Alexa Konstantinos
Director, Marketing

Stephanie Domas
Lead Security Engineer

Jeanne Greathouse
Director, Business Development

Medical Device Cyber Security
Why It Matters

January 27, 2017

Market Background

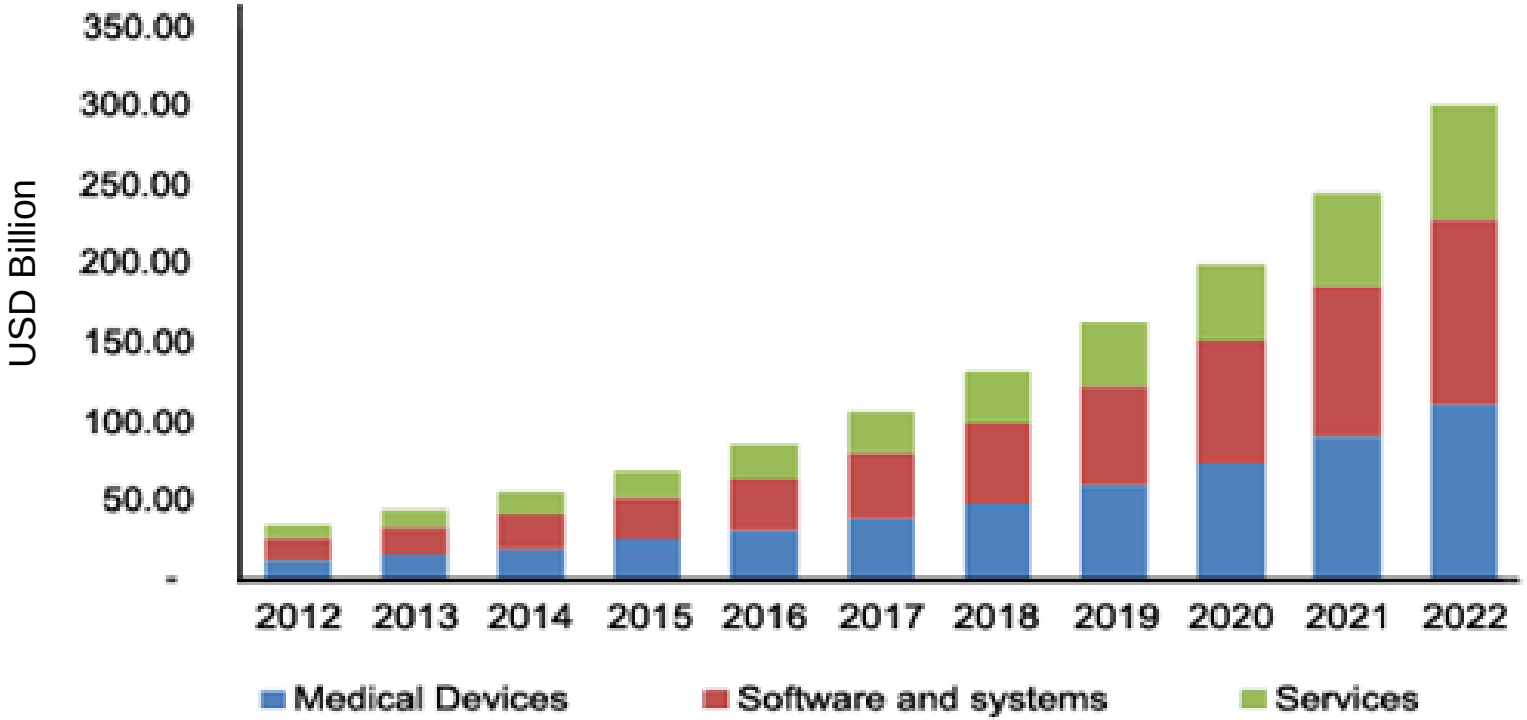
- U.S. is nearly half of global med device market and generally has the most advanced technology[1]
- Fragmented: >7,000 companies; top four have ~60% of revenues[1,2]
- ~700 companies with legacy “high risk devices” having embedded software and/or wireless communication[3]
  - Implantable devices (pacemakers, neurostimulators), patient monitors, infusion systems and drug delivery devices with network connection (insulin pumps and pens), feeding pumps, medical device apps

Any device with software, *regardless of connectivity*, has a cyber attack surface.

[1] http://marketrealist.com/2015/11/must-read-overview-medical-device-industry/
[2] http://www.ibisworld.com/industry/default.aspx?indid=764
[3] Battelle analysis of FDA database

IoT in Healthcare

North American Market, by Component



1 Grand View Research Published: May 2016 | ISBN Code: 978-1-68038-857-2

“The top five industries in 2015 for cyberattacks: healthcare, manufacturing, financial services, government and transportation”

IBM X-Force Report, 2016

“Five of the eight largest healthcare security breaches that occurred since the beginning of 2010, took place during the first six months of 2015,”

IBM X-Force Report, 2016

Why It Matters

- IoMT – devices are becoming increasingly connected, and *any device with software, regardless of connectivity, has a cyber attack surface*
- Regulatory
  - FDA is now requiring proof that cyber security was considered in the design of your device.
  - FDA Pre-market Guidance – 2014
  - Final FDA Post-market Guidance – 2017
- Stakeholders
  - Healthcare systems don't want to take on the liability of a device that is not secure
    - Purchase agreements are assigning all cyber liability to the manufacturer

Which came first?

