The Internet of Absolutely Everything, Connected Medical Devices and BYOD - Securing the Information They Access and the Information They Can Leak

Presented at the Healthcare Security Summit BOSTON by Stephen Grimes, **Chief Technology Officer of ABM Healthcare Support Services**

Any device that can communicate with anything else provides a potential open door for the valuable information it accesses and that an organization is responsible for protecting. In our rush to connect everything together, secure information handling is very often an afterthought, if ever even a thought at all.

The broad array of BYOD handsets used for both personal and official use can easily provide a direct gateway from the public internet to some very private information. Networked medical devices are also vulnerable to malicious access as are all insecurely created IoT devices. In this session we'll look at the best practices for securing this information while limiting usage "friction", from a number of key perspectives:

- BYOD Security - as medical staff who may not even be hospital employees, routinely access patient records with their personal devices, what mechanisms can be put in place to insure the security of that information?
- Medical Device and IoT Security - these devices, while created to save and enhance lives, are often highly vulnerable to malicious attack, can this risk be mitigated?
- Could it be considered negligent to develop and or allow use of devices and applications that are fundamentally insecure?

---

http://www.healthcareinfosecurity.com/webinars/-w-651?rf=trending

The Internet of Absolutely Everything, Connected Medical Devices and BYOD: Securing the Information They Access and the Information They Can Leak

Stephen L Grimes, FHIMSS FACCE FAIMBE | ABM Healthcare Support Services

Healthcare Information Security Summit Boston
June 11, 2015 – Boston, MA

About the Speaker

Stephen L Grimes, FHIMSS FACCE FAIMBE

Chief Technology Officer, ABM Healthcare Support Services

Mr. Grimes has more than 30 years' experience with hospitals, shared service organizations, and healthcare consulting firms. He is a nationally recognized authority on topics ranging from future challenges facing clinical engineering and healthcare technology integration to medical device security and risk management. Mr. Grimes is a frequent author and speaker at both national and international venues. He is past chair of HIMSS Medical Device Security Task Force and current chair of HIMSS Patient Safety Task Force. He is a Fellow of the Healthcare Information and Management Systems Society (HIMSS), the American Institute of Medical and Biological Engineering (AIMBE) and the American College of Clinical Engineering (ACCE) where he is also a past President. In February 2011 he received the joint industry ACCE/HIMSS Excellence in Clinical Engineering & Information Technology Synergies Award. In April 2015 he received ACCE's highest honor, their Lifetime Achievement Award. Mr. Grimes is a graduate of Purdue University's Biomedical Engineering Program.

Session Description

The Internet of Absolutely Everything, Connected Medical Devices and BYOD

Securing the Information They Access and the Information They Can Leak

Any device that can communicate with anything else provides a potential open door for the valuable information it accesses and that an organization is responsible for protecting. In our rush to connect everything together, secure information handling is very often an afterthought, if ever even a thought at all.

