United States Department of

Health & Human Services

Office of the Assistant Secretary for Preparedness and Response

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

Health Care Industry Cybersecurity (HCIC) Task Force Meeting

Meeting Information

Date: Wednesday, October 26, 2016, 9:00am-11:00am
Location: Hubert H. Humphrey Building, 200 Independence Ave, SW, Washington, DC 20024

Key Highlights

Held panel discussions with U.S. Department of Health and Human Services (HHS) and private sector representatives to discuss information sharing from the Federal and commercial sector perspectives.

Discussion Summary

Welcome

Emery Csulak, CISO, Centers for Medicare & Medicaid Services (CMS) and Task Force Co-Chair

Mr. Emery Csulak welcomed members of the Task Force and the public to the third in-person meeting of the HCIC Task Force. He stated that the public portion of the meeting would include two panels focused on information sharing from the Federal and the private sector perspectives.

Panel Discussion: The Federal Approach for Healthcare Industry Cybersecurity

Leo Scanlon – Acting CISO, HHS
Iliana Peters – Senior Advisor for Health Insurance Portability and Accountability Act (HIPAA) Compliance and Enforcement, Office for Civil Rights (OCR)
Lucia Savage – Chief Privacy Officer, Office of the National Coordinator for Health Information Technology (ONC)
Steve Curren – Director, Division of Resilience, Office of the Assistant Secretary for Preparedness and Response (ASPR)
Suzanne Schwartz, MD – Center for Devices and Radiological Health (CDRH) Associate Director for Science and Strategic Partnerships, U.S. Food and Drug Administration (FDA)
Theresa Meadows (Moderator) – Senior Vice President and Chief Information Officer (CIO), Cook Children's Health Care System and Task Force Co-Chair

Ms. Theresa Meadows asked each panelist to introduce themselves, provide an overview of their areas of expertise, and discuss how they share information. Mr. Leo Scanlon began by stating that the Office of the CIO (OCIO) conducts information sharing through an array of initiatives to include the:

- White House Cyber Strategy Implementation Plan;
- Cybersecurity National Action Plan – contains three major components to include the identification of high-value assets, the U.S. Department of Homeland Security (DHS) EINSTEIN program, and the Continuous Diagnostics and Mitigation program;
- *Cybersecurity Information Sharing Act* (CISA) Section 405 – established HHS as the sector specific agency to provide threat sharing capabilities and data to the healthcare sector; and
- Presidential Policy Directive-41 (PPD-41) – in alignment with PPD-41, OCIO supports ASPR in conducting threat sharing and all hazards emergency planning.

Mr. Scanlon stated that a critical element and common theme of all of these initiatives is the existence of public-private partnerships (PPP) for threat information sharing. He added that the concept of information sharing is not new and that fusion centers have been in existence for many years because organizations dealing with dynamic threats need ways to communicate about threats in real-time. What is new is the ability to leverage the information to conduct security threat analysis. Organizations that deal with dynamic threats need the ability to communicate in real-time to understand what is occurring across the ecosystem. Mr. Scanlon added that there can be too much information and that multiple humans need to communicate with one another and to analyze the data. Mr. Scanlon stated that OCIO and DHS are developing an information sharing feed for public and private sector organizations that includes the automated flow of threat data. He noted that while some organizations can ingest, analyze, and utilize real-time information, other organizations do not have the ability to conduct such activities due to the lack of financial or personnel resources. Mr. Scanlon provided an anecdote from Indian Health Service that they can detect phishing attacks and know that attackers are using social engineering, but the organization does not know who the attackers are, what will happen next, or what it should do to combat these threats.

Ms. Iliana Peters stated that OCR regulates HIPAA covered entities and business associates, and that the organization's two primary focuses include enforcing the HIPAA Privacy Rule and sharing information about identified breaches inside and outside HHS. OCR's methods to share information include: 1) the OCR website; 2) a monthly cyber newsletter; 3) fact sheets and frequently asked questions documents (i.e., information sharing under CISA, ransomware, cloud services, and information blocking); and 4) participation in task forces. Ms. Peters stated that OCR communicates this information throughout the sector by remaining current on the threats to healthcare and drafting documents in a way that all parties can use the information to increase their awareness of the current threat environment.

