www.pwc.com

Medical device security – The transition from patient privacy to patient safety

Scott Erven

pwc

Who i am

Scott Erven - Managing Director – Healthcare Industries Advisory – Cybersecurity & Privacy

- Medical Device Security Lead For PwC
- Over 5 Years Leading Medical Device Security Research
- Over 15 Years IT Security Experience
- Over 5 Years Managing Security For Healthcare Systems & Providers

What we'll be covering today

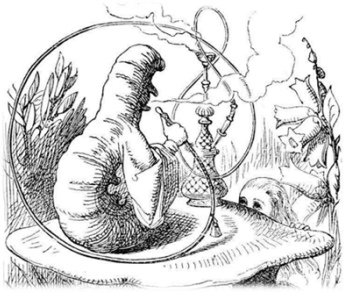
1. *Why medical device security matters.*
2. *Vulnerabilities inside the medical device security landscape.*
3. *Are attacks a reality?*
4. *Diagnosis and problem awareness.*
5. *Treatment plans.*

Why medical device security matters

Personal impact

- Many of us rely on these devices daily.
- When we are at our most vulnerable, we will depend on these devices for life.
- Even at times when we aren't personally affected, people we care about may be.

Malicious intent is not a prerequisite to patient safety issues



Research – Device vulnerabilities

Device vulnerabilities

Weak default/hardcoded administrative credentials

- Treatment modification
- Cannot attribute action to individual

Known software vulnerabilities in existing and new devices

- Reliability and stability issues
- Increased deployment cost to preserve patient safety

Unencrypted data transmission and service authorization flaws

- Healthcare record privacy and integrity
- Treatment modification

Research– Internet exposure

Shodan search initial findings

Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.

Located a public facing system with the Server Message Block (SMB) service open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.

Initial healthcare organization discovery

Very large U.S. based healthcare system consisting of over 12,000 employees and over 3,000 physicians. Including large cardiovascular and neuroscience institutions.

Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.

Exposed numerous connected third-party organizations and healthcare systems.

Did we only find one?

No. We found hundreds!!

Generic Search Examples:

shodan port:445 org:health*/clinic/hospital

health* - http://www.shodanhq.com/search?q=por .health 148 hits

clinic - http://www.shodanhq.com/search?q=port clinic 18 hits

hospital: http://www.shodanhq.com/search?q=por. hospital 119 hits

medical: http://www.shodanhq.com/search?q=port% medical 255 hits

Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

Let me paint the picture

System with Lockout Exemption:

```
060580     Echo Vas OR 1 -   _ScreenLock_0_Exception
060581   _ScreenLock_0_Exception
060583       OR 1-   _ScreenLock_0_Exception
060585     Echo Vas OR 2 -   _ScreenLock_0_Exception
```

Impact:
System May Not Require Login

EMR:

```
EP03 EPIC Cogito Clarity RDBMs Server
EP04 EPIC Clarity Test Console
EP05 EPIC Business Objects test
EP06 EPIC Healy BCA Server 1
EP07 EPIC Hyperspace
EP08 EPIC Hyperspace Web Server 1
EP09 EPIC Hyperspace Web Server 2
EP10 EPIC Hyperspace Web Server 3
EP11 EPIC Web BLOB Server
EP12 EPIC Kuiper Server
EP13 EPIC EPS Server 1
EP14 EPIC EPS Server 2
EP15 EPIC Interconnect
EP16 EPIC Care Everywhere
EP17 EPIC Soap Proxy
EP18 EPIC System Pluse
EP19 EPIC Multipurpose SQL Server
EP20 EPIC - Citrix XenApp 6.5 License/Web
EP21 EPIC - Citrix XenApp 6.5 Application Server
EP22 EPIC - Citrix XenApp 6.5 Application Server/DC
EP23 EPIC My Chart
EP24 EPIC Care Link
EP25 EPIC File Service
```

Impact:
Electronic Medical Record Systems

Getting a little warmer!

Cardiology Systems:

```
060768        1 - Dr.
060911        D, Dr. C    , Cath Lab Admin
061463        C - Cardiac Core Lab
063012        C - EP -
064320 Adrienne C          - Cardiovascular Lab
065772        c pacemaker
#069454 Go:    first floor Peds Nuclear Medicine
046142 Anestisia OR
046774
046785 Me     A
046798
/046799 Da    Fa
047271 Anesthesia Work Room
```

Impact:
Pediatric Nuclear Medicine
Anesthesia Systems

Summary of devices inside organization

- Anesthesia Systems – 21
- Cardiology Systems – 488
- Infusion Systems – 133
- MRI – 97
- PACS Systems – 323
- Nuclear Medicine Systems – 67

Potential attacks – Physical

- *We know what type of systems and medical devices are inside the organization.*
- *We know the healthcare organization and location.*
- *We know the floor and office number.*
- *We know if it has a lockout exemption.*

Potential attacks – Phishing/Pivot

- *We know what type of systems and medical devices are inside the organization.*
- *We know the healthcare organization and employee names.*
- *We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP. We know the hostname of all these devices.*
- *We can create a custom payload to only target medical devices and systems with known vulnerabilities.*

Are attacks a reality?