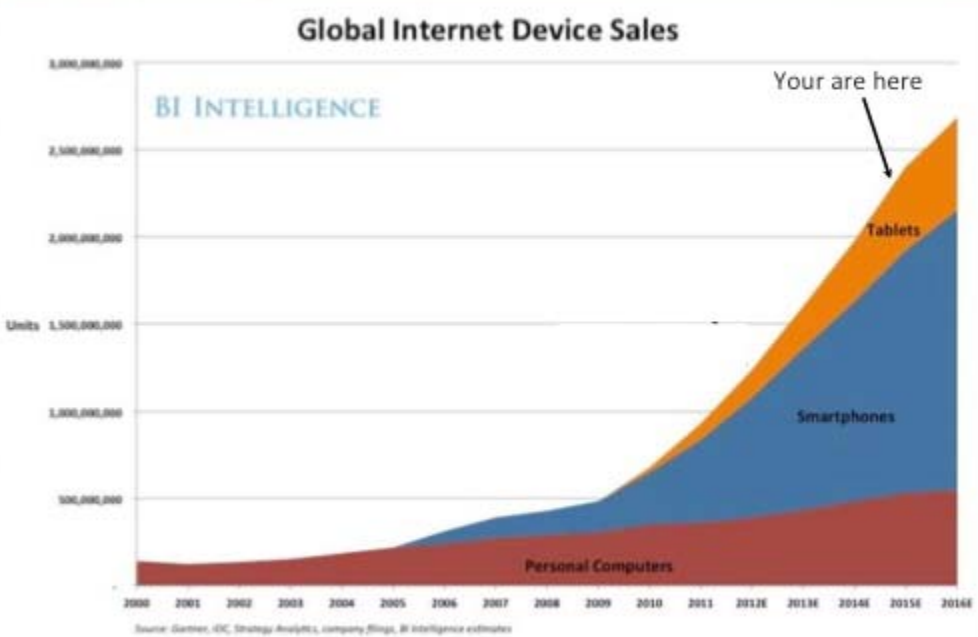
The broad array of BYOD handsets used for both personal and official use can easily provide a direct gateway from the public internet to some very private information. Networked medical devices are also vulnerable to malicious access as are all insecurely created IoT devices. In this session we'll look at the best practices for securing this information while limiting usage "friction", from a number of key perspectives:

- ✓ BYOD Security - as medical staff who may not even be hospital employees, routinely access patient records with their personal devices, what mechanisms can be put in place to insure the security of that information?
- ✓ Medical Device and IoT Security - these devices, while created to save and enhance lives, are often highly vulnerable to malicious attack, can this risk be mitigated?
- ✓ Could it be considered negligent to develop and or allow use of devices and applications that are fundamentally insecure?

The Challenge of BYOD

- Connected personal "smart" devices (smartphones, tablets, wearables) are becoming ubiquitous
  - ✓ Estimated 1.2 billion smartphones & tablets purchased in 2013 [1]
  - ✓ 89% of U.S. consumers had mobile broadband subscription as of Dec 2012 [2]

A Tsunami of Smart Devices



The Challenge of BYOD

- Owners of smart devices want increased functionality …
- Most owners would like to use one device for both their personal and their professional applications (e.g., why carry two phones, two tablets, etc.)
- Trend is for applications & data to move to cloud … and for applications/data to be platform agnostic

Smart Mobile Devices – Bigger Bang for the Buck

- Advantages of using personal device at work for owner
  - ✓ Convenient: familiar, portable, ease of access
  - ✓ Performance: faster, more powerful,
  - ✓ Greater functionality: generally more seamless integration of applications
  - ✓ Availability of wide number of business & personal applications
- Disadvantages of using personal device at work for owner
  - ✓ May have to accept inconvenience of additional security (which may limit some non-work functionality or capabilities)
  - ✓ Responsible for cost of acquiring / maintaining device and for connecting to broadband

Smart Mobile Devices – Bigger Bang for the Buck

- Advantages of using personal smart device for hospital
  - ✓ Less cost if individual purchases own device (and service)
  - ✓ Less support cost (owner responsible for obtaining support of their device and for broadband service)
- Disadvantages for hospital
  - ✓ In native configuration, mobile devices may be insufficiently secure to run business apps
  - ✓ Hospital has very limited control of smart device outside of its walls (subject to theft, loss, and other compromises)
  - ✓ Potentially unlimited number of platforms (difficult to support)

BYOD – A Reality in the Today's Hospital Environment

- Smart mobile devices –*surveys/studies showed*
  - ✓ 80% of U.S. physicians already regularly use their devices professional purposes [4]
  - ✓ 75% of U.S. physicians own a tablet [4]
  - ✓ 70% of physician's use a mobile device to access the EHR [4]
  - ✓ almost 70% of nurses at point of care are using their personal smartphones without permission [6]
- 85% of hospitals allow some use of personal smart mobile devices –
  - ✓ 53% allow access to the Internet
  - ✓ 24% provide limited access to hospital applications
  - ✓ 8% allow full access to the hospital network with user owned devices [7]

You Can't Escape the Tsunami of Mobile Smart Devices