INCOSE Healthcare Working Group

4th Annual Systems Engineering in Healthcare Conference

Imagination at work.

Building a System for Cyber Security in Healthcare

19 April 2018

Steve Abrahamson
Sr. Director, Product Cyber Security
GE Healthcare

HARM

Javelin

Paveway

HARM

Javelin

Paveway

Little Professor

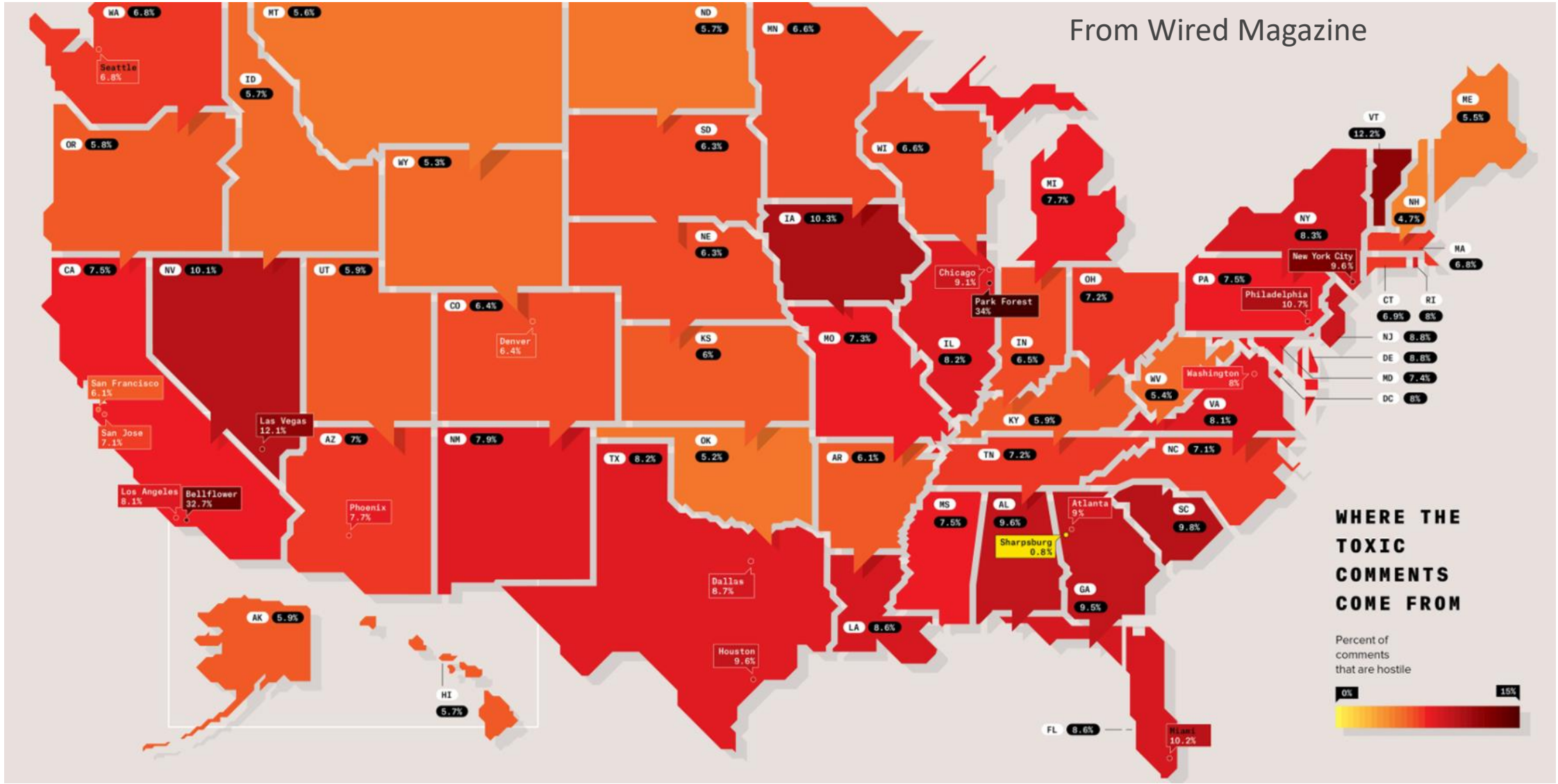
The Foundation

Cyber Security – Security in “Cyberspace”, a term coined by author William Gibson

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...”
— William Gibson, *Neuromancer*


Washington
Oregon
California
Idaho
Nevada
Montana
Wyoming
Utah
Arizona
Colorado
New Mexico
North Dakota
South Dakota
Nebraska
Kansas
Oklahoma
Texas
Minnesota
Iowa
Missouri
Arkansas
Louisiana
Wisconsin
Illinois
Michigan
Indiana
Ohio
Kentucky
Tennessee
Mississippi
Alabama
Georgia
Florida
South Carolina
North Carolina
Virginia
West Virginia
Pennsylvania
New York
Maryland
Delaware
New Jersey
Connecticut
Rhode Island
Massachusetts
Vermont
New Hampshire
Maine
Alaska
Hawaii

On-Line Behavior: Toxic Social Media (darker red = more toxic)



June 14, 2013

THE WALL STREET JOURNAL.

DOW JONES

FRIDAY, JUNE 14, 2013 - VOL. CCLXI NO. 138

WSJ.com

★★★★ $2.00

DJIA 15176.08 ▲ 180.85 1.2% NASDAQ 3445.37 ▲ 1.3% NIKKEI 12445.38 ▼ 6.4% STOXX 600 290.51 ▼ 0.1% 10-YR. TREAS. ▲ 15/32, yield 2.178% OIL $96.69 ▲ $0.81 GOLD $1,377.60 ▼ $14.20 EURO $1.3375 YEN 95.37

What's News—

Business & Finance

U.S. stocks staged a strong rally as upbeat economic readings helped insulate share prices from Tokyo's plunge into bear-market territory. The Dow industrials gained 180.85 points. C1, C4

■ **Many investors have** cut their inflation expectations, which could get the attention of Fed officials as they consider the course of bond buying. A2

■ **U.S. consumers showed** a renewed willingness to open their wallets in May, as retail sales posted a strong gain after two sluggish months. A2

■ **A surprise spike** in mortgage rates threatens to halt a refinancing boom that has delivered strong profits for U.S. banks in the past two years. A1

■ **Continued turmoil** in Japan's financial markets is fueling a debate about the effectiveness of Abe's package of growth-enhancing policies. A7

■ **The recent turbulence** rattling global bond markets has rekindled fears about the vulnerability of the euro zone's weakest countries. C1

■ **Senior finance officials** in the euro zone are working to polish details of a plan to allow the bloc's bailout fund to directly support ailing banks. C1

■ **The extension** of a big R&D tax credit boosted the profits of dozens of companies in the first quarter, a Wall Street

World-Wide

■ **House lawmakers trained their fire on the NSA leaker.** The top two members of the intelligence panel raised questions as to whether Edward Snowden has any ties to China. The charges came after Snowden said he believed there had been over 61,000 NSA hacking operations globally, including in Hong Kong and on the Chinese mainland. A4

The NSA doesn't collect data directly from T-Mobile and Verizon Wireless, due in part to foreign ownership ties.

■ **Obama authorized** the U.S. to arm Syrian rebels after the White House said it confirmed the regime had used chemical weapons. The U.S. military is also proposing a limited no-fly zone in Syria, officials said. A1

■ **Turkey's President Erdogan** issued a final warning for protesters to leave an Istanbul park. Police and protesters clashed in Ankara. A6

■ **The Supreme Court** unanimously held that human genes can't be patented, a ruling expected to quickly expand access to genetic testing. B1

■ **The Justices denied** a Texas agency's bid to go into Oklahoma to obtain water, in a blow to a drought-plagued region. A2

■ **The FDA is warning** makers of medical devices that their gear is at risk of being infected with computer viruses that

U.S. to Arm Syrian Rebels

In Shift, Obama Aids Faltering Insurgents, Finds Assad Used Chemical Weapons

By Adam Entous And Julian E. Barnes

WASHINGTON—President Barack Obama authorized his administration to provide arms to rebels fighting Syrian President Bashar al-Assad, officials said Thursday, a major policy shift after the White House said it had confirmed that Damascus used chemical weapons in the country's civil war.

The classified order directing the Central Intelligence Agency to coordinate arming the rebels in concert with its allies reverses a long-standing policy that limited the U.S. to providing nonlethal support.

The White House declined to comment on the authorization, saying only that Mr. Obama had decided to ramp up "military support" to moderate rebels both in "scope and scale."

U.S. officials also told The Wall Street Journal on Thursday that the U.S. military proposal for arming the rebels also calls for a limited no-fly zone inside Syria that would be enforced by U.S. and allied planes from Jordanian territory to protect Syrian refugees and rebels who would train there.

Such a move, if the White House goes ahead, would represent a significantly bigger U.S. engagement in Syria's civil war.

The developments followed a series of high level meetings at the White House and consultations with allies in which officials discussed the intelligence findings and proposals for arming the rebels.

U.S. officials said the issue divided Mr. Obama's national security team but that the administration faced little choice other than to step up its support or risk watching as rebels lose still more ground to a resurgent Assad regime backed by Russia, Iran and soldiers from the militant Hezbollah group.

Rebels requested specific weapons to hold off Mr. Assad's forces and Hezbollah fighters who are closing in on rebel positions in the city of Aleppo, the

Wednesday.

Please turn to page A6

Court Bars Patents on Human Genes

Patients Put at Risk By Computer Viruses

By Christopher Weaver

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of being infected with computer viruses that can endanger patients.

"We are aware of hundreds of medical devices that have been infected by malware," or dangerous computer software, said Bill Maisel, a senior official at the FDA's device unit. Though the agency doesn't know of deaths or injuries resulting from this, he said, "it's not difficult to

seeking FDA approval for [illegible] agency also advised hospitals to be more vigilant in reporting cybersecurity failures, which can be tough to detect.

