Regulatory Responsibilities for Medical Device Security

Kevin Fu, Ph.D.

Associate Professor

Security & Privacy Research Group

Computer Science & Engineering

http://spqr.eecs.umich.edu/

Regulatory Affairs Professionals Society (RAPS), Oct 29, 2012

Supported in part by a Sloan Research Fellowship, NSF CNS-0831244, HHS 90TR0003/01.

Disclosures

- Support from NSF, HHS, DHS, IOM, Microsoft Research, Symantec, McAfee
- Visiting scientist, FDA NoE
- Board member, NIST ISPAB
- Patent pending technology:
  - Ultra-low power flash memory

Hat: zazzle.com

- This presentation is based on both my own research and the research of others. None of the opinions, findings, or conclusions necessarily reflect the views of my past or present employers.

Responsibility of Manufacturer

- Medical device cybersecurity risks are now **foreseeable**
  - Design controls should address foreseeable risks (510(k), PMAA)
- **FALSE**: ~~FDA rules prevent software updates~~
  - No, but I can understand where that perception comes from
  - Pre-market review **rare** in cybersecurity updates of COTS software
  - But no one said manufacturing medical device software is easy

How Much SW in Medical Devices?

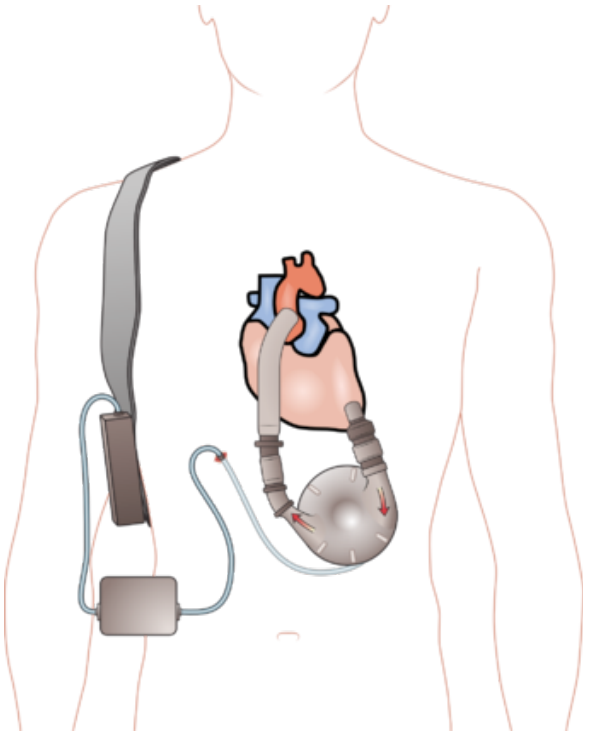
- 1983-1997
  - 6% of all recalls attributed to SW
- 1999-2005
  - **Almost doubled**: 11.3% of all recalls attributed to SW
  - 49% of all recalled devices relied on software (up from 24%)
- 1991-2000
  - **Doubled**: # of pacemakers and ICDs recalled because of SW
- 2006
  - Milestone: Over half of medical devices now involve software
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,527,311+ devices

[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001, Computer history museum, eurogramer.net, wikipedia, businesspundit.com, imdb.com, coverbrowser.com, thefilmtalk.com]

FDA Center for Devices and Radiological Health

Regulatory pathways

Pre-market approval



Credit: Madhero88

It's complicated.

http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-MAR-01.aspx

FDA Center for Devices and Radiological Health

Regulatory pathways

Pre-market notification [510(k) clearance]

Credit: Nemo's great uncle

It's complicated.

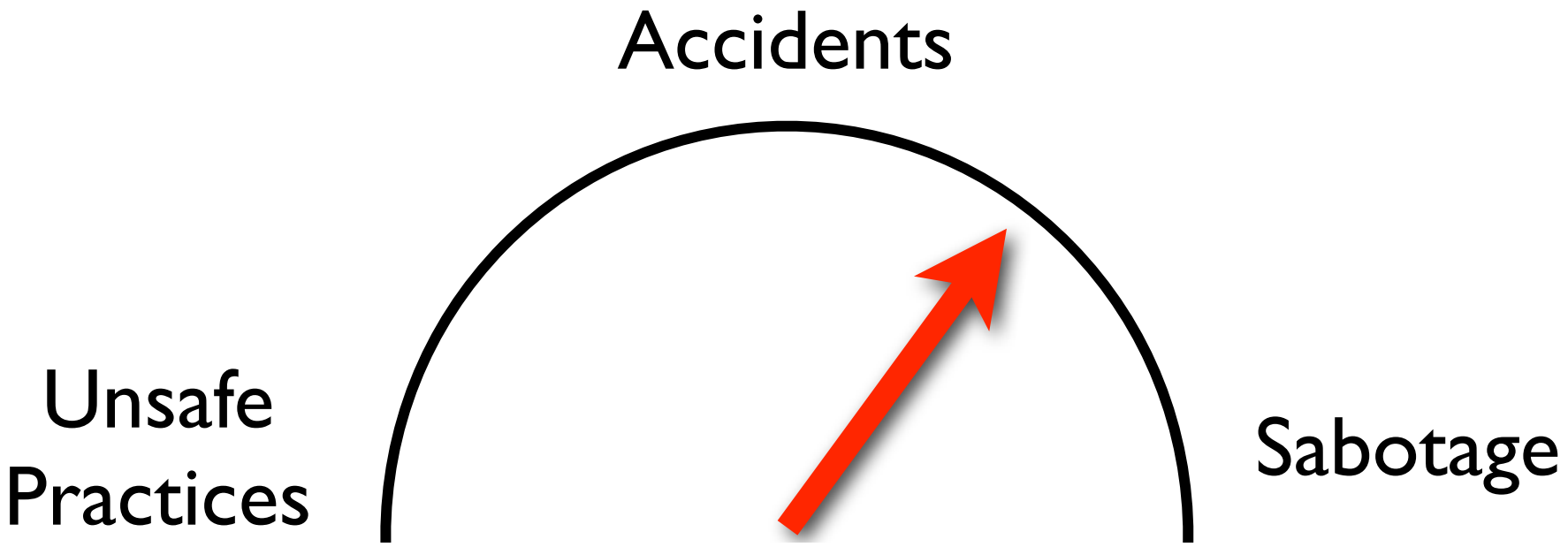
http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-MAR-01.aspx

510(k) Substantial Equivalence

- "One of the interesting classes is radiation equipment...Even the software, which I wonder where they got the first **predicate for software**."

  -David Feigal
  Fmr. Director, FDA Center for Devices and Radiological Health (CDRH)
  [Institute of Medicine Meeting 2, June 2010:
  Public Health Effectiveness of the FDA 510(k) Clearance Process]

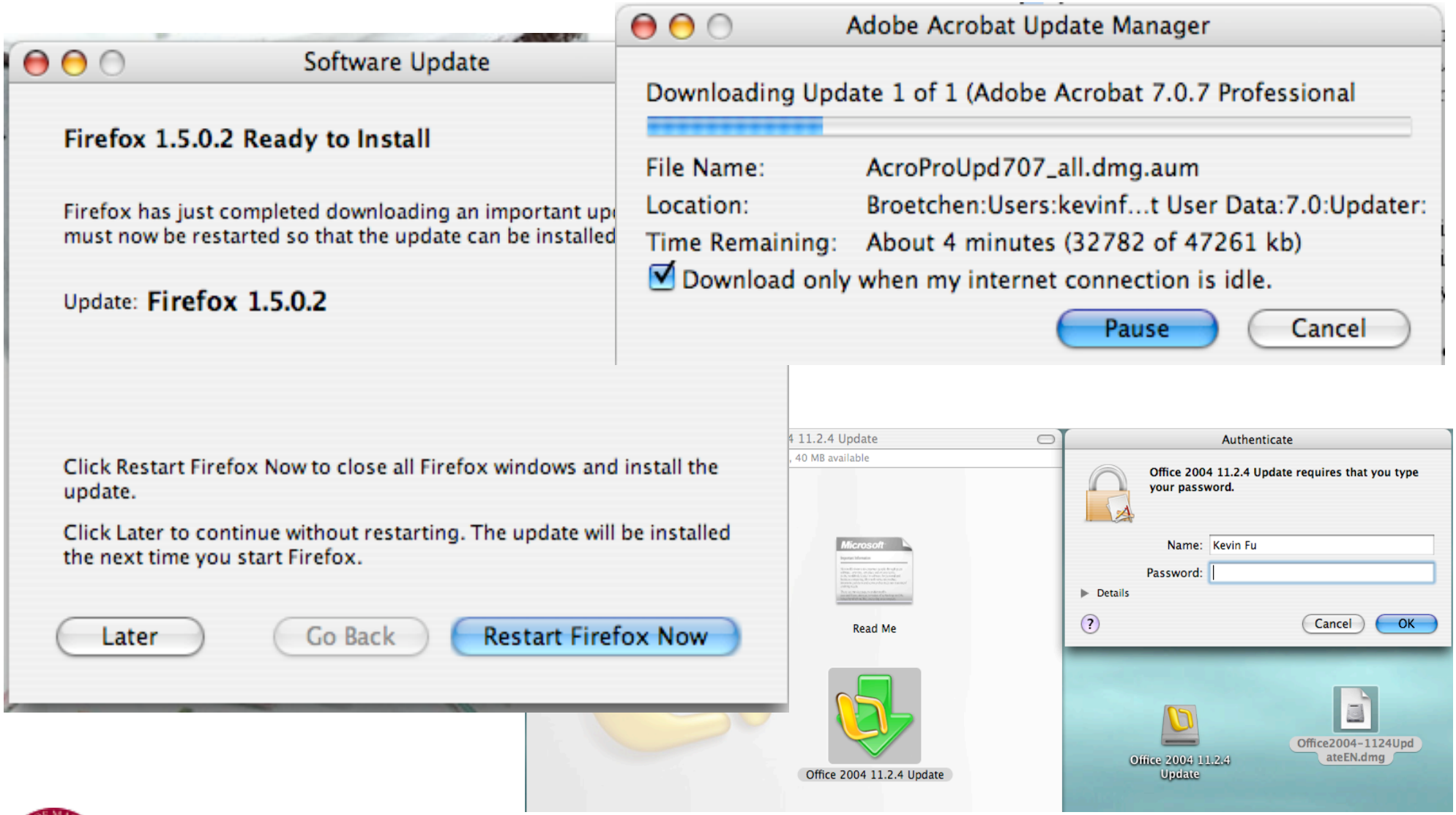
Foreseeable Cybersecurity Risks...



