Cybersecurity: You and I Are the Weakest Links
March 3, 2016
Servio F. Medina
Acting, Policy Branch Chief of Operations, Cybersecurity Division
Health Information Technology
Defense Health Agency
Conflict of Interest

Servio F. Medina

Has no real or apparent conflicts of interest to report.
Agenda

• Sources of publicly tracked/posted incidents
• Interactive exercise - triage and understand the nature/cause of an incident
• Discern trends in incidents - what these trends mean to you/your organization
• Emerging efforts
• Effective practices
Learning Objectives

By the end of this presentation, the audience should be able to:

• **Interpret** leading root-causes of healthcare data breaches from current statistics

• **Identify** emerging efforts to address trends in breaches that emphasize the importance and impact of the human element

• **Recognize** practical examples of effective cybersecurity, with emphasis on individual behavior and organizational culture
An Introduction of How Benefits Were Realized for the Value of Health IT

This presentation falls within “E” – Electronic Secure Data, with secondary value tied to Satisfaction and Savings.
I have received a notification letter and PIN from OPM.

SIGN UP FOR SERVICES
Lead-in Thought

• In 2006, a Veteran’s Affairs laptop was stolen from a residence potentially compromising millions of current/former service members’ PII. **LED TO:** full disk encryption on portable computing devices

• In 2007, The Johns Hopkins Hospital started a new hand hygiene program that included a communications/training campaign. **LED TO:** hand hygiene compliance rates more than doubled
Why Do People Want Medical Data Anyway?

• The switch by hackers from targeting retail systems to medical information systems is no mystery: it’s easier money
  – Stolen health records bring more money with low cost
  – Stolen healthcare information can go undetected for years and be leveraged to submit fraudulent charges to insurers

• Healthcare providers and insurers have moved quickly to implement EHRs in organizations, however, often don’t have mature data protection programs and systems in place

https://www2.idexpertscorp.com/blog/single/big-breach-targets-why-healthcare-why-now
A Few Sources of Incident Reports

• The Office of Civil Rights posts incidents involving 500+ PHI records (Google “OCR Wall of Shame”) - since 2009

• Identity Theft Resource Center (ITRC): nonprofit organization tracks and compiles statistics on data breaches - since 2005

• Privacy Rights Clearinghouse: nonprofit organization tracks and trends PII data breaches - since 2005

• DHA Privacy fields PII/PHI incident reports and guides MHS hospitals - since 2007

We will triage a few PII incidents to determine root-cause
Recall the Backup Tape Incident of 2011?

• EHR backup tapes containing PHI being transported from a hospital are stolen from an unattended vehicle

What went wrong and who is responsible for handling the incident

• Triage
  – Data on tapes is from an EHR the hospital does not administer directly
  – Backup tapes transported by an authorized contractor
Triage of Incident Exercise #1

Aurora-based University of Colorado Health began notifying more than 800 patients Thursday that an employee inappropriately gained access to their health records out of "personal curiosity."

<table>
<thead>
<tr>
<th>Company or Agency</th>
<th>State</th>
<th>Published Date</th>
<th>Breach Type</th>
<th>Breach Category</th>
<th>Records Exposed?</th>
<th>Records Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Colorado</td>
<td>CO</td>
<td>12/7/2015</td>
<td>Electronic</td>
<td>Medical/Healthcare</td>
<td>Yes - Published #</td>
<td>827</td>
</tr>
</tbody>
</table>

Source: Identity Theft Resource Center, 2015 Data Breach Report
Triage of Incident Exercise #2

A laptop and smartphone belonging to an assessment nurse were stolen from the nurse’s apartment, affecting approximately 2700 people. The laptop was password-protected and encrypted; however, the encryption key was stolen with the laptop bag. The smartphone was neither password-protected nor encrypted.

Source: Identity Theft Resource Center, 2015 Data Breach Report
Anthem, Inc. announced that outside hackers breached a database containing the personally identifiable information (PII) of approximately 80 million individuals. Just this week Anthem revised that number to 78.8 million compromised records.

Source: Identity Theft Resource Center, 2015 Data Breach Report
Interpret the Data: Statistics, Trends

Not easy to glean meaningful statistics from the raw data. You don’t have to!


- And others
Trend Micro Analysis

Identity theft and fraud victims by industry

- Healthcare: 29.8%
- Retail: 15.9%
- Government: 13.6%
- Financial: 11.2%
- Education: 10.9%
- Banking: 3.9%

Data breach methods used for identity theft and fraud

- Insider Leak: 44.2%
- Hacking or malware: 15.5%
- Portable device loss: 12.8%
- Physical loss: 9.3%
- Unintended disclosure: 6.2%
- Payment card fraud: 1.4%
- Stationary device loss: 2.3%

“PII is the likeliest data stolen; financial data, second”

Trend Micro Analysis of Privacy Rights Clearinghouse
2005–2015 Data Breach Records
Ponemon Benchmark Study on Privacy & Security of Healthcare Data (5th Annual)

• Even though medical identity theft nearly doubled in five years...the harms to individuals affected by a breach are not being addressed

• Nearly two-thirds of both healthcare organizations and BAs do not offer any protection services for patients whose information has been breached
Ponemon Benchmark Study on Privacy & Security of Healthcare Data (5th Annual)

• What security threats healthcare organizations worry about most:
  – Employee Negligence: 70%
  – Cyber attacks: 40%
  – Public cloud services: 33%

• Security incidents healthcare organizations experienced:
  – Lost or stolen: 96%
  – Spear-Phishing: 88%
  – Web-borne malware attack: 78%

• What was the root cause of the healthcare organizations’ data breach?
  – Criminal attack: 45%
  – Lost or stolen computing device: 43%
  – Unintentional employee action: 40%

