April 4, 2017

Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships

Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, United States House of Representatives, One Hundred Fifteenth Congress, First Session

Hearing Contents:

Member Statements

Greg Walden
Chairman, Committee on Energy and Commerce
[View pdf]

Tim Murphy
Chairman, Subcommittee on Oversight and Investigations
[View pdf]

Witnesses

Denise Anderson
President, National Health Information Sharing and Analysis Center
[View pdf]

Michael McNeil
Global Product Security & Services Officer, Philips
[View pdf]

Terry Rice
Vice President, IT Risk Management & Chief Information Security Officer
Merck & Company, Inc.
[View pdf]

Available Webcast(s)*:

[View Webcast]

Compiled From*:

https://energycommerce.house.gov/hearings-and-votes/hearings/cybersecurity-heath-care-sector-strengthening-public-private

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Opening Statement of Chairman Greg Walden
Subcommittee on Oversight and Investigations
Hearing on "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships"
April 4, 2017

(As prepared for delivery)

We are well aware of the threats posed by our increasingly connected society, but nowhere do these risks hit closer to home than on the very technology we rely on for our own health care. The threats range from ransomware, breaches of patient data at heath care organizations, to the vulnerabilities in pacemakers and other medical devices. Taken in isolation, these and other threats pose serious challenges to health care organizations. Collectively, they demonstrate the breadth, complexity, and unavoidable nature of cyber threats in modern society – both now and for the foreseeable future.

As technology becomes increasingly integrated with all levels of our health care, cyber threats pose a challenge to the entire sector. Everyone - from the smallest rural hospitals, to large providers and device manufacturers - faces some level of exposure and risk.

Breaches, exploits, and vulnerabilities are inevitable realities of modern society, even for the most well-resourced and sophisticated organizations. But this does not mean doom-and-gloom for everyone with an internet connection. It is simply reality and must serve as the baseline for any discussion about cybersecurity. We may not be able to stop every attack, but as the threats continue to escalate, we must do more to minimize the risk.

Improving security is a collective responsibility. When we work together – government and private sector, large companies and small – we can do more to improve security than if we attempt to solve it on our own.

An attack on one organization may be prevented elsewhere if we have the infrastructure and mechanisms necessary to communicate effectively with others across the sector. Further, if an event has widespread or national implications, we need to coordinate an effective and efficient response – with unity of effort, not confusion over roles and responsibilities.

That is why, for almost two decades, the U.S. has worked to establish public-private partnerships to coordinate security planning and information sharing within and across our 16 critical infrastructure sectors, which includes health care.

Effective collaboration between government and the private sector is vital to elevating our security posture,. These partnerships provide a vital link between those responsible for the safety and security of the nation with those who own and operate the infrastructure critical to those objectives.

To date, these public private partnerships have experienced mixed results. Some sectors have been more successful than others in coming together – both with private sector and government partners. The health care sector, in particular, has struggled to coalesce around these public-private partnerships for cybersecurity. It is this shared, goal that brings us together today.

This hearing marks an important opportunity to hear from our distinguished panelists about what is necessary to bring the health care sector together and continue building momentum in the right direction. Simply put, the cost of inaction is too great. As the threats continue to escalate, so too do our cybersecurity challenges. We've seen the headlines – we know the attacks will continue. But today is about what improvements can be made so we can be prepared for the inevitable.

Opening Statement of The Honorable Tim Murphy
Subcommittee on Oversight and Investigations
Hearing on "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships"
April 4, 2017

We are here today to talk about cybersecurity in the health care sector. Strong cybersecurity practices are essential in this industry. This isn't just about protecting patient data or information – this is about patient safety.

For nearly two decades, a cornerstone of the nation's efforts to combat cyber threats have been public-private partnerships designed to facilitate engagement and collaboration between the government and private sector. Over time this model has evolved, but the objective remains the same – unity of effort between those responsible for protecting the nation and those who own and operate the infrastructure that is critical to that mission.

The focal point of these efforts are 16 critical infrastructure sectors—one of which is the health care sector. Each sector is organized around several key institutions – a Sector Specific Agency, Government Coordinating Council, Sector Coordinating Council and Information Sharing and Analysis Center. Each of these institutions plays an important role in ensuring participation, collaboration, and unity of effort of the government and private sector participants within each sector.

Despite a number of efforts to improve this model over the years, it has achieved mixed results across the various sectors. Some sectors have succeeded in developing robust support and engagement with both government and industry participants.

The gold standard, to date, has been the financial sector. This sector enjoys a strong, collaborative relationship with their government partner – the Department of the Treasury – which is noteworthy because Treasury is also their regulator. In addition, despite having a very diverse sector, they have succeeded in encouraging support and participation from a wide variety of institutions – from small community banks to large multi-national financial institutions. This extensive membership has helped the sector to establish the nation's most sophisticated and well-resourced ISAC, which improves its value to the entire sector.

Another, more recent, success story has been the electricity sector. This sector has improved collaboration and engagement – both with government partners at the Department of Energy and across private industry – through senior executive participation on the sector coordinating council. In addition to elevating the priority for industry partners, it has improved coordination and unity of effort with the government.

Despite the relative success of these and several others, every sector has unique characteristics and challenges that influence the pace of adoption and engagement in these institutions. What works for one sector may not work for others. As each sector figures out what works best for their participants, however, the lessons from others should not be overlooked or ignored – especially for those sectors that continue to evolve.

Which brings us to the focus of today's hearing – the health care sector. This sector has long struggled to coalesce around the public-private partnership model, especially with respect to cybersecurity. This may be partially attributable to the fact that cybersecurity is a relatively new challenge for much of this sector. However, as health care becomes increasingly digitized, the need to improve cybersecurity must be a priority.

Gaining the acceptance and support necessary to overcome historical obstacles will not be easy for this sector. To start, health care is an incredibly diverse and complex sector, with a wide range of industries and institutions of varying sizes, technological sophistication, and resources. It is also a sector where cybersecurity often becomes conflated with privacy or compliance, complicating the discussion. This, in turn, is exacerbated by the fact that a successful public-private partnership depends on collaboration and trust with HHS – an understandable challenge given the many participants in the sector who are regulated by various entities within the Department.