The risk of computer viruses in hospitals and clinics is one side-effect of efforts to digitize health care and develop "smarter" medical devices. Malware in critical medical systems is widespread but little-understood, according to interviews with engineers and hospital executives and government documents reviewed by The Wall Street Journal.

For instance, previously unre-

August 15, 2013

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium — Register | Sign In

BloombergBusinessweek
Technology

Search

Follow @BW

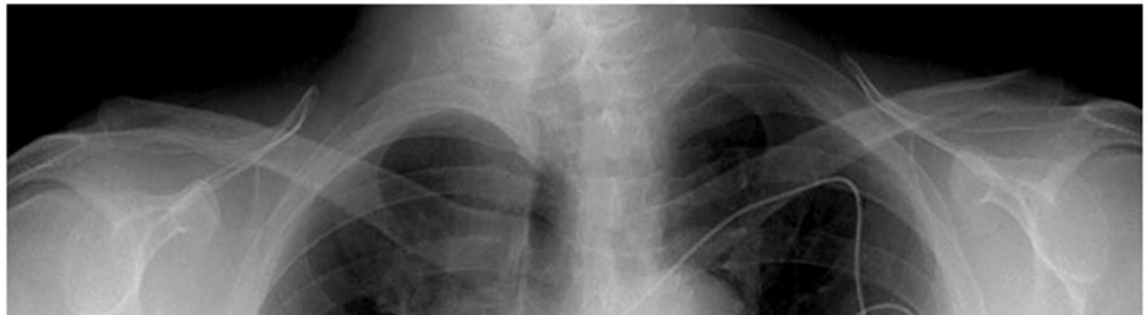
Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Lifestyle | Business Schools | Small Business | Video & Multimedia

Security

Medical Hacking Poses a Terrifying Threat, in Theory

By Joshua Brustein | August 15, 2013

SEND TO kindle



Most Popular Feed

Read | Shared | Discussed

How the NRA Defeated Obama's Surgeon General Choice: 4 Blunt Points

In Kiev, Armed and Masked Men Protect Parliament

To Make a Plane Disappear, Start by Getting Through the Cockpit Door

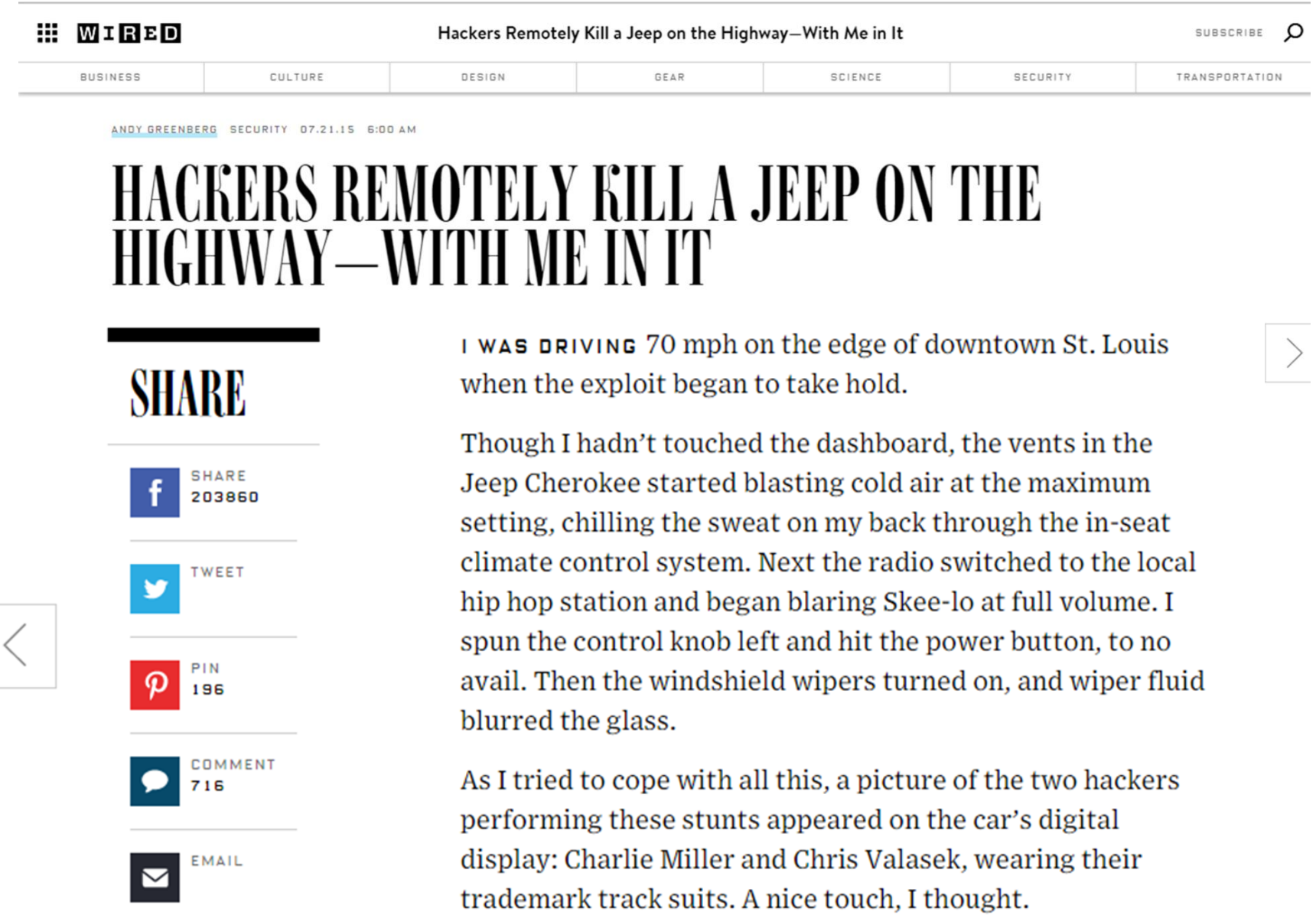
As Investors Flee, Russia Inc. Is Feeling the Pain

Alibaba's IPO Could Put $15.4 Billion Into Yahoo's Pocket

Subscribe to our daily Newsletter Sample copy

I'm in

July 21, 2015



WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It SUBSCRIBE

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

SHARE

SHARE 203860

TWEET

PIN 196

COMMENT 716

EMAIL

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.

July 31, 2015

FDA warns of security flaw in Hospira infusion pumps

BOSTON | BY JIM FINKLE

The U.S. Food and Drug Administration on Friday advised hospitals not to use Hospira Inc's Symbiq infusion system, saying a security vulnerability could allow cyber attackers to take remote control of the system.

The agency issued the advisory some 10 days after the U.S. Department of Homeland Security warned of the vulnerability in the pump, which is used to deliver medications directly into the bloodstream of patients.

"Security vulnerability could allow cyber attackers to take remote control of the system…"

Infusion Pump Case

Citing hacking risk, FDA says Hospira pump shouldn't be used

Monday, 3 Aug 2015 | 7:22 AM ET The Associated Press – CNBC

The federal government says health care facilities should stop using Hospira's Symbiq medication infusion pump because of its vulnerability to hacking.

The Food and Drug Administration said Friday it's the first time it has warned caregivers to stop using a product because of a cybersecurity risk. It comes at a time of rising concerns about breaches of products that connect to the Internet. A week ago, automaker Fiat Chrysler recalled 1.4 million vehicles because of a flaw that made them vulnerable to hackers.

The FDA says the computerized pumps could be accessed remotely through a hospital's network, but it doesn't know of any cases where that has happened. In recent months cybersecurity experts and the Department of Homeland Security have warned that the device could be hacked and remotely controlled, possibly allowing an intruder to change the amount of medication a patient received.

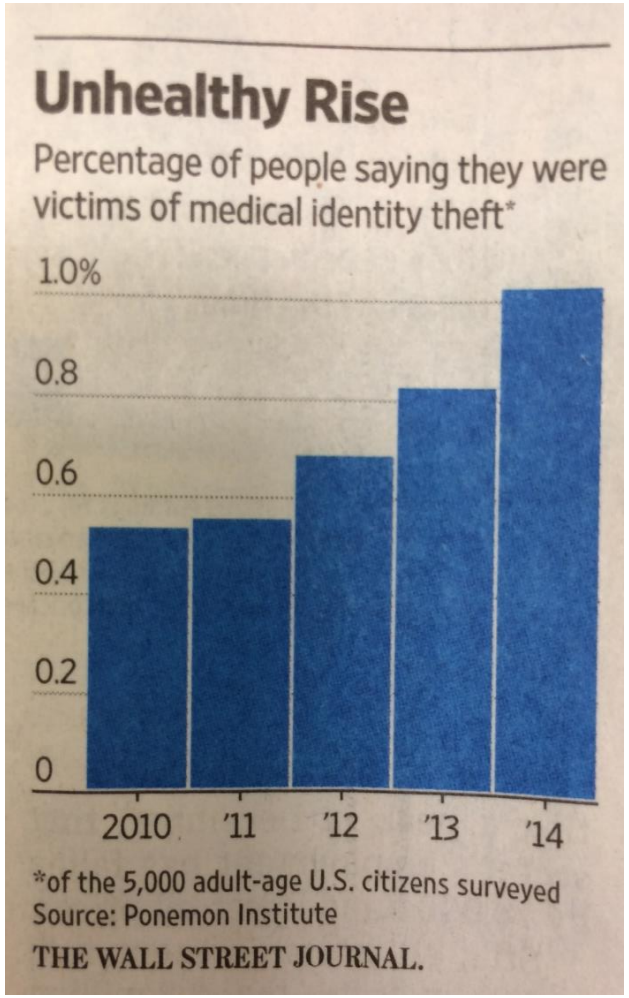
August 9, 2015 – The Wall Street Journal

THE DOCTOR BILL FROM IDENTITY THIEVES

Unhealthy Rise

The Voters Spoke, but This Politician Didn't Listen

Lost election aside, European parliamentarian still comes to work



How many patient records were stolen in the US in 2016?