Foreseeable risk-o-meter

Managerial issues:
Diffusion of responsibility

Dirty Secrets: SW Maintenance



Software Update Woes

- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
  - Rhode Island: a third of the hospitals were forced ``to postpone elective surgeries and stop treating patients without traumas in emergency rooms.”
  - Upstate University Hospital in New York: 2,500 of the 6,000 computers were affected.


THE VANCOUVER SUN

Web-security giant McAfee paralyzes computers at hospitals, universities worldwide with update

Windows Microsoft Office

WHY?
Why is support ending for Windows XP SP3 and Office 2003?

WHAT?
What does end of support mean to customers?

HOW?
How will Microsoft help customers?

Windows 7

Get a free IDC assessment on migrating from Windows XP to Windows 7.

See how your organization can benefit from making the switch.

GET STARTED

WHAT?

What does end of support mean to customers?

It means you should take action. After April 8, 2014, there will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates.

Running Windows XP SP3 and Office 2003 in your environment after their end of support date may expose your company to potential risks, such as:

- **Security & Compliance Risks** – Unsupported and unpatched environments are vulnerable to security risks. This may result in an officially recognized control failure by an internal or external audit body, leading to suspension of certifications, and/or public notification of the organization's inability to maintain its systems and customer information.
- **Lack of Independent Software Vendor (ISV) & Hardware Manufacturers support** — A recent industry report from Gartner Research suggests "many independent software vendors (ISVs) are unlikely to support new versions of applications on Windows XP in 2011; in 2012, it will become common." And it may stifle access to hardware innovation: Gartner Research further notes that in 2012, most PC hardware manufacturers will stop supporting Windows XP on the majority of their new PC models.

Get current with Windows 7 and Office 2010. This option has upside well beyond keeping you supported. It offers more flexibility to empower employees to be more productive, while increasing operational efficiency through improved PC security and management. It also enables your organization to take advantage of latest technology trends such as virtualization and the cloud.

To help you get started in deploying a modern PC today, download the Microsoft Deployment Toolkit.
Download Free tool now.

How will Microsoft help customers?

WHAT?

What does end of support mean to customers?

It means you should take action. After April 8, 2014, there will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates.

Running Windows XP SP3 and Office 2003 in your environment after their end of support date may expose your company to potential risks, such as:

- **Security & Compliance Risks** - – Unsupported and unpatched environments are vulnerable to security risks. This may result in an officially recognized control failure by an internal or external audit body, leading to suspension of certifications, and/or public notification of the organization's inability to maintain its systems and customer information.
- **Lac** — A recent industry report fro of app inn Wi

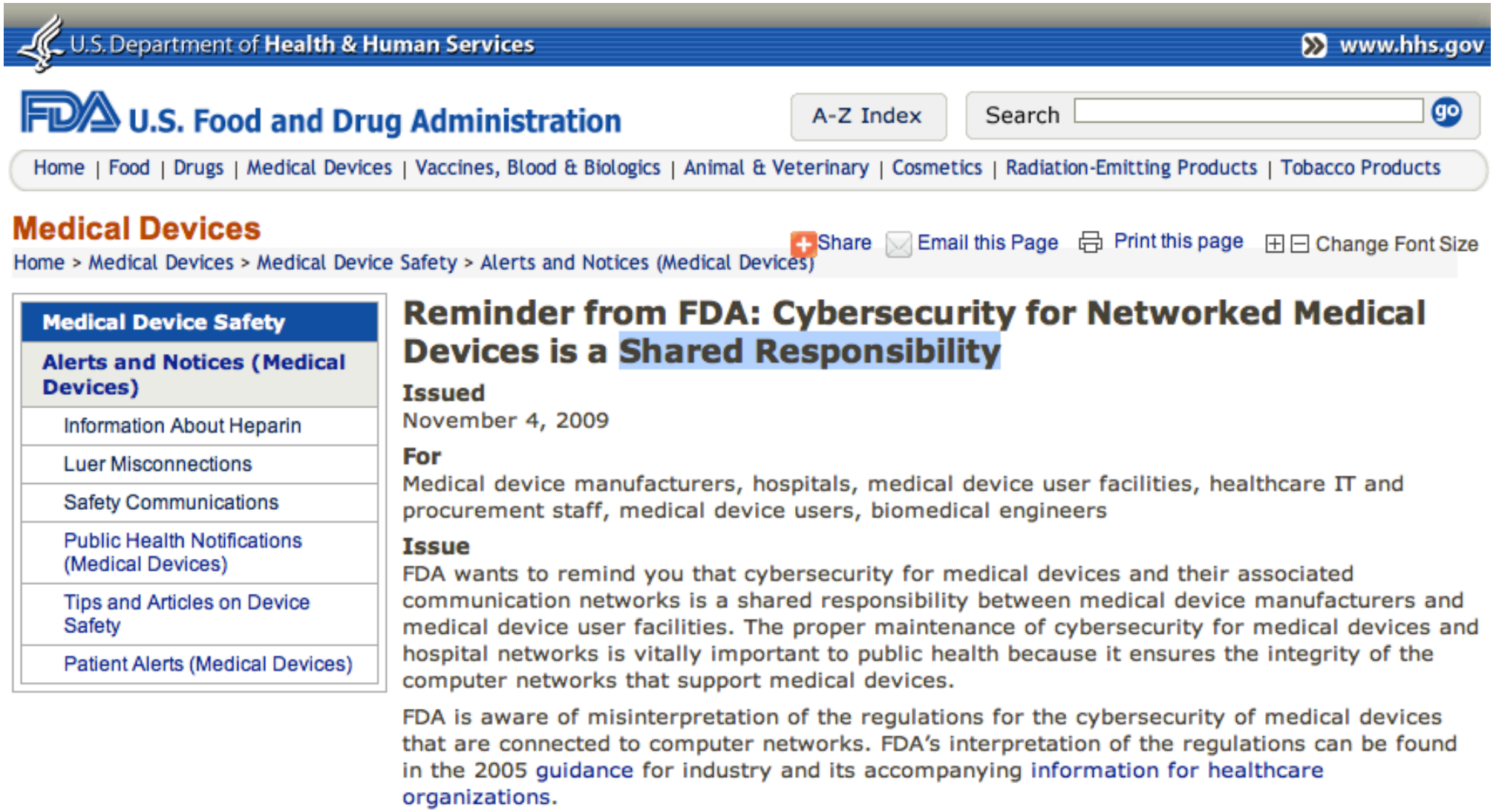
Products Released	Lifecycle Start Date	Mainstream Support End Date	Extended Support End Date	Service Pack Support End Date
Windows XP Embedded	1/30/2002	1/11/2011	1/12/2016	10/22/2004
Windows XP Professional	12/31/2001	4/14/2009	4/8/2014	8/30/2005
Windows XP Service Pack 1	8/30/2002	Not Applicable	Not Applicable	10/10/2006

Get cu rs more fle d PC security virtualiz

To help you get started in deploying a modern PC today, download the Microsoft Deployment Toolkit.
Download Free tool now.

How will Microsoft help customers?

Still Not It: Hospitals, Manufacturers



U.S. Department of Health & Human Services www.hhs.gov

FDA U.S. Food and Drug Administration A-Z Index Search go

Home | Food | Drugs | Medical Devices | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Radiation-Emitting Products | Tobacco Products

Medical Devices

Share Email this Page Print this page Change Font Size

Home > Medical Devices > Medical Device Safety > Alerts and Notices (Medical Devices)

Medical Device Safety

Alerts and Notices (Medical Devices)

- Information About Heparin
- Luer Misconnections
- Safety Communications
- Public Health Notifications (Medical Devices)
- Tips and Articles on Device Safety
- Patient Alerts (Medical Devices)

Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility

Issued
November 4, 2009

For
Medical device manufacturers, hospitals, medical device user facilities, healthcare IT and procurement staff, medical device users, biomedical engineers

