CYBER SECURITY SUMMIT 2017

Threat Briefing: Manufacturer View

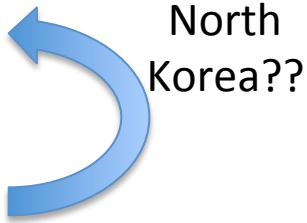
Ken Hoyme – Director, Product Security
Boston Scientific

Threat history – Med Devices

- White hat demonstrations of exploitable vulnerabilities
- Black hats focusing on exfiltration of health records through “traditional” means
  - Phishing via IT/business systems
- No major attack that impacted the device side of hospital networks

Threat Actor's Interests

- Cyber-criminals – anything that can be converted to money
  - Health records, ransomware
- Nation States – Information, intellectual property
- Hacktivists – a cause (one example hospital hacked by Anonymous)



Recent History

- WannaCry and NotPetya had significant impacts on medical devices in hospital settings
  - Not targeted to devices
  - Exploited slowness to patch known Windows vulnerabilities
  - No direct patient harm, but the loss of device availability impacted patient care

New “Threat Actor” Emerging

- The hospital contracting department
- Rapid rise in the level of security expectations in new hospital contracts
- Threat that you cannot sell your products unless you step up and fill these expectations