Vendor Cybersecurity in the Connected World

University of St Thomas
Steve Hoge, Senior Legal Director, Medtronic
December 6, 2017

What is going on out there?

- February, 2016. Hollywood Presbyterian Medical Center pays ransom to regain control of its computer network that had been paralyzed by hackers for 10 days.
- August 2016 MedSec and Muddy Waters short sale of St Jude Medical stock
  - February, 2017 FDA Quality enforcement action
- April, 2017. Office of Civil Rights settlement with CardioNet, Inc.
  - Multiple breaches involving laptops violate HIPAA
  - $2.5 Million and a corrective action plan requiring annual review
- May, 2017 Global ransomware attack, including England's health service
- 2016-2017 Russians hack DNC

Common Risks to Manage

Patient Risk

- Stop therapy or change settings
- Delay in care to address unauthorized access
- Access to PHI
  - Change records
  - Privacy Breach
- Loss of confidence in the device

Legal Risk

- HIPAA
- FDA
- EU General Data Protection Regulations
- FTC
- Litigation
- Contract

Reputation Risk

- Breach
- Hackers and related publicity

Response Dynamics

- Board of Directors Attention at Customers and Large Vendors
  - Brand, Stock Price, Customer relationships, Business Operations, Secure Confidential Assets
  - Cybersecurity Becomes a Priority
- Media
- Government
  - Politicians
  - Regulators, e.g., FDA, FTC
  - Homeland Security ICS-Cert

Healthcare Provider Perspective

- NIST Cybersecurity Framework
  - Understand the risks of your assets
    - Know your devices
    - Analyze and understand the risks of those assets
  - Deploy compensating controls
    - Firewalls, network access controls, antivirus controls
  - Continuously measure the effectiveness of your controls

Provider Perspective (cont.)

- Provider Priorities
  - Securing Devices
    - Existing Devices
      - Reframe thinking about the need to secure
      - Focus on compensating controls
      - Don't just let devices languish
    - New Devices
      - Focus on procurement
      - Centralize the function (try not to allow device purchases throughout the organization or on an ad-hoc basis)
      - Analyze and monitor vendor/supplier's information security program

Contracting: Where it comes together

- Provider perspective
  - Strong security language – Incorporate regulatory requirements into contract language
  - Address cybersecurity incident notification and responses
  - Audit rights
  - Representations/warranties and related consequences
  - Consider publishing vendor/device contracting guidelines for upfront and transparent negotiations with device vendors

Contracting: Where it comes together

- Manufacturer perspective
  - Manufacturers and Provider Customers have common concerns so no resistance to reasonable contract terms
  - Manufacturer must look up, down, and sideways
    - Provider/Customers –must meet requirements to win business
      - Security questionnaires
      - Security agreements
      - Government: Software bill of materials?
    - Vendors
      - Strong security is table stakes
      - Assess security as part of vendor selection - questionnaire or audit
      - Must meet end user customer requirements
    - Regulators. We must meet both regulator and customer requirements

Questions?


CYBER
SECURITY
dark web
servers
internet
backdoor
remote administration tools
root
data
data dump
information technology
cross site scripting
blackhat
worms
firewall
malwares
distributed denial of service
defacement
encryption
stuxnet
surveillance
access
financial institutions
cyberspace
porn
adwares
trojan
bitcoin
antivirus
keylogger
script kids
hackers
wikileaks
corporations
SSL
government
spoofing
world wide web
activism
warez