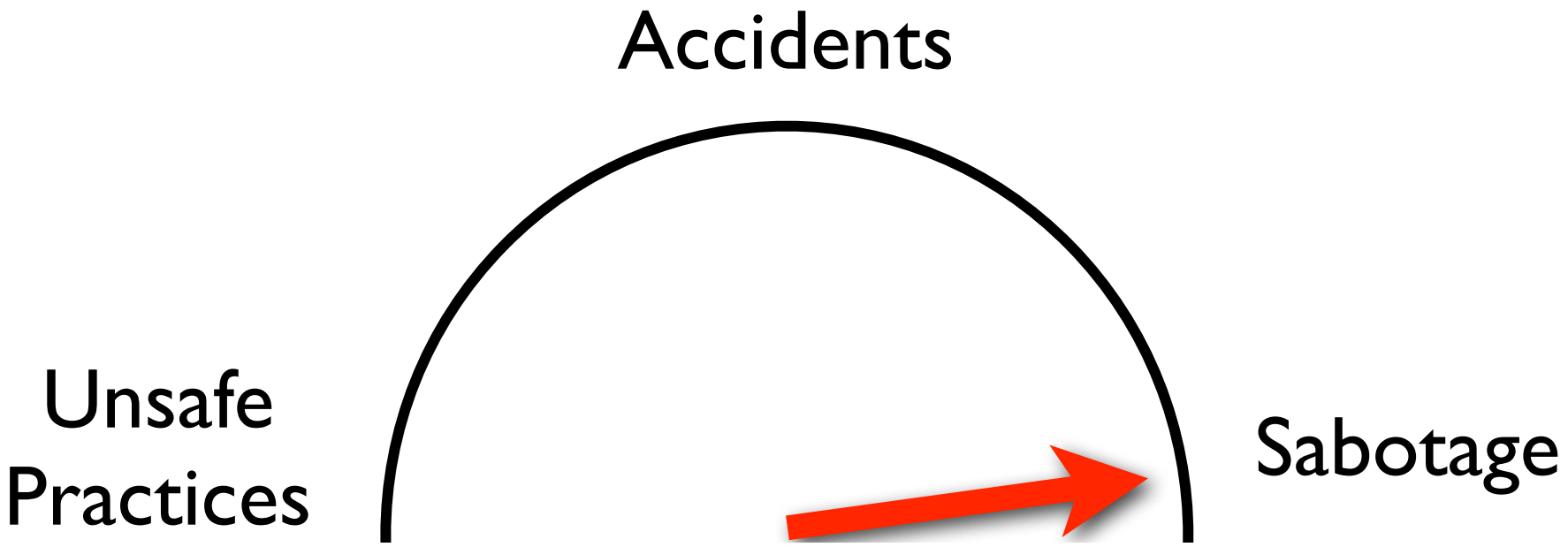
Issue
FDA wants to remind you that cybersecurity for medical devices and their associated communication networks is a shared responsibility between medical device manufacturers and medical device user facilities. The proper maintenance of cybersecurity for medical devices and hospital networks is vitally important to public health because it ensures the integrity of the computer networks that support medical devices.

FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA's interpretation of the regulations can be found in the 2005 guidance for industry and its accompanying information for healthcare organizations.

Managerial issues:
Diffusion of responsibility

Who's covered when
Secure Health IT hits the fan?

Foreseeable Cybersecurity Risks...



Foreseeable risk-o-meter

Implantation of Defibrillator

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Device Programmer

Photos: Medtronic; Video: or-live.com

Implantation of Defibrillator

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

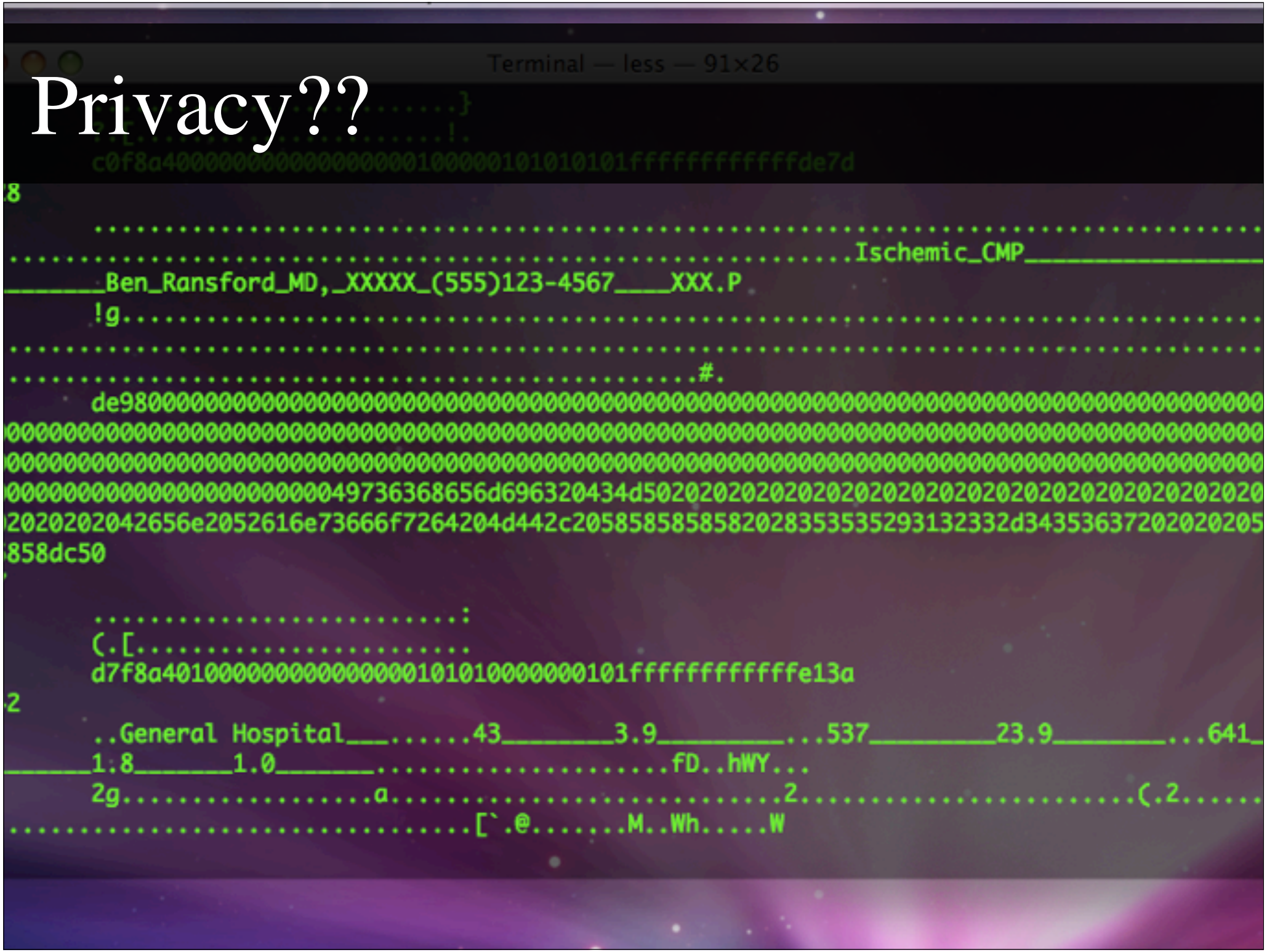
Photos: Medtronic; Video: or-live.com

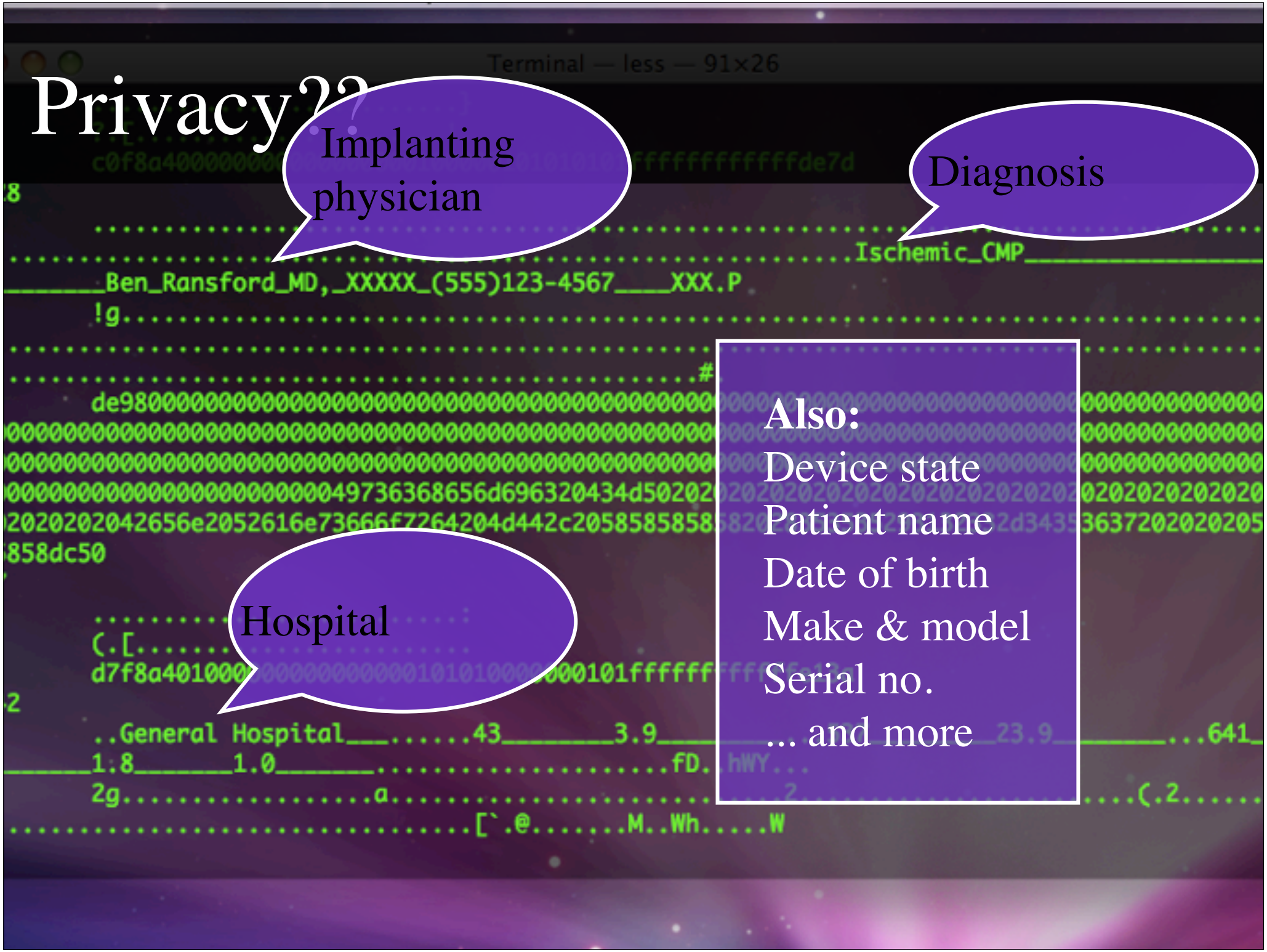
Implantation of Defibrillator

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Home monitor

Photos: Medtronic; Video: or-live.com


Terminal — less — 91×26
Privacy??
Ischemic_CMP
Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
General Hospital