15 December 2017

Forbes CommunityVoice™ Connecting expert communities to the Forbes audience. What is this?

DEC 15, 2017 @ 07:30 AM 2,394

The Little Black Book of I

The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards

Forbes Technology Council

Elite CIOs, CTOs & execs offer firsthand insights on tech & business. FULL BIO

Opinions expressed by Forbes Contributors are their own.

POST WRITTEN BY

Robert Lord

Co-Founder and President of Protenus, an analytics platform that detects inappropriate activity in healthcare institutions.

…the theft and sale of our health records on the black market, a thriving business with "dark web" online stores that don't look much different from an Amazon marketplace. In fact, there were nine times more medical than financial records breached in 2016 — 27 million — representing nearly 10% of the U.S. population…. I have seen the devastating aftermath these incidents can have on affected patients.

There's a metaphorical holiday feast of enticing data served up in your average health record. Family history, demographic data, insurance information, medications, etc. means there's enough information to completely steal an individual's identity and commit medication fraud, financial fraud, insurance fraud and a wide array of other crimes. When this very private, unchangeable information gets into the wrong hands, devastation can ensue.

In addition, in the case of any sensitive patient diagnoses like HIV, a history of plastic surgery or behavioral health challenges, medical blackmail remains a tempting option, with recent instances of hackers compromising a plastic surgery clinic as a terrifying recent reminder of this vulnerability.

As a result of this illicit versatility, medical records fetch quite a bit on the black market. While debate remains open on exactly how much they are worth and I've heard many different estimates from experts I trust, public estimates have put the resale value of a medical record up to $100 each, depending on how comprehensive it is and what type of patient it belongs to. The bottom line is these records can add up to real money, allowing bad actors to profit while wreaking havoc for the victims.

Complicating this further is that it's also terrifyingly easy for health care employees to go "shopping" for your data with little oversight. Electronic health record systems are generally built so that anyone who works at a hospital can access nearly the entire record, meaning that doctors, nurses, techs, admins and anyone else entrusted with patient care has free reign to look at your information.

The Guardian, 12 May 2017 - WannaCry

February 18, 2016

Forbes LOGIN

YOUR READING LIST

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

+289,642 views in the last 24 hours

Apple Leak Confirms Massive New iPhone 7

+15 comments in the last 24 hours

If Xbox One Becomes Immortal, Where Does That Leave PS4?

Active on Facebook

The Rainbow Mountains Of China Are Earth's Paint Palette

+1 comments in the last hour

Reducing Harassment In Science: Funding Follows Trainees

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FOLLOW ON FORBES (170)

FULL BIO

Across the world, hackers are taking control of networks, locking away files and demanding sizeable ransoms to return data to the rightful owner. This is the ransomware nightmare, one that a Hollywood hospital has been swallowed up by in the last week. The body confirmed it agreed to pay its attackers $17,000 in Bitcoin to return to some kind of normality. Meanwhile, FORBES has learned of a virulent strain of ransomware called Locky that's infecting at least 90,000 machines a day.

The Hollywood Presbyterian Medical Center's own nightmare started on 5 February, when staff noticed they could not access the network. It was soon determined hackers had locked up those files and wanted 40 Bitcoins (worth around $17,000) for the decryption key required to unlock the machines. Original reports had put the ransom at 9,000 Bitcoin (worth roughly $3.6 million), but Allen Stefanek, president and CEO of Hollywood


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:59:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:59:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

FBI Report – 17 October 2017

TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 October 2017

PIN Number

171017-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Medical Device Vulnerabilities Pose Growing Risk to US Healthcare Services and Patient Care

Summary

This year's WannaCry (WCry), aka WanaCrypt 2.0 ransomware attack marked the first FBI observed cyber attack that affected medical device operability in the United States. Medical devices were especially vulnerable to the WCry attack due to their reliance on outdated, unsupported software. Medical devices almost certainly will remain vulnerable to cyber attacks exploiting such software.

The ransomware attack highlighted the industry's challenges to provide timely patching and remediation for medical devices software. For example, in the case of WCry, Microsoft released a Windows 7 security patch several months earlier to protect against such an attack, but healthcare providers were victimized because some medical devices operated on other unsupported Windows versions. Based on FBI assessments from the WCry attack, contributing factors to medical device vulnerabilities include (but are not limited to) the following:

- Many devices rely on commercial off-the-shelf software and do not receive routine, if any, security testing or updates.
- If not clearly defined in vendor agreements, responsibility for post-market device cybersecurity is often unclear between manufacturers, vendors, and healthcare providers.
- Manufacturers, vendors, and providers may not have a full or accurate understanding of the requirements for deploying cyber security updates and the potential impact (if any) updates could have on devices' US Food and Drug Administration (FDA) clearance or approval.
- Providers depend heavily on compensating control measures, such as increased network defense tactics and use of virtual local area networks, to provide security for devices on their networks. However, secure device implementation can be difficult given the complexity of device systems and provider network environments, especially without effective change management policies.

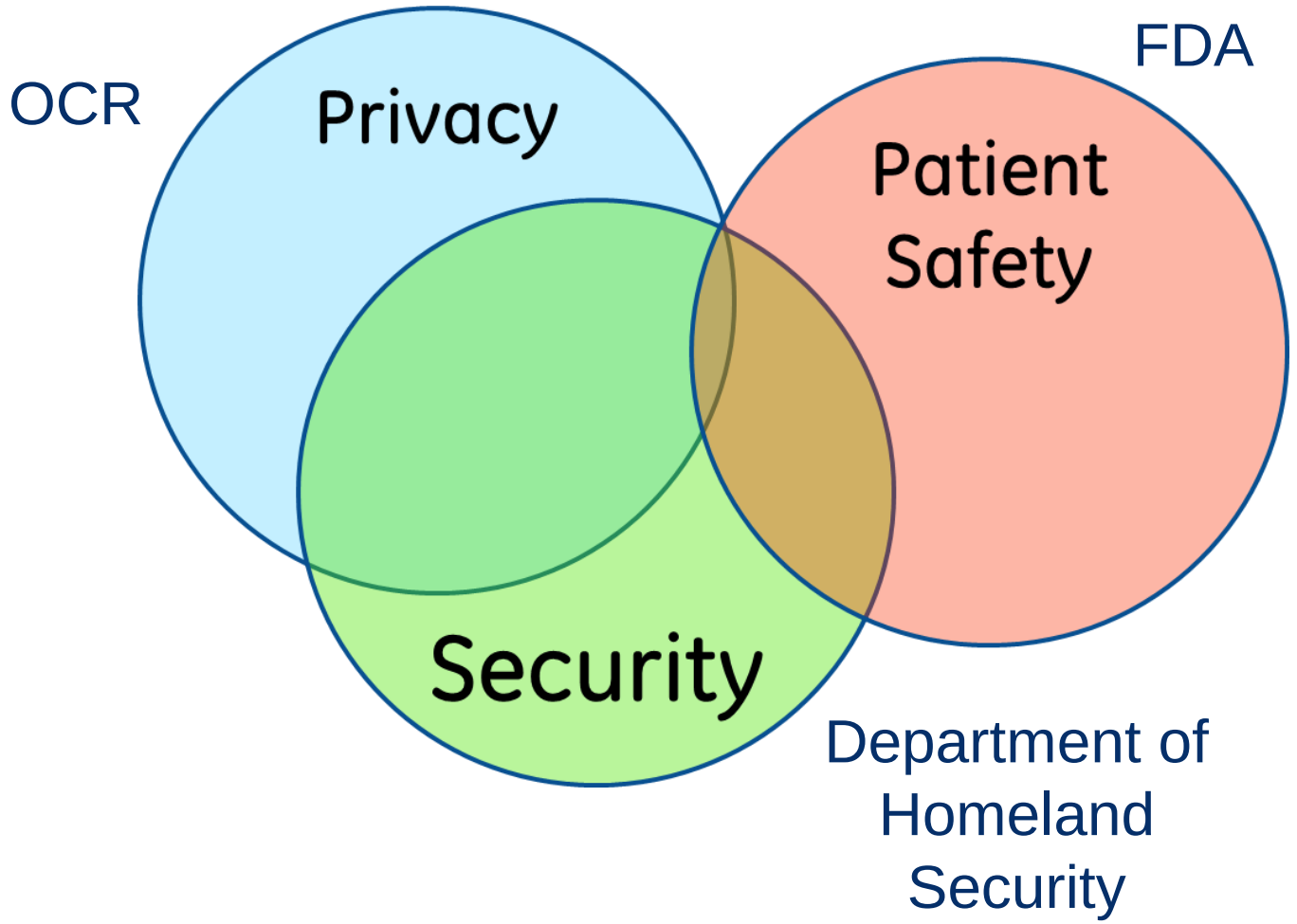
Recommendations:

Healthcare providers, medical device manufacturers, and device vendors who (a) clearly define cybersecurity responsibilities through provider/vendor agreements, (b) implement changes necessary to develop, enforce, and maintain device security, and (c) proactively communicate cybersecurity challenges between one another, are more likely to avoid falling victim to cyber attacks against medical devices and healthcare networks. The FBI leads and encourages participation in the Cyber Health Working Group through the InfraGard Program, which encourages IT professionals in the healthcare industry to share real-time tactical information about threats, trends, and best practices.[a]

The FDA provides pre[b] and post[c] -market guidance for the management of cybersecurity in medical devices. An "FDA Fact Sheet" is available online detailing the FDA's role and addressing many of the misconceptions surrounding medical device cybersecurity issues.[d] In addition, medical device stakeholders are encouraged to reference the recently published UL 2900-1

