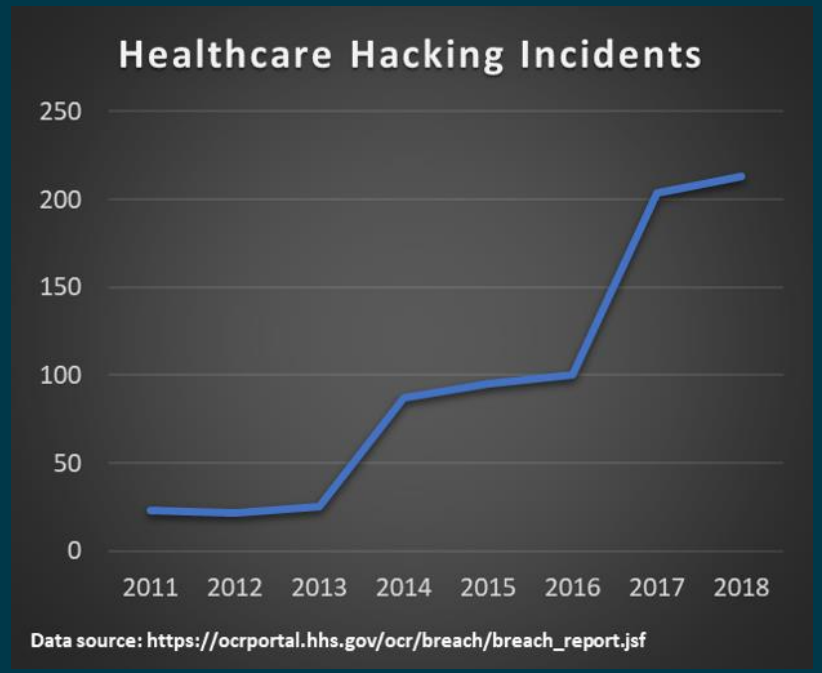
Practical Cybersecurity for Medical Devices

tracesecurity

tracesecurity

Medical Devices as Targets in 2018

tracesecurity



- Easy pivot to clinical / business systems
- Expensive equipment with long lifecycles
- Lack of detection / removal options to remediate attacked medical devices.
- Remote access to data is baked-in
- Hospitals are already understaffed – technology is enabling
- Lack of Security Awareness Training
- 10-15 Networked Medical devices PER Bed
- EHR at its core is designed to be transportable
- Aging technology & FDA regs makes devices easy targets
- Ownership issues between Clinical & IT
- Then there's the bad stuff……

tracesecurity

Wouldn’t Happen to me…..

tracesecurity

MedStar Hospitals R
'Ransomware' Hack

10 Biggest Attacks:

Health Equity → 190,000 Records < 2.65 MM → Atrium Health

July 9: Cass Regional Medical Center reports ransomware attack

- **Date of attack:** July 9
- **Date of disclosure:** July 9
- **Source of breach/inf**
- **Damage:** One week w
diverted

Montana hospital employ
traveling, 8.4K patients' d

Rural Tennessee hospital hacked by cryptocurrency mining software

Parsons, Tennessee-based Decatur County General Hospita
notified patients of a breach in which a hacker remotely inst
unauthorized software on its EHR system. The hospital does
any patient data was accessed.

U.S. hospitals have
attack

The ransomware is linked to a leaked v

Hancock Regional Pays Bitcoin Ransom After Computer System Hacked

The ransomware attack affected the Indiana hospital's email syst
health records and internal operating systems.

UK's NHS struggling with security after WannaCry, losing 10K patient records last year

