldn't say I'm excited or worried, but you know, it's going to be taking a step back. Cause I mean, going forward, that's going to be definitely something I'm going to be dealing with in the field. If it's 20 years from now or whatnot, I'm still going to be working

for the most part. So it'll be interesting to see. Going back on some of the stuff you were saying earlier with the certificates. You said you had a networking certificate. I know here at Minnesota State University, Mankato we offer information security certificates, a networking technology certificate, which are two kind of the big ones that I personally am going for. And then we have graduate degrees here, like risk assessment.

Michael Hart: Yeah. So, we definitely have a number of different degrees here at Minnesota State University. We have the PSM program. It's a professional master's degree. It's information security and risk management is what it is. And so, now, it is tailored toward working professionals, but also students across a broad array of spectrum take this program. It starts with different types of security and risk management courses. So there's a researching and analyzing information security course, there's a research topics in information security. But it also covers data communications and networking, and there's a networking course that's in the required courses. We also go into information warfare.

Nathan: Yeah. I'm taking that class right now with Dr. V. So I'm enjoying that right now.

Michael Hart: And the cyber risk analysis graduate certificate, that covers a lot of those same courses. It's just nine credit hours though. So it covers the research side, the reporting and information security risks, and then the information risk management. We have similar information warfare undergraduate versions of those and risk undergraduate versions of those as well, as well as network security, as you mentioned. So certainly a number of different degrees there at the graduate level. And then undergraduate again, computer science, computer information technology, management information systems, health informatics, all of these areas are excellent feeder programs into information security.

Nathan: Okay. Certifications – if someone wants to get into cybersecurity, there's a billion different certifications that you can get. The biggest one, especially for undergraduates or entry level positions – CompTIA – your Security Plus certificate. And even on the upper end of the spectrum, you have things like your CISSP – your Certified Information System Security Professional certificate. That's one of the top notch certificates that you can get. So I'd like your opinion on for a student going in, what certifications would you recommend for someone wanting to get into the general cybersecurity field?

Michael Hart: Yeah, that's a great question, Nathan. CompTIA is an excellent organization. They have a lot of good entry-level security certifications. And sometimes for a student, they just have to get that first certification to build that confidence. So I don't really recommend necessarily that students take a very specific certification, I just call my students – let's get number one, let's get the first certification, you know? So just get one, get one out of the way. Once you start studying for them and you get one, it bolsters that confidence, and then hopefully it builds to other certifications. But yeah, that CompTIA that you mentioned – CompTIA has Security Plus, they have the Network Plus certification, there's a PenTest Plus, there's a cybersecurity analyst. They're really starting to become a little bit more granular. If I can kind of carve something out with CompTIA and the EC-Council, I would suggest take the Network Plus to get that networking foundation, then take the Security Plus, then potentially take the Certified Ethical Hacking or PenTest Plus. And then if you want to go to the management side, the analyst side, do the cyber analyst.

And then you could go into, perhaps, the CASP Plus, but that's where I would start to kind of move over into like a GIAC, so the Global Information Assurance Certification, the GIAC, that's an entry level one. It's well-respected with the government. In fact, the National Security Agency recognizes that when it gets into cryptography, as well as the soft side, such as incident response, network security, active defense. So that's kind of the direction I would take. There is a number of other areas. So ISACA has got a couple of good ones. They have a Certified Information Systems Auditor on the soft side. On the management side, the Certified Information Security Manager – the CISM. So you've got some good options there. And then as you mentioned, really, that top one is the CISSP, Nathan. So that's probably the most recognized, which is the Certified Information System Security Professional, and it covers a broad array of areas everywhere. You know, everything from risk management to asset security, uh, you know, so on and so forth.

Nathan: For introduction though, CompTIA I've heard from mentors and just other professors, that's a really good one to get your foot in the door for that first entry-level job that you have out of college, that's a great one to have and get you a leg up over other people who are applying.

Michael Hart: Yeah, absolutely. And you can even throw in some heavier certifications on the Microsoft and Oracle side. Software. Oracle Certified Associate in Java. Because you have to have that software background, so I recommended a software certification for my informationsecurity students. Database certification too, you know, would be great. But networking side, Cisco again, really good. Juniper, they've got great simulators. So I love Packet Tracer, Cisco Packet Tracer. I love GNS, GNS3 because these are simulators where you can make a lot of mistakes and not break anything.

Nathan: Moving off of certificates. You know, in your opinion, resources besides just college that people can refer to, to learn from? If you want to dip your toe in the water of cybersecurity, where you can go.

