Cybersecurity: Decisions, Habits, Hygiene

Session 148, February 22, 2017

Servio F. Medina, Acting Cybersecurity Policy Branch Chief, Defense Health Agency
Speaker Introduction

Servio F. Medina, CISSP, MAT
Acting Cybersecurity Policy Branch Chief
Defense Health Agency
Health IT Directorate, J-6

Bring the past only if you are going to build from it
~Doménico Cieri Estrada
Conflict of Interest

Servio F. Medina, CISSP, MAT

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

• Cybersecurity hygiene for healthcare systems parallels ongoing personal health hygiene.
Learning Objectives

• Demonstrate the inadequacy of today's cyber security training and awareness efforts

• Recognize how human behavior contributes to cyber incidents

• Illustrate ways to track and trend incidents that can trace back to bad choices and habits

• Describe innovative approaches to enhance cybersecurity awareness and understanding
A Summary of How Benefits Were Realized for the Value of Health IT

This presentation falls within E = Electronic Secure Data.

1. E: Data Sharing, Improved security of patient records, EHR Security Prevents Privacy Breaches

2. E: Enhanced Communication, Increased use of patient portals, Secure Communication with Doctor

The focus is on various elements/influencers of human behavior that contribute to breaches of healthcare information, and considerations for sustainable changes to reduce corresponding root causes.
22 Years Ago I Was a Patient

• At the University of Florida teaching math, blew my knee out
  – Became obsessed with recon and rehab
  – Interrogated my surgeon and physical therapist
  – Created a website
Most Patients Probably

• Trust their doctor’s guidance
  – Tell me what to do (physical therapy, nutrition, etc.)
  – Spare me the details

• Regardless, do patients consistently comply?
  – Many may eventually forget, neglect, outsmart/dismiss
  – Regardless the reason, non-compliance is “risky” behavior
Risky Behavior

<table>
<thead>
<tr>
<th>Risky Driving</th>
<th>Curb Risky Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reckless</td>
<td>Quick/frequent ticket</td>
</tr>
<tr>
<td>Texting</td>
<td>Increase risk awareness</td>
</tr>
<tr>
<td>W/o Seatbelt</td>
<td>Click it or Ticket</td>
</tr>
<tr>
<td>Fatigued</td>
<td>Rumble strips</td>
</tr>
</tbody>
</table>

Drivers for and influencers of risky behavior are fairly universal.
True or False?

Your healthcare provider washes his/her hands before they meet/treat you

• **NOT necessarily true.** In 2007, The Johns Hopkins Hospital launched a get-well campaign; compliance increased
  – 35% in the first 6 months to 77% in the last 6 months of the study period among nursing providers
  – 38% to 62% among medical providers
  – 27% to 75% among environmental services staff

Source: Infection Control and Hospital Epidemiology, Vol. 33, No. 2 (February 2012), pp. 144-151.
Reported barriers to Hand Hygiene compliance include:

- lack of knowledge
- poor role models
- lack of time
- skeptical attitudes
- dermatologic problems
- poor placement of hand cleaning stations

Source: Infection Control and Hospital Epidemiology, Vol. 33, No. 2 (February 2012), pp. 144-151.
Cyber Incidents

- Ponemon: Employee mistakes, third-party snafus, and stolen computer devices are the root cause of 50% of data breaches in healthcare.
- Tend Micro: Healthcare (at 29.8%) is forerunner for identity theft and fraud victims by industry.
- DoD: **80% of all successful cyber incidents can be traced back** to poor user practices, poor network and management practices, and poor implementation of network architecture.
“80% of all successful cyber incidents”

• There’s often a lack of recognition and, in some cases, denial that human error may have been root cause

• The failure to recognize this cause and effect relationship leads individuals to sometimes place personal convenience ahead of operational security

• Cybersecurity culture does not yet include constant assessment and learning that is driven by engaged leaders who instill and reinforce needed behaviors
### Parallel: Barriers to Compliance

<table>
<thead>
<tr>
<th>Contributing Factors</th>
<th>Hopkins: Hand Hygiene</th>
<th>DoD: Cybersecurity Hygiene</th>
</tr>
</thead>
<tbody>
<tr>
<td>lack of knowledge</td>
<td>lack of constant learning</td>
<td></td>
</tr>
<tr>
<td>poor role models</td>
<td>leaders are not engaged</td>
<td></td>
</tr>
<tr>
<td>time/dermatologic problems</td>
<td>personal convenience &gt; security</td>
<td></td>
</tr>
<tr>
<td>skeptical attitudes</td>
<td>denial human error = cause</td>
<td></td>
</tr>
<tr>
<td>poor cleaning station placement</td>
<td>poor implementation/management</td>
<td></td>
</tr>
</tbody>
</table>
The Johns Hopkins Hospital

- Discovered root causes why people were not compliant
- Identified motivators and measures to change risky behavior
  - Communication campaign
  - Education
  - Environment optimization
  - Leadership engagement
  - Performance measurement and feedback

*Behavior is the mirror in which everyone shows their image*
~Johann Wolfgang von Goethe (1749-1832)
Why Don’t We Comply with Cybersecurity?