Ms. Lucia Savage stated that ONC writes, interprets, and enforces privacy, security, and breach notification rules. Because cybersecurity is a shared responsibility, ONC makes it a priority to facilitate information sharing to help prevent threats from occurring and to keep systems secure. Ms. Savage stated that while the Government and private sector have independent roles to protect against cyber threats, a Government and private sector coordination role exists due to the need for available and actionable information across the entire vertical. This role is the basis of the recent ONC grant for the Information Sharing and Analysis Organization (ISAO). She continued that the grantee must meet three requirements: 1) account for the HCIC Task Force findings as it develops its long-term plans; 2) develop programs to share information; and 3) distribute information in a way that small and medium-sized organizations can act on. Ms. Savage compared the concept to a neighborhood watch ("cyber-hood") and stated that all entities must look out for one another, provide actionable information, and make information available to everyone regardless of their size or ability to pay for the information. Ms. Savage concluded by saying that ONC also maintains a rich website were the public can access information for free that includes a security risk assessment tool, training games, and educational materials.

Mr. Steve Curren stated that ASPR coordinates public health and medical response to emergencies and provides resources across HHS and to private sector partners. ASPR has become more focused on cybersecurity issues due to the increase in the size and scope of the threats and challenges. Cyber threats such as ransomware can cripple operations in a healthcare facility, compromise continuity, and ultimately impact patient care. Mr. Curren noted the importance of a PPP to address cyber issues. He added that in the past, cybersecurity was viewed as an IT issue and not an organizational issue. Mr. Curren reported that information sharing has been occurring for a long time and that access to information is something that people can continually use. He added that there will never be enough grant funding or programs to address all issues or directly support all organizations, but that ASPR and HHS can provide information to help organizations protect their systems and information. ASPR shares information publically through its website and also shares non-classified information with its partners through a portal. Anyone wishing to access the portal should contact cip.hhs.gov.

Dr. Suzanne Schwartz began by stating that CDRH provides oversight of medical devices and that much of the Center's work focuses on how to enhance and strengthen medical device security. She began by mentioning the recent distributed denial of service attack that leveraged consumer devices. She added that this could occur in hospitals and healthcare systems, and that the community is vulnerable to attacks that would have devastating consequences to hospital operations and patient safety. She also stated the *Digital Millennium Copyright Act* exemption will enable the sharing of medical device security research with manufacturers. This exemption has the capacity to illicit an avalanche of information about medical device vulnerabilities that were not previously shared because of concerns about retribution or organizational liability. She added that this is an opportunity for coordinated vulnerability disclosure and for researchers and manufacturers to work with the Government for early identification and vulnerability remediation. Dr. Schwartz quoted James Clapper, "Security was never an integral part of the internet. It wasn't a consideration. We're kind of paying the price for that now." She continued that information sharing is critical for the healthcare and medical device ecosystem to anticipate and respond to the recent rise in ransomware attacks. FDA recently published draft cybersecurity guidance that includes the active participation of the ISAOs. Dr. Schwartz added that the FDA believes information sharing enables the community to lean forward and identify information early, including from other critical infrastructure sectors that could have cascading consequences for healthcare and public health, and allows the community to put the necessary measures in place before harm occurs. The FDA accomplishes information sharing through a PPP and believes the ISAOs are a critical component to sharing information in a trusted manner and enabling stakeholders to include additional mitigations or protections, which will ultimately increase the lifespan of a device.

Ms. Meadows thanked the panelists for their remarks and asked Dr. Schwartz what medical device disclosures the FDA believes are in the public's best interest. Dr. Schwartz replied that "coordinated vulnerability disclosures" can provide an enormous benefit to bring parties together that have the expertise, knowledge, and know-how to work with manufacturers as new vulnerabilities are identified. She added that having a process in place for engaging parties who understand the potential device functionality exploits and compensating controls to have an open dialog with vendors can reduce the potential impact to the patient safety. Dr. Schwartz concluded by saying that a lack of coordination may erode public confidence in the systems and devices and the worst thing that could happen would be for a patient to refuse a life-saving device because a disclosure was not fully vetted.

Ms. Meadows asked how the private sector could use automated indicator sharing (AIS). Mr. Scanlon replied that DHS developed the AIS feed and that it is available to private sector organizations. The feed has a standard format that provides contextual information associated with particular threats and indicators, and was designed to be applied by other control mechanisms at an automated level. DHS provides the feed and HHS incorporates unbranded information (e.g., raw threat indicators, raw event information) to conduct analytics and the Homeland Security Information Network provides branded analytics to the sector (e.g., what we know, how we know it, what it does, what you need to do).
Mr. Scanlon added that the ability of organizations to provide unbranded information helps to develop branded information to disseminate through currently existing channels.