These and other challenges are understandable and daunting. If I am a small, rural health care institution – where cybersecurity falls to one employee who is also responsible for managing IT systems and fixing copiers, among other duties – what value do I get for the cost of joining the ISAC or listening to guidance from the sector coordinating council? At present, it is hard to answer that question, especially for those institutions already operating on negative margins.

These challenges, however, must be overcome. The cost of failure – for patients, as well as health care institutions – is too great. Cybersecurity incidents can result in life or death situations if a medical device is hacked, or an attack shuts down a hospital's computer systems. Cybersecurity is a collective responsibility and that is why it is imperative that this sector find a way to come together to find a sustainable path forward.

I look forward to hearing more from our witnesses about the challenges of this sector and what is needed to bring unity and commitment from all participants. These are the folks working in the trenches and while the sector has shown signs of progress, much work remains to be done.

Testimony of

Denise Anderson

On Behalf of the

The National Health Information Sharing & Analysis Center and the

National Council of Information Sharing and Analysis Centers

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

April 4, 2017

ISAC BACKGROUND

Chairman Murphy and members of the Subcommittee, my name is Denise Anderson. I am President of the National Health Information Sharing & Analysis Center (NH-ISAC) and Chair of the National Council of ISACs (NCI). I want to thank you for this opportunity to address the Oversight and Investigations Subcommittee about the industry perspective on cybersecurity and information sharing as well as the importance of collaboration and coordination between the public and private sectors.

ISACs were formed in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After 9/11, in response to Homeland Security Presidential Directive 7 (its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, ISACs expanded their role to encompass physical threats to their respective sectors. Many ISACs have been in existence over a decade and in some cases almost two decades.

ISACs are primarily trusted communities that promote the sharing of timely, actionable and reliable information for their respective critical infrastructure sectors and provide forums for owner and operator sharing around threats, incidents, vulnerabilities, best practices and mitigation strategies. ISACs are operational in nature and have strong reach into their sectors in order to gather and disseminate information quickly and efficiently. ISACs have been thriving and growing in recent years as owners and operators have seen the benefit to participating in these trusted communities, which is a testament to the value ISACs deliver to their members.

NCI BACKGROUND

The NCI is a voluntary organization of ISACs formed in 2003 in recognition of the need for the ISACs to share information with each other about common threats and issues. The mission of the NCI is to advance the physical and cyber security of critical infrastructure in North America by establishing and maintaining a framework for valuable interaction among and between the ISACs and with government. There are currently 21 individual ISACs that represent their respective critical infrastructure sectors or sub-sectors and 3 like organizations who are members of the NCI. The NCI has made it a goal to be inclusive of each critical infrastructure sector and sub-sector's operational arm.

The ISACs collaborate with each other daily through the NCI daily operations centers cyber call, and the NCI listserver. The NCI also hosts a weekly operations centers physical call and meets monthly to discuss issues and threats. The organization is a true cross-sector partnership engaged in sharing cyber and physical threats, mitigation strategies and working together and with government partners during incidents requiring cross-sector response as well as addressing issues affecting industry. In addition, the NCI conducts and participates in cross-sector exercises, works with the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) during steady-state and incidents, holds emergency calls as needed and develops joint white papers around threats. The ISACs have been instrumental in embracing, developing and advancing the automatic exchange of data within their memberships and across the ISACs, as well as with government as possible.

ISACs AND GOVERNMENT PARTNERSHIPS

ISACs, which are not-for-profit organizations, work closely with various government agencies including their respective Sector Specific Agencies (SSAs) where they exist, intelligence agencies, law enforcement and state and local governments. In partnership with the Department of Homeland Security (DHS), several ISACs participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the critical infrastructure sectors. Having ISACs on the floor has allowed for effective collaboration on threats and incidents and there have been many examples of successful information sharing. The ISACs also serve as liaisons to the National Infrastructure Coordinating Center (NICC) and play a vital role in incident response and collaboration under the Critical Infrastructure Partner Annex to the Incident Management Plan.

Finally, it should be noted that the ISACs collaborate with their sector coordinating councils as applicable and work with other critical infrastructure partners during steady state and incidents.

NH-ISAC BACKGROUND

The NH-ISAC, founded in 2010, is a 501(c)6 nonprofit organization and is funded primarily by its member firms through member dues. Since 2010 the membership has expanded to over 200 organizations including healthcare delivery organizations (HDOs), pharmaceutical and medical device manufacturers, retail pharmacy, laboratory and radiological, electronic medical record providers and payers representing approximately one-third of the US Health and Public Health GDP*.

The NH-ISAC is a global organization that has members in several different countries and membership is growing rapidly.

Besides offering a trusted forum and community for sharing, the NH-ISAC offers a number of other services such as workshops, two annual summits, webinars, a daily report, monthly newsletter, white papers, special interest groups, a number of working groups and committees and various technical tools for member sharing. The ISAC provides alerts, has a representative on the NCCIC floor, and participates in exercises such as the national Cyberstorm series. The NH-ISAC was one of the first organizations to adopt STIX and TAXII, which are protocols for automated indicator and intelligence sharing and fosters a robust member machine to machine sharing environment.

*Based on the annual revenue of all NH-ISAC member organizations. ($1.3 Trillion).

The NH-ISAC is also engaged in two ground-breaking initiatives. The first is the CyberFit suite of services that allows members to leverage the NH-ISAC community to realize cost savings and efficiencies.

Included in the initial suite of services is a third party risk assessment platform with over 80 questions tailored for healthcare organizations that will then be stored in an accessible database for the benefit of participating members, a benchmarking offering, as well as a ‘shared security operations center (SOC)’ program that will offer affordable services for malware analysis, penetration testing, vulnerability scanning and incident response.

