Cyber Fluency: Si Vis Pacem Para Bellum

Session #215, February 14, 2018

Justin Hodges, Chief, Cybersecurity Operations Center, DHA J-6

Servio Medina, Chief Cybersecurity Oversight, Governance and Strategy, DHA J-6

Justin Williams, Deputy Chief, Cybersecurity Operations Center, DHA J-6
Conflict of Interest

• Justin Hodges, C|EH, MTS
  – Has no real or apparent conflicts of interest to report
• Servio Medina, CISSP, MA
  – Has no real or apparent conflicts of interest to report
• Justin Williams, CISSP, DSc.
  – Has no real or apparent conflicts of interest to report.
Agenda

• Learning Objectives

• Meaning of Cyber Fluency

• Panel Discussion of Cyber Fluency

• Questions
Learning Objectives

- Discuss significance of being cyber fluent and identify cyber implications of decisions
- Discuss cyber security deltas between DoD and Commercial
- Explain process behind determining mission objectives and risk tolerance
- Compare and contrast business decisions against mission objectives to provide an informed decision
- Propose methods that can be used to evaluate/measure cyber fluency
Si vis pacem, para bellum

“If you want peace, prepare for war”

• Commonly used to affirm one of the most effective means to ensure peace is to be armed to defend oneself. Must:
  • Recognize opportunities to integrate cybersecurity into mission objectives allows for self reflection
  • Manage operational risk against business requirements
  • Hold employees accountable

DHA/MHS: Ready Medical Force, Medically Ready Force. Prepare IT and humans
Cyber Health: Prepare IT

- **HARDEN DEVICES**: reduce internal and external attack vectors into DoD [hospital] information networks
- **REDUCE ATTACK SURFACE**: reduce external attack vectors into DoD [hospital] information networks…
- **STRONG AUTHENTICATION**: degrade the adversaries' ability to maneuver on DoD information networks
- **ALIGNMENT TO CYBERSECURITY SERVICES**: improve detection of and response to adversary activity

Source: DoD Cybersecurity Discipline Implementation Plan
What makes DoD Hospitals Different?

HARDEN DEVICES

• via Security Technical Implementation Guides (STIGs) = how to securely configure a host: consistent across the DoD

• Formally “Authorize” IT to operate: Assess for risk, configure with appropriate security controls, and then certify and document that the device/network is approved to operate/connect
What makes DoD Hospitals Different?

REDUCE ATTACK SURFACE

• Medical Community of Interest (Med-COI) = one DoD health enterprise to rule them all
  • 12-Zone Architecture: Zone 6a is Medical Devices and Equipment (MDE), Zone 6b is Facilities-Related Control Systems
• Desktop-to-Datacenter (D2D) Program = Migrating Military Treatment Facilities to Med-COI and subsequently connecting to MHS GENESIS (new EHR)
  • Inheritance of cyber controls and monitoring
What makes DoD Hospitals Different?

STRONG AUTHENTICATION

• Two-Factor authentication (Public Key Infrastructure)

• Required for “all” IT access: workstations, servers, web sites, EHRs in operating rooms…
What makes DoD Hospitals Different?

ALIGNMENT TO CYBERSECURITY by monitoring activity at the perimeter, on the DoDIN, and on all DoD information networks: ensures rapid identification and response to potential intrusions

- Cybersecurity Operations Centers = Operational governors of Military Health’s cyberspace
- CSSP = Computer Network Defenders, Monitors, Analysts and Incident Responders
Cyber Health: Prepare Humans

• **FLUENT**: leaders and their staffs need to be “cyber fluent” so they can fully understand the cybersecurity implications of their decisions. *2018 DoD Cyber Strategy*

• **FIT**: ongoing promotional campaign directed at 9.5M beneficiaries. *Defense Health Agency, 2016-Present*

• **HYGIENE**: cybersecurity hygiene = personal hygiene in that it is the individual’s responsibility; it includes all online behaviors. *2017 Health Care Industry Cybersecurity Task Force Recommendation*
## Cyber Health: Do or Don’t?

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Do/Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognize human error as a root cause</td>
<td></td>
</tr>
<tr>
<td>Base separation of duties on separated functions</td>
<td></td>
</tr>
<tr>
<td>Rely on annual HIPAA and Cybersecurity training</td>
<td></td>
</tr>
<tr>
<td>Configure medical IT with DoD requirements</td>
<td></td>
</tr>
<tr>
<td>Balance mission objectives against risk tolerance</td>
<td></td>
</tr>
</tbody>
</table>
Questions

- Justin Hodges, Chief, CyOC
- Servio Medina, Chief COGS: @SecurityServio; /in/servio
- Justin Williams, Deputy Chief

If you want more sessions like this (or not), please complete the evaluation

Everybody got mixed feelings
About the function and the form
Everybody got to elevate from the norm
~Rush, Vital Signs
Acronyms

• C|EH: Certified Ethical Hacker
• CISSP: Certified Information Systems Security Professional
• CSSP: Cybersecurity Service Provider
• CyOC: Cybersecurity Operations Center
• D2D: Desktop To Datacenter
• DHA: Defense Health Agency
• DoD: Department of Defense
• DoDIN: Department of Defense Information Networks
• EHR: Electronic Health Record
• eMASS: Enterprise Mission Assurance Support Service
• HCIC: Health Care Industry Cybersecurity
• HHS: Health and Human Services
Acronyms (continued)

• HIPAA: Health Insurance Portability and Accountability Act
• IT: Information Technology
• JFHQ-DoDIN: Joint Forces Headquarters – Department of Defense Information Networks
• Med-COI: Medical Community of Interest
• MDE: Medical Devices and Equipment
• MHS: Military Health System
• NIPR: Non-Classified Internet Protocol Router Network
• NIST: National Institute of Standards and Technology
• PIN: Personal Identification Number
• PHI: Protected Health Information
• SIPR: Secret Internet Protocol Router Network
• STIG: Security Technical Implementation Guides
References


• 2018 DoD Cyber Strategy (Summary): https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF


• STIG standards: https://iase.disa.mil

• NIST: https://www.nist.gov