Transcript of Podcast Interview:
Cyber & Supply Chain Threats to the Health Care Sector

Matt Halvorsen: Thank you for listening today. We at the National Counterintelligence and Security Center, or NCSC, in the Supply Chain and Cyber Directorate decided to begin a series of audio interviews with experts and practitioners from government, industry, research, and academia to add to our robust outreach efforts. These interviews and outreach efforts are designed to help reduce threats to key U.S. supply chains and prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the United States.

The exploitation of key supply chains by foreign adversaries—especially when executed in concert with cyber intrusions and insider threat activities—represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure.

My name is Matthew Halvorsen, the Strategic Program Manager for the Supply Chain Directorate, I will be conducting the interviews. It is our hope that this series of interviews will help educate people to supply chain threats and we hope it highlights the efforts of many to help mitigate these threats.

We are using Covid protocols, and as such until these interviews will be conducted using teleconference software. Please excuse any audio quality challenges. Thanks again for listening in.

Alright next, we have with us, Greg Garcia. He is the Executive Director for Cybersecurity of the Health Sector Coordinating Council, the convening organization for critical healthcare infrastructure organizations working in partnership with HHS and other government agencies to protect the security and resilience of the sector, patient safety, and public health. Greg, thanks for being with us today.

Greg Garcia: Good to join you, Matt.

Matt Halvorsen: So, Greg, let's start out with some simple baseline here. Can you please sum up the Health Sector Coordinating Council and just give us a little background on it?

Greg Garcia: Yes, The health sector is one of sixteen federally designated critical infrastructure sectors, thinking of electricity, and financial service, and telecommunications, and water, and healthcare, and public health. There are sixteen sector coordinating councils just like us. And we are, in effect, federally advising committees.

We work in partnership with the government, with the recognition that these critical sectors every day are facing any number of hazards and threats, whether they are natural threats like pandemics or hurricanes or whether they are man-made like cyberattacks. So we work together to identify those threats and figure out ways to mitigate them over the long term strategically policy-wise. And we work in partnership with the more tactical and operational sector representatives known as the ISAACS - the Information Sharing and Analysis Centers, and of

course, there is a health ISAAC. Together we are engaged in critical infrastructure protection of the healthcare sector, and doing it in partnership among ourselves, across the industry, and with the government.

Matt Halvorsen: That's great. Where do you fit into all of that Greg?

Greg Garcia: So, I am the executive director of the Sector Coordinating Council, and it is actually sort of a unique position because most of the sector coordinating councils are coalitions of the willing: volunteer organizations doing the best they can to organize themselves. I, as executive director, basically am running an industry association: Making sure that the trains are running on time, that there is a government structure, that we are able to document our activities and provide all of the support needed so that the experts, the stakeholders the ones who have the jobs of protecting their hospitals and their medical device companies and the pharmaceutical companies, can actually contribute content and thought leadership to developing ways to get better, to be more secure and resilient, and they just need someone at a full-time level to making sure that process is facilitated. So, I am a full-time executive director, a full-time trade association manager.

Matt Halvorsen: Now, Greg, whether it's the election or the pandemic, those issues have caused, you know, health care to be recognized as an important topic for people. We want to make sure that from its workers to the people it serves to industry advancements, all that is in the discussion. Despite the obstacles from all these angles, we don't hear a lot of talk about cybersecurity for the healthcare systems; right now, what would you say is the biggest cyber threat to the healthcare system?

Greg Garcia: Yes, good question. I will say we are talking about cybersecurity a whole lot more than we were three to four years ago, primarily because the healthcare sector has become such a big, rich, juicy target. It's as if they moved on from the financial services sector. Willie Sutton robbed banks because that is where the money is; they did that with mouse clicks on the financial sector but, now they are doing it on the healthcare sector.

Over the past several years, the biggest threats and attacks have been in ransomware. Ransomware, of course, being delivered by what is typically used by email phishing, and they drop a payload in, and the payload infiltrates a hospital network and, it extracts all of the data and then encrypts it. It sends, to the hospital, a notice that if you want your data back you will have to pay a ransom in Bitcoin. And of course, this data includes things like patient information, diagnostic data, payment data, and scheduling for surgeries. Everything that enables a hospital to do its work, suddenly, becomes encrypted, and they cannot get back to work until they get the data back.

So do they pay the ransom? This is a development that is now extremely common, almost an epidemic. But, in the sector council, we have been putting together a lot of best practices, a lot of guidance documents to help hospital systems and others in the healthcare value chain to prepare against those events and to be able to respond to them when and if they do happen.

Matt Halvorsen: So, Greg, as we continue this conversation, with obviously the pandemic in mind. You know, the COVID-19 pandemic has created this vaccine race, and everybody is paying extremely close attention to this race. Where does cybersecurity fit into protecting the research and development on these projects for vaccines or for therapeutics for the COVID-19?