Fertility clinic hacked and held for ransom — why your hospital could be next

Published: Dec 6, 2017 7:02 p.m. ET

ACK: Hackers hijacking medical devices to backdoors in hospital networks

Example 1: Anesthesia machine shutdown

Bug can cause deadly failures when anesthesia device is connected to cell phones

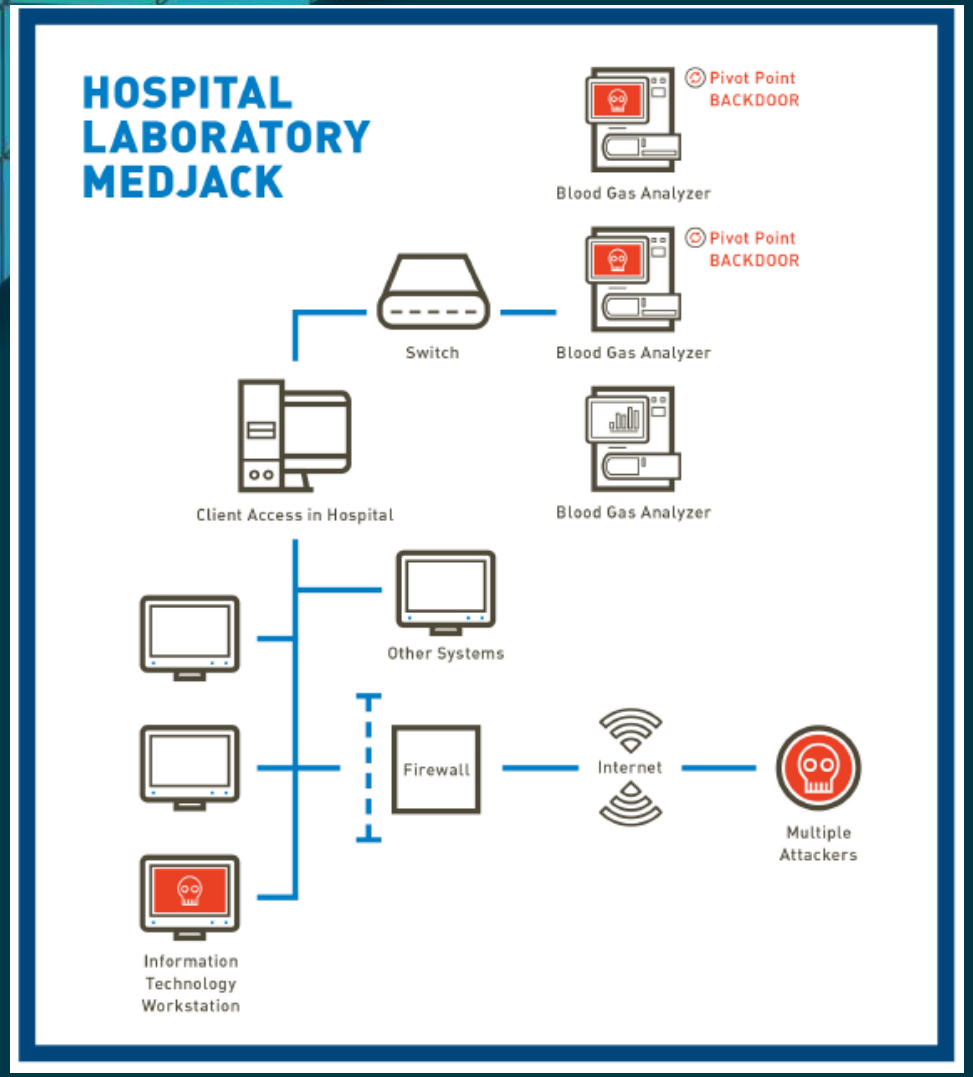
No, it's not clear why anyone would e

DAN GOODIN - 4/22/2014, 3:33 PM

SpaceLabs' Arkon anesthesia system recalled again

AUGUST 13, 2018 BY NANCY CROTTI — LEAVE A COMMENT

tracesecurity



Example 2: Hospital Lab Hijack

- Used old vulnerabilities not present in newest OS
- Strategically targeted legacy Windows OS
- Spreads across network & USB

*source: RSA

tracesecurity

Advisory (ICSMA-17-250-02A)

Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (Update A)

Original release date: September 07, 2017 | Last revised: December 12, 2017

"Smiths Medical has released update Version 1.6.1 to mitigate the vulnerabilities in the Medfusion 4000 Wireless Syringe Infusion Pump."

