Security and Clinical Devices. Oxymoron?

Monte Ratzlaff, CISSP, CISA
Cyber Risk Program
University of California Office of the President

UNIVERSITY
OF
CALIFORNIA

“During the first few months of 2016, the healthcare industry experienced

an increased number of cyber threats that struck numerous hospitals across North America and around the globe.”

- “ANATOMY OF ATTACK: MEDJACK.2”, TrapX Research Labs

Vulnerability alerts

Alert (ICS-ALERT-13-164-01)

Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013 | Last revised: October 29, 2013

Advisory (ICSA-15-174-01)

Hospira Symbiq Infusion System Vulnerability

Original release date: July 21, 2015

Advisory (ICSMA-16-089-01)

CareFusion Pyxis SupplyStation System Vulnerabilities

Original release date: March 29, 2016


Case Study
UNIVERSITY
OF
CALIFORNIA

"…(the) compromised medical device learned where the PACS systems were located, and attempted to perform a pass-the-hash attack to gain access to the PACS systems."

- "ANATOMY OF ATTACK: MEDJACK.2", TrapX Research Labs

“Our analysis enabled us to track the attacker back through the network to a backdoor within the MRI system...”

- “ANATOMY OF ATTACK: MEDJACK.2”, TrapX Research Labs

Threats, Risks, Vulnerabilities

UNIVERSITY
OF
CALIFORNIA

Threats to medical devices

- Malware (including ransomeware)
- Network attacks
- Lost/stolen devices (many contain ePHI on board)
- Tampering
- Unauthorized access

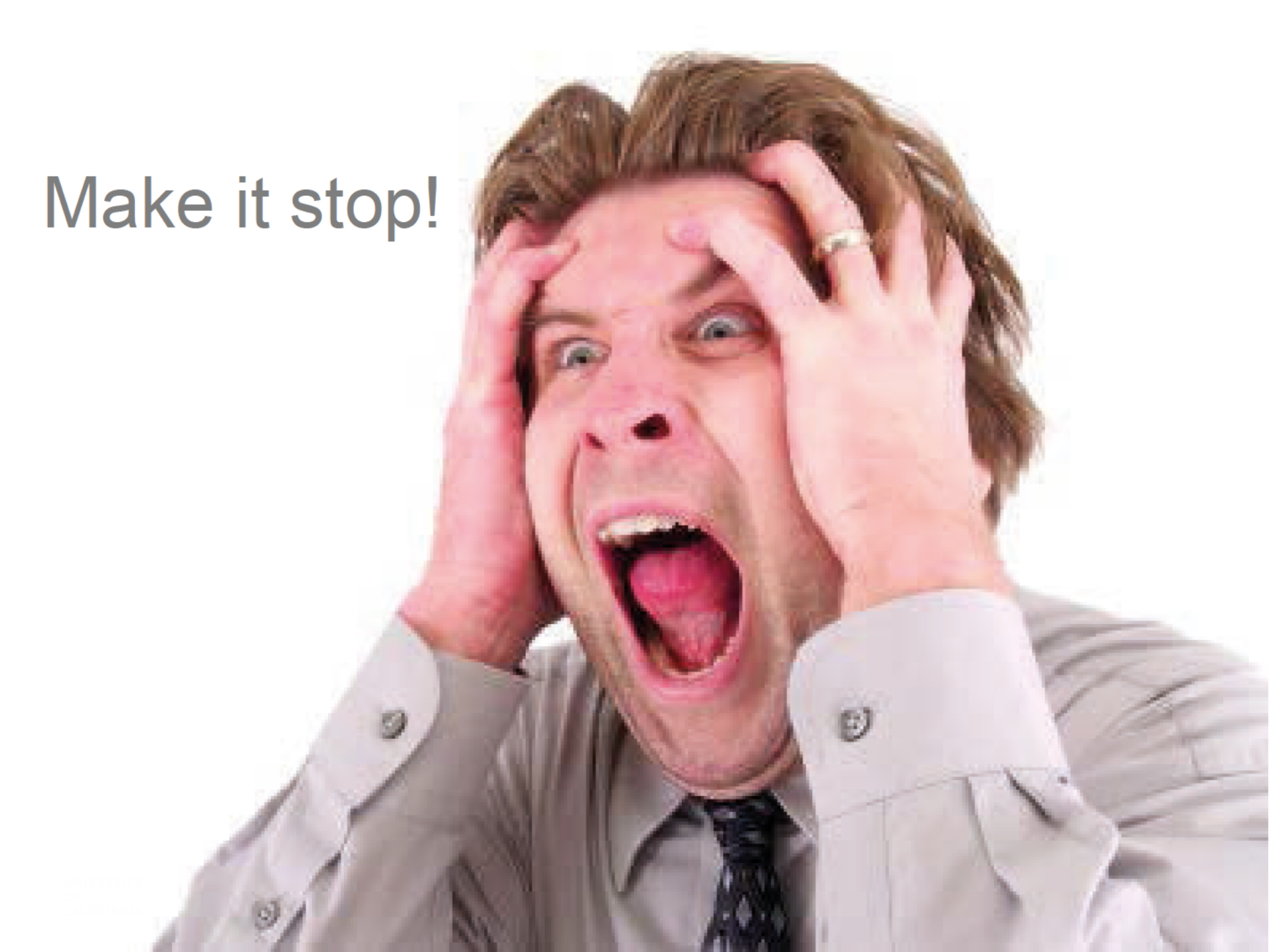
Medical device risks/vulnerabilities

- Lack of regular manufacturer patching
- Customers not able to patch either
- Typically no encryption – at rest or in transit
- Inconsistent anti-malware implementation

