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?*

*Paper: B. Stanton, M.F. Theofanos, S.S. Prettyman, S. Furman. Security Fatigue. IT Professional, Sept.-Oct. 2016.

Does This Make Sense? Example 1

- 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*

Does This Make Sense? Example 2

- 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

Risky Driving	Curb Risky Behavior
Reckless	Quick/frequent ticket
Texting	Increase risk awareness
W/o Seatbelt	Click it or Ticket
Fatigued	Rumble strips

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

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
lack of knowledge
poor role models
time/dermatologic problems
skeptical attitudes
poor cleaning station placement

“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

DoD Cybersecurity Culture and Compliance Initiative*, Sep 2015*

Parallel: Barriers to Compliance

Hopkins: Hand Hygiene	DoD: Cybersecurity Hygiene
lack of knowledge	lack of constant learning
poor role models	leaders are not engaged
time/dermatologic problems	personal convenience > security
skeptical attitudes	denial human error = cause
poor cleaning station placement	poor implementation/management

Changing Risky Behavior

Hopkins: Hand Hygiene

Communications Campaign

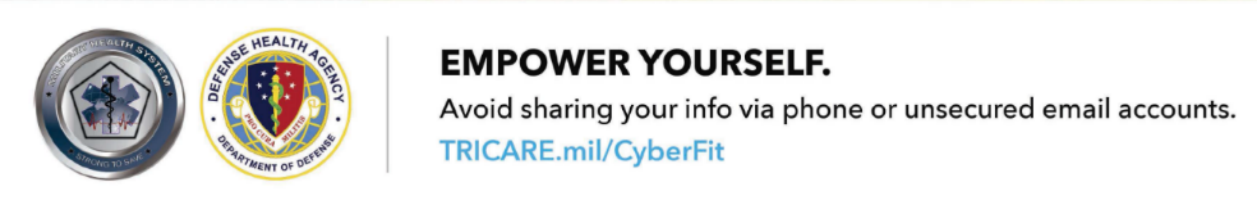
Education

Environment Optimization

Leadership Engagement

Performance measurement/feedback

> “The single biggest problem in communication is the illusion that it has taken place.”
> *~George Bernard Shaw*



EMPOWER YOURSELF.

Avoid sharing your info via phone or unsecured email accounts.

TRICARE.mil/CyberFit

- *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

Human Error	**5**
Failure to Follow Policy	**4**
Unauthorized Access	**3**
Theft	**2**
Mail Handling	**1**

Points derived from informal survey of privacy and security officials

X X X

Total possible points: 15

0

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%

Source: The Chronicle Review on Sunstein's *Nudge: Improving Decisions About Health, Wealth, and Happiness,* May 9, 2008

Nudge, Driving Examples

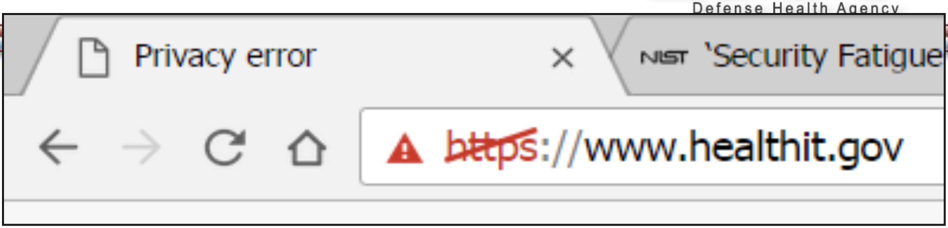
- Speed displays: effective in calling drivers’ attention to their driving speed, and possibly that it was recorded

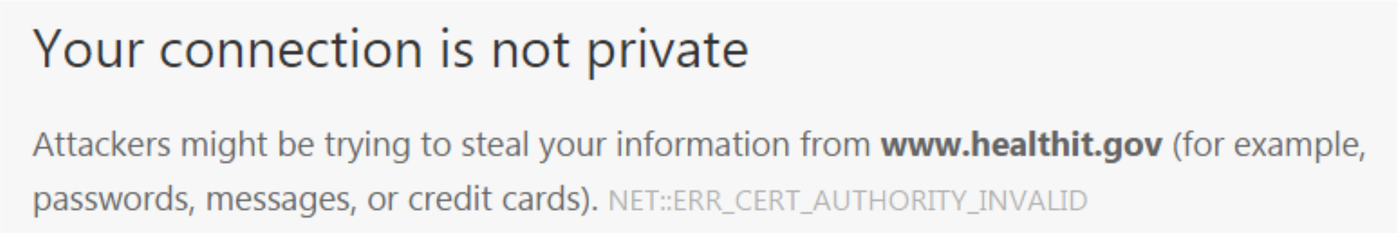
- Grid of lines on the road ahead: evenly spaced at first, begin to bunch closer near the apex of the curve, which gives impression of speeding up

