SoCal HIMSS 5th Annual Privacy & Security Forum: What Has Happened and Where We are Going

HIMSS

transforming health through IT

Overview – HIMSS National P&S Initiatives (Advocacy)

- HIMSS 2014-2015 Public Policy Principles (Privacy & Security)
- HIMSS Suggested Improvements to HHS SRAT
- HIMSS Comments to NIST Cybersecurity Preliminary Framework
  - NIST incorporated some HIMSS comments into NISTCSF v1.0
- HIMSS Comments to NIST on Cybersecurity Infrastructure Framework RFI
  - NIST incorporated HIMSS comments into 12/5/14 status update

Overview – HIMSS National P&S Initiatives (Advocacy)

- HIMSS Response to Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers
- HIMSS Offers Guidance to HHS on Certified EHR Technology
- HIMSS Response to the FDASIA Health IT Report: Proposed Risk Based Regulatory Framework
- HIMSS Response to Senators Grassley and Wyden on Data Availability
- HIMSS's Response to ONC's Draft Interoperability Vision

HIMSS Educational Initiatives

- Educational initiatives include those with FBI and US DHS (ICS-CERT).
- HIMSS partners with a number of associations to produce/disseminate educational deliverables.
  - AMA-HIMSS risk assessment podcast (CME credit)
  - NCSAM (HIMSS-NCSA joint initiative)
  - DPD (HIMSS-NCSA joint initiative)
  - Stay Safe Online (HIMSS-NCSA joint initiative)
  - Others

CISA Coalition Letter to US Senate

- HIMSS joined 34 associations in nearly every sector of the American economy urging the Senate to pass quickly cyber threat info sharing legislation.
- Letter of January 27, 2015 spearheaded by the US Chamber of Commerce.
- Media coverage of the letter included The Hill, Insider Cybersecurity, and Politico.

Cyber Threat Information Sharing

- U.S. Senate Committee on Homeland Security & Governmental Affairs Hearing on 1/28/15. Highlights include:
  - Information sharing (e.g., malware indicators, malicious IP addresses, etc.) does not always need to occur with government (but can)
  - Liability protection is needed for those that do share information & protect privacy & civil liberties
  - Cyber attacks can pose significant threats to CI (widespread damage – e.g., German iron plant)
  - Nation state actors (especially from China, Russia, North Korea, Iran, other countries)
  - Federal law enforcement oftentimes notifies a victim about a breach (only ~30% of the time does the victim ID on their own)
  - Intruders spend about 74 days within a network before someone notices.

HIMSS Participation in Cross-Sector Info Sharing Initiatives

- HIMSS participates in an informal cross-sector information sharing coalition (with the water, electrical, communications, energy, finance, ICT, manufacturing, transportation sectors).
- The coalition is spearheaded by the IT Industry Council (ITI).
- Objectives are to monitor progress and activities (public & private sectors) surrounding the NIST Cybersecurity Framework.
- Associations discuss their efforts surrounding cybersecurity risk management.

National Cybersecurity Protection Act of 2014 (S. 2519)

- What is this law about?
  - Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) will facilitate cross-sector sharing of cybersecurity information with Federal and non-Federal entities. The NCCIC will:
    - Conduct analysis of cybersecurity risks and incidents;
    - Provide, upon request, incident response and technical assistance; and
    - Recommend security and resilience measures to enhance cybersecurity.
- What is the value proposition for the healthcare industry?
  - Healthcare providers currently do not have a central repository for cyber threat intelligence. Providers need to know what the current threats are in order to be prepared (both in terms of prevention and defense with respect to cyber attacks).
  - Please see our recent HIMSS Privacy and Security Committee blog post and brief on cyber threat intelligence in healthcare.

Cybersecurity Enhancement Act of 2014 (S. 1353)

- Authorizes the National Institute of Standards and Technology (NIST) to facilitate and support the development of voluntary, industry-led cyber standards and best practices for critical infrastructure, in the same way in which the NIST Cybersecurity Framework was developed (and which HIMSS commented on).
- Strengthens cyber research and development by building on existing research and development programs, and ensure better coordination across the federal government.
- Improves the cyber workforce and cyber education by making sure the next generation of cyber experts are trained and prepared for the future.
- Increases the public's awareness of cyber risks and cybersecurity.
- Advances cybersecurity technical standards.

Governmental Initiatives

- Interagency Cybersecurity Forum (Federal agencies, including FTC, FCC, DHS, & FDA; advisor is NIST).
- Amendments to Computer Fraud and Abuse Act (CFAA) may be introduced to help combat insider threat.
- Cyber threat information sharing bill is expected to be introduced.
  - HIMSS joined 34 other associations urging the Senate to quickly pass a cyber threat information sharing bill.

What does Cyber look like now?

- Hacktivists
- Nation state actors (e.g., N. Korea, China, Iran, Russia, etc.)
- Malicious & negligent insiders (a complex problem)
- Destructive malware (not just adware)
- Mainstream media & trade press reports
- Hollywood
  - Movies & TV

The Evolving Threat Space

- Threats (including cyber threats) will be multi-dimensional and the equation to be solved will be much more complex. For example:
  - Malicious insiders + phishing attacks + nation state activity
- Occam’s razor / low hanging fruit for the picking. (Save the zero day for another day.)
  - Unencrypted data
  - Very weak passwords
  - Unsecured wireless connections
  - Significant, well-known vulnerabilities + effective exploits
  - Phishing (exploit the human)
  - Elicitation (befriend the human)
  - Aging IT infrastructure (exploit the tech)

To Prevent & Defend….

- Are we ready, as a nation, for a cyber war (an unconventional war)?
- We need all hands and resources on deck.
- Security should be a primary business line (not a secondary or tertiary one)
- We need innovation to stay ahead of the threat (and more automation/AI).
  - Humans are error prone.
- We need more cross-sector info sharing.
- Is cyber defense the only option for the private sector or can we amend the law to allow for cyber offense in response to an attack?

Pathways to Solutions

- Public-private partnerships
  - Secure the human & technology
  - Know & predict the threats
  - Cross-sector engagement
  - Work with the government (not against it)
- Innovation
  - Stay ahead of the threat with automation/AI
  - Current threats, predicted threats
- Train & prepare for the event (even if it never happens)

Get Engaged & Involved!

- HIMSS Privacy and Security Committee Applications accepted through March 9, 2015
- HIMSS Privacy and Security Policy Taskforce
- HIMSS Cloud Computing Workgroup
- HIMSS Privacy and Security Toolkit Content Review Taskforce
- HIMSS Risk Assessment Workgroup

Questions?

Lee Kim, BS, JD, FHIMSS

HIMSS

4300 Wilson Blvd., Suite 250

Arlington, VA 22203

+1(703)562-8806 (direct dial)

lkim@himss.org (e-mail)

Additional References

- HIMSS Privacy & Security Toolkit: http://www.himss.org/library/healthcare-privacy-security/toolkit?navItemNumber=21184
- HIMSS Cloud Security Toolkit: http://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit?navItemNumber=21185
- HIMSS Risk Assessment Toolkit: http://www.himss.org/library/healthcare-privacy-security/risk-assessment
- HIMSS Mobile Security Toolkit: http://www.himss.org/library/healthcare-privacy-security/mobile-security-toolkit?navItemNumber=21186
- NIST Cybersecurity Framework: http://www.nist.gov/itl/cyberframework.cfm