Michael Hart: Yeah, great question. One of the things that I recommend is that you head over to some type of simulation lab. I talked about GNS3 and Cisco Packet Tracer, but there's more exhaustive labs out there. One of the best labs out there is Cyberbit. And Cyberbit, it's just www.cyberbit.com. They have a virtual SOCC, a Security Operation Command Center and it allows you to actually work within the context of real attack scenarios. So Cyberbit is a good one. In Minnesota here actually, we have Cyrin, in Minneapolis, Minnesota. It's used a lot for military and first responders, but you can also get in there as well through different students scenarios, it's just cybersecurityintelligence.com. But there's a lot of other good cyber ranges out there. Cloud Range out in Nashville, Tennessee – one of the most advanced ones. Accenture, they've got their Cyber Fusion Center now in Washington, DC. That's done an extraordinary job training a lot of experts in the public sector and private sector really. So cyber ranges is one thing that I would look at.

Get yourself into a cyber range so you can just start to actually deal with attacks and work with the technology, with IT infrastructure, so on and so forth. We have a great club, a great student organization here – the Information Security Student Organization here at Minnesota State, and we do the national collegiate cyber defense competition. These competitions, just like I mentioned CyberPatriot. The CCDC competition is a national collegiate program. And these programs are excellent. They really train you in a lot of different areas of information

security. So one of the environments that they train in is all virtualized, it's right here on campus at Minnesota State. And they learn how to work with low level hardware issues, like buffer overflows. They do all kinds of ethical hacking, but they also do cyber defense. They work with intrusion prevention systems, with mainline ones, and intrusion detection systems. And then, you know, the server side, the virtual side, so on and so forth.

Nathan: So you brought up student organizations that you can join. Now, I don't know if there's a stigma around, you know, you need to know everything in order to join. Would do you mind filling in? Is it that students can just come and join, you know, you might not know anything?

Michael Hart: Yeah. So if you've never done anything beyond just the graphical user interface on a computer and you're like, there's no way that I can become a hacker or there's no way I could do programming. What I recommend is just head over to a lock room. And a lock room is just an area where you go in and you're given clues and hints to try to find things. You work with the team collaboratively and you see, can you get out of the lock room? Can you get out? And how long does it take you? A lock room is a great place just to see how some of this stuff works in a tangible form without using computers. And it's a lot of fun and if you have a curiosity in something as simple as a lock room, then perhaps you have a career in information security. It's that simple. You don't have to again have a degree or background. Another thing is a hackathon because you don't have to have any programming experience. Hackathons can be just hacking code. They can be hacking systems. There is a bunch of different types of hackathons, so that'd be another good event just to join in and see if, you know, if you've got any curiosity there.

Nathan: You're talking about the escape room – I personally never have considered that as a general interest. It plays so well with information security. I just hadn't ever thought of it myself. What would you say are good traits and skills to have going in when it comes to cybersecurity jobs?

Michael Hart: Curiosity, I think in general. We've talked about the math, the analytical skills, but the artistry side is just important. You know, you've talked about, you have a friends that are graphical artists. Well, you know, we need individuals that can create posters, but we also need people with imaginations. Because a lot of times, if you've got the analytical skills, you have to dream and imagine what a cybercriminal is going to come up with. They come up with some pretty creative ways to social engineer people.

A lot of good hackers, they're very good at just having a conversation with you and all of a sudden they have a key factor, a key piece of information from you that allows them to compromise the system that they're trying to get to. It's that simple. You have to be a good people person on the social side. On the mathematical side, yeah, if you can do proofs and you can work with new algorithms and encryption, that's excellent. So a lot of broad spectrum of skillsets there, but just imagination, I think critical thinking, and thinking outside the box. The ability to be artistic is a great skillset as well as mathematical and analytical.

Nathan: There's so many different ways to break an egg in this sort of sense with the field. So I definitely agree with you. That's a big soft skill to have – out of the box thinking. Going back on some of the stuff you were saying earlier, a lot of people would say the same thing,

that people are the biggest vulnerability in any organization you go to, especially on like a cybersecurity perspective. With that in mind, what would you recommend, I guess, some of your biggest tips and tricks, kind of a crash course that any general average Joe can do in order to keep safe? Both within their personal life and through something like school or their company.

Michael Hart: Yeah. No, that's a great question. We try to do training at every organization for anyone. Sometimes, you know, you have to just use your own, uh, senses, right? To determine whether something seems a little fishy. No pun intended. So, when you get an email from somebody you don't know, you shouldn't trust them. When somebody calls you that's not on your contact list, don't give them information. It's always hard because you want to trust people, you know, you want to expect the best out of people. But unfortunately what we're consistently seeing is in the most vulnerable of situations, we see some of the best of the best people and we see some of the worst of the worst people, unfortunately.