Ms. Meadows asked why ransomware attacks are considered breaches and if there are instances when they cannot or will not be reported. Ms. Peters replied that OCR provides guidance about how ransomware intersects with HIPAA and that OCR coordinated with HHS, DHS, and Federal Bureau of Investigation partners to understand what ransomware does, how it evolves, and the threats it poses to the industry. OCR is concerned with the disclosure of protected health information under the HIPAA Privacy Rule and she stated that ransomware is considered a breach because it results in the impermissible use of information. Additionally, OCR provides guidance to determine whether an organization must report the breach to the regulator. If an organization elects not to notify HHS or the media, it must conduct a risk assessment to demonstrate a low probability of a data compromise. Ms. Peters concluded by saying that entities should consider whether services were impacted, patient care was affected, or whether people were harmed as the result of a breach when determining whether to report the incident to regulators. Additionally, even if organizations do not report a breach, she hoped they will share information with their partners and industry (e.g., the exact variant of malware, if the integrity of the data was affected, and all systems affected by the malware) so everyone can better understand the threats to the healthcare sector.

Panel Discussion: Commercial Sector Information Sharing

Matt Hartley – Vice President Intel Operations & Products, FireEye
Anna Turman – CIO, Chadron Community Hospital
Angela Diop – Vice President Information Systems, Unity Health Care
Matthew Snyder – CISO, Penn State Hershey Medical Center and Health System
Daniel Nutkis – Founder and Chief Executive Officer (CEO), Health Information Trust Alliance (HITRUST)
Terry Rice – National Health Information Sharing and Analysis Center (NH-ISAC) Board of Directors Member, and Vice President IT Risk Management and CISO, Merck & Co.
Emery Csulak (Moderator) – CISO, CMS

Mr. Csulak thanked the members of the Federal panel and stated that any member of the public could provide comments to the Task Force through the blog posted on the Task Force website. He welcomed commercial sector panelists and asked each to provide an introduction. Mr. Matthew Hartley stated that his organization feels strongly that information sharing helps to protect against the attacks that we see across all sectors. He added that one organization's reactive is another organization's proactive because we can collectively take advantage of their findings. Mr. Hartley continued that one challenge with cybersecurity is that it has historically been implemented technologically and approached reactively. He continued that organizations need to think about it as an adversary problem and if we understand the adversary, their motivation, and how they can attack, then we can defend an organization more readily. Engaging in information sharing allows us to not only collect and share threat intelligence data, but also to invest in preventing those threats and developing a collective defense against attacks.

Ms. Anna Turman stated that she works for a small critical care hospital in rural Nebraska and has responsibilities covering all security and privacy issues. She emphasized that smaller organizations are not incompetent, but are stretched in their financial resources and ability to employ personnel with the appropriate cybersecurity skills. Therefore, her organization develops their security staff internally. Many small organizations do not have a CIO or CISO in place to support security initiatives. Ms. Turman stated that cyber threats do not discriminate based on organizational size and that small hospitals are large targets due to the level of maturity of their security programs. She noted that information sharing, communication, and networking is critical to the protection of her hospital's network and systems. But she added that smaller hospitals need the help of larger organizations to keep pace. Ms. Turman continued that her hospital leverages Government guidance, but that the guidance does not fill the gap of information sharing or help to identify lessons learned. She compared the need for information sharing and associated tools with getting a prescription. When you leave the hospital you receive a prescription and discharge instructions, but without those instructions one does not know to shut down a specific port and other actions to take in order to respond to an attack. She stated that awareness comes from the shared community and emphasized the need to create an environment of trust to share information.

Ms. Angela Diop stated that she works for a medium size organization that provides health and human services to the residents of the District of Columbia. Similar to Ms. Turman, she also has multiple security roles within her organization. Ms. Diop noted that increasing connectivity creates additional risks and exposure, but due to the number of competing priorities she expects her IT and security budget to continue to shrink in the future; these issues increase the need for coordination and information sharing. Ms. Diop added that the organization engages in information sharing through CHIME and AEHIS, but that organizations need additional, actionable information to identify threats and conduct response and mitigation efforts. She suggested the potential for more mature organizations to engage by providing technical assistance, boot camps, and pre-packaged information.

Mr. Matthew Snyder stated that he works for an academic medical center; in addition to the traditional healthcare threats, his facility also contends with the risk of intellectual property theft. He said that threat intelligence sharing is a key area for the Task Force to address because it is the conduit to collective defense. Mr. Snyder commented that many organizations do not understand the threats they face and that when one thinks about the organizations that suffered massive intrusions, many organizations cannot even detect events of this scale. He stated that information sharing will require a high level of trust to be effective and that a challenge to threat intelligence sharing includes concerns about brand damage and increased scrutiny from regulators and the public. Mr. Snyder added that an additional challenge is that many organizations do not know how to integrate and process intelligence data or how to prioritize the most significant threats.