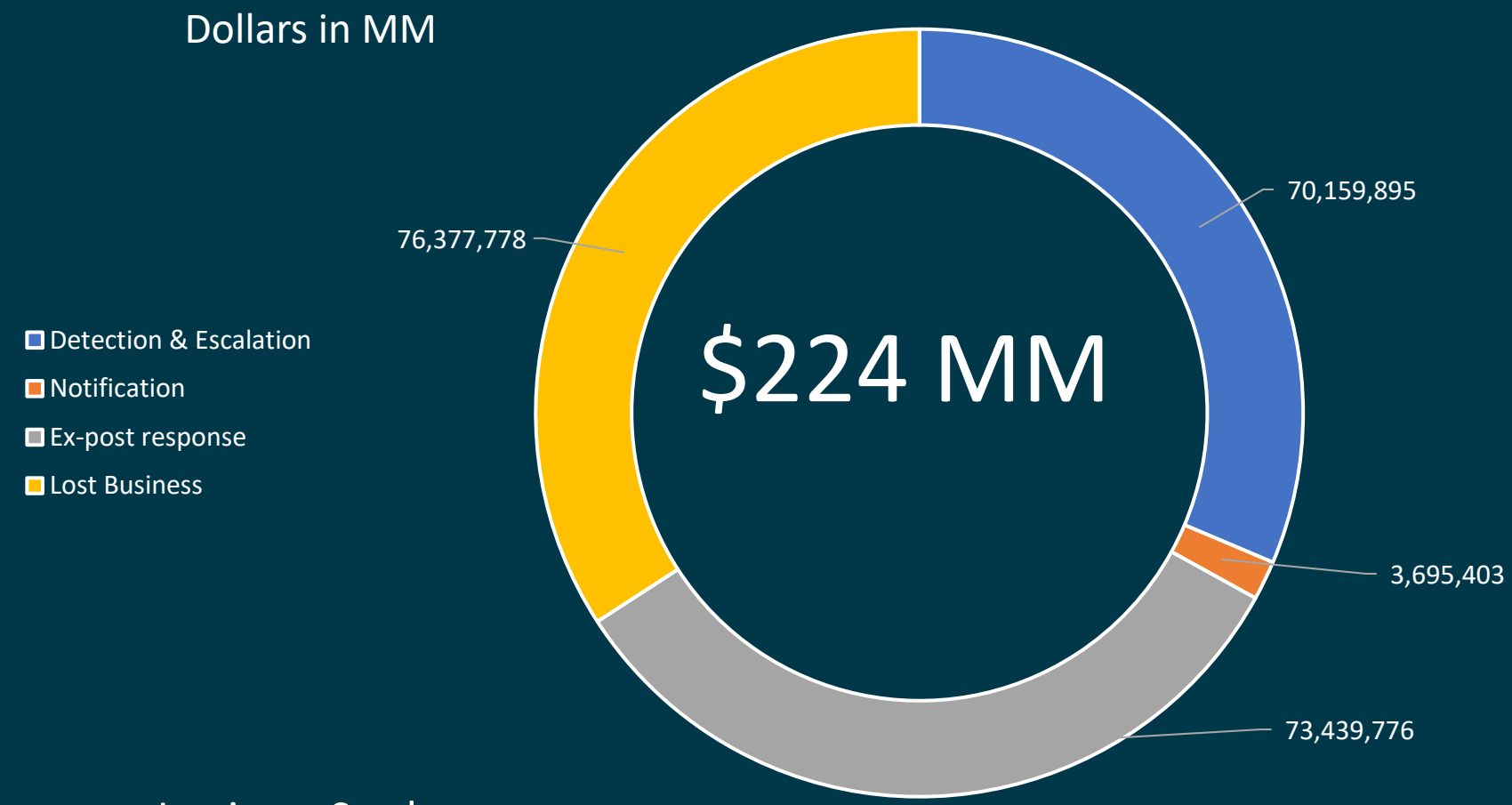
BUFFER COPY W/OUT CHECKING INPUT SIZE ('CLASSIC BUFFER OVERFLOW')
OUT-OF-BOUNDS READ
USE OF HARD-CODED CREDENTIALS
IMPROPER ACCESS CONTROL
USE OF HARD-CODED CREDENTIALS
USE OF HARD-CODED PASSWORD
IMPROPER CERTIFICATE VALIDATION
PASSWORD IN CONFIGURATION FILE

tracesecurity

What Does a Breach Cost?

Cost of a Mega Data Breach

(1-50 MM Records)



- 2018 Ponemon Institute Study
- Average cost of breach is $148 per record (up from $141.00)

tracesecurity

Practical Prevention

tracesecurity

Practical Prevention

- Solve the Clinical / IT problem (Assign program ownership)
- Maintain an Inventory
- Conduct a Risk Assessment – look for Unicorns! (Narwhals!)
- Implement the Basics
  - Antivirus
  - Windows Updates
  - Network Segregation
  - Network Encryption
  - Secure remote management for vendors

Practical Prevention (cont.)

- Secure Configuration (Don’t smell like a honey pot)
- Physical Security (USB Locks, Secure Storage)
- Supply Chain Management
- INCIDENT RESPONSE

tracesecurity

Questions?

tracesecurity

THANK YOU!

Rob Theriot

Rob@tracesecurity.com