The second is the Medical Device Security Information Sharing Council that is advancing efforts in the area of medical device security and safety. Under a Memorandum of Understanding between the NH-ISAC, the Medical Device Innovation, Safety and Security Consortium (MDISS), and the FDA; a number of national initiatives are underway to improve the security and safety of medical devices. These include: (1) MD-VIPER launched early this year to support the reporting of vulnerabilities and responsible medical device vulnerability disclosure per the FDA post market guidance (2) the National Cyber Safety Network for Health Technology, which leverages best public health practices to achieve national scale impact on patient safety and critical infrastructure and (3) the Medical Device Risk Assessment Platform, funded by DHS Cyber Security Division, a program for medical device assessments and threat intelligence with a database that HDOs use to understand and secure devices in their environment. Our programs include collaborations with DHS ICS-CERT, FDA, NIST National Cybersecurity Center of

Excellence, the Advanced Medical Technology Association (AdvaMed), manufacturers and national hospital networks as well as many other stakeholders.

NH-ISAC and MDISS also offer a community forum for manufacturers and HDOs to interact and collaborate through listservers, meetings, tracks at NH-ISAC summits, and workshops, among other things. The group has already held two medical device security workshops this year with many more scheduled and in February 2017, NH-ISAC and MDISS held an all-day medical device cybersecurity symposium at HIMSS, an industry conference.

The FDA has been very forward leaning in the medical device security collaboration space and the partnership with FDA, NH-ISAC and MDISS is a great example of how industry and government can come together to address cybersecurity issues. The partnership has been highly collaborative and is governed by a Memorandum of Understanding. Some examples of this public/private partnership include co-sponsoring of the FDA public workshop in January 2016, co-presenting at the FDA webinar on the post market guidance this past January 2017, presenting together at NH-ISAC Summits, and in particular, leveraging the NH-ISAC infrastructure for medical device vulnerability information sharing to meet the ‘ISAO functionality’ as described in FDA’s post market guidance, as a regulatory incentive.

THE UNIQUE NATURE OF HEALTH AND CYBER

Six years ago, ‘cyber’ and ‘healthcare’ were not even placed in the same sentence. Today because of the proliferation of advances in technology and the efficiencies of connecting devices and data via the internet, the cyber threat surface in healthcare has ballooned and the threat actors have followed. Threat actors have many motivations to attack whether for financial reasons, disruption, intellectual property theft, revenge or to make a political statement. Unfortunately, the stakes are very high. The focus has traditionally been on data and privacy but if HDOs cannot deliver services, as was seen in several recent ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities and payers to facilitate proper patient care and history as well as payment for those services. Many healthcare facilities such as hospitals operate in environments that are accessible to the public. Hospitals employ tens of thousands of medical devices, many using outdated operating systems, and many of which are connected to a network. These devices are made by a variety of manufacturers with various levels of security and patching protocols built in. Coupled with a diverse base within the sector, complex siloed departments, a lack of skilled cyber staff, a lack of cyber security situational awareness, a lack of knowledge and training for the medical staff as well as the CEO and Board level, and lack of cyber security strategy including a risk management approach, the health and public health sector faces an enormous challenge.

MEETING THE CHALLENGE

There are a number of great initiatives and efforts underway within the sector but there is still a lot more that can be done. Congress can help meet this challenge by focusing on four key areas:

1-EDUCATION, RECOGNITION AND FACILITATION OF THE IMPORTANCE OF INFORMATION SHARING

One of the greatest challenges for the NH-ISAC and all ISACs is the lack of awareness amongst the critical infrastructure owners and operators, particularly the smaller owners and operators, that the ISACs exist and are a valuable tool. Numerous incidents have shown that effective information sharing amongst robust trusted networks of members works in combatting cyber threats.

Government, and specifically the Sector Specific Agencies (SSAs) should regularly and consistently encourage owner/operators and especially at the Board and CEO level to join their respective ISACs. This has been very effective in the financial sector where the United States Department of the Treasury, the regulators and state agencies have been strongly encouraging membership in the FS-ISAC as a best practice. Currently, not all SSAs support their sector designated ISACs in the same manner.

The SSAs indeed have a policy reference for this kind of advisory to their sector representatives: the NIST Cybersecurity Framework. This Framework, developed over the course of a year collaboratively by government and private sector stakeholders, lays out a cyber risk management framework linked to five core functions: identify, protect, detect, respond and recover. Among the functional categories identified as part of a mature cyber risk management strategy is external communications and coordination around cyber security threats, response and best practices. In other words, membership in an ISAC or ISAO is an essential element of a successful cyber risk management strategy. Likewise, the most recent draft of the White House cybersecurity executive order calls for an assessment of how government can support critical sectors' cyber risk management programs. Accordingly, one of our key recommendations in response to that review would be a policy statement that provides explicit guidance to SSA's and their sectors to integrate into their cyber risk management and preparedness programs their participation in and collaboration with these information sharing and incident response organizations where applicable.

Another way to facilitate sharing and build robust communities is by providing financial incentives through tax breaks or other means to critical infrastructure organizations that join their respective ISACs.

2-PROTECT INFORMATION SHARING

Recently, the Automotive ISAC was served a non-party deposition subpoena to furnish all documentation related to communications between the Auto ISAC and one of its members. The Auto ISAC with the help of other ISACs was able to quash the subpoena with Judge Wilkerson of the U.S. District Court for the Southern District of Illinois effectively ruling that the subpoena was nothing more than a fishing expedition.

The concern with this subpoena however, is that if Courts were to allow broad sweeps for information and using ISACs as "one-stop-shops" to accomplish it, such actions would effectively kill information sharing and undermine Congress' important information sharing goals set forth by the Cybersecurity Information Sharing Act (CISA) and the government's interest in promoting national security through the ISACs and public-private information sharing.

The confidential information shared amongst the members of an ISAC should be considered protected information and not subject to disclosure.

