Health Care Industry Cybersecurity (HCIC) Task Force Meeting

Meeting Information

Date: Thursday, July 21, 2016, 1:00pm-2:30pm
Location: Conference Room 15108, 1919 N. Lynn St, Arlington, VA 22209

Key Highlights

- Received briefings about the activities of the Nation Health (NH) Information Sharing and Analysis Center (ISAC) and the U.S. Food and Drug Administration's (FDA) medical device workshop in the public session.
- Provided an update about the progress on HCIC Task Force progress.

Discussion Summary

Cybersecurity Best Practices – Finance and Healthcare ISAC Sector Panel

Jim Routh, Chief Security Officer, Vice President, Aetna Inc.

Mr. Emery Csulak welcomed Task Force members and public participants to the open session of the HCIC Task Force meeting and reviewed the agenda for the afternoon. Mr. Csulak welcomed Mr. Jim Routh to discuss the work of the NH-ISAC. Mr. Routh began by reviewing the questions posed by the HCIC Task Force members prior to the meeting. To address the question of, "How can the NH-ISAC be better leveraged by industry?" Mr. Routh stated that the ISAC membership continues to increase monthly and that the quality and quantity of information shared correlates directly to the personal relationships that individuals develop. Mr. Routh stated that the primary way to increase information sharing is by bringing people together through a summit or workshop to build trust and develop relationships. He also added that socializing the ISAC with influencing organizations (e.g., AMA, HIMMS, PhRMA, AHA) and active participation in ISAC webinars and exercises helps to promote information sharing. A Task Force member asked about what types of intelligence information members share. Mr. Routh responded that the primary threat information shared includes information related to ransomware, phishing, and software vulnerabilities. A Task Force member questioned whether developing a software bill of materials would assist small and medium size organizations. Mr. Routh replied a bill of materials would benefit organizations of all sizes, especially because the diversity of IT within the health care sector is greater than in many other sectors, such as finance. He added that a bill of materials may offer a pedigree for open source components that could remediate some of the challenges that stem from the lack of clarity about inherent security risks.

To answer the question, "Why have providers lagged in joining/participating?" Mr. Routh stated that while a compliance-based approach works to promote solid privacy practices, information security practices need to embrace a risk-driven approach due to continual changes in the threat landscape; understanding risks helps to drive information sharing. Mr. Routh continued that another factor affecting the health care sector are the investments made in electronic health record adoption, which subsumed funding for other IT security capabilities. He stated while the Healthcare Information and Management Systems Society recommends that health care organizations spend 10 percent of their IT budget on security; the average organization only spends three percent. Mr. Routh added that the techniques NH-ISAC members learn can be valuable to save limited financial resources.

Mr. Routh reviewed a scenario that documented techniques used for inbound phishing protection. As the number one threat vector across all industries, organizations can help to protect against phishing using a

sinkhole to block all inbound email traffic from any newly registered domain for 48 hours. He also stated that emails to consumers should use an approved DMARC to authenticate email originating from specific servers to ensure that malicious email is dropped and not delivered.

To answer the question, "What are the needs for data definitions, technical standards to facilitate cyber information sharing?" Mr. Routh replied that the STIX and TAXII capabilities are foundational for automated information sharing; both capabilities are established, continue to mature, and continue to gain acceptance across the public and private sector. He added that threat actors are known by different names depending on the source of the information and that the finance sector has engaged in an effort to develop a consistent nomenclature for threat actors.

A Task Force member questioned the demographic split for large health care providers and device manufactures vs. small and medium sized organizations. Mr. Routh replied that a line of demarcation exists within the provider space—termed the "technology/security poverty line"—where in the top tier provider space the Chief Information Officer (CIO) and security professionals are responsible for security across the enterprise. These organizations have some financial resources to ingest information (often machine-to-machine), make the information actionable to become more resilient, and have the personnel resources to implement security measures. He continued that the middle tier is "hit or miss" with limited financial and personnel resources. These organizations often do not have the infrastructure in place to support these capabilities, but have some personnel who can act on the information they receive. Smaller organizations have very limited capabilities. Even if these organizations have quality information, utilization of the information would be limited due to the lack of skilled personnel and infrastructure.