Greg Garcia: This is essential. We actually started two years ago to develop guidance, particularly for research universities and pharmaceutical companies that do tremendous amounts of research on critical intellectual property. In particular, patents and research data are vulnerable to cyberattacks, cyber exploitation, particularly from nation-states, states sponsored, and that we put together best practices for guarding against cyberattacks against intellectual property. For many pharmaceutical companies, that's their crown jewel.

Now, and as that document, we released it in May of this year. It is called The Healthcare Industry Cybersecurity Protection of Intellectual Capital-Innovation Capital. That is on our website at healthsectorcouncil.org. As we were finishing up the publication of that, COVID-19 struck. With COVID-19, came operation warp speed, a highly public and politically charged and visible operation by the government in partnership with industry. Clearly, that then becomes a target. So as organizations are ramping up their research for COVID vaccines, the cyber adversaries are ramping up their exploitation activities.

So, this is where cybersecurity and all the tools and techniques at our disposal need to be deployed to protect research data, vaccine data, pharmaceutical data from being exploited and exfiltrated by whether they are criminal gangs or whether they are nation-states in the race for vaccines.

Matt Halvorsen: Thanks for that, Greg. I would like to do a little transition here and look at cybersecurity as it relates to supply chain risk management. So a year ago, the Health Sector Coordinating Council released The Health Industry Cybersecurity Supply Chain Risk Management Guide; it was updated just this September of 2020. Can you briefly talk about the origins of this document?

Greg Garcia: Absolutely. So, it's become a cliche in cyber-security that we're only as strong as our weakest link. We have a value chain in healthcare, as does any major critical sector, that you have venders and you have service providers. Those vendors and service providers have their own vendors and service providers, and so that's the supply chain. That is the value chain, and unless we as major customers of these vendors and service providers have some level of confidence that our supply chain is secure from cyberattacks, that when we connect our systems together, or we buy these devices or technology from vendors, we don't have some level of assurance that those products and services are cyber secure than we ourselves as major customers are importing vulnerabilities into our system.

So supply chain security gets to the question of how you manage a complex supply chain in your environment, and we took our cue from the NIST cybersecurity framework. Originally published in 2014, which was revised a couple of years later to include a supply chain cybersecurity risk management process. And so, we simply took that tool, and we tailored it for the healthcare system. We tailored it to the healthcare system language so that hospital systems, and device

makers, and pharmaceuticals and plans and payers, and health IT that they can -they can integrate the NIST cyber framework supply chain process into their risk management program. So, we did version one of that.

When you look at the NIST framework supply chain guidance it's broken up into 5 Core functions. We took the first three, over the course of a year, we prepared that guidance and said "you know what this is really important information let's get it out now". So, that was released, it was about this time last year, and then the task group that was co-chaired by Johnson & Johnson and Merck. They immediately got to work, finishing the guidance document by adding the last two core functions in the NIST framework, so numbers 4 and 5. Now version 2 is simply a coherent whole. We have put that out on September 22, and we are doing everything with our government to evangelize its adoption and implementation across the sector. And, it's scalable for both small organizations and hospitals to medium and large.

Matt Halvorsen: Now on that outreach that you guys have been doing, how has it been received? The document itself.

Greg Garcia: Very well! Anecdotally, there is nothing but great compliments for it and comments like “we are implementing this” or “this is exactly what we have been doing”, so this validates our process. One of our priorities in 2021, I suspect, will be a much more systematic and structured measurement of the adoption and implementation of all of our guidance documents.

We have published eleven of them over the past two years from hospital cybersecurity best practices to medical device cybersecurity to workforce development information-sharing intellectual capital, as you mentioned, earlier supply chain. We want to start measuring how well the Healthcare System is doing in first being aware of these things, secondly adopting them and committing the resource investments necessary to implement, and then how are they over time. The most difficult question is, are they effective at improving security?

Matt Halvorsen: So Greg, I am going to ask you a question that comes up a lot in NCSC when we talk about cybersecurity, but in the supply chain realm as well, is how has the internet-of-things and embedded devices changed the landscape for security in the healthcare sector?

Greg Garcia: [short laughter]. By an order of magnitude, one of our key partners besides HHS in government is the Food and Drug Administration which, of course, has jurisdiction over regulating medical devices. And, as medical devices and the medical internet-of-things has become more and more connected, if not over the internet, than over Hospital networks and wireless and Bluetooth, these network connections medical devices have really improved healthcare because it gives doctors remote access to data about a patient's health improving or declining.

There are all kinds of benefits for the medical internet of things and connected medical devices, but there is also a risk. The risk is, of course, when you are putting anything over a network, wired or wirelessly, you are introducing vulnerabilities. Those vulnerabilities can have an impact on patient safety, and that is what we are laser-focused on.

Fortunately, we have no reported instances of a cyberattack on an implantable device. You know we have seen the horror story on the Series 24 or Homeland Security Programs where the Vice President's pacemaker was hacked into, and he was given a heart attack. Those scenarios, we know are possible, but we have not seen them happen to the extent that it has impacted patient safety. Nevertheless, to be a cyber-security expert is to be paranoid, and that means that we have to prepare for those instances and work together.