Privacy??
Implanting physician
Diagnosis
Hospital
Also:
Device state
Patient name
Date of birth
Make & model
Serial no.
... and more

The Register®

Insulin pump hack delivers fatal dosage over the air

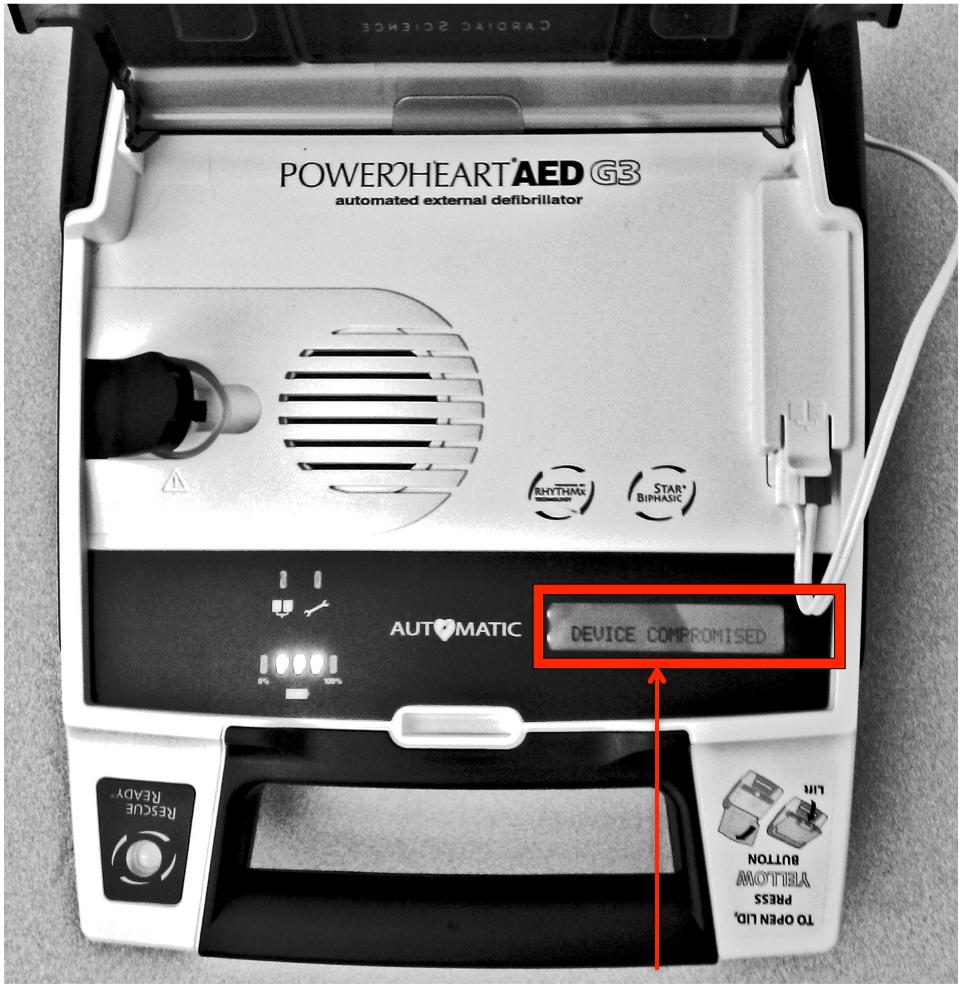
Sugar Blues, James Bond style

By Dan Goodin in San Francisco • Get more from this author

Posted in Security, 27th October 2011 06:23 GMT

In a hack fitting of a James Bond movie, a security researcher has devi
hijacks nearby insulin pumps, enabling him to surreptitiously deliver fata
patients who rely on them.

AED Firmware Replacement



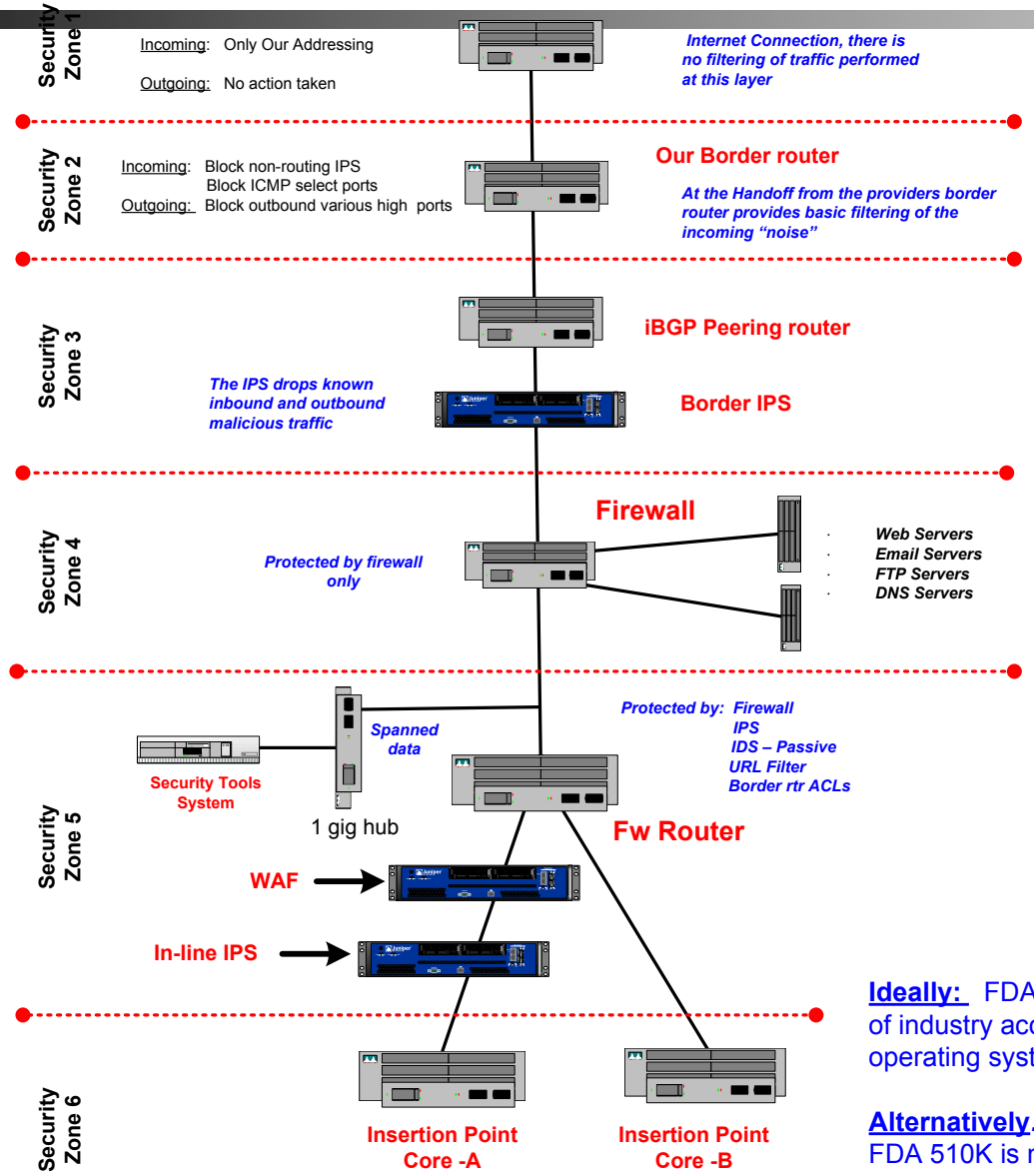
- Device accepts unauthentic firmware updates
- How do risks change when AEDs become wireless with Internet-based software updates?