A Task Force member stated that the Task Force is especially concerned with the third tier. Mr. Routh replied that some NH-ISAC members have invested in a shared services program termed CyberFit. The program pools infrastructure and information resources in an effort to drive down costs and bridge the security gap by making information more actionable for organizations in the middle and lower tiers. Mr. Routh noted that programs like CyberFit are not the only answer and that the sector still has work to do to solve this problem. Mr. Routh concluded by providing a list of working groups that focus on different topic areas that Task Force members or the public may want to engage.

Discussion of Medical Device Workshop – 2 Day Workshop Out brief

Aftin Ross, PhD, Senior Project Manager, FDA

Mr. Csulak welcomed Dr. Aftin Ross to provide an overview of the FDA's recent medical device workshop. Dr. Ross began by stating that the workshop was a collaboration of the FDA, NH-ISAC, Department of Homeland Security, and the Department of Health and Human Services (HHS). She provided an overview of the timeline and critical activities that lead to the development of the workshop, to include Executive Order 13636 and Presidential Policy Directive 21. Based on these initiatives, FDA undertook multiple activities to enhance cybersecurity in the health care sector through public workshops, stakeholder engagements, partnerships, and collaborations. FDA hosted the first workshop in 2014; following the workshop she noted that collaboration within the medical device sub-sector increased.

Dr. Ross stated the purposes of the 2016 workshop was to:

- Discuss the FDA's thinking on the management of cybersecurity throughout the medical device total product lifecycle;
- Highlight collaborative efforts within the workspace;
- Increase awareness of existing maturity models, standards, tools, and best practices; and

- Engage stakeholders in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity.

The overall goal of the workshop was to talk about the inherent challenges, but also discuss next steps and action plans with stakeholders. Dr. Ross noted that the key themes identified during the workshop were collaboration, increasing awareness, whole community approach, and being proactive. More than 100 individuals attended the workshop in-person and over 1000 people participating via webcast. Attendees represented a broad spectrum of the stakeholders in the medical device community, to include device manufactures, providers, other Government Agencies, patients, and cybersecurity researchers.

Dr. Ross next discussed the main takeaways from the workshop plenary and breakout sessions.

- **Threat Landscape**: A lot of information exists and originates from many sources, but this information is especially difficult for the middle and third tiers to prioritize, share, and turn into actionable information. A takeaway from the workshop was to determine how to make information more actionable in the future.
- **Current FDA Philosophy**: The philosophy is a comprehensive, total lifecycle approach to cybersecurity risk management, which means that stakeholders should take what they have learned during the workshop and reinvest that into information the design and development phase of the lifecycle.
- **Information Sharing and Analysis Organizations (ISAO)**: Confusion exists about what ISAOs are and what an ISAO should look like. ISAOs will need to develop a foundation of trust, similar to the ISACs, before information sharing can occur.
- **Vulnerability Management**: The concept of vulnerability management is both old and new. It is old in the sense that ISO standards about vulnerability exposure and handling processes exist, but these practices are not well known within the medical device space. Therefore, coordination is needed to increase the adoption of disclosure practices.
- **Manufacturer Challenges with Increased Collaboration**: Cultural change is needed to increase collaboration, and manufactures cannot proceed in the same ways they have in the past. To change the culture will take time and increased maturity.
- **Gaps and Action Plans**: Business owners must make the business case for addressing and closing gaps. Session participants discussed what can be done address the gaps and challenges, what to do with legacy devices, what incentives can help to address these areas, and what is the value proposition to invest resources in cybersecurity.
- **Current and Emerging Efforts**: Discussions helped to raise awareness ongoing efforts and reinforce the need to not engage in duplicative efforts due to the finite amount of time and personnel resources. Not engaging in duplicative efforts will be critical for success.
- **Risk Assessment Tools**: Participants examined risk assessment tools and which tool may be most appropriate, as well as a common vulnerability scoring system. Participants then discussed how to make the results actionable.
- **Cybersecurity Standards for Medical Devices**: The industry does not require additional standards; the key takeaway was to identify a previously developed standard and implement it across the space.

Dr. Ross noted the success of the event due to the collaboration of the various stakeholder groups and concluded her presentation by providing a link to the workshop resources and materials, noting that the site includes transcripts and webcasts for individuals to review.