2016 Ransomeware Renassaince

instances grew by more than 50 per cent in 2016 when compared to 2015

2016, businesses lost more than $850 million compared to $24 million in 2015

Computer World, 2017

20 incidents per day, with hospitals having paid nearly $1,000,000 in ransom bitcoin

Intel Security, 2017

“Dronejacking” and homejacking greatest threat for 2017

MacAfee Labs 2017

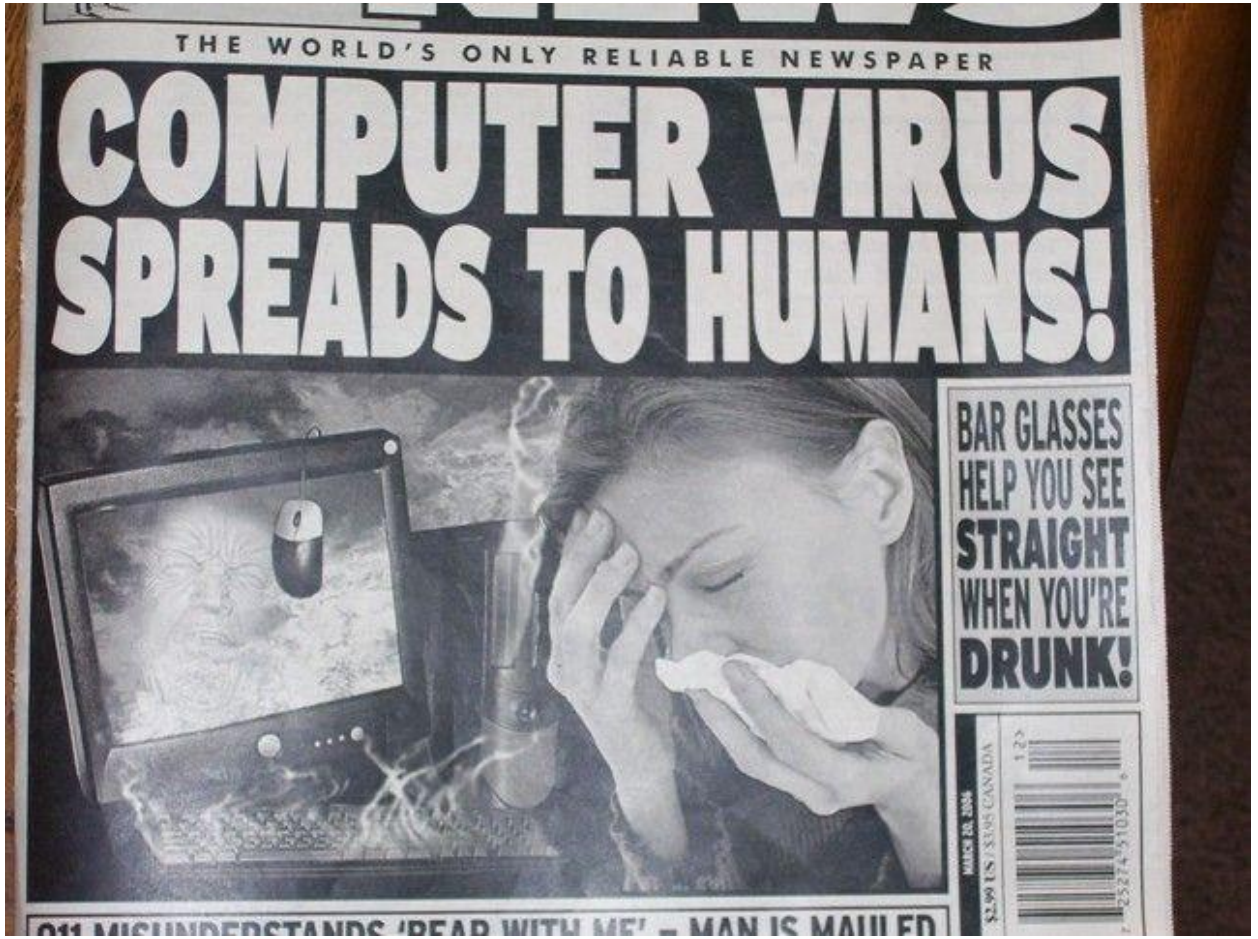
FDA

- FDA found 53% 510(k) submissions did NOT include cybersecurity data 10/2014 – 10/2015:
- FDA "expects" that companies have plans in place to mitigate risk to patient.
- Med Device Pre-market guidance cyber security 2014
- Med Device Post market management of Cyber security in Medical Devices (Final 2017)
  - Total Product Lifecycle Framework
  - Shared responsibility between stakeholders, HC facilities, patients, providers, and mfg
  - Use risk based framework to assure risks to public health are addressed continually
    - Suzanne Schwartz, M.D. MBA ,Assoc.Dir.Science & Strategic Partnerships CDRH

How to mitigate the risk

- Vulnerabilities are inevitable
- Liability or Full coverage?
- Manufacturers and HCO need to develop an incident response team made up of all the stakeholders
  - Med Device: R&D, cyber experts, legal, marketing and regulatory
  - HCO: Incident Response Team, Procurement Standards
  - Not a task or tactic – culture

What Next?


THE WORLD'S ONLY RELIABLE NEWSPAPER
COMPUTER VIRUS SPREADS TO HUMANS!
BAR GLASSES HELP YOU SEE STRAIGHT WHEN YOU'RE DRUNK!

Thank You

For more information, please contact

Alexa Konstantinos
Director, Marketing
konstant@battelle.org

Stephanie Domas
Lead Security Engineer
domas@battelle.org

Jeanne Greathouse
Director, Business Development
greathouse@battelle.org