DEVICE COMPROMISED

Hospitals & Malware

[Photo: Medical Real Estate Advisors and Kevin Fu]

Hospitals Stuck With Windows XP



General System Counts

Systems with AV…...6398
Printers……...2074
Medical equipment...**905**
Misc……2460

Total Devices:……..11837

OS Makeup – Medical

Windows 95……..1
Windows 98 ……15
Windows 2000……..23
Windows CE……..9
Windows Vista……..0
Windows XP……..600
Windows XP SP1…..0
Windows XP SP2….15
Windows XP SP3…..1

Total…….. 664

Last security patch: 2007

Average Time to Infection

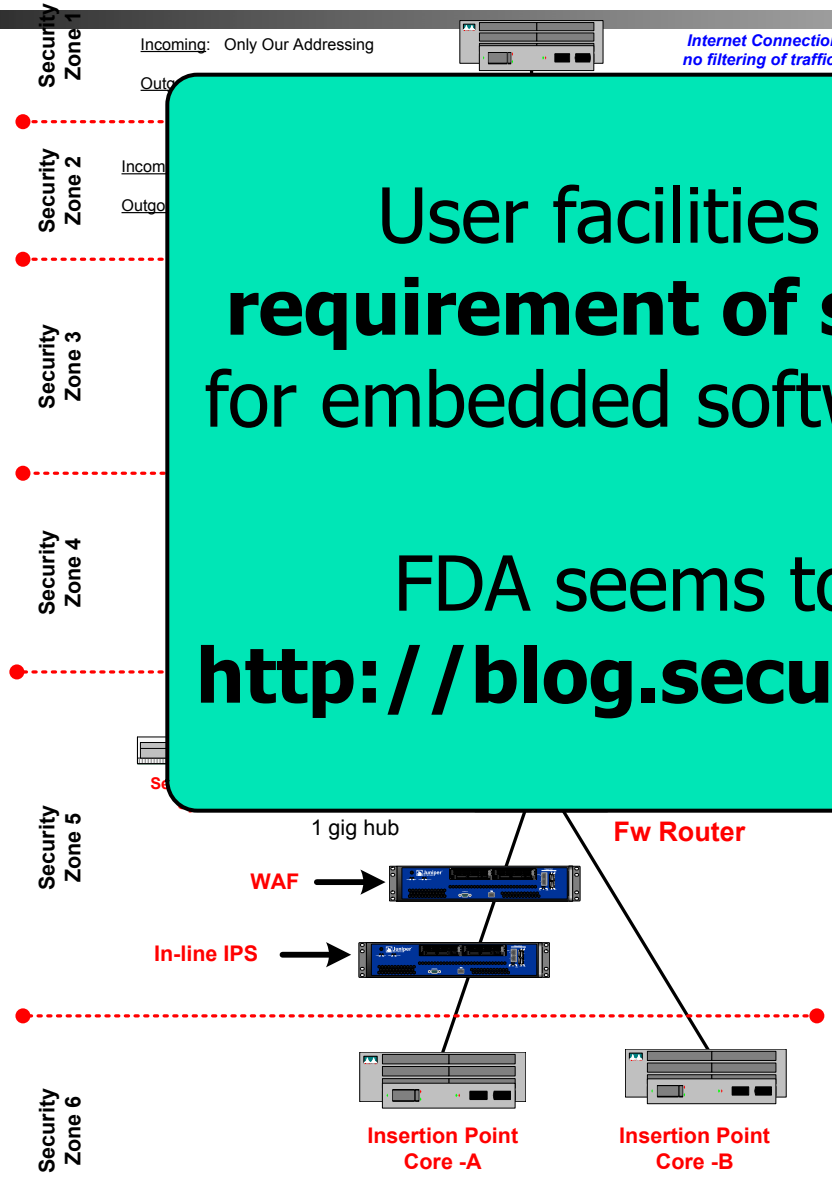
Clinical Systems , 510K, no AV..: **12 days**
Systems running AV/Patches…..: **300+ days**

Ideally: FDA 510K is updated to include a requirement for the provision of industry accepted security controls for devices utilizing embedded operating systems or other controllers associated with a medical device

Alternatively: The FDA issues a clear statement to the community that FDA 510K is not jeopardized by permitting Anti-Virus or Operating System patching to the supporting systems associated with a certified medical device

[Courtesy: Mark Olson, BIDMC Boston]

Hospitals Stuck With Windows XP



User facilities are asking for **requirement of security controls** for embedded software within 510(k).

FDA seems to be listening.

http://blog.secure-medicine.org/

General System Counts

398
074
5
460

837

Medical

1
15
23
.9
.0
600
.0
15
.1

664

Last security patch: 2007

Average Time to Infection

Clinical Systems , 510K, no AV..: **12 days**
Systems running AV/Patches…..: **300+ days**

Ideally: FDA 510K is updated to include a requirement for the provision of industry accepted security controls for devices utilizing embedded operating systems or other controllers associated with a medical device

Alternatively: The FDA issues a clear statement to the community that FDA 510K is not jeopardized by permitting Anti-Virus or Operating System patching to the supporting systems associated with a certified medical device

[Courtesy: Mark Olson, BIDMC Boston]

Waiter, there's a virus in my SW!

MAUDE Adverse Event Report: BAXA CORPORATIONBAXA EM2400 COMPOUNDER

FDA Home ◉ Medical Devices ◉ Databases

CDRH SuperSearch

510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA | TPLC

BAXA CORPORATION BAXA EM2400 COMPOUNDER Back to Search Results

Event Type Malfunction

Event Description

The (b) (6) pharmacy department uses a baxa em2400 compounder to make tpn's and other admixtures. Recently the compounder was infected with a virus. The virus has been contained on the em2400 compounder. It is unknown what effect this virus should have on the operating of the software. (b) (6) information systems department together with the pharmacy has requested that baxa provide a microsoft security patch to prevent this infection from occurring again. Baxa is unwilling to allow these patches to be applied to the baxa em2400. Instead baxa has recommend that we place a router with the functionality for a firewall between the compounder and the network (b) (4) as protection. In a single case, this may be a possible solution. (b) (6)'s manager indicates that if this was the routine solution, (b) (6) would then have to procure and maintain over 1000 routers institution wide. That approach is not sustainable by (b) (6) nor the marketplace. I am interested to hear about fda's requirement for medical devices to have security patches that protect the device from contamination.

Search Alerts/Recalls

Don't worry sir, they don't eat much!

MAUDE Adverse Event Report: BAXA CORP.EXACTA-MIX 2400

FDA Home ⊙ Medical Devices ⊙ Databases

CDRH SuperSearch

510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA | TPLC

BAXA CORP. EXACTA-MIX 2400 Back to Search Results

Model Number EM 2400
Event Date 02/26/2010
Event Type Other
Manufacturer Narrative

The em2400 compounder is designed to not be connected directly to the facility network, but should be installed behind a firewall that provides a protected subnet for the device. The device should be used only in accordance with its intended use and not for email, internet access, file sharing or other non-approved use. The device is designed to only reach out to the facility's network to collect text-based pat files, back up device databases or to issue a print job. The em2400 compounder is hosted on a (b)(4)-based embedded operating system and has been verified and validated only with the software, operating system and patches that were installed by baxa. Thus, any changes to the original, validated image, including installation of antivirus software, nullifies the validated state and could; therefore, constitute off-label use of this device. In addition, baxa does not regularly install operating system updates or patches, generally published by (b)(4), on this device. The online help file, preventing cyber attacks technical paper, specifies baxa's policies relating to product security and provides instructions for safeguarding baxa devices. If a device becomes infected, baxa technical support will send a replacement and assist the customer with proper facility network installation. Baxa has not received any reports of pt injury or illness as a result of this issue.

Event Description

Baxa received a letter from the fda on 04/08/2010 in reference to report number mw5014956. The report states that an em2400 compounder was infected with a virus. The customer requested that baxa provide a (b)(4) security patch to prevent the infection from occurring again. Upon receipt of the mw letter, the complaint database was reviewed to determine if an associated complaint was received by baxa prior to this report. No prior complaint was found. Therefore, a complaint was initiated to further investigate this issue. This mdr is being filed per baxa corporation's procedure to submit an mdr for all medwatch forms submitted.

But According to FDA…

"Virtual Patient Safety: Worms, Viruses and Other Threats to Computer-Based Medical Technology" by Al Taylor of FDA CDRH

The burning question…

FDA
Center for Devices and Radiological Health

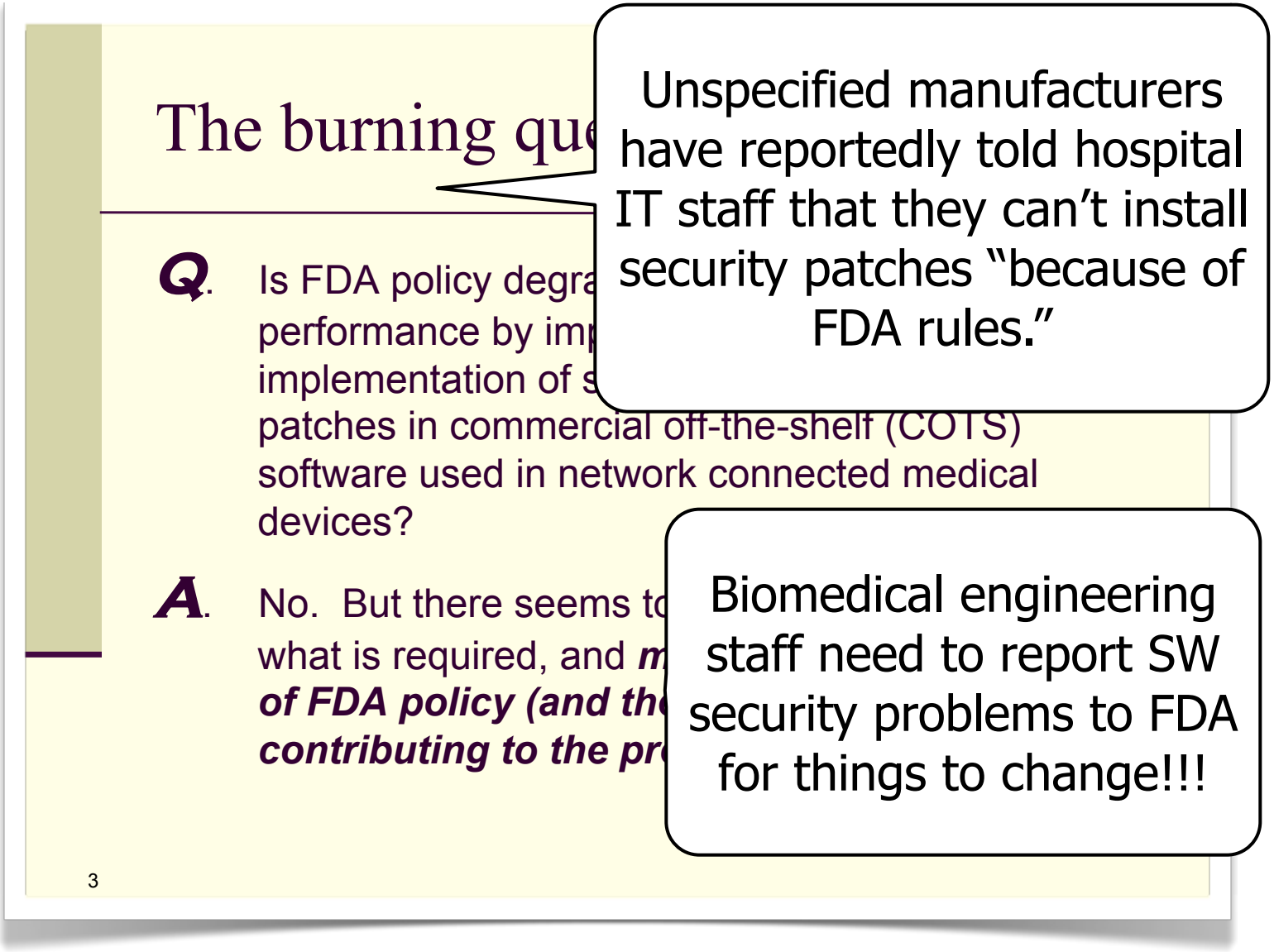
Q. Is FDA policy degrading network security and performance by impeding the timely implementation of security and other maintenance patches in commercial off-the-shelf (COTS) software used in network connected medical devices?