3-ELIMINATE THE CONFUSION BETWEEN THE TERMS ISAC AND ISAO

The Executive Order, Promoting Private Sector Cybersecurity Information Sharing, signed February 15, 2015 by President Obama is commendable in its intent to foster information sharing. Information Sharing and Analysis Organizations (ISAOs) were first defined in the Homeland Security Act of 2002. ISACs were created under Presidential Decision Directive 63 (PDD-63). Effectively ISACs were the original ISAOs and are the subject matter experts in information sharing with a majority of ISACs having been in existence for over a decade.

Indeed, there is a need for many groups that may not fall in with the critical infrastructure sectors such as legal and media and entertainment organizations, who are increasingly becoming targets for cyber incidents and attacks, to share information. The private sector is already organizing efforts in this area and as an example; the FS-ISAC, working with the legal industry, formed the Legal ISAO.

However, ISACs are much more than ISAOs. ISACs offer several vehicles to share effective techniques and practices for preventing, detecting and managing cyber security risk that are often un-conventional controls (definition: controls that are designed and implemented independent of any risk framework, standard or regulatory guidance). ISAOs don’t offer vehicles for this type of sharing.

For example: enterprises can choose to obtain an intelligence feed to identify newly registered domains and choose to drop all email originating from newly registered domains. This is an example of a technique shared at last year's NH-ISAC Summit. This information is not shared in any other forum or event. Another example is the focus put on the adoption of the use of DMARC as a standard for improving trust in email and constraining the use of email for phishing attacks. This was initially shared at the FS-ISAC and today is offered through the NH-ISAC. These two examples have a material impact on improving industry resiliency and these techniques, like many others, are indicative of the unique services an ISAC offers to its members.

ISACs also serve a special role in critical infrastructure protection and resilience and play a unique role in the sector partnership model. While the White House has noted that the EO seeks to "not limit effective existing relationships that exist between the government and the private sector" the EO and prominent coverage of ISAOs has led to much confusion within industry as to the impacts to ISACs. It is absolutely essential that the successful efforts ISACs have established over the years should not be disrupted. It is clear that ISACs by their success meet the distinct and unique needs of each of their sectors and the owner and operator members of those sectors.

We have seen this clearly in the Health and Public Health Sector. When the FDA in its post market guidance for medical device security announced the need for manufacturers to participate in an ISAO, confusion ensued. The NH-ISAC is effectively serving as the ISAO and as mentioned is doing a large ground-breaking body of work in the medical device arena with the

FDA, but the guidance by using the term ISAO resulted in sector stakeholders immediately thinking some new organization needed to be created and has caused a lot of confusion that is still being sorted out.

The solution to easing this confusion is very simple. The White House, SSAs and other relevant agencies need to call out, recognize and support the unique role ISACs play in critical infrastructure protection and resilience and not apply the term ISAO as a blanket term for all information sharing. For instance, ISACs have the responsibility to maintain sector wide threat awareness within their respective sectors. It is critical that our federal partners continue to respect and support that role to avoid undermining one of the main duties of ISACs to their members and sectors. It is vital that the process is not diluted and remains streamlined to facilitate effective situational awareness and response activities particularly when an incident occurs.

4-ESTABLISH CYBER SECURITY PROFESSIONALS AS SSA LIAISONS

Given that cyber security has only recently come to healthcare, it is understandable that there has not been a need previously for a cyber security professional to act as a strong, government liaison and advocate for the public private partnership when it comes to cyber matters. It has become increasingly apparent that industry needs a government representative who understands cyber security issues, threats, vulnerabilities and impacts as well as the blended threats between physical and cyber security. Having an established, clear government ‘go to’ lead in this area is imperative to strengthening the partnership and improving the overall cyber security posture of the health and public health sector.

EFFECTIVE INFORMATION SHARING

It is important to note that the goal of information sharing is not to share information in and of itself but to create situational awareness in order to inform risk based decisions as well as allow operational components within owner/operation organizations that have direct actionable control over the content they are sharing, to perform an action. The focus needs to be on enhancing the ability of operational groups to work closely with each other.

The ISACs are successful organizations with almost two decades of proven case studies of information sharing and collaboration. They are the subject matter experts on information sharing. For information sharing to be effective it must be:

- Voluntary – not mandated or regulated
- Industry Driven
- Actionable, Timely and Relevant
- Bi-directional and Collaborative

Government can help this effort by:

- Encouraging owners and operators of critical infrastructure to join their respective sector ISACs
- Offering financial incentives such as tax breaks for owners and operators to join ISACs
- Recognizing ISACs and the unique operational role that they play in critical infrastructure protection and resilience

- Protecting information sharing by ensuring confidential data shared amongst members is protected from disclosure
- Place strong, defined and permanent cyber security liaisons and leadership within the SSAs to advocate the public private partnership when it comes to cyber matters. Cyber security liaisons and their leadership, should be experienced and certified cyber security professionals.

This concludes my testimony. Thank you again for the opportunity to present this testimony and I look forward to your questions.

AdvaMed
Advanced Medical Technology Association

Michael C. McNeil, Philips
AdvaMed, the Advanced Medical Technology Association
Testimony

Energy & Commerce Committee, Subcommittee on Oversight and Investigations
"Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships."

Tuesday, April 4, 2017

Thank you Chairman Murphy, Ranking Member DeGette, and members of the Committee for the opportunity to testify today. My name is Michael C. McNeil, and I am testifying on behalf of Philips and our trade association, AdvaMed. As the Global Product Security and Services Officer at Philips, a leading healthcare technology company, my responsibility is to oversee efforts to ensure that consistent repeatable cybersecurity processes are deployed throughout the development and maintenance of products. Philips is driving the convergence between professional health systems and personal consumer technologies to seamlessly and securely connect devices, data, systems and people across the entire health continuum, from the hospital to the home.

AdvaMed is the world's largest trade association representing medical technology manufacturers. AdvaMed member companies produce the medical devices, diagnostic products and health information systems that are transforming health care through earlier disease detection, less invasive procedures and more effective treatments. Collectively, we are committed to ensuring patient access to life-saving and life-enhancing devices and other advanced medical technologies.