Real world attacks – Honeypot research

What we were looking for…

- Using known default login information for remote access?
- Leveraging existing exploits for remote command execution?
- Custom malware?
- Malicious intent to interfere with the device (or worse, someone using the device)?
- Campaigns against specific vendor devices?

Real world attacks – The data

Data	
Honeypots	10
Successful logins (SSH/Web):	55,416
Successful exploits (Majority is MS08-067)	24
Dropped malware samples	299
Top 3 Source Countries	Netherlands, China, South Korea
HoneyCreds login	8

HoneyCred logins are unique to the honeypot ssh/web service, someone did some research.

Real world attacks – Conclusion

What did the attacker do once he got in?	*Nothing*
Did they realize they had root on a MRI machine?	*Probably not*
Are there compromised medical devices calling back to a command and control server?	*Absolutely*
Did the command and control owners know what the information they are sitting on?	*Didn't appear so*

Problem awareness

Problem awareness

1. ***Medical devices*** *are* ***increasingly accessible*** *due to the nature of healthcare*
2. *HIPAA focuses on patient privacy, not* ***patient safety****.*
3. *U.S. Food and Drug Administration* ***does not*** *validate* ***cyber safety*** *controls.*
4. ***Malicious intent*** *is* ***not*** *a prerequisite for adverse patient outcomes.*

Technical properties

Exposed, vulnerable systems

- All software has flaws.
- Connectivity increases potential interactions.
- A software-driven, connected medical device is a **vulnerable**, **exposed** one.

Lack of patient safety alignment in medical device cyber security practices

A brief history of United States Food and Drug Administration (U.S. FDA) and medical device cybersecurity

February 2013
President Obama issues executive order on improving infrastructure cybersecurity

June 2013
FDA issues general warning on device cybersecurity based on "known vulnerabilities"

July 2015
FDA issues first-ever warning about cybersecurity vulnerability of a device

January 2016
FDA issues draft guidance document on post-approved monitoring of medical device cybersecurity

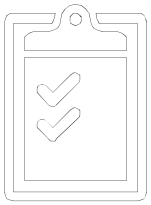
January 2005
FDA releases final guidance on cybersecurity for networked medical devices containing off-the-shelf software

June 2013
FDA issues draft guidance on medical device cybersecurity

October 2014
FDA issues its final guidance document on including medical device cybersecurity information in premarket applications

December 2016
FDA issues final guidance document on post-approved monitoring and remediation of medical device cybersecurity

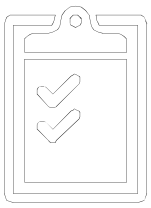
U.S. FDA premarket guidance for medical device cybersecurity



U.S. FDA asks that cybersecurity information be ***submitted as part of a device's application for approval***, including:

- Hazard analysis of cyber risks
- Controls to mitigate specific risks
- A plan of how to patch devices
- Controls to maintain device integrity
- Instructions on how to use related controls like antivirus software

U.S. FDA's post-market guidance for medical device cybersecurity



U.S. FDA highlights if ***the following criteria are met*** they will not enforce 806 reporting requirements:

1.) ***No serious adverse events*** are known to have been caused by the vulnerability

2.) Fixes are made and users are notified ***within 60 days (Two 30 Day Periods Defined In Requirements)*** of the discovery of the vulnerability

3.) The manufacturer is a member of an ***Information Sharing Analysis Organization (ISAO) and has a coordinated disclosure process***

Treatment plans

A shift in how we think about medical technologies

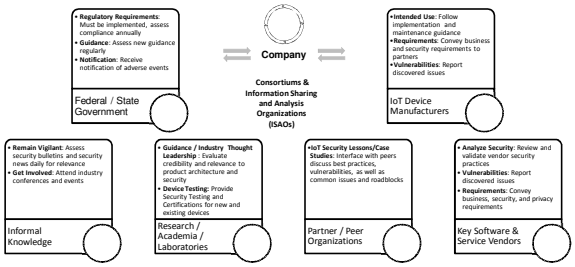
Before	***Now***
Devices are connected to patients physically	Devices are connected wirelessly to patients and other devices
Data obtained from devices are stored on paper or locally	Data obtained from devices are stored in the cloud
Devices are physical products	Devices include software and even databases of health information
Care is hand-administered at a health care location	Care is available to patients in the palm of their hand through apps
Physical access is needed to view health data	Health data can be accessed anywhere on earth