A. No. But there seems to be some confusion over what is required, and ***mistaken interpretations of FDA policy (and the law) may be contributing to the problem***.

3

But According to FDA…

"Virtual Patient Safety: Worms, Viruses and Other Threats to Computer-Based Medical Technology" by Al Taylor of FDA CDRH



Unspecified manufacturers have reportedly told hospital IT staff that they can't install security patches "because of FDA rules."

Biomedical engineering staff need to report SW security problems to FDA for things to change!!!


FDA rules prevent software security updates.
FALSE! But continue.
ICANHASCHEEZBURGER.COM

How significant are **intentional, malicious malfunctions** in software?

21 CFR 211.132 and Security

TITLE 21--FOOD AND DRUGS
CHAPTER I--FOOD AND DRUG ADMINISTRATION
DEPARTMENT OF HEALTH AND HUMAN SERVICES
SUBCHAPTER C--DRUGS: GENERAL

PART 211 -- CURRENT GOOD MANUFACTURING PRACTICE FOR FINISHED PHARMACEUTICALS

Subpart G--Packaging and Labeling Control

Sec. 211.132 Tamper-evident packaging requirements for over-the-counter (OTC) human drug products.

(a)General. The Food and Drug Administration has the authority under the Federal Food, Drug, and Cosmetic Act (the act) to establish a uniform national requirement for tamper-evident packaging of OTC drug products that will **improve the security** of OTC drug packaging

The Tylenol Scare of 1982

The Tylenol Terrorist

Print Email SHARE

T Smaller | Larger

By Rachael Bell

The Tylenonl Terrorist: Death in a Bottle

Extra-Strength Tylenol package

On September 29, 1982, 12-year-old Mary Kellerman of Elk Grove Village, Illinois, woke up at dawn and went into her parents' bedroom. She did not feel well and complained of having a sore throat and a runny nose. To ease her discomfort, her parents gave her one Extra-Strength Tylenol capsule. At 7 a.m. they found Mary on the bathroom floor. She was immediately taken to the hospital where she was later pronounced dead. Doctors initially suspected that Mary died from a stroke, but evidence later pointed to a more sinister diagnosis.

[Source: truTV crime library]

Fatal tampering case is renewed

FBI searches a condo in Cambridge

FBI agents carrying items seized from an apartment building on Gore Street in Cambridge walked out before a phalanx of television photographers. Five boxes and a computer were removed, but the FBI would not comment on their contents. (JIM DAVIS/GLOBE STAFF)

February 5, 2009

Email | Print | Single Page | Yahoo! Buzz | ShareThis Text size

This story was reported by Jonathan Saltzman, John R. Ellement, Milton J. Valencia, and David Abel of the Globe staff. It was written by Saltzman.

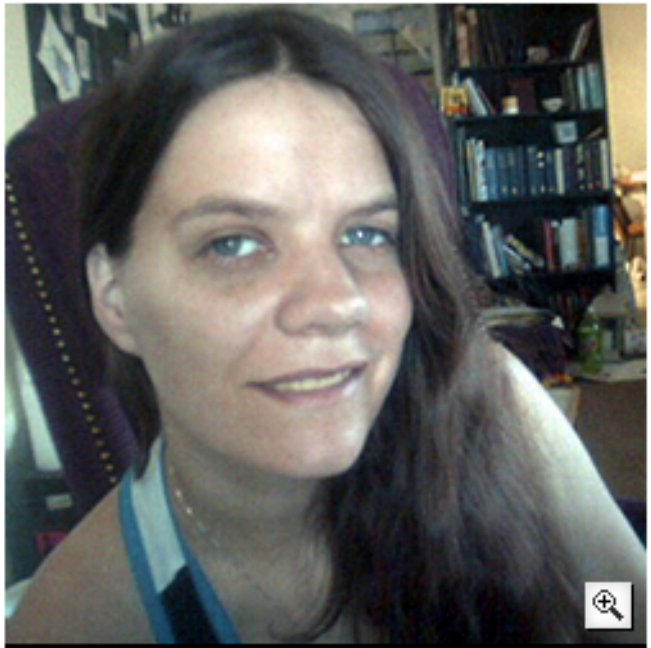
Discuss
COMMENTS (5)

CAMBRIDGE -- FBI agents and State Police investigators searched a Cambridge condominium yesterday that is the longtime home of a leading suspect in the 1982 deaths of seven people from cyanide-laced Tylenol capsules in the Chicago area, one of the most notorious unsolved crimes in the last generation.

Bad People Do Exist: Vandals

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM



RyAnne Fultz, 33, says she suffered her worst epileptic attack in a year after she clicked on the wrong post at a forum run by the nonprofit Epilepsy Foundation.
Photo courtesy RyAnne Fultz

Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

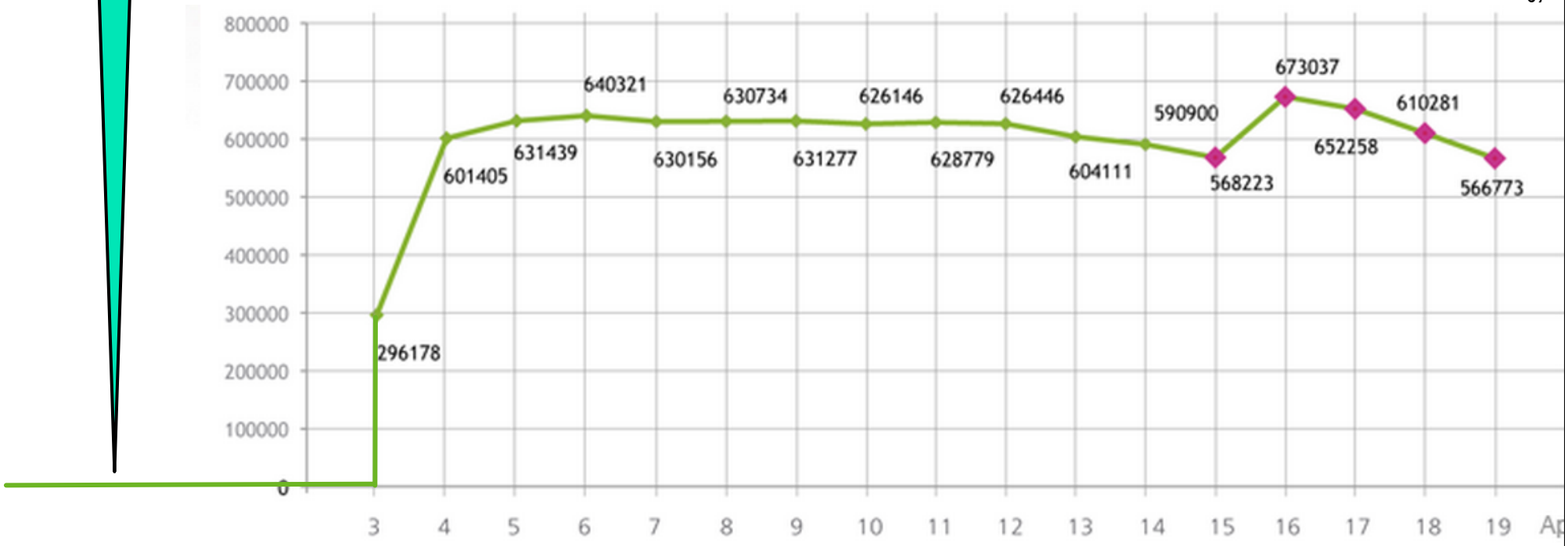
"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs.

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.

Lack of Exploits is Not Assurance

Pre-April 2012:
No Mac threats,
therefore never will be.



