



## Privacy and Security Information Sharing A Public-Private Partnership



On November 2, 2017, eHealth Initiative and PwC held an invitation-only, roundtable meeting for privacy and security executives from the healthcare industry and government agencies. The purpose of the meeting was to discuss public-private partnerships, share information, and foster collaborations among attendees. Executives addressed the current privacy and security landscape, ways to improve data sharing, cyber threat mitigation, and industry best practices.

### CYBERSECURITY OVERVIEW

The day began with a multi-stakeholder panel that provided an overview on cybersecurity information sharing and readiness. Mike Darling, Director, Cyber Security Practice, PwC; Thien La, Vice President and Chief Information Security Officer (CISO), Wellmark Blue Cross Blue Shield; and Kathy Jobes, Vice President, CISO, OhioHealth shared their thoughts on the collaborative efforts organizations are undertaking to improve cyber data sharing, the resources and personnel allocated to support initiatives, and lessons learned.



As a part of their security protocols, OhioHealth collaborates with CISOs from various organizations and has data sharing agreements with several entities. OhioHealth successfully avoided the [Nuance Communications cyberattack](#), which occurred in June 2017 and affected multinational companies in at least 65 countries. Nuance Communications is a U.S. based technology company that works with 86% of all U.S. hospitals, providing more than a dozen products that range from cloud-based dictation and transcription services to radiology critical test results. More than 500,000 clinicians and 10,000 healthcare facilities worldwide use the company's clinical documentation solutions.

Data breaches of this scale have been forcing organizations to take new perspectives. Participants found that [forums and calls set up by Health and Human Services \(HHS\)](#) have been helpful to threat planning. Provider and payer participants specifically credited this series of roundtable discussions, hosted by PwC and eHealth Initiative, for their decisions around data sharing and for spurring them to greater action. During the last roundtable, FBI Supervisory Special Agent, Ed You, shared information on the threat China continues to represent to cybersecurity. PwC does not allow any offshore data sharing even when their own employees are offshore. Additionally, concerns raised prompted organizations to stop sharing data with Chinese corporations. [The China threat continues to grow](#), particularly in genomics and the life sciences.

Thien La joined the conversation via phone. He collects data on vendors who use the same products. As with the Nuance Communications example, instead of attacking an individual company, such as CVS or Walgreens, attackers look for a vendor that is used by multiple companies. Thien is a board member of the [National Health Information Sharing & Analysis Center \(NH-ISAC\)](#) and believes it is more important for smaller companies to become involved with organizations like NH-ISAC, which serves as an "official health care information sharing and analysis center, offering non-profit and for-profit health care stakeholders a community and forum for sharing cyber and physical security threat indicators, best practices and mitigation strategies." Organizations like [HITRUST Cyber Threat XChange \(CTX\)](#) also offer a platform for sharing threats. Thien stated that by 2018 there will be a million roles in information security that do not have sufficient talent. Given these dynamics, it is time to start building information sharing capabilities that can be leveraged.

The [NotPetya](#) ransomware was a variant of Petya and hit many firms in the U.S., causing major financial damage. NotPetya cost Merck pharmaceuticals [more than \\$300 million](#) in the third quarter alone and is on track to cost that amount, again, in the fourth quarter. The media reported that the ransomware was spreading through social engineering, such as phishing, but in reality the cyberattack was coming from the Ukraine through software updates. As Thien pointed out, it takes longer to realize a problem when everyone is working independently. It was through collaboration, *It's not who's first it's who puts the industry first*, that stakeholders realized no one actually received a phishing email and found the root of the problem. Leaving distracting chatter behind is important to cybersecurity, as is a system that allows stakeholders to discover the details around what is happening in the constantly changing landscape.

**Threat intelligence is not easy.**



CVS frequently provides intelligence to their vendors so they are aware of issues occurring. CVS's size and resources position them to better monitor and handle threats than the smaller organizations with which they work. Premise Heath discovered it was much more cost effective, and timely, to have vendors purchase a good firewall and several hours of time with Premise engineers before allowing them into their supply chain. Their original process required a threat analysis, that could take months, with

vendors who were sometimes skeptical about complete transparency. Receiving raw data from the vendors allowed Premise to assist them with plugging leaks and alleviating threats at an early stage. Dialogue about how to solve a problem could have a vendor up and running within a week and proved more useful.