Contrast root cause of MHS breaches
FY15 MHS Breach Trends

- Misdirected Postal Mail: 13.5%
- Unauthorized EHR Access: 12.4%
- Misdirected Fax: 12.2%
- Human Error: 7.9%
- Unencrypted Email: 0.4%
- Unsecure Upload: 53.6%

© HIMSS 2016
Emerging Efforts in DoD

• Department of Navy CIO Policy prohibits use of fax machines to send PII

• SSN reduction

• Data Loss Prevention
Emerging Efforts in DHA

• Privacy Overlay: enhance integration of HIPAA Security with existing DoD cybersecurity safeguards

• Increased awareness, understanding, and collaborative efforts

• Accountability and sanctions
Privacy Overlays

• Determine PII confidentiality impact level of the information (i.e., low, moderate, or high)

• Distinguish between PII and PHI to clearly document the supplemental guidance and security safeguards (controls) that apply to both

• Complement the security safeguards in place for a given system
Awareness

Screensavers (Oct 2015)

You are the weakest link in the cybersecurity chain

Want to know more?
https://info.health.mil/HIT/infosec/SitePages/KnowledgeBase.aspx
Or, search for “KnowledgeBase” from DHA HIT SharePoint

October is Cybersecurity Awareness Month

Unless you want your boss to know about it, don’t sign up with your @mail.mil

Want to know more?
https://info.health.mil/HIT/infosec/SitePages/KnowledgeBase.aspx
Or, search for “KnowledgeBase” from DHA HIT SharePoint

October is Cybersecurity Awareness Month

Cyber threat is the #1 strategic threat to the U.S. – ahead of terrorism

~ 2015 DoD Cyber Strategy

Want to know more?
https://info.health.mil/HIT/infosec/SitePages/KnowledgeBase.aspx
Or, search for “KnowledgeBase” from DHA HIT SharePoint

October is Cybersecurity Awareness Month
Understanding

• DHA CS FAQs/Knowledge Base

  – Source. Generated by: users, the organization (perception based); derive from existing policy/requirements

  – Form/Function. Many FAQs start great, but remain static. Usefulness wanes quickly; no incentive to revisit

• This can help satisfy one of the HIPAA Security requirements
Can't find the answers you need? Click here to Ask an Expert!

**Most Recently Asked Questions**

Where is the MOA between DHA and MEDCOM for transition of AO authority from Army to DHA?

AI 80 says that users are not permitted to connect personal *wireless* devices to DHA IT. Does that mean I can connect my iPod with a USB cable?

Can I plug a mobile device into my GFE laptop/desktop if it is only to charge the device?

Regarding security categorization (Step 1 of RMF), are we still going to have to go through the paper drill of having to go through categorization and approved by the Security Control Assessor and Authorizing Official Designated Representative (AODR), or is that function going strictly through eMASS?

Can my security clearance be impacted if I plug an unauthorized USB device (flash drive/iPod/phone) into my Government Furnished computer or other IT equipment?

**Most Frequently Asked Questions**

My personal email is a lot more convenient than my work email. And, I am really, really careful with all of emails (work and personal). Is use of personal email for official business prohibited even if I am really careful?

True or False? DHA employees can use commercial or personal e-mail accounts to conduct official business.

T/F: it is a common requirement to complete cyberawareness challenge more than once per fiscal year, e.g., when someone transfers from a Service to the DHA.

How do I take and track completion of cyberawareness challenge?

How do I use the CS Knowledge Base?
Collaboration: DHA Privacy

DHA Privacy & Civil Liberties Office holds two annual events that involve leaders, officials, and end users from across the organization.

• Incident Response Table Top Exercise with active participants comprised of senior leadership, including: Chief of Staff, Legal, Cybersecurity, Facilities, Public Affairs/Communications, and more

• Health Information Privacy and Security Training for all DHA and Military Health System workforce members
Collaboration: Agreements

• How do you know whether a vendor or contractor is required to meet cybersecurity/HIPAA Security requirement

• DHA CSD Service
  – Ensure cybersecurity requirements are incorporated in agreements/contracts
  – System Transfer Agreement

• Recall: Standard: Business associate contracts or other arrangements
Collaboration: Governance

• When CS requirements are not considered up front – as a functional requirement:
  – Inaccurate cost projection
  – Inefficient lifecycle sustainment
  – Delays in deployment, impact to business
  – Increased risk
Accountability

• Annual cyber awareness training tied to individual performance plans
• Increased sanctions for repeat offenses of PII breach
• Suspend network privileges for violations (e.g., USB flash drive)
Summary

• Protection of healthcare information goes way beyond technology
• The value of a conference presentation could be gauged by what you do with the information thereafter
• How does the information provided apply to your organization
• How can you use this information to make a difference in your organization
A Summary of How Benefits Were Realized for the Value of Health IT

Electronic Secure Data: effective cybersecurity
Satisfaction: impact to patient confidence if/when information is breached
Savings: cost of breaches and inefficient/ineffective cybersecurity

http://www.himss.org/ValueSuite
Questions ?
Contact Information

Servio F. Medina
Acting, Policy Branch Chief of Operations Cybersecurity Division
Health Information Technology Directorate
Defense Health Agency
Email: servio.f.medina.civ@mail.mil
Sources/References

• OPM Breach Notification:
  https://www.opm.gov/cybersecurity


• Hand hygiene:
  – http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080102591.html;
  – http://lgreen.net/precede%20apps/HandwashingPREDICEModelICHE0212.pdf

  https://www2.idexpertscorp.com/blog/single/big-breach-targets-why-healthcare-why-now

• Incident Tracking/Trending
  – http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties

• Emerging Efforts
  – https://info.health.mil/hit/infosec/SitePages/KnowledgeBase.aspx (CAC required)