Source: System Analysis of Automated Speed Enforcement Implementation, April 2016
Source: Chronicle Review on Sunstein's Nudge: Improving Decisions About Health, Wealth, and Happiness, May 2008

Nudge, Cyber Example 1

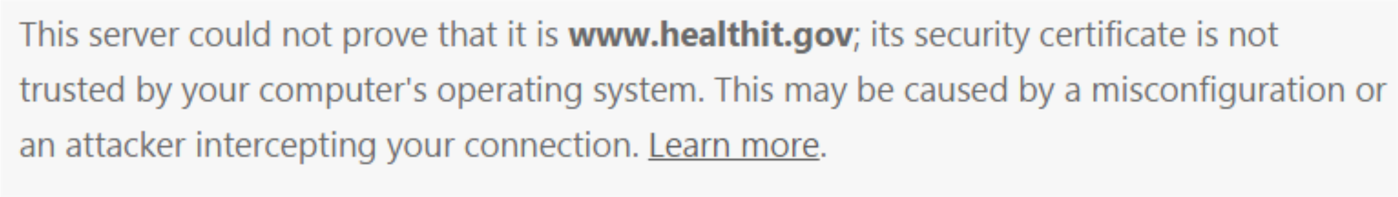
Browser habits





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.

Nudge, Cyber Example 2

-----Original Message-----
From: OCR HIPAA Privacy Rule information distribution
Sent: Tuesday, Nov 29, 2016
Subject: [Non-DoD Source] OCR-PRIVACY-LIST Digest

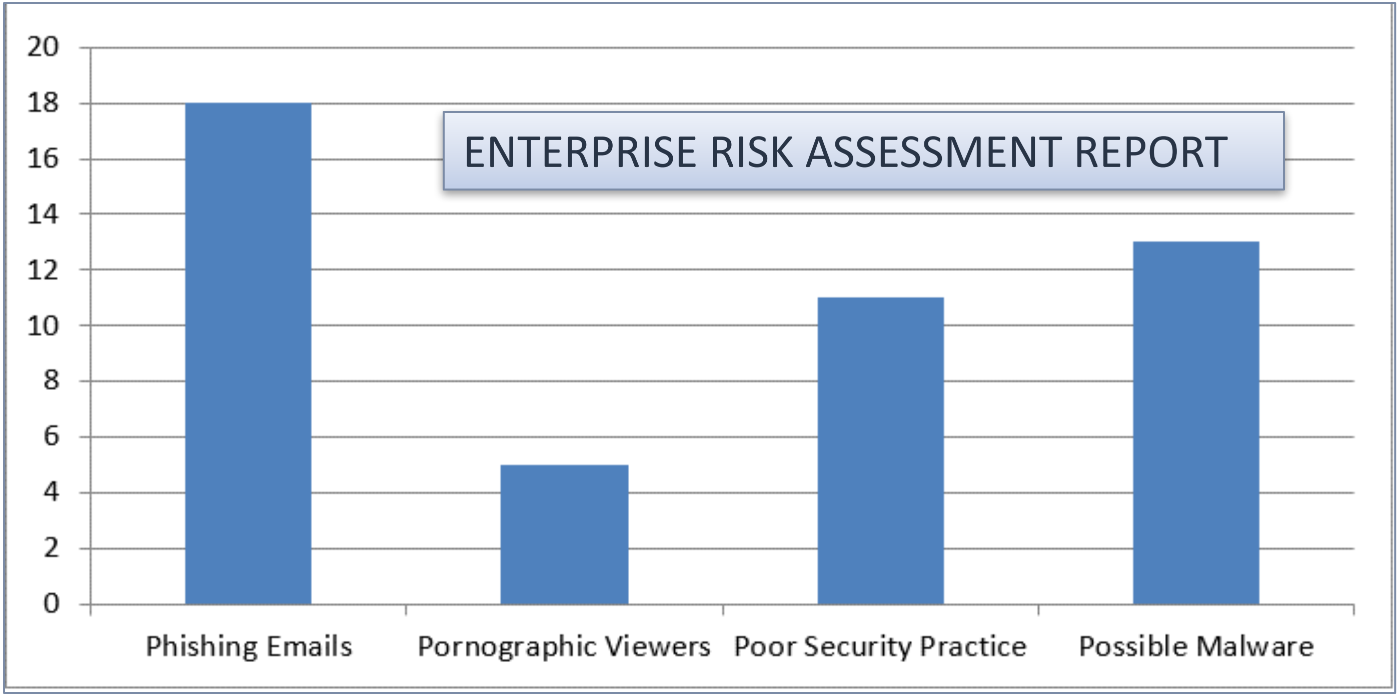
All active links contained in this email were disabled. Please verify the identity of the sender, and confirm the authenticity of all links contained within the message prior to copying and pasting the address to a Web browser.