Other salient discussion points:

- Smaller organizations are critical **producers** of intelligence because their size enables them to notice breaches first
- With the interconnectedness of the world, "bad neighbors" are everywhere
- Collaboration, economics, and internal/external paradigms for value propositions matter
- For data to be useful, it must be collected and delivered in a meaningful format
- **Trust is key** in cybersecurity collaboration
- Geo-blocking is becoming more prevalent
- [H.R. 1313](#) has numerous ethical, privacy, and cybersecurity concerns because it allows employers to offer substantial health insurance premium rebates to workers who take part in genetic screenings under company "wellness programs," while charging employees who decline to participate much higher premiums

This panel concluded with more information from Ed You on China and the role of government in cybersecurity. China was trying to enter the U.S. cell phone market for many years, but was unsuccessful until Samsung batteries, which were produced in China, began spontaneously combusting. Chinese cell phones are now sold at Walmart and other stores. The privacy and security implications are plentiful. Along the genomics front, China started working in partnership with companies around the world, including those in the U.S. These partnerships allow China to collect DNA data on numerous foreign nationals; however, it passed laws restricting entities outside of China from collecting DNA, and other data, on the more than a billion Chinese within its border. This dynamic has numerous privacy, security, economic implications.

**China remains a threat to cybersecurity.**

Ed stated that the government is only as good as the data provided to them. Although HHS, DHS, and NIST have established partnerships, the siloed nature of government means that cyber threat information does not have one central repository and multiple agencies receive various pieces of information. Industry leaders at the

roundtable would like government to play a data collection and repository role. An executive noted that industry has more data than the government and although the government can inform industry of threats, they cannot do the work of determining exactly how a threat will affect industry. The group consensus was that public-private partnerships require a value proposition on both sides. If industry is to share data with government, government must provide something in return.

## PUBLIC-PRIVATE PARTNERSHIPS



The next panel discussed the coordination, support, and resources for established public-private partnerships, which function to allow federal agencies, Congress, and private industry to collaborate in proactively sharing cybersecurity information. Speakers included Steve Curren, Director, Division of Resilience, Office of Emergency Management, Office of Assistant Secretary for Planning and Resilience (ASPR), Health and Human Services (HHS); Kara Sidener, Special Agent, InfraGard Coordinator, Federal Bureau of Investigation (FBI), Washington Field Office, Intelligence Division; and Kwadwo Burgee, Senior Analyst, National Cybersecurity & Communications Integration Center, U.S. Department of Homeland Security (DHS).

HHS has been designated the Sector Specific Agency for the health care and public health (HPH) sector through the Presidential Policy Directive 21 (PPD-21). In coordination with the U.S. Department of Homeland Security (DHS), HHS is responsible for working collaboratively with public and private sector organizations to increase the security and resilience of the sector and address risks that threaten the ability of organizations to provide healthcare.

The Cybersecurity Act of 2015 contained several elements related to HHS's role in improving the cybersecurity posture of the healthcare industry. HHS has responded by clarifying the Department's governance structure for private sector cybersecurity efforts, chartering an internal Cybersecurity Working Group; establishing the Healthcare Cybersecurity Communications Integration Center (HCCIC); and convening the [Health Care Industry Cybersecurity Task Force](#). The 21-member Task Force spent a year receiving input from a wide range of healthcare and non-healthcare stakeholders and subject matter experts and delivered a report to Congress in June. The report puts forward six general "imperatives" encompassing 104 specific action items for consideration by government and industry stakeholders. HHS expects the report to serve as a roadmap for the long-term collaborative effort with industry to improve cybersecurity within healthcare.

InfraGard is a partnership between the FBI and members of the private sector. The program "provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure." According to FBI Agent and InfraGard Coordinator, Kara Sidener, the FBI has an Office of Private Sector and the 56 FBI field offices and 85 InfraGard chapters nationwide understand the sensitivities involved in data breaches. Every FBI field office has a cyber task force and the FBI encourages businesses to report breaches.

**Information sharing  
stops cybersecurity  
breaches and  
threats.**

InfraGard is open to *individuals*, who are vetted via a security risk assessment. The group has thousands of national members, including business executives, entrepreneurs, military and government officials, computer professionals, academics, and state and local law enforcement. InfraGard members are dedicated to



contributing industry specific insight and advancing national security. The D.C. chapter is primarily comprised of IT professionals. It initiated a national listserv for health IT professionals, which allows members to share information. The listserv has been working well. Roughly 600 individuals from around the country, who are at the intersection of healthcare and IT, participate in the group and exchange IOCs, best practices and lessons learned. Early on, a log-in system was developed in addition to the listserv and it proved too cumbersome, as members did not want to remember another username and password. The listserv allows members to have an immediate exchange with like-minded peers.