- Ignorance
- Inconvenience
- Judgement call
  - makes sense to me
  - benefit > risk
- Security Fatigue

The single biggest problem in communication is the illusion that it has taken place
~George Bernard Shaw
• Put patients at the center of their healthcare ~HHS Asst. Sec. DeSalvo and DHA Director VADM Bono (HiMSS 2016)

• Military Health System: 9.4M beneficiaries; 220K employees
Education, Training, Awareness

• The Minimum Necessary Standard* does not apply
  – 1-2 hours/year is woefully inadequate
  – Perceived as an inconvenience

• Judgement call: “Makes sense to me”
  – Forward meeting invite to personal email
  – Prioritize work to justify workaround

*45 CFR 164.502(b), 164.514(d)
Name a cause of a medical data breach

<table>
<thead>
<tr>
<th>Cause</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Error</td>
<td>5</td>
</tr>
<tr>
<td>Failure to Follow Policy</td>
<td>4</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>3</td>
</tr>
<tr>
<td>Theft</td>
<td>2</td>
</tr>
<tr>
<td>Mail Handling</td>
<td>1</td>
</tr>
</tbody>
</table>

Total possible points: 15

Points derived from informal survey of privacy and security officials
Security Fatigue, a NIST Study

Defined as a weariness or reluctance to deal with computer security, which can lead to

- avoiding decisions
- choosing the easiest option among alternatives
- making decisions influenced by immediate motivations
- behaving impulsively
- failing to follow security rules

Security Fatigue, a NIST Study

Suggests ways to alleviate security fatigue and “help users maintain secure online habits and behavior”

- Limit the number of security decisions
- Make it very simple to choose the right security action
- Design to encourage consistent decision making

Nudge Theory

• A nudge is any noncoercive alteration in the context in which people make decisions
  – placing fruit at eye level in school cafeterias: enhances its popularity by as much as 25%
  – a fly etched into the wells of urinals, giving male patrons something to aim at: spillage was reduced by 80%

Nudge

• Speed displays: effective in calling drivers’ attention to their driving speed

• Grid of lines on the road ahead: evenly spaced at first, begin to bunch closer near the apex of the curve, which gives impression of speeding up

Sources: Motivations for Speeding Volume II: 2013 Findings Report, NHTSA
Nudge

• Browser habits

Your connection is not private

Attackers might be trying to steal your information from www.healthit.gov (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is www.healthit.gov; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.
All active links contained in this email were disabled. Please verify the identity of the sender, and confirm the authenticity of all links contained within the message prior to copying and pasting the address to a Web browser.

A phishing email is being circulated on mock HHS Departmental letterhead that prompts recipients to click a link. In the event that you or your organization has a question as to whether it has received an official communication from our agency regarding a HIPAA audit, please contact us via email at OSOCRAudit@hhs.gov <Caution-mailto:OSOCRAudit@hhs.gov>
Performance measures and feedback

• DHA Annual Performance Evaluations
  – All: Completion of Cyber Awareness Training
  – HIT: Timely/Acceptable reporting of cybersecurity

As long as you have humans, you have human errors. So what you try to do is layer your defenses against human error.

~WMATA Chief Safety Officer Patrick Lavin (Nov 22 2016)
Closing Thoughts, Part I

- management of "human controls" need improvement
- most employees consider security a detriment to productivity
- incorporate computer security into performance evaluations
- individual must be held accountable
- advisory and counseling can short-circuit stresses and problems

*Observations made during Congressional testimony on the Computer Security and Training Act of 1985*
One Last Question, Then Your Turn

- **True/False**: Technical controls alone are enough to adequately configure/protect an information system?
  
  (hopefully you answered **False**; refer to HIPAA Security)

- Education, Marketing, Nudging: ideally we integrate technical and non-technical controls to positively influence human behavior
References

Questions

• If you want more sessions like this (or not), please complete the evaluation
• Welcome your reachout
  • @SecurityServio
  • servio.f.medina.civ@mail.mil

If you choose not to decide, you still have made a choice
~Rush, Freewill
Credit for Nudging Cybersecurity?

• SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment, Conference Paper, June 2104*

• Abstract. Behavior-change interventions are common in some areas of human computer interaction, but rare in the domain of cybersecurity. This paper introduces a structured approach to working with organisations in order to develop such behavioral interventions or ‘nudges’.

*Lynne Coventry\textsuperscript{a}, Pam Briggs\textsuperscript{a}, Debora Jeske\textsuperscript{a}, Aad van Moorsel\textsuperscript{b}
\textsuperscript{a} Psychology & Communication Technology Lab, Northumbria University, Newcastle-upon-Tyne, UK
\textsuperscript{b} Head of Computing Science, Newcastle University, Newcastle-upon-Tyne, UK
A Summary of How Benefits Were Realized for the Value of Health IT

This presentation falls within E = Electronic Secure Data.

1. E: Data Sharing, Improved security of patient records, EHR Security Prevents Privacy Breaches

2. E: Enhanced Communication, Increased use of patient portals, Secure Communication with Doctor

The focus is on various elements/influencers of human behavior that contribute to breaches of healthcare information, and considerations for sustainable changes to reduce corresponding root causes.