Let me first say a few words about Philips' cybersecurity strategy. Our strategy includes not just staying on top of emerging software-based vulnerabilities and potential external threats while anticipating how they might affect Philips products, it also includes collaborating with regulatory agencies, industry partners, and health care providers to close security loopholes. This includes participating in the Health Care Industry Cyber Security Task Force, under the auspices of the Department of Health and Human Services.

Working with these organizations, we can understand how other industries have addressed cybersecurity threats, identified challenges to health care environments, and provide health care industry stakeholders guidance on preparing for, and responding to, cybersecurity threats. Moreover, we can help develop effective and uniform application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

We also work with health system partners like Augusta University Health, as part of visionary public-private programs like the one created by Governor Nathan Deal in Georgia, to address the cyber security challenges facing the US healthcare system. We also actively participate in industry groups like AdvaMed.

Overview of Medical Technology Sector and Cybersecurity

Let me now describe an overview of the medical technology sector and cybersecurity. AdvaMed and its member companies, are committed to a robust cybersecurity framework as part of the development and postmarket management of medical technologies. Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

Principles for Robust Medical Technology Cybersecurity

Working with my colleagues at AdvaMed, we have developed the following five foundational principles for the management of medical device cybersecurity:

1. *Medical device development and security risk management*

First, an effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to disposal. In addition, medical device security risks should be addressed through a risk management process that is based on consensus-driven recognized standards and reference documents. This risk management process should include a process to monitor the ongoing security of devices in use.

2. *System-Level Security*

Second, medical technology cybersecurity is a shared responsibility among all stakeholders within the healthcare community. Because systems are only as secure as their weakest point, all elements of the system must be appropriately managed and secured.

3. *Coordinated Disclosure*

Third, medical device manufacturers should deploy a coordinated disclosure process that provides a pathway for researchers and others to submit information, including potential vulnerabilities, to the organization. Coordinated disclosure processes should clearly define the responsibilities of both the manufacturer and researcher. It is important to emphasize that whenever potential vulnerabilities involving a medical device are discovered, these findings should first be brought to the attention of the manufacturer and / or FDA for review, analysis, and possible remediation. Any other approach potentially places patients’ lives at risk.

4. *Information Sharing*

Fourth, to assist manufacturers in continuously managing their device's cybersecurity throughout the product's lifecycle, industry should judiciously share threat and vulnerability information.

5. *Consensus Standards, Regulatory Requirements, and Education*

Finally, the development of cybersecurity-related consensus standards and regulations should be accomplished collaboratively among regulators, medical device manufacturers, independent security experts, academia, and health care delivery organizations. We also believe the health care industry should leverage the experiences and expertise of other critical infrastructure sectors and government agencies, such as NIST.

Engagement with FDA and Public-Private Partnerships

I would also like to take this opportunity to commend the U.S. Food and Drug Administration ("FDA" or "Agency") for its proactive leadership role over medical device cybersecurity. The FDA has worked closely with the medical technology industry and the broader healthcare ecosystem to ensure medical device cybersecurity is considered and addressed throughout all stages of product design and use. For example, in 2013, FDA released final guidance concerning premarket cybersecurity-related issues device manufacturers must consider when designing a connected medical device. And most recently, in December 2016, FDA released final guidance addressing the postmarket management of medical device cybersecurity. Taken together, these documents represent significant – and welcomed – achievements by the Agency to inform manufacturers of their medical device cybersecurity obligations.

Moreover, the FDA entered into a Memorandum of Understanding ("MOU") with the National Health Information Sharing and Analysis Organization ("NH-ISAC") and the Medical Device Innovation, Safety and Security Consortium ("MDISS") to promote cybersecurity information sharing for medical devices. These efforts have led to the creation of a medical device-specific information sharing and analysis organization, which has recently launched a program called the Medical Device Vulnerability Intelligence Program for Evaluation and Response, or MD-VIPER. MD-VIPER provides a streamlined mechanism for medical device manufacturers to submit and share information concerning cybersecurity-related issues, as well as other members of the broader healthcare ecosystem.

In light of the FDA's significant work and achievements to date, and the Agency's staff ongoing engagement with industry, we believe that the FDA serves as an example to all regulatory bodies with respect to the type of interaction, collaboration, and guidance an agency should provide to its regulated industry.

Conclusion

I want to underscore how critical it is to our industry that medical devices are safe for patients and risks, including cybersecurity threats, are appropriately and safely managed. Healthcare technology companies, like Philips, take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve. Manufacturers make every effort to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

We work very closely with the FDA and look forward to continuing to work with Congress and the Administration to ensure that the medical technology industry maintains a collaborative approach to cybersecurity and device safety.

Written Testimony of

Terence M. Rice

On Behalf of

Merck & Co., Inc.

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

April 4, 2017

INTRODUCTION

Chairman Murphy, Ranking Member DeGette, and Members of the Oversight and Investigations Subcommittee, my name is Terry Rice. I have been involved in healthcare cybersecurity for more than fifteen years in a wide variety of roles including my current assignment as the Vice President and Chief Information Security Officer (CISO) at Merck & Co., Inc. I also participate in a number of public-private partnerships that are working to improve cybersecurity across the healthcare sector. These partnerships include the National Health-Information Sharing and Analysis Center (NH-ISAC), the Healthcare Sector Coordinating Council (SCC), the SAFE BioPharma Association, and the Healthcare Industry Cybsecurity Task Force, the latter of which was created by the Cybersecurity Information Sharing Act of 2015. I appreciate the opportunity to testify before you on the topic of cybersecurity in the healthcare industry and to discuss how public-private partnerships have assisted and can do even more to address the complex challenges we are facing.