Another collaborative mentioned was the [Cyber Security Information Sharing Partnership \(CiSP\)](#) based in the U.K. According to their website, CiSP is “a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.”

Roundtable participants also discussed audit protocols implemented by government. As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, in April 2016 the HHS Office for Civil Rights (OCR) began its [next phase of audits](#) of covered entities and their business associates. Audits and other tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI). It was mentioned that the Department of Defense (DoD) is also coming up with protocols. The group expressed concern that two different sets of protocols will become the standard.

Other salient discussion points:

- **Cybersecurity is everyone’s responsibility**
- Spear phishing works because someone *always* clicks on the link
- There are several joint FBI / DHS sector initiatives
- It is recommended that companies [stop using Kaspersky](#)
- There are many factors that determine classification; two pieces of unclassified information can be considered classified dependent on the purpose for which said information is shared

## CYBERSECURITY FRAMEWORKS AND TECHNOLOGY WITH NIST

Voluntary guidelines to support the adoption of the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) Cybersecurity Framework and HPH sector risk reduction and resilience must be developed. This discussion was led by Celia Paulsen, a cybersecurity expert from NIST. Celia provided guidance to help organizations better assess risk and allocate resources.



Celia’s work at NIST has the potential to be associated with an executive order on critical infrastructure. She is working on a [NIST IR 8179: Criticality Analysis Process Model](#), which is a method for identifying and prioritizing information systems and components; increasing the understanding of an organization’s IT/OT (and other) assets; better decision making around risk management, project management, acquisition, maintenance, and upgrade; and informed distribution of finite resources. The tool is not another Failure Mode Effects and Criticality Analysis (FMECA), Business Continuity Planning Tool, FIPS Level / Classification, or Framework (RMF, CSF, etc.). It leverages and informs existing practices and does not duplicate them.





















**Privacy and Security Information Sharing**  
**A Public-Private Partnership**



**END OF THE DAY KEY TAKEAWAYS**

- The power of information sharing is tremendous
- The work of the FBI’s Weapons of Mass Destruction Directorate, Biological Countermeasures Unit has been getting more traction and efforts are expanding
- Capitalism trumps common sense and safety when dealing with China
- There are too many security tools to track all of them
- Participants have agreed to share certain agreements and reports with one another
- PwC has data on the number of cybersecurity professionals within healthcare and other industries
- As the industry works towards consensus, this group should produce a set of principles or whitepaper

ROUNDTABLE ATTENDEES		
<p><b>Jennifer Covich Bordenick</b> Chief Executive Officer</p> 	<p><b>Kwadwo Burgee</b> Senior Analyst, National Cybersecurity and Communications Integration Center</p> 	<p><b>Stephen Curren</b> Director, Division of Resilience, Office of Emergency Management, Office of Assistant Secretary for Planning and Resilience</p> 
<p><b>Michael Darling</b> Director, Cyber Security Practice</p> 	<p><b>Jeremy Diebling</b> Director, Health Industries Cybersecurity &amp; Privacy</p> 	<p><b>Amy Eckenroth</b> Senior Vice President</p> 
<p><b>Dean Galitsis</b> Associate Counsel</p> 	<p><b>Lisa Gallagher</b> Managing Director, Health Industries Advisory, Cybersecurity &amp; Privacy</p> 	<p><b>Laura Hoffman</b> Assistant Director, Federal Affairs</p> 
<p><b>Kathy Jobes</b> Vice President Chief Information Security Officer</p> 	<p><b>Joseph “Joey” Johnson</b> Chief Information Security Officer</p> 	<p><b>Thien La</b> Vice President, Chief Information Security Officer</p> 
<p><b>Jason Newman</b> Chief Information Security Officer</p> 	<p><b>Celia Paulsen</b> Security Engineering and Risk Management</p> 	<p><b>Diane Sacks</b> Principal, Diane Sacks LLC</p> <p>Consultant</p> 
<p><b>Kara Sidener</b> Special Agent, InfraGard Coordinator, FBI Washington Field Office. Intelligence Division</p>  <p>Federal Bureau of Investigation</p>	<p><b>Chad Thiemann</b> Privacy Corrector</p> 	<p><b>Ed You</b> Supervisory Special Agent, FBI Weapons of Mass Destruction Directorate, Biological Countermeasures Unit</p>  <p>Federal Bureau of Investigation</p>