Government Response

Healthcare Security Risk Domains and US Government Stakeholders



US Critical Infrastructure

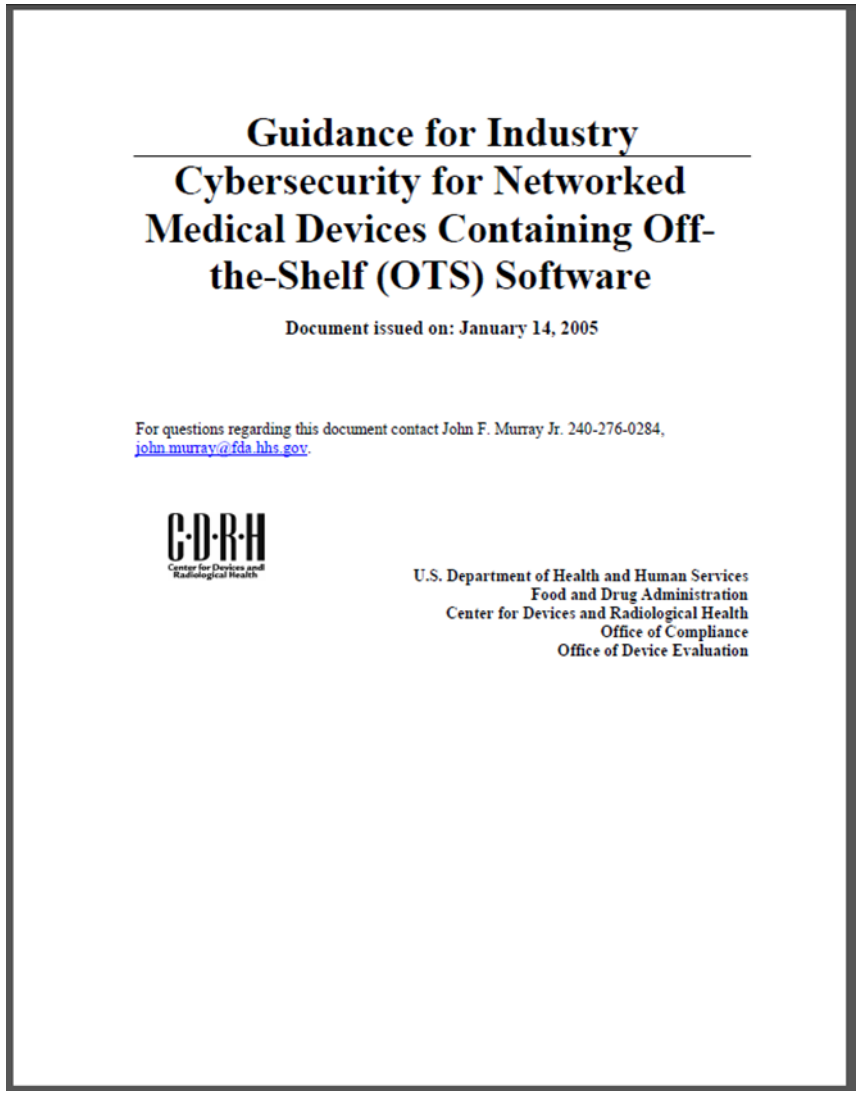
Established by Presidential Decision Directive PDD-63 (22 May 1998), Critical Infrastructure Protection

Latest Version: Presidential Policy Directive PPD-21 (12 Feb 2013) Critical Infrastructure Security and Resilience

Memo to HHS Secretary from Chairman, National Committee on Vital and Health Statistics, March 2005

- "..there are a wide variety of challenges associated with bringing medical devices into compliance with the Security Rule, as well as providing effective security."
- "…much of the medical equipment in use is no longer manufactured and may not be upgradeable by the manufacturer. As a result, it may not be possible to bring these "legacy devices" into compliance with the Security Rule."
- "Because of the critical nature of the medical equipment, any software updates (including those released by COTS software manufacturers in response to specific security threats) must be tested to ensure that the updates do not adversely affect the operation of the medical device. This testing often delays implementing critical security related software updates. Further, some customers update medical equipment with the latest software updates from third party software and operating system suppliers without first verifying whether the update affects the safe operation of the medical device for its intended purpose. "
- "…the FDA's primary focus has historically been the safe and effective use of medical devices, and therefore the FDA has not evaluated security in approving the use of a medical device."

FDA Guidance on Commercial Off-The-Shelf (COTS) Software



Guidance for Industry

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

Document issued on: January 14, 2005

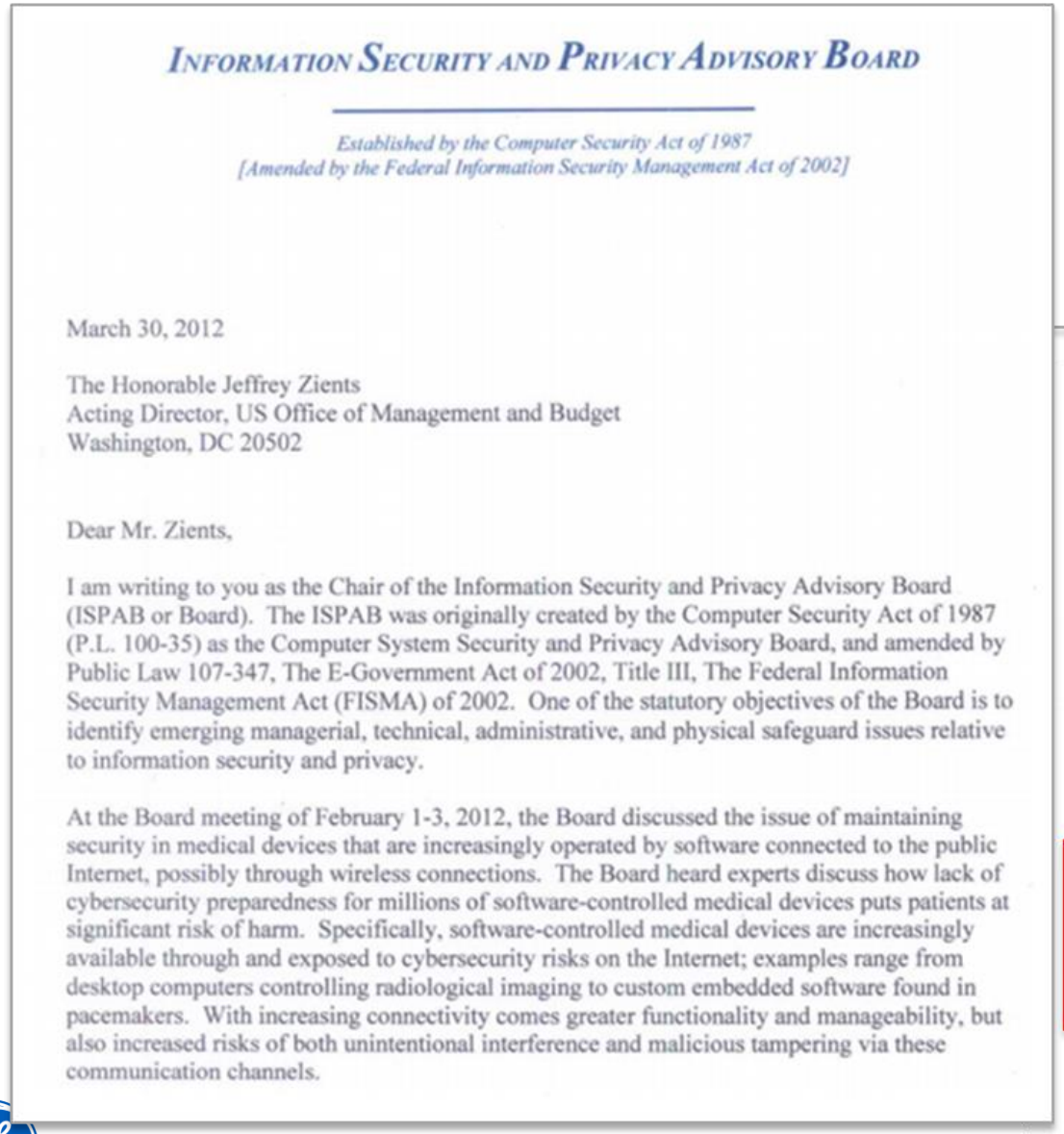
For questions regarding this document contact John F. Murray Jr. 240-276-0284, john.murray@fda.hhs.gov.

C·D·R·H Center for Devices and Radiological Health

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Compliance
Office of Device Evaluation

A growing number of medical devices are designed to be connected to computer networks. Many of these networked medical devices incorporate off-the-shelf software that is vulnerable to cybersecurity threats such as viruses and worms. These vulnerabilities may represent a risk to the safe and effective operation of networked medical devices and typically require an ongoing maintenance effort throughout the product life cycle to assure an adequate degree of protection. FDA is issuing this guidance to clarify how existing regulations, including the Quality System (QS) Regulation, apply to such cybersecurity maintenance activities.