THE STATE OF HEALTHCARE CYBERSECURITY

Cybersecurity has rapidly become a top concern for governments and industries around the world. In just the last four years, cybersecurity has jumped from the fifteenth greatest risk facing companies to the third highest risk in the Allianz Annual Risk Barometer, a global survey that measures the sentiments of corporate risk professionals.[i] Cybersecurity has also been listed as a top concern by many national governments and has been included as a top risk in the US Intelligence Community's annual Worldwide Threat Assessment since at least 2013.[ii] Nowhere is the situation more acute than in the healthcare industry. In just the last few years we have seen over one hundred million health records exposed in a number of well-publicized security breaches, we have observed cybersecurity researchers demonstrate how software vulnerabilities in insulin pumps and pacemakers could be exploited to cause a lethal attack, and we have witnessed entire hospitals in the United States and the United Kingdom shutting down for periods of time to combat a ransomware infection on critical systems. It is because of these events and many others that IBM named the healthcare industry as the most attacked industry in its 2016 IBM Cyber Security Intelligence Index.[iii]

Unfortunately, I believe the news stories and reports underrepresent the risk we are facing as an industry. I make this statement based on five observations:

1. The total number of cybersecurity incidents is significantly underreported. Today, organizations are only required to report cybersecurity incidents when a) personal health information is breached, b) the incident directly impacts patient safety, or c) the loss of information or disruption of service would be considered a financially material event[iv]. Organizations are unlikely to report security incidents if not required to do so given the potential reputational harm that might occur. The reports we read about are only a small fraction of the incidents that actually occur. Furthermore, the incidents that do get reported (e.g. breaches of personal health information) also create a narrow focus on privacy protections for personal health information instead of considering the full spectrum of impacts caused by healthcare cyber incidents.
2. The healthcare industry consists of many small to mid-sized businesses that lack the capital and personnel to deal effectively with all but the most basic cybersecurity issues. According to one statistic, more than 90% of firms in the healthcare services subsector employ less than 100 people and about 70% of these firms employ less than 10 employees.[v] To complicate this, the healthcare services and hospital subsectors have some of the lowest profit margins across industry.[vi] These two factors make it difficult

for these firms to acquire the advanced tools and services necessary to prevent, or at least detect, sophisticated attacks. These small to mid-sized firms often face the difficult choice of investing in the latest cybersecurity tool or purchasing a crucial medical system. More often than not the latter will win. Even if these entities are able to make the capital investments required, they are almost always unable to acquire the talent necessary to install, operate, and maintain these capabilities and develop a broader cybersecurity program.

3. The portability of healthcare information increases the risk. Unlike other industries, the healthcare industry requires information to be shared among multiple companies to provide patient care. Primary care physicians must share data with specialists, specialists must share data with labs, labs provide information to pharmacies and pharmaceutical benefits managers, and all of them share subsets of this data with insurance companies. To facilitate this information sharing, most of these entities interconnect their networks and systems. Consequently, a failure anywhere in the ecosystem may lead to impacts across the sector.
4. Proliferation of software into the healthcare ecosystem increases the attack surface. The healthcare industry was somewhat of a laggard in the adoption of software services and solutions. The Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 provided both incentives and penalties to increase the adoption of electronic health records. This rapid adoption of electronic health record technology has spurred the development of new software solutions and services that can create, input, and analyze patient health information. While these advances offer tremendous potential healthcare benefits and

may help to reduce cost across the industry, we are rapidly increasing the cyber attack surface in the healthcare sector. The risk is exacerbated by the fact that software developers have not yet come up with a way to prevent errors and mistakes in the software they create. In fact, computer programmers continue to make many of the same mistakes in their code that were made 15-20 years ago. Today we measure software errors in the number of defects per thousand lines of code; many of medical applications being developed contain millions if not tens of millions of lines of software code. We will be dealing with these inadvertent flaws for a decade or more from now. So we must account for this with additional preventative and detective controls.

5. Anecdotal electronic evidence also suggests there are a lot more security incidents than what is currently reported. As part of normal information security monitoring, it is quite common to find information about other companies that have been attacked or even compromised. These indicators might be something as simple as malware traffic emanating from a partner's network or the observation of another company's name showing up in a data dump released by an attacker. In fact, there are web services like Shodan that specialize in identifying and cataloging vulnerable systems and devices including many from the healthcare industry in an easily searchable web interface.

When all of these observations are combined, it leads me, and many of my peers, to believe that the cybersecurity situation in the healthcare industry is far worse than what public reporting indicates. Neither private industry nor the government can solve this problem alone; we must work collaboratively and transparently to reduce this risk.

THE VALUE OF PUBLIC-PRIVATE PARTNERSHIPS IN CYBERSECURITY

The notion of public – private partnerships for cybersecurity first gained traction in 1997 following the publication of recommendations from the President's Commission on Critical Infrastructure Protection. These recommendations were codified in Presidential Decision Directive/NSC 63- Critical Infrastructure Protection which specified the industry segments that should be considered critical infrastructure, appointed a sector specific agency to coordinate the public-private partnership, and identified ten tasks that should be accomplished by each sector. A Government Coordinating Council and Sector Coordinating Council were created to represent the myriad of government departments/agencies and private sector participants respectively. The tasks included an assessment of threats and vulnerabilities that might impact the sector, the development of a sector-wide remediation/protection plan, and the sharing of intelligence information between the government and private sector. Although subsequent administrations have tweaked the industries and functions that make up the critical infrastructure and have made minor modifications to the tasks on which each sector should focus, by and large there has been support for the concept for two decades.

The healthcare and public health sector has been designated a part of the critical infrastructure since PDD-63. The Department of Health and Human Services (HHS) has been the sector specific agency since that time. However, it is only in recent years that the topic of cybersecurity has become a prominent issue. The Sector Coordinating Council now devotes a regular portion of its meetings and monthly teleconferences to discussing developments in the cybersecurity space and has established working groups to tackle items of common interest among the members. The NH-ISAC, created in 2010, has grown from about a dozen original members to more than 200 participating companies and it continues to attract more and more of the thousands of healthcare entities that exist in the United States. More importantly the quantity and quality of actionable intelligence shared by members has increased substantially in the last 12-18 months. The NH-ISAC has stood up working groups that work collaboratively to identify new sources of threat intelligence and ways to disseminate to all parties in the most effective manner, and to collaborate on ways to more effectively secure "big data" within the healthcare industry, but both organizations have the potential to do even more.