A Task Force member questioned whether the topic of a software bill of materials arose during the workshop. Dr. Ross replied that the discussions about a bill or materials and the need to understand what

each device contains, especially given that many vendors use third party software. She noted that a software bill of materials could serve as a powerful tool to address vulnerabilities in medical devices. A Task Force member questioned whether FDA will examine how to properly deploy medical devices throughout the health care community to ensure the maximum level of security. Dr. Ross commented that while the FDA understands the interconnectedness of the environment, the FDA only has regulatory authority over medical devices. This interconnectedness was the reason to include a large number of providers and other members of the community in the workshop.

Task Force Progress Out-Brief

Theresa Meadows, Senior Vice President and CIO, Cook Children's Health Care System and HCIC Task Force Co-Chair

Ms. Theresa Meadows provided public session participants with an overview and history of the HCIC Task Force, to include its establishment and charge under *Cybersecurity Information Sharing Act of 2015* (CISA), goals of the Task Force and membership composition. She noted an additional Task Force goal to maintain an open dialog with the public and stated that HHS would communicate the time and location of future public meetings through the Task Force website. Ms. Meadows continued that HHS will establish a blog on the Task Force's website to communicate progress and to seek insight and perspective from the public.

Ms. Meadows provided a status update on the recent activities and progress of the Task Force since the previous public session in April 2016. She stated that the Task Force meets monthly to continue to advance its charge, but also that internal working groups have been established to tackle the broad and diverse range of issues that Task Force is responsible for addressing. She added that the membership has also developed a Framework that maps the CISA requirements to the group's work products, identified gaps and challenges. Ms. Meadows concluded by stating that the entire membership includes a wide variety of expertise and that the Task Force continues to work diligently to collect and aggregate the data that will assist members in developing the report to Congress.

Task Force Member Attendance

Table 1 Task Force Member Attendance

LAST NAME	FIRST NAME	ORGANIZATION
Corman	Joshua	I Am The Cavalry
Csulak	Emery	Centers for Medicare and Medicaid Services
DeCesare	George	Kaiser Permanente Health Plan
Fernando	Anura	UL, LLC
Finn	David	Symantec Corp.
Jarrett	Mark	Northwell Health/Hofstra Northwell School of Medicine
Johnson	Alissa	Stryker Corp.
McNeil	Michael	Philips Healthcare
McWhorter	Dan	FireEye, Inc.
Meadows	Theresa	Cook Children's Health Care System
Mellinger	Roy	Anthem, Inc.
Monson	Jacki	Sutter Health
Ramadoss	Ram	Catholic Health Initiatives
Rice	Terry	Merck & Co.
Sardanopoli	Vito	Quest Diagnostics
Sublett	Christine	Augmedix, Inc.
Thompson	Lauren	U.S. Department of Defense/Department of Veteran Affairs
Ting	David	Imprivata, Inc.
Trotter	Fred	CareSet Systems

Non-Member Attendance

Table 2 Non-Member Attendance

LAST NAME	FIRST NAME	ORGANIZATION
Carmody	Seth	FDA
Centola	Joanna	Deloitte
Curren	Steve	U.S. Department of Health and Human Services
Edison	Nicole	U.S. Department of Health and Human Services
Kim	Oliver	Mousetrap
Kranbuhl	Paige	Stryker Corp.
Krigstein	Leslie	CHIME
Leitsch	Darren	Deloitte
Marsh	William	Department of Defense/Department of Veterans Affairs
Mandelbaum	Karen	Centers for Medicare and Medicaid Services
Ross	Aftin	U.S. Food and Drug Administration
Savage	Lucia	U.S. Department of Health and Human Services
Savickis	Mari	CHIME
Shoultz	David	Philips
Struse	Richard	U.S. Department of Homeland Security, NCCIC
Suarez	Walter	Kaiser Permanente
Trumpoldt	Ken	Deloitte
Weber	Rick	Inside Cybersecurity
Wolfe	Laura	U.S. Department of Health and Human Services
Zuk	Margie	MITRE

Additionally, 25 members of the public joined the meeting through the Skype dial-in line.