US Information Security and Privacy Advisory Board – Letter to OMB (March 2012)



INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

March 30, 2012

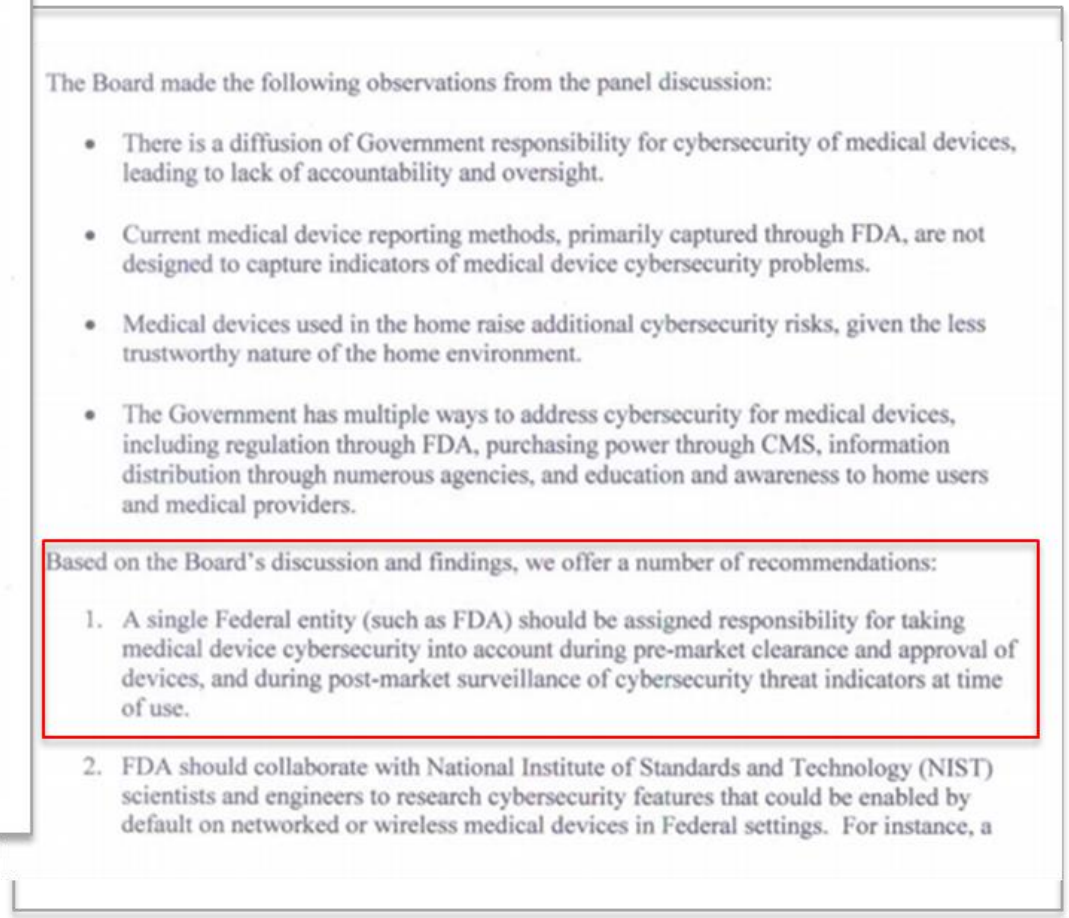
The Honorable Jeffrey Zients
Acting Director, US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board meeting of February 1-3, 2012, the Board discussed the issue of maintaining security in medical devices that are increasingly operated by software connected to the public Internet, possibly through wireless connections. The Board heard experts discuss how lack of cybersecurity preparedness for millions of software-controlled medical devices puts patients at significant risk of harm. Specifically, software-controlled medical devices are increasingly available through and exposed to cybersecurity risks on the Internet; examples range from desktop computers controlling radiological imaging to custom embedded software found in pacemakers. With increasing connectivity comes greater functionality and manageability, but also increased risks of both unintentional interference and malicious tampering via these communication channels.

"A single Federal entity such as FDA should be assigned responsibility for taking medical device cyber security into account during pre-market activity…and during post market surveillance…"



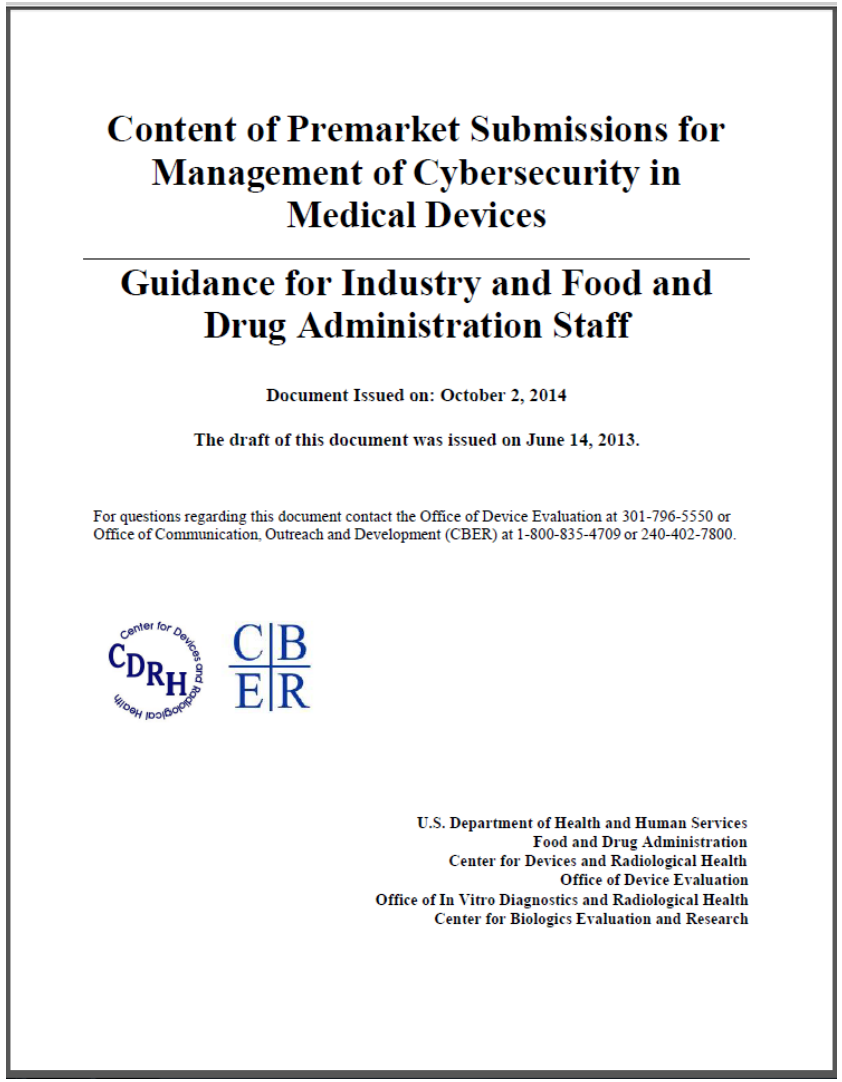
The Board made the following observations from the panel discussion:

- There is a diffusion of Government responsibility for cybersecurity of medical devices, leading to lack of accountability and oversight.
- Current medical device reporting methods, primarily captured through FDA, are not designed to capture indicators of medical device cybersecurity problems.
- Medical devices used in the home raise additional cybersecurity risks, given the less trustworthy nature of the home environment.
- The Government has multiple ways to address cybersecurity for medical devices, including regulation through FDA, purchasing power through CMS, information distribution through numerous agencies, and education and awareness to home users and medical providers.

Based on the Board's discussion and findings, we offer a number of recommendations:

1. A single Federal entity (such as FDA) should be assigned responsibility for taking medical device cybersecurity into account during pre-market clearance and approval of devices, and during post-market surveillance of cybersecurity threat indicators at time of use.
2. FDA should collaborate with National Institute of Standards and Technology (NIST) scientists and engineers to research cybersecurity features that could be enabled by default on networked or wireless medical devices in Federal settings. For instance, a

FDA Cybersecurity Guidance – Premarket
(02 October 2014)



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

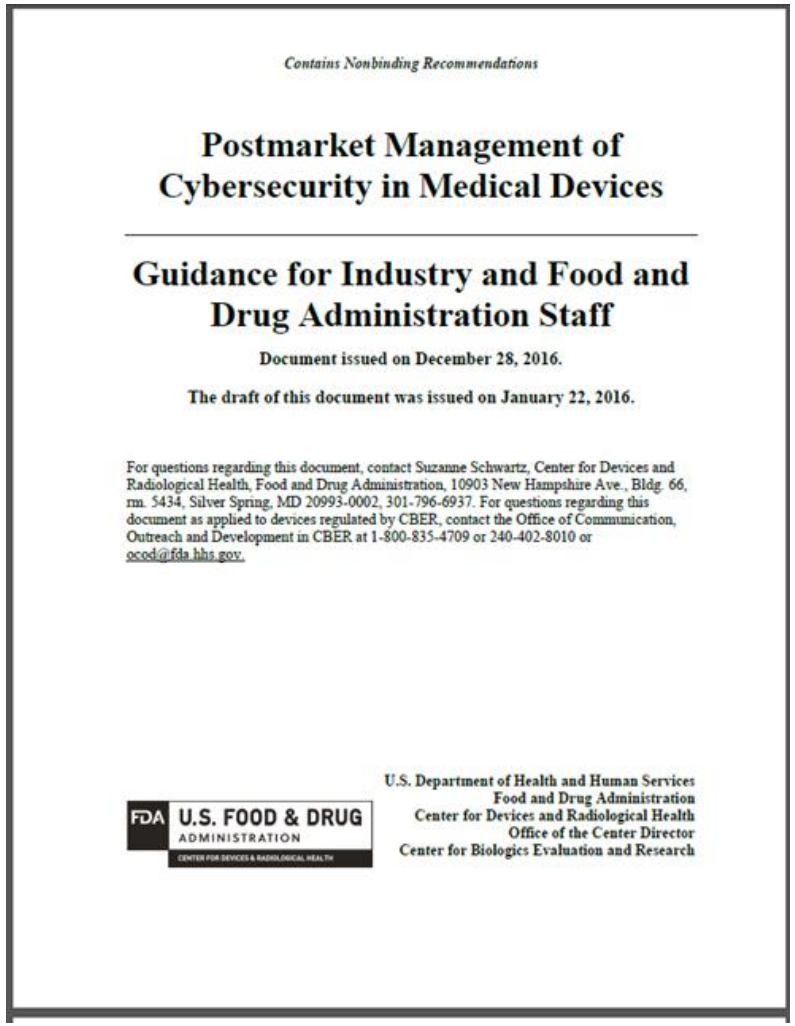
The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

The need for effective cybersecurity to assure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network- connected devices, and the frequent electronic exchange of medical device-related health information. This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.

FDA Cybersecurity Guidance – Postmarket
(28 December 2016)



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the overall risk to health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.