At the same time, other public-private partnerships have grown out of a desire to reduce the cost and complexity of business. The SAFE BioPharma Association was founded more than a decade ago out of a shared desire between the government and private industry to reduce the cost and complexity of submitting new drug applications to the Food and Drug Administration (FDA). In order to move away from paper-based submissions, all parties needed to agree on a mechanism that would ensure data integrity, provide for non-repudiation, and ensure trust in the identity of the signer. The members of SAFE BioPharma worked closely with the FDA, the National Institute for Standards and Technology (NIST), the General Services Administration (GSA), and regulators in the European Union and Japan to create a digital identity and digital signature standard that today is accepted by all parties. The standard creates an interoperable digital identity ecosystem in which all identities can be trusted at known risk-levels. It allows government agencies and private sector healthcare providers to have standardized trust for authentication and signing. Vendors have a tool for standardizing trust in their products and applications and the user can have a single identity for use across the ecosystem. The standard has been certified to meet US government federal identity standards[vii] and is used on electronic submissions, contracts, and other critical workflows that require integrity, identity trust, and non-repudiation around the world. More importantly, the industry has recently started adopting this digital identity standard for authentication purposes, much in the manner the US Federal Government rapidly adopted the use of Personal Identity Verification (PIV) cards for strong authentication following the Office of Personal Management (OPM) breach. According to Verizon's 2016 Healthcare Data Breach Report[viii], two out of every three healthcare data breaches have been caused by hijacked user names and passwords. SAFE BioPharma members hope to increase the use of standards-based authentication credentials across the healthcare industry. Particular emphasis is being placed on multi-factor authentication capabilities across the healthcare industry using the SAFE BioPharma standard and other recognized standards that meet the same level of security – all based on NIST and GSA standards.

As a participant and user of services provided by all three public-private partnerships, I feel each provides tremendous value and has become an essential part of my organization's cybersecurity program. We leverage the intelligence provided by the NH-ISAC to update our defenses on a continuous, 24x7 basis, we use the NH-ISAC's benchmarking service to identify areas in where we may learn from our peers, we leverage SAFE BioPharma compliant digital identities in collaborating with peer organizations, and we actively participated in the recent DHS Cyberstorm table top exercise. But there are many opportunities to further mature and develop these capabilities.

OPPORTUNITIES FOR FURTHER PARTNERSHIP AND COLLABORATION

1. **Appoint a Healthcare Sector Cybersecurity Liaison**. HHS should appoint a senior cybersecurity professional as a liaison to the private sector. Today the Assistant Secretary for Preparedness and Response (ASPR) has the responsibility for ensuring the healthcare sector is prepared to respond to a critical health emergency such as a pandemic flu outbreak or the disruption of critical health infrastructure from a natural disaster as occurred in New

Orleans during Hurricane Katrina. The Office of National Coordinator (ONC) has a Chief Privacy Officer who, along with the HHS Office of Civil Rights (OCR), works with the private sector on privacy policies and implements enforcement actions when necessary. HHS also has a Chief Information Security Officer (CISO) within the Office of the Chief Information Officer (CIO) who is primarily responsible for protection of HHS systems and services. All four of these offices interact with the private sector but none of them have cybersecurity outreach as their primary mission. A cybersecurity liaison would be the primary focal point for outreach to the private industry on topics of cybersecurity. The role would not supplant current responsibilities, but instead focus on education and awareness of cybersecurity risks within the sector, advocacy for the use of cybersecurity tools and capabilities provided by the Department of Homeland Security (DHS), and collection of key issues from the sector. The liaison would also chair a GCC working group on cybersecurity that would work closely with the Sector Coordinating Council equivalent.

2. **Develop Cybersecurity Appendix to Healthcare & Public Sector Specific Plan**. While cybersecurity concerns were captured in the latest iteration of the Healthcare and Public Health Sector Specific Plan - May 2016[ix], a more thorough and detailed appendix should be added to the existing plan to better assist public and private sector entities in developing their own cybersecurity incident response plans. This appendix should include templates and guidelines to help smaller and less mature organizations create at least a rudimentary cybersecurity response plan.
3. **Increase the Quality of Cybersecurity Intelligence and the Speed with Which It is Shared.** While there has been a significant increase in the quantity and timeliness of information shared by government agencies via DHS over the last 24 months, there is still

opportunity to improve both the quality of information and speed at which it is shared. Cybersecurity defenders need to respond to threats in minutes, if not seconds. Waiting days or even weeks for information to be shared diminishes the value of the information. For example, if an entity discovers a sophisticated phishing email that has been able to bypass an organization's email filters, it is critical that information on the subject line, sender's address, and other data about the message be sent out to others as quickly as possible so that the other security teams can search for and delete these messages before their users fall victim to an attack. Today, members of the NH-ISAC are sharing this type of information in near real-time. We still need to increase the percentage of members willing to share but we also need the government to share healthcare related cyber intelligence at similar speeds. Ultimately, we need to automate the entire process to minimize any delays in responding to rapidly changing threats.

4. **Facilitate Healthcare Cybersecurity Table Top Exercises and Simulations**. DHS conducts a nation-wide, cybersecurity exercise every two years. The latest exercise, Cyber Storm V, was conducted March 8-10, 2016. It was the first year in which the healthcare sector had dedicated participation in the exercise. The exercise included a number of healthcare specific scenarios that tested the readiness of the sector to respond to a cybersecurity emergency. The lessons learned were invaluable . As the SSA for the healthcare sector, HHS should consider conducting smaller and more frequent exercises with a broader array of healthcare firms and include scenarios that substantially test the resilience of the sector.
5. **Collaborate on the Implementation of a Digital Healthcare Identity Based on Leading Government and Private Sector Standard That Are Mature and In Place.** Passwords

are still the most frequently used authentication mechanism to gain access to healthcare data and systems and should not be. Passwords are one of the least effective mechanisms to protect sensitive data and applications. Users tend to select easy to remember passwords that can be defeated with widely available password guessing tools. If users employ complex passwords, they tend to reuse these on different systems. Consequently, if one system gets breached the attacker can use the same password to access other systems and potentially escalate the breach/attack. Most security professionals recommend utilizing multi-factor authentication solutions to protect critical systems. This technique combines a token (e.g. smartcard, smartphone, or one-time password generating device) or a biometric method (e.g. fingerprint reader) plus a password to reduce the likelihood of a breach. The problem with this approach is that without standards that allow a digital identity to be reused, users will quickly be encumbered with a wide array of smartcards, devices, and biometric readers to gain access to the many systems they need. This would be costly and extremely complex to manage and would create significant confusion for the user. The government and industry The government and industry have standards and solutions today that will work for patients and healthcare.