Mr. Daniel Nutkis stated that HITRUST was established approximately 10 years ago with a focus on information sharing from a risk management and cyber resilience perspective. He mentioned the Cyber Threat Exchange and the ability to distribute high-value indicators of compromise (IOC). At the beginning of this program, participants responded that the IOCs were not actionable, non-consumable, and people did not know what to do with them. As a result, HITRUST established a collection mechanism. An October 2015 progress report showed that organizations did not contribute indicators and the indicators were not timely; 4.1 percent of organizations contributed IOCs, of which only 50 percent were actionable and indicators averaged seven week old. As a result, HITRUST established collection guidelines and requested that organizations submit robust indicators within 5 minutes of discovery and that cover multiple protocols. He continued that HITRUST discovered that many organizations do not have capability to consume the data and did not have a full understanding of the labor involved in reviewing the indicators. As a result HITRUST implemented technology that increased the number of collected IOCs by more than 700 over the course of a year. It also implemented the ability for organizations to upload their syslogs and receive a report of the IOCs present within their systems. To engage medical organizations with less than 80 employees, HITRUST developed the CyberAid program to provide high-tech, low-touch resources to these entities that do not have the time or resources to dedicate to contributing IOCs. Mr. Nutkis concluded by saying that information sharing cannot take a one-size fits all approach and that it has to work for the largest to the smallest entities.

Mr. Terry Rice began by noting that his organization has a large security staff and still has trouble maintaining constant situational awareness of the threat environment. He continued that this is an ecosystem challenge that has to be dealt with as industry at the organizational, national, and international levels. Mr. Rice stated that the concept of the ISAC dates back to the Clinton Administration, and while the Energy, Financial Services, and Defense Industrial Base ISACs were established early, the NH-ISAC was not established until 2010 and was reconstituted in February 2013. While he noted that the NH-ISAC processed over 3,900 indicators of malware in the last month, he did not know how small entity could consume and respond to that volume of information even with automated systems in place. Mr. Rice continued that the entire community needs to come together to figure out how to respond and that information sharing is not limited to threat information, but also extends to sharing best practices. As such, the NH-ISAC has established working groups for medical devices, identify and access management, big data for healthcare, and awareness and education. The NH-ISAC is also working to provide smaller entities with services such as legal and regulation surveillance, risk assessment sharing, a benchmarking capability, and a shared utility for penetration and vulnerability scanning.

A Task Force member commented that real-time information sharing and actionable intelligence will be a critical component for organizations that live below the security poverty line and that do not have a CIO or CISO. The Task Force member continued that the resource constraint issue is a large challenge and expressed his concern that information sharing may not be helpful if the majority of small and medium-sized organizations do not have the ability or capacity to consume the information. Mr. Rice replied that software has pervaded every part of healthcare and that no one has solved the problem of how to write secure code (e.g., software subject to SQL injections, cross-site scripting, use of default usernames and passwords) and the problem will continue until the software development process is fixed. Mr. Nutkis agreed and noted the struggle to identify the vendor’s role in developing better software products. He added that there has to be a recognition about how to manage risk, a determination about what prioritizations to make, and identification of where information sharing fits into an organization’s risk profile. Ms. Turman added that not all technology problems have technological solutions and that empowering people through education can increase awareness. Ms. Diop stated that how an organization leverages its resources and develops creative solutions (e.g., a virtual CISO) could help smaller organizations make the most of limited resources. Mr. Hartley expressed the need to challenge vendors from a technological and security perspective and examine emerging technologies that can automate and act on information sharing before a human is ever in the loop.

Mr. Csulak questioned how different organizations measure success and value of information sharing, as well as how do they justify the expenses and measure value. Ms. Turman replied that her organization collaborates with others in the region and that through information sharing, monthly meetings, and lessons learned from recent attacks they have identified resource strengths and weaknesses. Mr. Snyder commented that when nothing negative happens that executive will not devote money to cyber initiatives; the Board and executives focus on cyber after an incident has occurred. He added that there are no accepted baseline metrics for a “good” cybersecurity program and that people could consider adopting maturity models to understand their programs. Ms. Diop stated that her organization suffered a small data loss and since that time the Board has remained involved and requests regular updates on the security posture of the organization. Mr. Nutkis commented that there is no model for cyber because no one knows which indicators have the most value. Because breaches will continue to occur, cyber resilience is needed to minimize the impact of the attacks. He added that as organizations become harder targets to infiltrate, attackers will target other organizations that possess the same data due to the level of interconnectivity within the sector. Mr. Rice added that his organization leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework to conduct baseline assessments and uses the assessment to report to the Board on information sharing activities. Ms. Diop, Ms. Turman, and Mr. Snyder stated that their organizations had adopted the NIST Framework and Mr. Snyder added that his organization also utilizes a modified version of the Capability Maturity Model Integration to communicate more easily.