Source: Andy Greenberg, Forbes

19 Days in April 2012

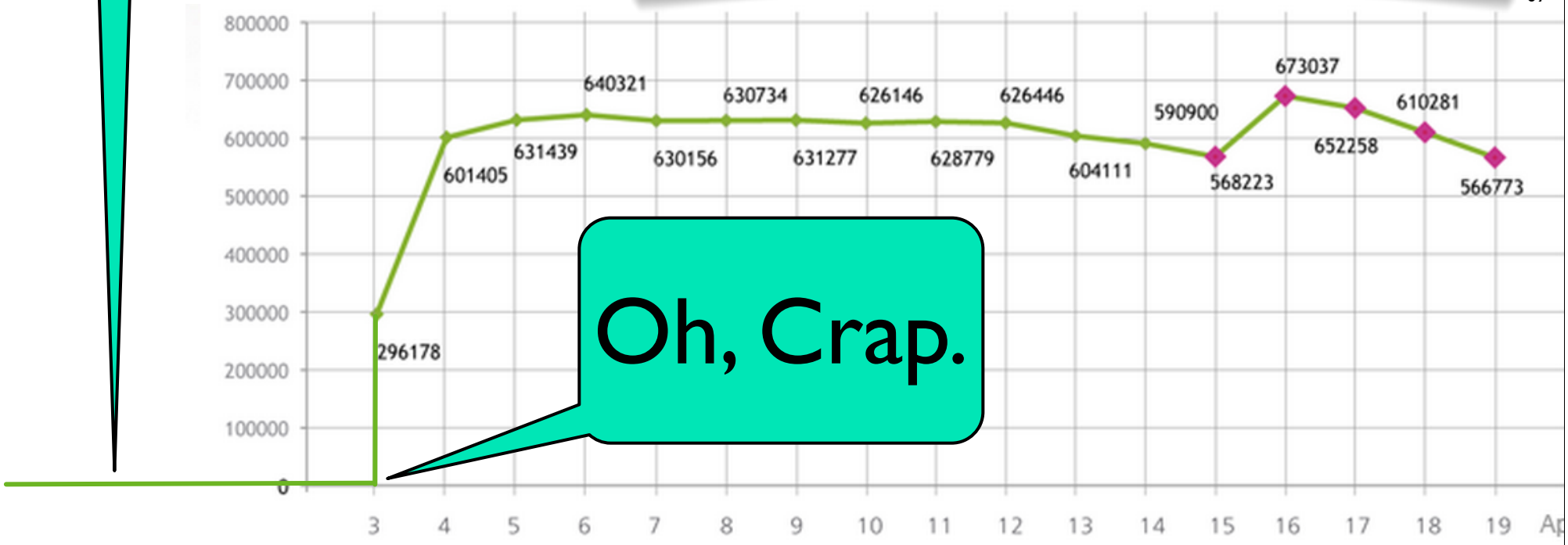
Lack of Exploits is Not Assurance

Pre-April 2012:
No Mac threats,
therefore never will be.

SECURITY | 4/20/2012 @ 5:28PM | 2,173 views

Antivirus Researchers Confirm: Flashback Still Infects More Than 500,000 Macs

Source: Andy Greenberg, Forbes



Oh, Crap.

19 Days in April 2012

Halo of Improved Security on Horizon!

"This is an evolution from having to think about **security and safety** as a healthcare company, and really about keeping people safe on our therapy, to this different question about keeping people safe around criminal or malicious intent."

Catherine Szyman
President, Medtronic Diabetes

[Reuters, 10/26/2011, HBS, Medtronic]

Security Built In: A New Hope?

- Slide excerpt from **Boston Scientific**
- (not me)

Security Risk Assessment Process

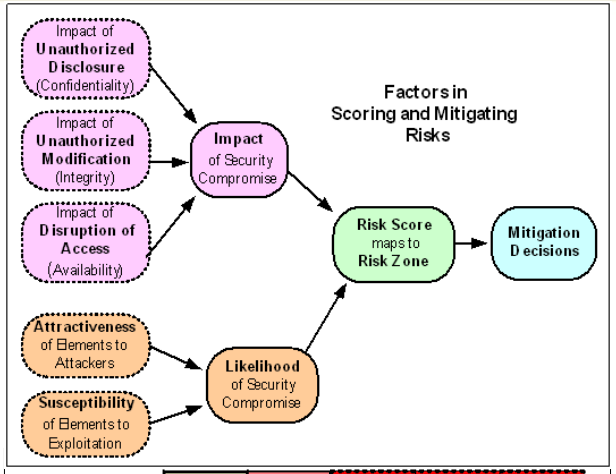
Boston Scientific

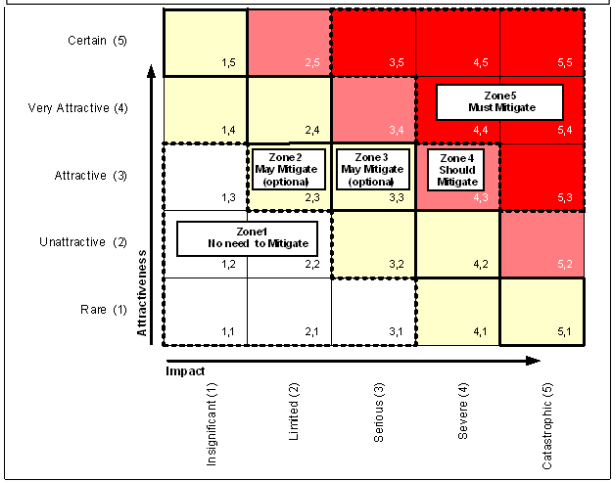
Security Risk process parallels safety risk
- Driven by IEC 14971

Cross-functional analysis, maintained across development lifecycle
- Starting at concept phase

Broad list of threat classes and protectable assets to consider

Risk axes
- Attractiveness (likelihood)
- Impact (severity)





39

CRM-92205-AA JUN20

OPEN ACCESS Freely available online

PLoS one

Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance

Daniel B. Kramer[1]*, Matthew Baker[1], Benjamin Ransford[2], Andres Molina-Markham[2], Quinn Stewart[2], Kevin Fu[2], Matthew R. Reynolds[1]

1 Department of Medicine, Beth Israel Deaconess Medical Center, Harvard Medical School, Boston, Massachusetts, United States of America, **2** Department of Computer Science, University of Massachusetts, Amherst, Massachusetts, United States of America

Abstract

Background: Medical devices increasingly depend on computing functions such as wireless communication and Internet connectivity for software-based control of therapies and network-based transmission of patients' stored medical information. These computing capabilities introduce security and privacy risks, yet little is known about the prevalence of such risks within the clinical setting.

Methods: We used three comprehensive, publicly available databases maintained by the Food and Drug Administration (FDA) to evaluate recalls and adverse events related to security and privacy risks of medical devices.

Results: Review of weekly enforcement reports identified 1,845 recalls; 605 (32.8%) of these included computers, 35 (1.9%) stored patient data, and 31 (1.7%) were capable of wireless communication. Searches of databases specific to recalls and adverse events identified only one event with a specific connection to security or privacy. Software-related recalls were relatively common, and most (81.8%) mentioned the possibility of upgrades, though only half of these provided specific instructions for the update mechanism.

Conclusions: Our review of recalls and adverse events from federal government databases reveals sharp inconsistencies with databases at individual providers with respect to security and privacy risks. Recalls related to software may increase security risks because of unprotected update and correction mechanisms. To detect signals of security and privacy problems that adversely affect public health, federal postmarket surveillance strategies should rethink how to effectively and efficiently collect data on security and privacy problems in devices that increasingly depend on computing systems susceptible to malware.

Citation: Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, et al. (2012) Security and Privacy Qualities of Medical Devices: An Analysis of FDA

OPEN ACCESS Freely available online

PLoS one

Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance

D
K
1
S

Regulators and manufacturers should carefully weigh the **premarket evaluation of security and privacy** elements of their devices and systems, and to design postmarket systems that enable effective collection of cybersecurity threat indicators for medical devices.

Methods: We used three comprehensive, publicly available databases maintained by the Food and Drug Administration (FDA) to evaluate recalls and adverse events related to security and privacy risks of medical devices.

Results: Review of weekly enforcement reports identified 1,845 recalls; 605 (32.8%) of these included computers, 35 (1.9%) stored patient data, and 31 (1.7%) were capable of wireless communication. Searches of databases specific to recalls and adverse events identified only one event with a specific connection to security or privacy. Software-related recalls were relatively common, and most (81.8%) mentioned the possibility of upgrades, though only half of these provided specific instructions for the update mechanism.

Conclusions: Our review of recalls and adverse events from federal government databases reveals sharp inconsistencies with databases at individual providers with respect to security and privacy risks. Recalls related to software may increase security risks because of unprotected update and correction mechanisms. To detect signals of security and privacy problems that adversely affect public health, federal postmarket surveillance strategies should rethink how to effectively and efficiently collect data on security and privacy problems in devices that increasingly depend on computing systems susceptible to malware.

Citation: Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, et al. (2012) Security and Privacy Qualities of Medical Devices: An Analysis of FDA

United States Government Accountability Office

GAO

Report to Congressional Requesters

August 2012

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

To access this report electronically, scan this QR Code.
Don't have a QR code reader? Several are available for free online.

GAO
Accountability * Integrity * Reliability

GAO-12-816

technology review
Published by MIT

Computer Viruses Are "Rampant" on Medical Devices in Hospitals

A meeting of government officials reveals that medical equipment is becoming riddled with malware.