Another thing that I spoke a lot on recently in speeches is just how COVID, how our pandemic that we're going through right now is being used. You know, you have a lot of individuals right now, unfortunately, that are using their health to leverage an advantage in our discipline in information security. And so they'll send an email that says, oh, you know, "here's a new medicine that's going to help you fight this pandemic, this virus." And you click on it, you know, and it's a phishing attempt. You're entering your credentials into a fake website and they've got you. Unfortunately we're seeing a lot of attacks that are just out of the necessity for somebody else to gain advantage. And criminals, uh, are people just like everyone else and they have a need. They need potentially food. And so how did they get food? Well, they're using some type of illicit behavior to take advantage of somebody else that has money to gain money. So we have to look at it from the other side of the perspective too. What's the motive of the hacker, of the criminal. And sometimes it's somebody that just needs something as simple as food to survive the next day.

Nathan: Stepping into your attacker's shoes is a big thing to know. It's these mock situations and hypothetical risk assessments. Understanding where you're vulnerable. See where the holes in the ship are, you know, and offer how you can patch them. We're coming close to our time here. For our listeners here, you know, your top three tips or takeaways that you can just offer to everybody.

Michael Hart: I think that, uh, specific to our discipline in particular, you always have to be curious. And out of curiosity and imagination, always try to identify through your passions the best avenue for success. It's really important out of curiosity to take action. And to carve out your pathway. Start somewhere. Don't just essentially take the safe route, you know, start somewhere. I tell students a lot of times to get into this discipline, you can start just as a help desk technician. Take that curiosity and do something with it. Just do something somewhere in IT. I don't care where in IT, just start somewhere.

Nathan: Great advice. I agree with you 100 percent.

Michael Hart: Make sure you're always true to yourself, that you have a value system, that you have integrity, that you have a good attitude. For you to be successful, it's really important for you to have a positive outlook at all times. To treat people with respect and

have gratitude and thankfulness for others. You know, you never know, Nathan, who your next boss is going to be. I don't know how many times I've seen somebody that said, oh, you know, "you're my boss now?" After essentially the opposite being true. You know, I was next in line for a position and somebody else got the position and now I'm under that person. They're my superior. And how did you treat that person?

Nathan: Yep, relationships change. The person you might've been hanging out with on the weekend and you guys always would whine about your old boss together, now they're in that position.

Michael Hart: Absolutely. So yeah, always have a positive outlook, have a good attitude. Work well with people. Just have integrity and respect others, care for others. That would be a second element. And then third, always be passionate and love what you do. Life is short. It is so short. And we just can't emphasize that enough. You have to love what you do. You have to be passionate and you have to enjoy life day to day. Take it easy sometimes, give yourself a little bit of a break. Don't be too intense. And just love those around you and support others and be encouraging. And so it's really just an honor to be here and I'm so thankful again that you are taking action. A podcast is precisely what we would define as one of those action items, where you have a passion and you have curiosity, you've gone after it and you've developed something. And you've made something of yourself because of it. And this is an extraordinary opportunity that everyone can learn from that's listening to the podcast is just go out and do something. Take action in an area you're passionate about. And it can be a small step first that will turn into a giant step and something extraordinary. Most big things start with something very miniscule, very small. So thank you so much for doing this podcast. We really appreciate it.

Nathan: Well again, thank you for joining us today. We're honored to have you as a guest and I'm hoping our listeners here and I, myself as well, learned a lot from you this episode. So again, thank you so much for coming and joining us today. I really appreciate it.

Michael Hart: Absolutely. Thank you so much, Nathan.

Nathan: Well, I guess that about wraps up this episode for the cybersecurity field. Hopefully we have a few people who take an interest in cybersecurity and are able to do something with what they learned today. And now let's get into the news.

Hey everyone, Nathan Sloneker here filling in for Mercy with the news. I'll be updating you with what's going on in the cybersecurity world. Before I get into the headlines, please make sure to subscribe to our podcast. Today's headlines are –

A confirmed data breach at Panasonic. On November 26th, 2021, Panasonic, a Japanese based electronics company, announced a data breach that had been ongoing for several months. The cybercriminal accessed the internal file server of the company. This was discovered on November 11th, 2021, and Panasonic still is unsure about the total damage that incurred after the incident and further investigations are still in process. This attack becomes the second after another attack on Panasonic India in 2020, when financial and sensitive data was exposed.

Secondly, over two million people were affected in a cyberattack on an Ohio DNA testing center. In November 2021, a DNA testing center called DNA Diagnostics Center reported to have suffered a cyberattack where a database was hacked and financial and account information from over two million people were accessed by a cybercriminal. The company confirmed that genetic testing information had not been compromised. Information accessed by the cybercriminal includes names, credit and debit card information along with security pins, financial account information, and passwords. This information was on an older database from a genetic testing organization that is currently inactive. Be advised and monitor your bank . Accounts regularly for any wary or fraudulent activities.

And that wraps up the news for this week. Thanks again for listening to the CyberAware Podcast!