Mr. Csulak questioned whether panelists see challenges that result from the variety of relationships that exist within the sector, and how could this inform the Task Force’s work to identify best practices and practices to avoid. Mr. Snyder stated that his organization shares information based on relevance of context; one should not discover after the fact that the information shared was not of value. Therefore, the parameters for threat intelligence sharing should be defined up-front to make the most of the return on investment. Mr. Hartley added that it would be beneficial for industry to become involved in the standards making process to provide additional context and benefit to the private sector. Mr. Rice noted the auto industry's requirement to disclose vulnerabilities in automobiles, which if not quashed could impact information sharing across all sectors due to concerns over legal liabilities.

A Task Force member asked about the contractual limitations for information sharing. Mr. Snyder stated that his organization utilizes vendor agreements and that some contracts include clauses that restrict the sharing of product issues or vulnerabilities. He said the challenge around transparency and the need to have secure discussions about these issues and vulnerabilities, but also noted the need to be cognizant not to share information that could put patients at risk. Mr. Nutkis commented that the HITRUST vulnerability disclosure program received pushback from vendors and the organization had to determine how to strip organizational data and tags; HITRUST also destroys all data that organizations share.

Mr. Csulak thanked panelists from the Federal and commercial panels. He reminded members of the public to reach to the Task Force through its website and closed the open session of the meeting.

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
Finn	David	Symantec Corp.
Jarrett	Mark	Northwell Health/Hofstra Northwell School of Medicine
Laybourn	Laura	U.S. Department of Homeland Security
McNeil	Michael	Philips Healthcare
Meadows	Theresa	Cook Children’s Health Care System
Monson	Jacki	Sutter Health
Ramadoss	Ram	Catholic Health Initiatives
Rice	Terry	Merck & Co.
Sardanopoli	Vito	Quest Diagnostics
Stine	Kevin	National Institute of Standards and Technology
Suarez	Roberto	BD (Becton, Dickinson and Company)
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
Anderson	Carl	HITRUST
Bailey	Michelle	Centers for Medicare and Medicaid Services
Centola	Joanna	Deloitte
Chacko	Sarah	The Hill Extra: Healthcare
Chapman	Stuart	Thorn Run Partners
Chase	Penny	MITRE
Chua	Julie Anne	U.S. Department of Health and Human Services
Curren	Steve	ASPR
D'Amato	Jordan	Deloitte
DeCarlo	Michael	Blue Cross Blue Shield Association
Diop	Angela	Unity Health Care
Dykehouse	Rodney	Penn State Hershey Medical Center
Edison	Nicole	ASPR
Eggers	Matthew	U.S. Chamber of Commerce
Fleet	Eli	HIMSS
Gray	David	HIMSS
Hartley	Matthew	FireEye
Higgins	Joshua	Inside Cybersecurity
Hodges	Andrea	Emagine IT
Holmes	Scott	FireEye
Hoover	Thompson	PA eHealth Partnership
Krigstein	Leslie	CHIME
Leary	Thomas	HIMSS
Leitsch	Darren	Deloitte
Marinella	Ryan	Deloitte
Marsh	William	U.S. Department of Defense/Department of Veterans Affairs
Miller	Kati	Deloitte
Nutkis	Daniel	HITRUST
Odderstol	Thad	U.S. Department of Health and Human Services
Peters	Iliana	OCR
Ross	Aftin	U.S. Food and Drug Administration
Savage	Lucia	ONC
Savickis	Mari	CHIME

LAST NAME	FIRST NAME	ORGANIZATION
Scanlon	Leo	U.S. Department of Health and Human Services
Schwartz	Suzanne	U.S. Food and Drug Administration
Smith	Malikah	ONC
Snyder	Matthew	Penn State Hershey Medical Center
Thompson	Kelly	PA eHealth Partnership
Todd	Nickol	ASPR
Trumpoldt	Ken	Deloitte
Viola	Allison	Kaiser Permanente
Wellington	David	U.S. Department of Defense/Department of Veterans Affairs
Worzala	Chantal	AHA
Zuk	Margie	MITRE