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>

Nudge, Cyber Examples 3-5

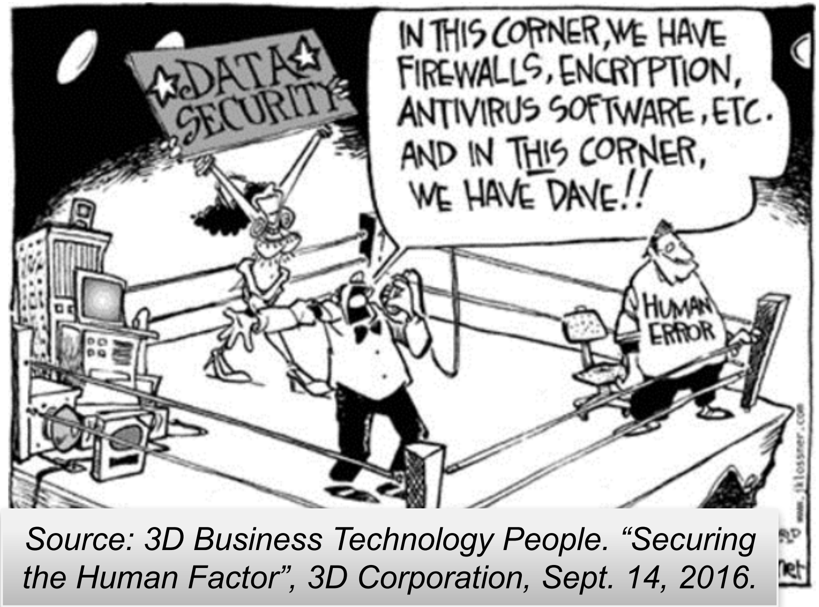
- Data Loss Prevention: screen every email for possible loss of PII/PHI?
- Outlook Classification Tool: prompt for classification of every email?
- Others?

Track and Trend – Network Assessment



Key Takeaways

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


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com

Source: 3D Business Technology People. “Securing the Human Factor”, 3D Corporation, Sept. 14, 2016.

How do we know whether cybersecurity training/awareness works?

Have the right message to the right people, at the right time<u>s</u>

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

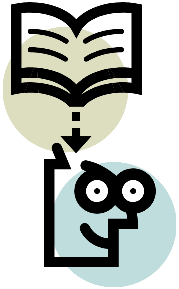
Questions?

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

"If you choose not to decide,
you still have made a choice"
~Rush, Freewill

References

1. http://www.beckershospitalreview.com/quality/20-hospitals-with-great-hand-hygiene-programs.html
2. http://lgreen.net/precede%20apps/HandwashingPRECEDEModelICHE0212.pdf
3. http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080102591.html
4. http://www.law.uchicago.edu/news/chronicle-review-sunsteins-nudge
5. https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents
6. http://jonahberger.com/books/contagious/
7. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
8. http://www.idtheftcenter.org/id-theft/data-breaches.html
9. http://www.privacyrights.org/data-breach
10. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf
11. http://www.fiercehealthit.com/story/hospital-cyberdefense-high-dods-priority-list/2016-02-19
12. https://www2.idexpertscorp.com/blog/single/big-breach-targets-why-healthcare-why-now
13. http://www.himss.org/News/NewsDetail.aspx?ItemNumber=48552
14. http://www.hhs.gov/about/news/2016/02/29/hhs-announces-major-commitments-healthcare-industry-make-electronic-health-records-work-better.html
15. http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf
16. http://www.healthcareitnews.com/news/cybersecurity-special-report-ransomware-will-get-worse-hackers-targeting-whales-medical-devices
17. https://www.nhtsa.gov/staticfiles/nti/pdf/812257_SystemAnalysisASE.pdf
18. https://www.nhtsa.gov/Driving-Safety/Aggressive-Driving
19. https://www.nhtsa.gov/staticfiles/nti/pdf/811996-InvestUseFeasSpeedWarnSys.pdf
20. https://www.nhtsa.gov/staticfiles/nti/pdf/2011_N_Survey_of_Speeding_Attitudes_and_Behaviors_811865.pdf
21. https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly
22. https://www.researchgate.net/publication/268502835_SCENE_A_Structured_Means_for_Creating_and_Evaluating_Behavioral_Nudges_in_a_Cyber_Security_Environment
23. http://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html
24. http://www.npr.org/2017/02/15/515441751/unsafe-driving-leads-to-jump-in-highway-deaths-study-finds
25. https://www.researchgate.net/publication/268502835_SCENE_A_Structured_Means_for_Creating_and_Evaluating_Behavioral_Nudges_in_a_Cyber_Security_Environment



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[a], Pam Briggs[a], Debora Jeske[a], Aad van Moorsel[b]
[a] Psychology & Communication Technology Lab, Northumbria University, Newcastle-upon-Tyne, UK
[b] Head of Computing Science, Newcastle University, Newcastle-upon-Tyne, UK