Health Insurance Portability and Accountability Act (HIPAA)

- Includes provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.
- Recognizing that advances in electronic technology could erode the privacy of health information, incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.
- The Privacy Rule (December 2000, modified in August 2002) sets national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- The Security Rule (February 2003) sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

The HIPAA Privacy Rule

- Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically
- Requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The HIPAA Security Rule

- Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
- The Security Rule requires protection against reasonably anticipated threats, appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (PHI).
- Administrative requirements include: assigned security responsibility, malicious s/w procedures, log-in monitoring, and password management
- Physical safeguards include facility access controls, workstation security, device and media controls, and media disposal, re-use, back-up, and storage procedures
- Technical safeguards include access control, unique user ID, auto log-off, encryption/decryption mechanisms, data authentication, personal authentication, network transmission security, integrity controls, encryption process (as appropriate)

Quiz – Breach Notification

Which US President signed into law a breach notification requirement for Protected Health Information?

Health Information Technology for Economic and Clinical Health (HITECH)

- In February 2009, President Obama signed the HITECH Act as part of his overall economic stimulus plan (American Recovery and Reinvestment Act of 2009)
- Imposes requirements on vendors of personal health records (and other related entities) in the event of certain security breaches relating to protected health information
- Continues the effort of the Health Insurance Portability and Accountability Act (HIPAA) to encourage movement to electronic patient records and to deliver stricter data protection regulations for more secure patient privacy
- Also extends HIPAA requirements beyond the traditionally covered entities of "payors, providers and clearinghouses" to include their business partners.
- Mandates a breach notification requirement for stored health information that is not encrypted or otherwise made indecipherable, as well as increasing penalties for violations
- In August 2009, the Department of Health and Human Services (HHS) issued a statement specifying only "encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals."

2018 HIPAA Fines

Date	Organization	Fine Total	Link to OCR Settlement
February 1, 2018	Fresenius Medical Care North America (FMCNA)	$3,500,000	Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
February 13, 2018	Filefax, Inc.	$100,000	Consequences for HIPAA violations don't stop when a business closes
	2018 TOTAL:	**$3,600,000**	

2017 HIPAA Fines

Date	Organization	Fine Total	Link to OCR Settlement
January 9, 2017	Presence Health	$475,000	First HIPAA enforcement action for lack of timely breach notification settles for $475,000
January 18, 2017	MAPFRE	$2,200,000	HIPAA settlement demonstrates importance of implementing safeguards for ePHI
February 1, 2017	Children's Medical Center of Dallas	$3,200,000	Lack of timely action risks security and costs money
February 16, 2017	Memorial Healthcare Systems	$5,500,000	$5.5 million HIPAA settlement shines light on the importance of audit controls
April 12, 2017	Metro Community Provider Network (MCPN)	$400,000	Overlooking risks leads to breach, $400,000 settlement
April 20, 2017	The Center for Children's Digestive Health (CCDH)	$31,000	No Business Associate Agreement? $31K Mistake
April 24, 2017	CardioNet	$2,500,000	$2.5 million settlement shows that not understanding HIPAA requirements creates risk
May 10, 2017	Memorial Hermann Health System (MHHS)	$2,400,000	Texas health system settles potential HIPAA violations for disclosing patient information
May 23, 2017	St. Luke's Roosevelt Hospital System Inc.	$387,200	Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k
December 18, 2017	21st Century Oncology	$2,300,000	$2.3 Millon Levied for Multiple HIPAA Violations at NY-Based Provider
	2017 TOTAL:	**$19,393,200**	

$5.5 million HIPAA settlement shines light on the importance of audit controls

Memorial Healthcare System (MHS) has paid the U.S. Department of Health and Human Services (HHS) $5.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and agreed to implement a robust corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

"Access to ePHI must be provided only to authorized users, including affiliated physician office staff" said Robinsue Frohboese, Acting Director, HHS Office for Civil Rights. "Further, organizations must implement audit controls and review audit logs regularly. As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen."

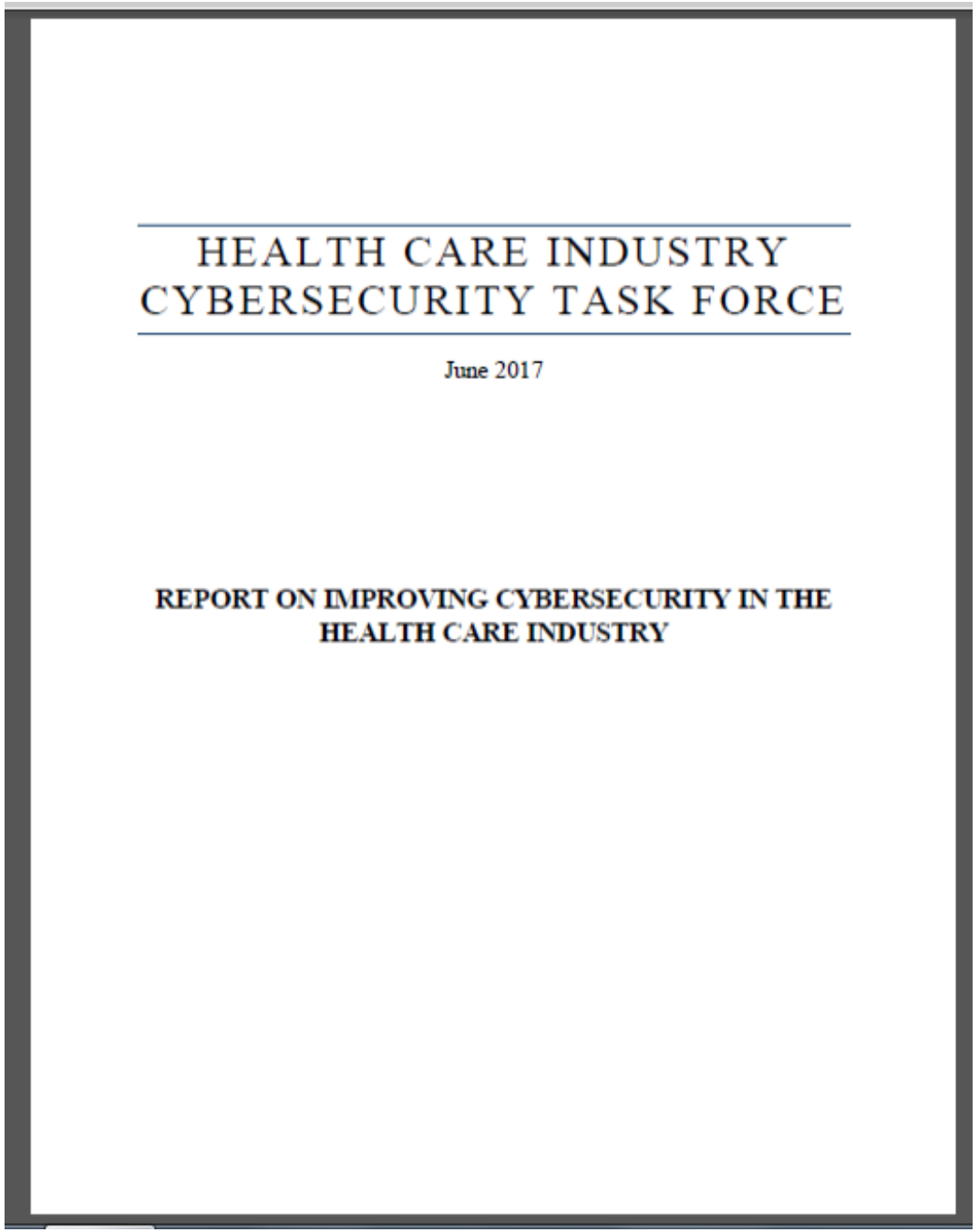
Protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers.

The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals.

MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules.

Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information

June 2017



HEALTH CARE INDUSTRY
CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

Congressional Action:

BROOKS, TROTT Introduce Legislation to Safeguard Americans' Healthcare Technology During National Cyber Security Awareness Month

Oct 5, 2017

News Releases

Washington, D.C. – Today, during National Health IT Week, U.S. Representatives Susan Brooks (R-IN05) and Dave Trott (R-MI11) introduced the Internet of Medical Things Resilience Partnership Act, which creates a public-private stakeholder partnership to lay out a cybersecurity framework to protect protects Americans' sensitive healthcare information from cyber-attacks.

"There are millions of medical devices susceptible to cyber-attacks and often times, we are wearing these networked technologies or even have them imbedded in our bodies," said Rep. Brooks. "Bad actors are not only looking to access sensitive information, but they are also trying to manipulate device functionality. This can lead to life-threatening cyber-attacks on devices ranging from monitors and infusion pumps, to ventilators and radiological technologies. As the number of connected medical devices continue to grow, so does the urgency to establish guidelines for how to prevent these kinds of dangerous attacks…I am proud to introduce a bill with my colleague Rep. Trott that brings together public and private sector counterparts to address potential vulnerabilities of medical technologies."

(4) APPOINTED MEMBERS.—The chairperson shall appoint to the working group a minimum of 3 qualified representatives from each of the following private sector categories: (A) Medical device manufacturers. (B) Health care providers. (C) Health insurance providers. (D) Cloud computing. (E) Wireless network providers. (F) Enterprise security solutions systems. (G) Health information technology. (H) Web-based mobile application developers. (I) Software developers. (J) Hardware developers.

10 (c) REPORT.—Not later than 18 months after the date of enactment of this Act, the Commissioner shall submit to Congress a report on the recommendations developed under subsection (a), including—an identification of existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to mitigate vulnerabilities in the devices described in subsection (a); (2) an identification of existing and developing international and domestic cybersecurity standards, guidelines, frameworks, and best practices that mitigate vulnerabilities in such devices; (3) a specification of high-priority gaps for which new or revised standards are needed; and (4) potential action plans by which such gaps can be addressed.