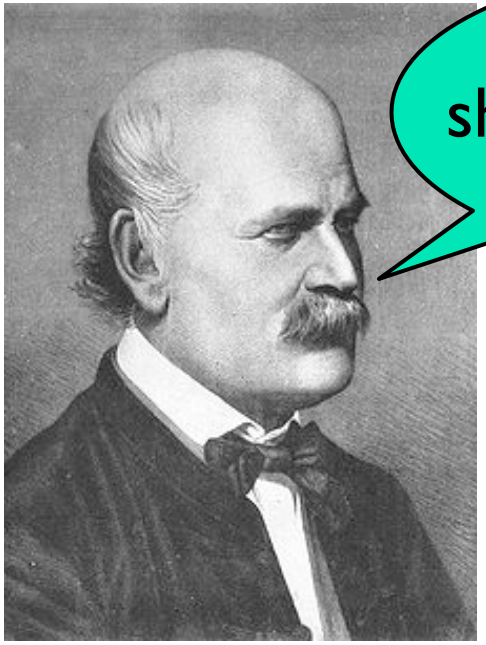
DAVID TALBOT
Wednesday, October 17, 2012

Health scare: Much hospital equipment uses software that can be vulnerable to viruses.
PR Newswire

Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable.

Semmelweis to Software Sepsis

1. Implantable medical devices should be trustworthy
2. Improved security will enable medical device innovation



Physicians should their wash hands.

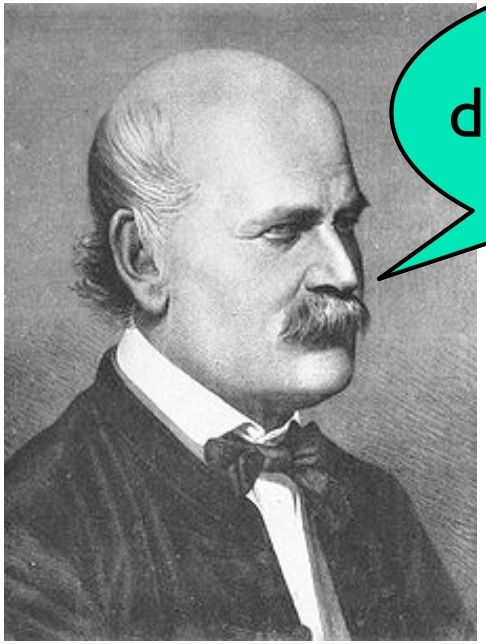
Doctors are gentlemen and therefore their hands are always clean.

Dr. Ignaz Semmelweis
1818-1865

Dr. Charles Meigs
1792-1869

Semmelweis to Software Sepsis

1. Implantable medical devices should be trustworthy
2. Improved security will enable medical device innovation



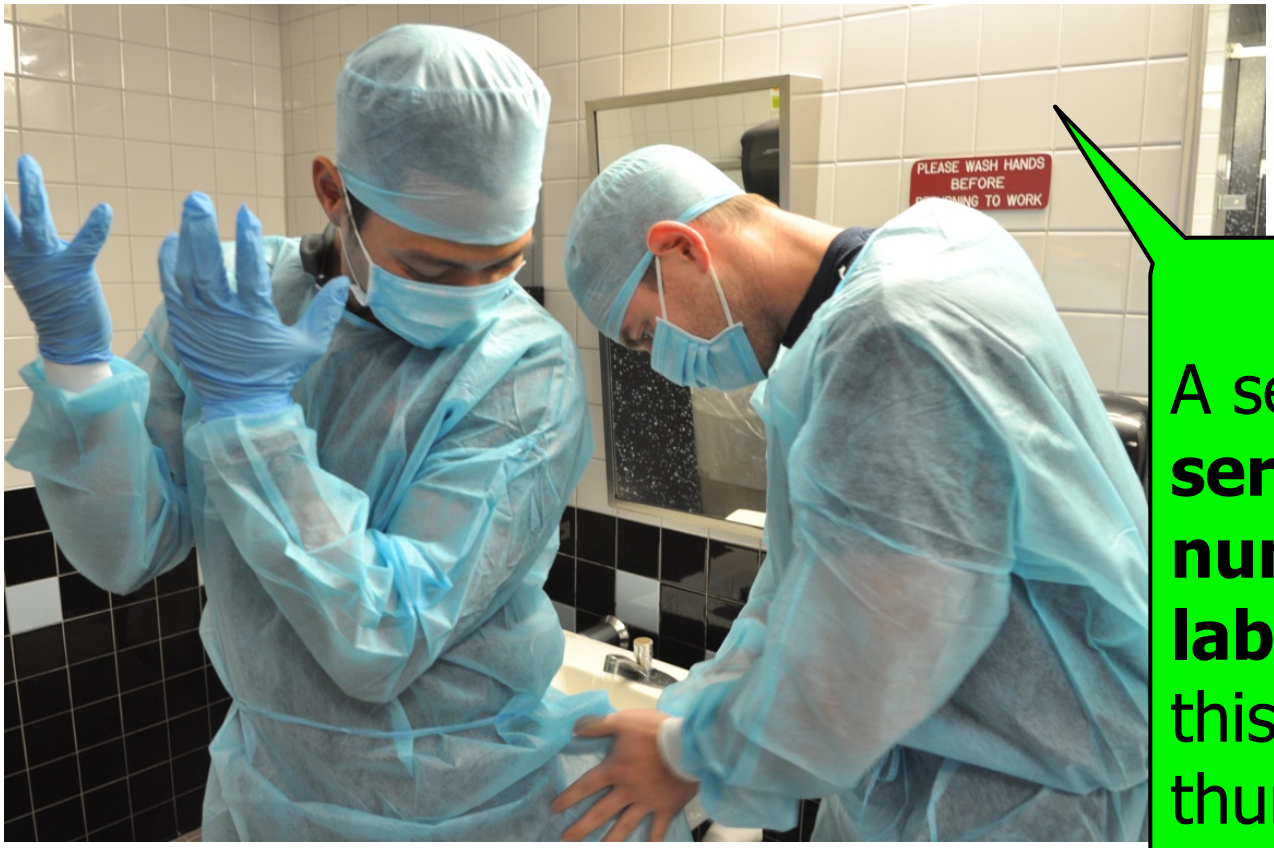
Medical devices should be secure.

Doctors are gentlemen and therefore their computers are always secure.

Dr. Ignaz Semmelweis
1818-1865

Dr. Charles Meigs
1792-1869

Sterile Technique or Software Sepsis?



A senior faculty member **serially infected a number of cath and EP lab systems,** and solved this problem by plugging thumb drives into a fellow's laptop to erase the malware he was spreading.

-Dr. Anonymous

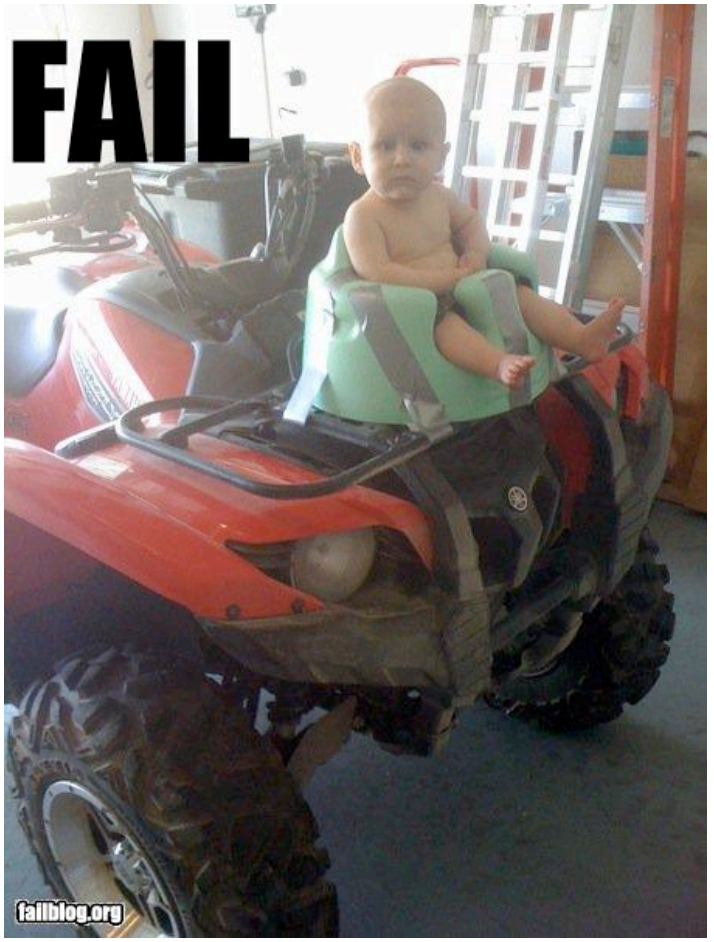
Compliance? Ask your Engineers…

- What design controls address cybersecurity risks?
  - Using wireless? Radio? USB port? Networking? Cloud?
  - A manufacturer can no longer claim unawareness of security risks
- How often are **software updates** issued to customers?
  - Windows XP has several critical security flaws per year
  - Engineers need resource$ to regularly issue software updates
- **Oxymorons** that raise my eyebrows. Watch out for:
  - Windows XP security
  - Cloud security
  - Wireless security
  - Unbreakable cryptography
  - Firewall-based security
  - Proprietary security
  - Private networks

←Ways Forward ↗

Security should be **designed** in

not **bolted** on



Summary: Responsibility is Yours

- Biggest risk:
  - ~~Hackers breaking into medical devices~~
  - Wide-scale **unavailability** of patient care
  - **Integrity** of medical sensors

- Security can't be bolted on. **Build it in.**

- Cybersecurity responsibility
  - Cybersecurity risks are now considered **foreseeable risks**
  - Design controls in early manufacturing should address risks
  - Update your Windows software!! Don't party like it's 1999.

Safety

Effectiveness

Meaningful use

Patient/clinic acceptance

Security part of the solution:

safe and effective medical device software

Assurance

Reduce costs

Predictability

Reliability

Dependability

Ann Arbor Research Center for Medical Device Security

secure-medicine.org