Number one, to build security into connected devices, whether they are implantable or whether they are on-premises in a hospital. Build security from the medical device manufacturer side is number one. Number two is to work with the healthcare providers to strengthen the management of the security of those devices in the clinical environment. It is really two pieces: it is building it in and maintaining the security of the legacy devices as they age throughout the life cycle of a product used in the clinical environment. As you said, how has it affected the cyber landscape?

It has certainly complicated it and expanded the footprint of cyber adversaries. So, we just have to be exponentially more vigilant, and we are getting there. There is a tremendous amount of cooperation between medical device manufacturers and the clinical operations to be sure that we understand who is responsible for security at this point of the life cycle of a product, who is accountable, and how we work together to make sure we have optimal situational awareness.

Matt Halvorsen: So, Greg, you mentioned the outreach when we were talking about the guide earlier. When you look at some of the topics we've covered today under cybersecurity ransomware, the supply chain, internet of things. What are some of the strategies that the council's using to consistently communicate with an industry that has a large multinational corporation down to smaller healthcare providers?

Greg Garcia: Great question. And it is really important to us we have a membership now of about 300 organizations. It literally grows every day, and these organizations are across the sub spectrum, as I have mentioned, device manufacturers in hospitals, and so on. About three dozen industry associations- Industry associations like the American Hospital Association, AdvaMed, America's Health Insurance Plans; these all have a large membership base. So, when put out our publications, and mind you, the sector coordinating council does not charge dues. We do not have a budget. As a federal advisory committee, we cannot be charging dues.

So we rely on our member organizations, whether it is the trade associations that have the membership or indeed we have some advisor companies. Some large consulting firms and some small consulting firms have a lot of clients, and we asked them when out in the field to consult with the clients or trade association when you communicate with your member anything about cyber-security you should be advocating the use of the sector coordinating council guidance documents because the documents are by the industry and for the industry.

Similarly, the government helps us out with this. I mentioned medical device security: In January of last year, we introduced the medical device to join a security plan on how to build security into medical devices. The Food and Drug Administration co-chaired that task, along with the Mayo Clinic and Becton Dickinson. So FDA, when they go out into public, into conferences, in some of their guidance documents, they recommend that organizations, companies, and medical

devices use the joint security plan. The HHS Office of the Chief Information Officer (OCIO) co-chaired the task group that resulted in the healthcare industry's cybersecurity practices HICP. It is called HICP. HICP is a guidance document for hospitals on better cybersecurity practices, “here are the top ten practices that you need to deploy”. HHS co-chaired that, so they are advocating for it. They are devoting resources to it.

We are using this coalition of participants to actively drive these guidance documents out into the field and endorse their use. And as I mentioned, over time, we are going to try to gather all of the data or the feedback to those surrogate markers, if you will, the government, the trade associations, the consulting firms, and then structure some kind of measurement process. Then we can report back to the public, the healthcare sectors, the Congress if they invite us up, the FBI, and the intelligence community. Are we doing better today than we were five years ago in cybersecurity? I very well want to be able to say yes, and here is how, and here are the numbers.

Thank you for that question because that is really going to be one of our priorities in the next year.

Matt Halvorsen: So, Greg, you mentioned the outreach when we were talking about the guide earlier. When you look at some of the topics that we have covered today under cybersecurity ransomware, the supply chain, the internet- of- things. What are some of the strategies that the council's using to consistently communicate with an industry that has a large multinational corporation down to smaller healthcare providers?

Matt Halvorsen: Greg, as we come to a close here, over at NCSC, we want to help with your outreach. So, I will ask you if people want to learn more about the Health Care Coordinating Council, where can they get that information?

Greg Garcia: Well, thank you. The first stop is healthsectorcouncil.org. That is our website, and all of our documents are freely available on that website. If you are a healthcare organization and you would like to get involved, there is a contact page.

I would also strongly recommend that if you are a healthcare organization and are not yet a member of the health ISAC that I mentioned before, you should be. That, for very small dues, enable your membership, is the community awareness that you need to be a part of. It is the neighborhood watch that brings together all of the stakeholders in the healthcare sector, and they openly share information with each other about attacks and threats and how they are dealing with it.

It is a whole community approach where the notion that none of us is as smart individually as all of us collectively. That is a principle that we live by. If you are participating in the ISAC and in the sector coordinating council you have your bases covered. To have important partnerships with the FBI, NSCS, HHS, Department of Homeland Security, Cybersecurity Infrastructure Agency, and others, we are forearmed and forward against the hackers.

Matt Halvorsen: Greg listen, we really appreciate all the work that the council is doing for the healthcare industry and obviously for our families. We really appreciate you being here today, we value your time, and it has been a great conversation.

Greg Garcia: Thanks Matt, for your partnership, and I appreciate all the good questions. It gives us an opportunity to get the word out because we are all in this together. We cannot have patient safety without cyber safety.