Servio Medina
Lead, Cybersecurity Policy
Defense Health Agency, J-6

Cybersecurity: Decisions, Habits, Hygiene
June 19, 2017

Bring the past only if you are going to build from it
~Doménico Cieri Estrada
Learning Objectives

1. Demonstrate the inadequacy of today's cyber security training and awareness efforts.
2. Recognize how human behavior contributes to cyber incidents.
3. Illustrate ways to track and trend incidents that can trace back to bad choices and habits.
4. Explore innovative approaches to enhance cybersecurity awareness and understanding.
First: Show of Hands

• How many of you use Social Media?

“6 in 10 of you will share this link without reading it, a new, depressing study says” ~Washington Post, June 6, 2016

• We are inundated with and often succumb to click-bait, soundbite information. *Marketing!*
And in the Workplace

• Doing more with less resources/time
• Suffering not only Decision Fatigue, but also “Security Fatigue”*
• Expected to have answers now, vice ability to produce answers
• *Is cybersecurity supposed to make sense?*

• Medical devices: “If it's got IP, it's IT.”

• What about non-networked device/IT? They pose less risk than networked ones…therefore, require less cybersecurity (effort, cost). Makes sense?

Whether medical devices or massive weapons systems, "if it's got a computer in it, it can be cyberattacked…It doesn't matter if it's connected to a network.” ~DoD CIO Richard Hale, 2016
Federal official: lessen end-user involvement; make IT sophisticated enough to safeguard information and systems. Make sense?

“94 percent of fatal crashes are caused by human error…top three killers are speed, alcohol and distraction…[even] after significant improvements in safety features built into cars”

~Source: NPR, Unsafe Driving Leads To Jump In Highway Deaths, Study Finds, 2/15/2017
Did you hear about…?

- British Airways: power surge hit servers…

- Paper operating room schedules containing 836 PHI records went missing. $475,000 settlement with HHS OCR.

- Made sense to someone = risky behavior
Risky Behavior

Your keyboard is like the wheel of your car: both get you where you need to go, but getting behind either comes with risk

<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>
Inadequacy of Training? Part 1

• **Verizon.** Privilege misuse, miscellaneous errors and physical theft and loss represent **80% of breaches** within healthcare

• **Ponemon.** Root cause of healthcare organizations’ data breach:
  - Criminal attack: 50%
  - Third-party snafu: 41%
  - Lost or stolen computing device: 39%
  - Unintentional employee action: 36%
Inadequacy of Training? Part 2

- DHA Privacy & Civil Liberties. Most PII incidents trace to human error.

- 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.
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.
# Barriers to Compliance

## Hopkins: Hand Hygiene

<table>
<thead>
<tr>
<th>Lack of Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor Role Models</td>
</tr>
<tr>
<td>Time/Dermatologic Problems</td>
</tr>
<tr>
<td>Skeptical Attitudes</td>
</tr>
<tr>
<td>Poor Cleaning Station Placement</td>
</tr>
</tbody>
</table>
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.

DoD Cybersecurity Culture and Compliance Initiative, Sep 2015
**Parallel: Barriers to Compliance**

<table>
<thead>
<tr>
<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>
</tr>
<tr>
<td>poor role models</td>
<td>leaders are not engaged</td>
</tr>
<tr>
<td>time/dermatologic problems</td>
<td>personal convenience &gt; security</td>
</tr>
<tr>
<td>skeptical attitudes</td>
<td>denial human error = cause</td>
</tr>
<tr>
<td>poor cleaning station placement</td>
<td>poor implementation/management</td>
</tr>
</tbody>
</table>
Changing Risky Behavior

Hopkins: Hand Hygiene

<table>
<thead>
<tr>
<th>Communications Campaign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Environment Optimization</td>
</tr>
<tr>
<td>Leadership Engagement</td>
</tr>
<tr>
<td>Performance measurement/feedback</td>
</tr>
</tbody>
</table>

“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 Sec. Matthews-Burwell and DHA Director VADM Bono (HiMSS 2016)

• Military Health System: 9.4M beneficiaries; 205K employees
FAMILY FEUD

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>

Points derived from informal survey of privacy and security officials

Total possible points: 15
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, Driving Examples

- Speed displays: effective in calling drivers’ attention to their driving speed, and possibly that it was recorded

- 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

Source: System Analysis of Automated Speed Enforcement Implementation, April 2016
Nudge, Cyber Example 1

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>
• Data Loss Prevention: screen every email for possible loss of PII/PHI?

• Outlook Classification Tool: prompt for classification of every email?

• Others?
Key Takeaways

This presentation “works” if it sticks with/influences you after you return to your workplace.

How do we know whether cybersecurity training/awareness works?

Have the right message to the right people, at the right times

Closing Thoughts, redux

RECAP?

• 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
Questions?

• Feel free to contact me:
  o @SecurityServio
  o servio.f.medina.civ@mail.mil

“If you choose not to decide, you still have made a choice”
~Rush, Freewill
References

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