A shift in how we think about regulating medical devices

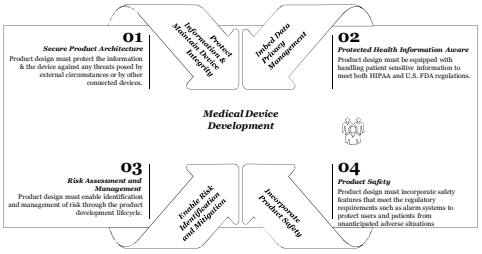
Traditional considerations meet technology

Traditional	Safety	Is a medical device safe for use in humans? Does it cause adverse events? Are its risks tolerable in relation to its benefits?
	Efficacy	Is a device effective for its given purpose? What is the magnitude of the effect?
Evolving	Quality	After approval, a device must be kept safe and effective through adherence to quality manufacturing standards established by FDA
	Security	Once a medical device is networked with other devices or the internet, is it still safe and effective?

Interaction with the broader industry is also core to developing an overarching threat landscape, responding to Cybersecurity events, and developing more secure devices.

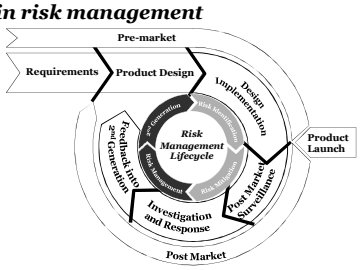


A security centric, risk based product development process is core to the deployment of a secure effective medical device…



To meet the current regulatory requirements and protect the device from cybersecurity attacks, it is critical to embed security within the lifecycle of the product and in risk management considerations…

Risk Management Considerations
Inevitable need to explore unidentifiable risks including foreseeable tampering
Established mechanism to feed post market monitoring data into next-gen device design
Continuous compliance with HIPAA and other privacy regulations
IT compliance function with expertise to evaluate compliance with various regulations
Effective security and data standards with an ability to rapidly respond to emerging threats



Medical Device Cyber Security Approach

Strategy Execution, Design, and Implementation

Develop the Medical IoT cybersecurity strategy in accordance with business, operational, risk and compliance needs. Design the program operating model, identify the resources to carry out the day to day activities and provide architecture and implementation support.

- **Integrated Medical IoT and Enterprise Security Strategy**
- **Medical IoT Governance and Program Development**
- **Data Flow Mapping, Identification, Classification, Use and Protection**
- **Software/Systems Development Lifecycle (SDLC) Process Enhancement**

Information Risk and Incident Management

Comprehensive approach to identify and mitigate cybersecurity risks and evaluate the effectiveness of the Medical IoT cybersecurity program.

- **Control Profile Development**
- **Medical IoT Risk Management Policy Development and Alignment**
- **Medical IoT Vendor Risk Management**
- **Medical IoT Incident Response Playbook Development**

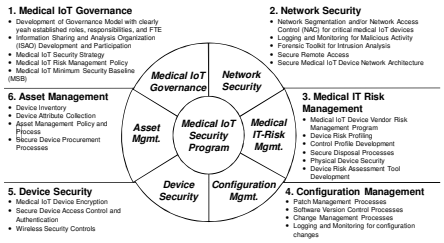
Regulatory Compliance

Preparation for regulatory audits and assess the health of the overall privacy and security programs

- **Mock Regulatory Audits**
- **Medical IoT Cybersecurity Risk Assessments**
- **Regulatory Framework Alignment and Compliance**
- **Medical IoT Risk Assessment Process Development**

Medical Device Cybersecurity Framework

The following diagram outlines the key components of a Medical Device Cybersecurity Framework, including roles and responsibilities for management of security risks:



Invest in personnel and processes

- Companies should establish and support cybersecurity programs to support devices throughout their lifecycles
- Cybersecurity experts should be hired or third-parties consulted to vet cybersecurity information.
- Established information-sharing processes – including ISAOs – may lead to more and better disclosures.
- Companies should consider how to best engage with the cybersecurity community as a strategic advantage.

Support can lead to opportunity

Device companies can become ***essential partners*** to healthcare providers by helping them support and secure their devices and networks.

Device companies can benefit by giving providers a level of ***comfort and assurance*** about product security, potentially leading to increased sales, and insight into how their devices are used and misused, ***benefiting future device development***.

Thank you

Contact

Scott Erven
Managing Director, Healthcare Cybersecurity
E: scott.erven@pwc.com