In some respects, the government and private sector are de facto administrators of a public-private partnership for the healthcare sector. Government agencies are responsible for public health, for regulation of therapies, medicines, and healthcare providers, and for insurance coverage of a significant portion of the US population. The private sector provides the services, products, medicines and delivery system. Government agencies and larger healthcare firms should build out the healthcare identity ecosystem by implementing existing Healthcare Digital Identity standards. Such an ecosystem would not only significantly improve cybersecurity, but also streamline business processes and rationalize the current fragmented, redundant identity trust issue in healthcare. Further, government agencies and private sector entities should facilitate the adoption of strong authentication by their small firm partners.

6. **Develop Healthcare Sector Implementation Guide to Complement the NIST Cybersecurity Framework (CSF).** Under Executive 13636 – Improving Critical Infrastructure Cybersecurity, the White House tasked NIST to develop a cybersecurity framework that "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." NIST published the first version of the Cybersecurity Framework in February 2014. The Framework has been quickly adopted by many industry sectors as the baseline against which the members measure the maturity of their cybersecurity programs. A recent study by HIMSS[x] found that 61% of healthcare companies have already adopted the standard to some degree. However, there is a growing demand within the sector for implementation guidelines that specify how to align with the NIST controls given the unique nature of industry. NIST has already developed a draft implementation guideline for the critical manufacturing industry. HHS should consider working with NIST and the private sector to produce a set of specific guidelines for the implementation of the NIST Cybersecurity Framework within healthcare entities.

7. **Collaborate with Global Agencies and Institutions.** Although healthcare delivery and healthcare insurance are conducted by and large nationally based companies, pharmaceuticals, medical device companies, research facilities, and some public health entities operate at an international scale. It is critical that HHS and the private sector work

together with peers in other countries to ensure the adoption of common cybersecurity standards and identify ways in which threat intelligence may be shared more broadly across borders.

8. **Collaborate on Ways to Address the Small Business Challenge**. One of the growing challenges we face in sharing threat intelligence throughout the sector is that smaller, less mature entities without cybersecurity teams have a significant challenge consuming the information that is shared among NH-ISAC members. This is particularly true for the rapid dissemination of indicators of compromise that are in a machine-readable format. This information facilitates the rapid response necessary to deal with quickly evolving threats, but it hinders the ability of less mature entities to consume the information. As larger organizations move to automated sharing and response, this is likely to increase the gap between them and the small entities. HHS should work with the private sector to identify ways in which smaller entities can stay aligned with the quickly changing methods of automated sharing.

9. **Recruit Departing Service Members to Help Offset the Shortage of Cybersecurity Personnel in the Critical Infrastructure Segments**

   One of the greatest challenges we face in the healthcare sector and many other critical infrastructure segments is the shortage of adequately trained personnel to address the rapidly changing cybersecurity threat. Some studies have indicated that there as many as 200,000 open cybersecurity roles in the United States alone and that number is sure to rise as new software and devices work their way into every aspect of our lives[xi]. HHS, DHS, and other Sector Specific Agencies should work with private industry to identify critical cybersecurity roles within the private sector for departing military personnel. The departing military personnel would be required to take a basic cybersecurity curriculum at Cyber Command before leaving active duty. In return for this valuable training, the service member would be required to serve an additional period of time in the National Guard or Reserves during which time the service member would be subject to recall in a national or state-level cyber emergency within any critical infrastructure segment. The private sector would assist the service member in the completion of any degree required for the private sector role. This would provide an immediate pipeline of cybersecurity talent to the private sector. It would also provide states and the federal government with a cadre of trained cyber professionals upon which they could draw. Finally, and perhaps most importantly, it would create opportunities for departing service members to enter a lucrative and growing field.

I believe that if these recommendations were implemented, we would significantly improve the state of cybersecurity in the healthcare industry. We would be able to respond to emerging threats in a more rapid and effective manner while we made it harder for those threat actors to gain a foothold in any healthcare entity. More importantly, these recommendations would help create a greater level of trust among public and private members of the sector which would ensure better collaboration in a time of crisis.

I will conclude my testimony on one final note. If we are unsuccessful in these endeavors and we are unable to significantly reduce the cybersecurity risk that we face, we may delay or even lose the opportunity to utilize promising new health information technology that has the potential to save and improve lives around the world. We may also hinder the ability to take cost out of the healthcare system through more aggressive automation. We cannot let that happen. Thank you again for the opportunity to present and I look forward to your questions.

[i] http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

[ii] https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

[iii] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEJ03320USEN

[iv] The reporting of material events is only required at publicly traded companies. Many, if not most, of the healthcare delivery entities are privately-held or operate as non-profit associations and this requirement would not apply.

[v] https://www.aei.org/wp-content/uploads/2014/06/-american-health-economy-illustrated_145021349951.pdf

[vi] http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html

[vii] The SAFE BioPharma standard meets both the US Federal Public Key Infrastructure (PKI) and Federal Identity, Credential, & Access Management (FICAM) standards. The SAFE BioPharma PKI Certificate Authority is cross-certified with the US Federal PKI Bridge.

[viii] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[ix] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

[x] The second annual HIMSS Analytics HIT Security and Risk Management Study

[xi] http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/