Medical device risks/vulnerabilities

- No authentication
- Default passwords
- Unnecessary services
- Many contain ePHI on board

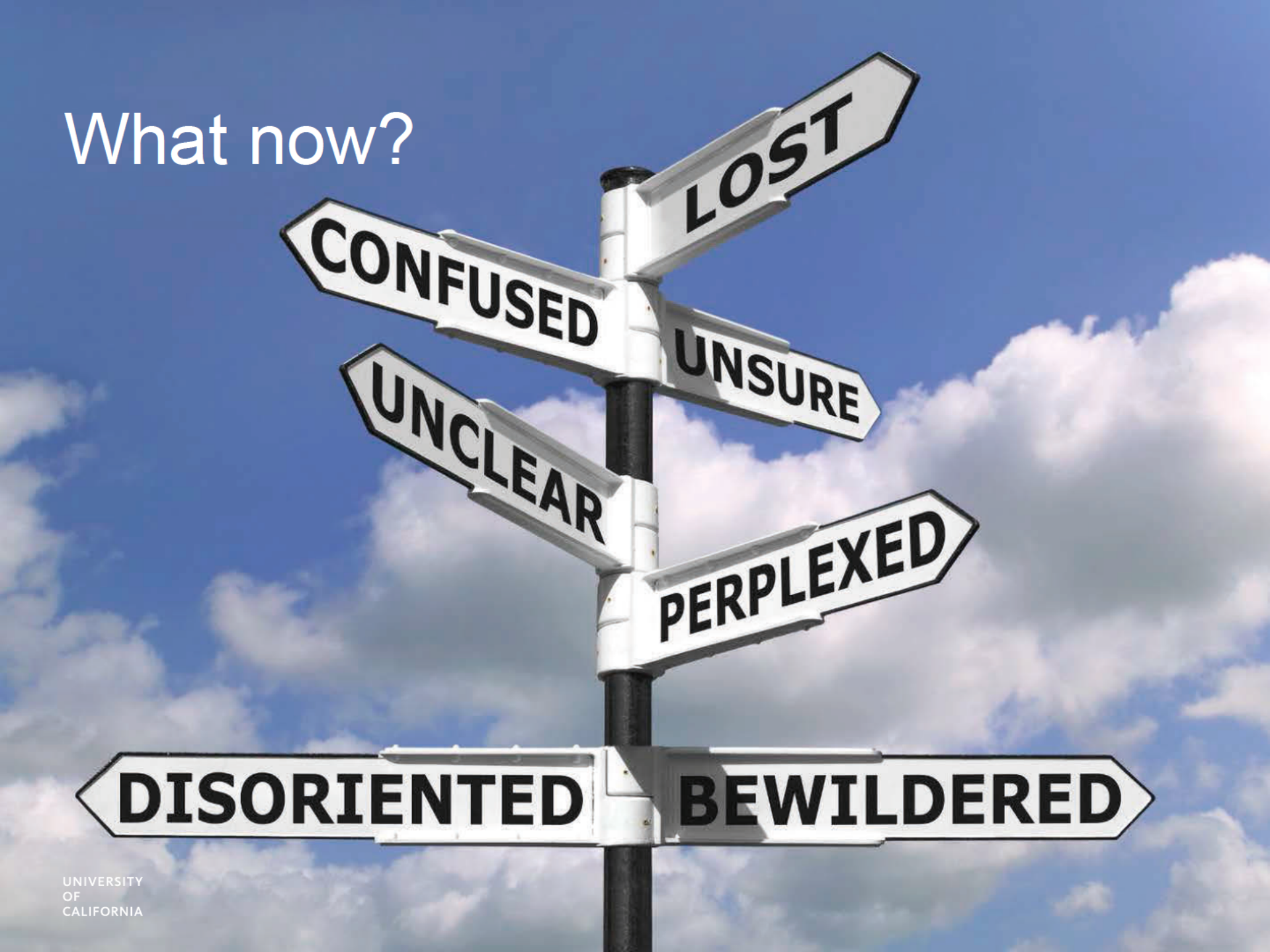
Make it stop!



Medical device manufacturer issues:

- Security has not been top of mind
- Patient safety is the focus
- FDA cybersecurity guidance is not a requirement/mandatory
- Most still do not incorporate security (source code analysis, encryption, authentication)

What now?



UNIVERSITY
OF
CALIFORNIA

UC Davis Health

- Risk assessment
- Segmented clinical networks
- Security “perimeter” controls on clinical networks
- Vendor reviews for all new technology
- Participation in FDA workgroups
- Strong partnership between IT and Clinical Engineering

What can you do?

- Know your environment – what do you have?
- Know your risks
- Network controls: segmentation/isolation/protection
- Vendor reviews and accountability– demand security
- Participate in FDA workgroups

What can you do?

- Participate in Information Sharing Analysis Organization (ISAO) and ISACs
- Physical security - devices that aren't connected still matter (ePHI on board)
- Build/foster relationship between IT and Client Engineering

What questions do you have?


Thank you!
UNIVERSITY
OF
CALIFORNIA