Risk Management

Security is Risk Management

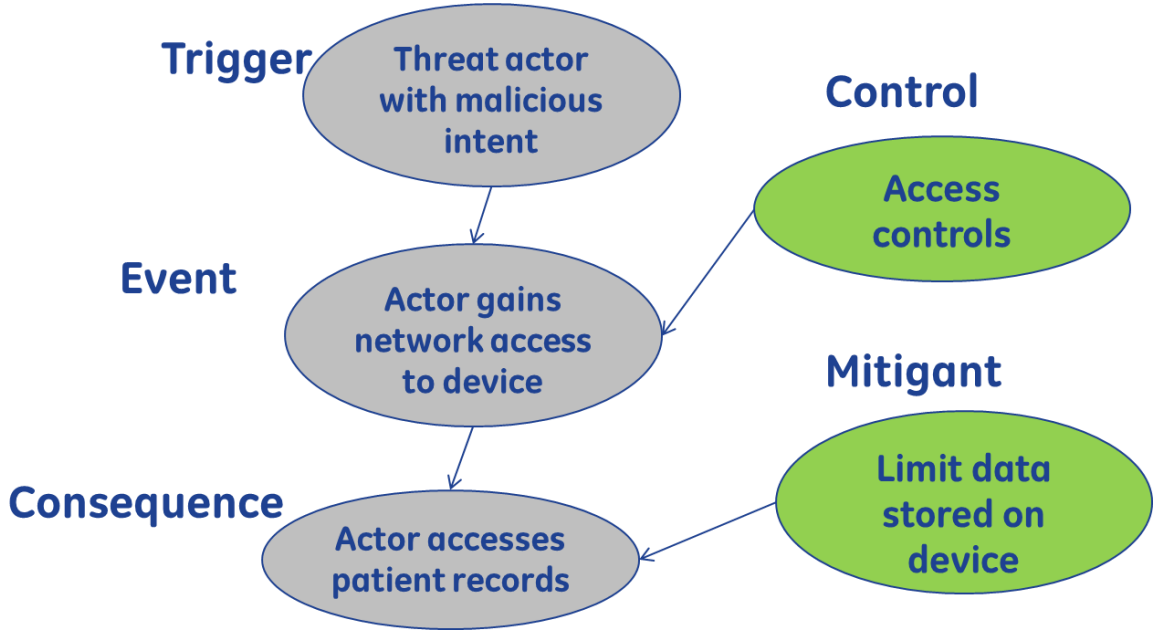
Protecting against risks to Confidentiality, Availability, and Integrity of Assets

Risk = f (assets, threats, vulnerabilities) – controls

Assets = data, device, what you want to protect
Threats = person/thing/action with intent to harm
Vulnerabilities = exploitable weaknesses in design
Controls = actions or mechanisms to protect assets

Security Controls
- Access Controls
- Authentication
- Audit Logs
- Media Protection
- Others

A simple network model for risk assessment:



A Further Look at the Risk Function

Risk = f (Likelihood, Impact)

Risk = f (assets, threats, vulnerabilities) – controls

Asset = data, device
Threats = malicious actions, malware
Vulnerabilities = exploitable weaknesses in design
Controls = security safeguards to block exploits (access controls, authentication, etc.)

Likelihood = f (threat actor motivation, capability, ease of exploit) - controls

Impact = f (threat actor motivation, asset value, type of harm) - mitigants

Motivation or Intent – what the threat actor seeking to gain:

- Cyber Criminals = $
- Nation States = political/economic/offensive advantage
- Hactivists = cause promotion
- Malicious Actor = desire to cause harm

9

Risk Factors: Static vs Temporal

How can risk assessment change over time?

Risk = f (asset x threats x vulnerabilities) – controls

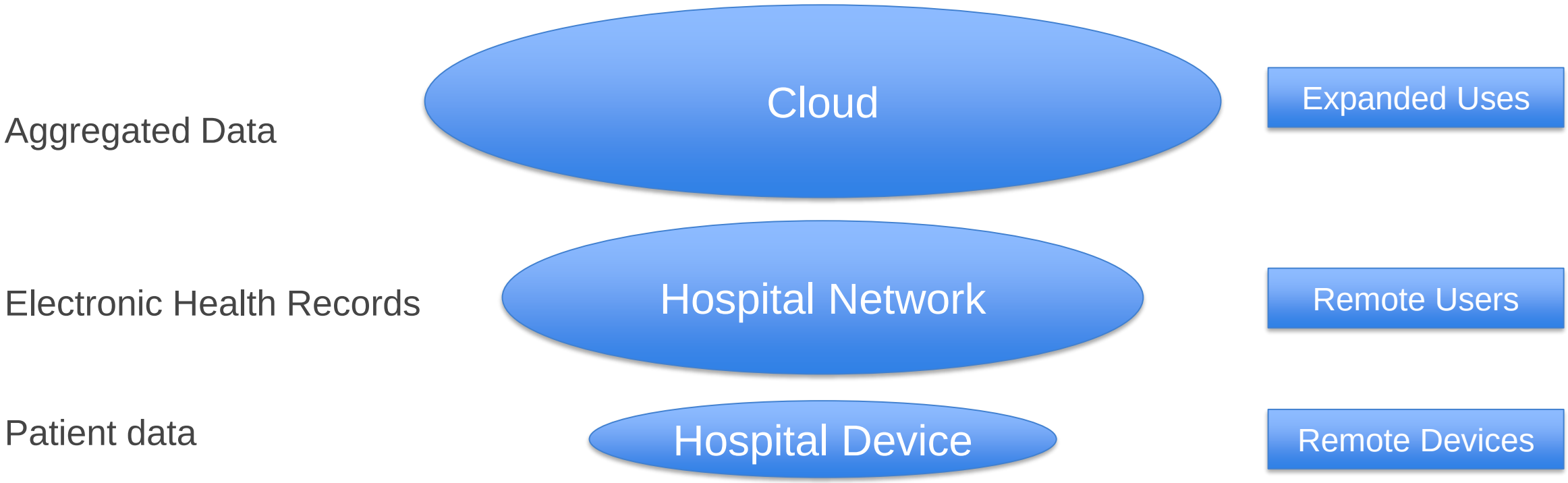
Asset = data, device
Threats = malicious actions, malware
Vulnerabilities = exploitable weaknesses in design
Controls = security safeguards to block exploits

Change in asset value?

More threat actors?

New discovered vulnerabilities?

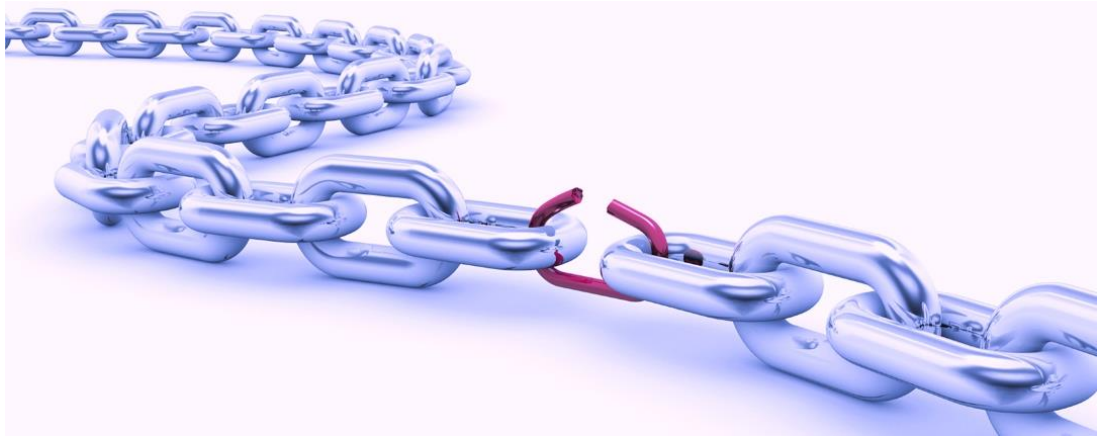
Assets at Risk – Connected Electronic Health Data



Increasing Asset Value, More Vulnerabilities…Attracts New Threats

Security Vulnerabilities

How many software security vulnerabilities were identified in 2017?



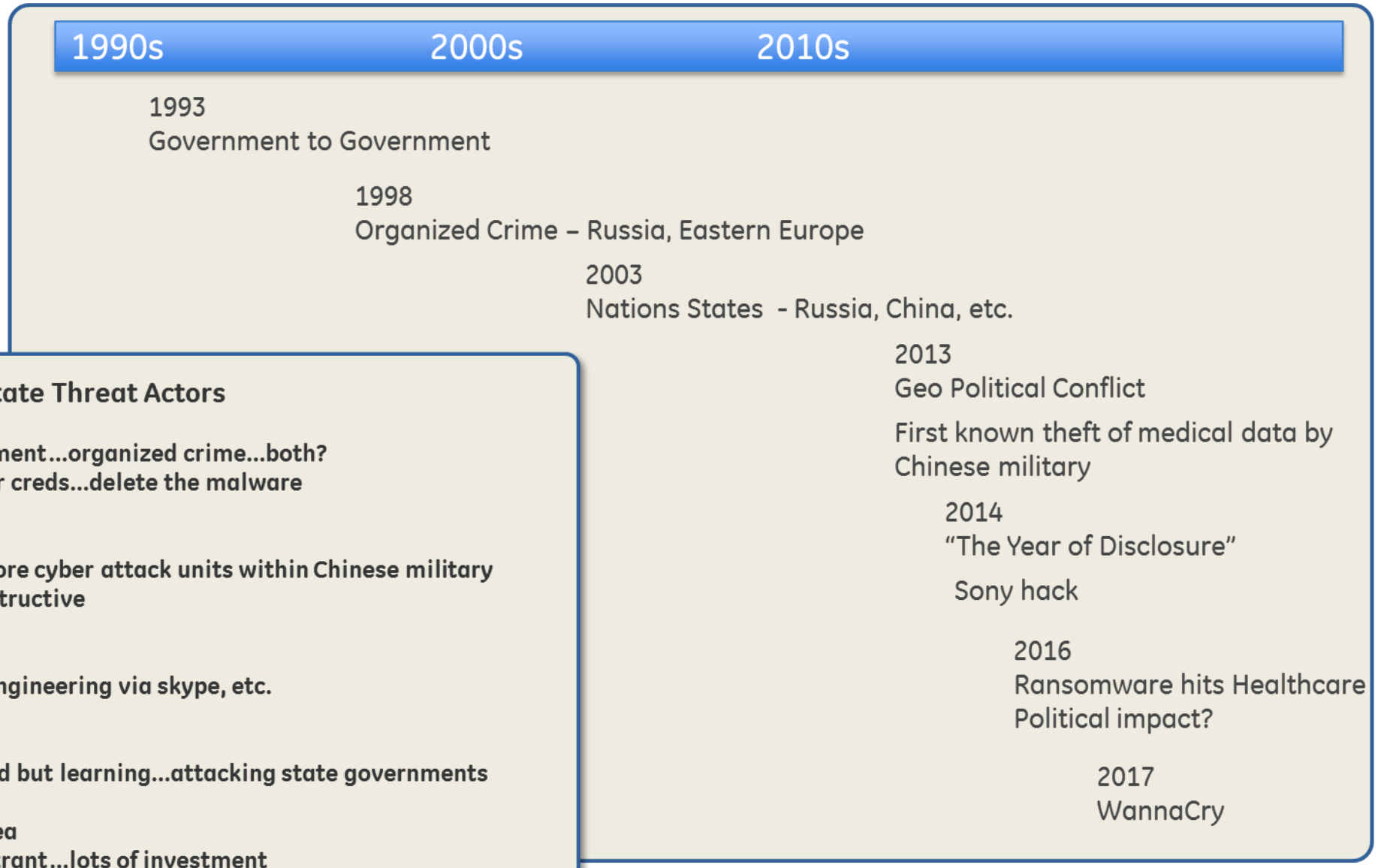
Security Vulnerabilities

How many software security vulnerabilities were identified in 2017?

Last year was another one for the record books when it came to software vulnerabilities: published security flaws jumped by 31% in 2017.

The number shot up to 20,832 for the year, with nearly 40% of them with CVSSv2 severity scores of 7.0 and higher, according to new data from Risk Based Security.

A Brief History of Cyber Threats



Nation State Threat Actors

Russia
- **Government…organized crime…both?**
- **Get your creds…delete the malware**

China
- **10 or more cyber attack units within Chinese military**
- **Non destructive**

Syria
- **Social engineering via skype, etc.**

Iran
- **Not good but learning…attacking state governments**

North Korea
- **Late entrant…lots of investment**
- **WannaCry, Sony hack attributed to North Korea**

Nation State Threats to Privacy?

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said Thursday.

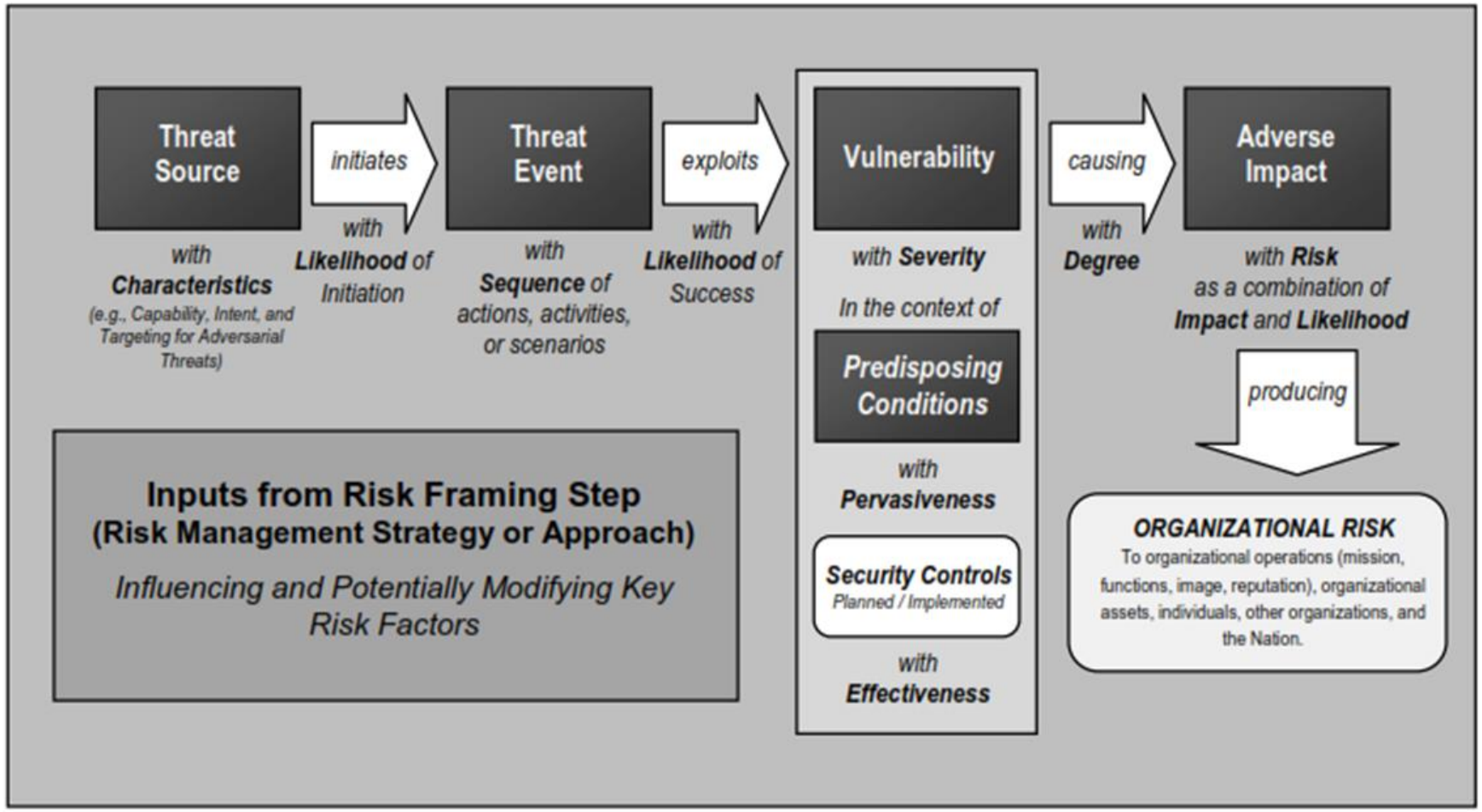
…cyber intrusions that U.S. officials have privately said were traced to the Chinese government.

But even beyond the rising number of apparent victims, U.S. officials said the breaches rank among the most potentially damaging cyber heists in U.S. government history because of the abundant detail in the files. Officials said hackers accessed not only personnel records of current and former employees but also extensive information about friends, relatives and others listed as references in applications for security clearances for some of the most sensitive jobs in government.

“It is a very big deal from a national security perspective and from a counterintelligence perspective,” FBI Director James B. Comey said at a meeting with reporters Thursday at the FBI headquarters. “It’s a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government.”

Other U.S. officials said that a foreign intelligence service could use the information to identify U.S. intelligence operatives, and that China is suspected of stealing large amounts of data on Americans as part of a “strategic plan” to increase its intelligence collection.

Risk Model (from NIST 800-30)



Impact Assessment (from NIST 800-30)

Harm to Operations
- Inability to perform current / future missions / business functions.
- Direct financial costs.
- Damage to trust relationships / reputation

Harm to Assets
- Damage / loss of: physical facilities / information systems / equipment / parts or supplies / information assets / intellectual property

Harm to Individuals
- Injury or loss of life.
- Physical or psychological mistreatment.
- Identity theft.
- Loss of Personally Identifiable Information
- Damage to image or reputation

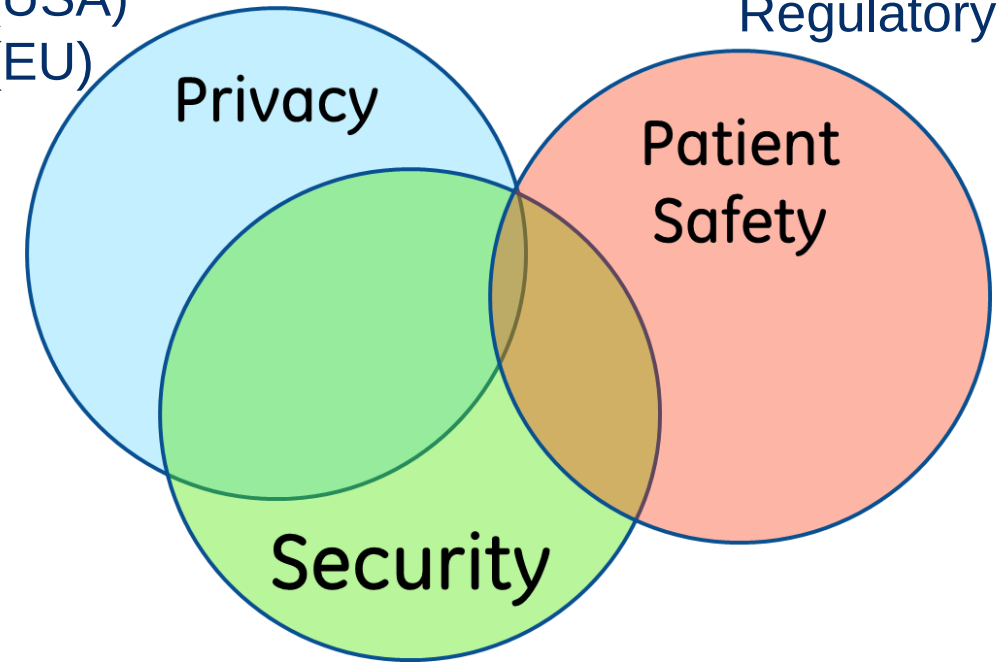
Harm to Other Organizations
- Financial / Regulatory / contractual / trust relationships / reputation

Harm to the Nation
- Damage to or incapacitation of a critical infrastructure sector

Healthcare Security Risk Domains

HIPAA (USA)
GDPR (EU)
+ global

Patient Care Mission
Regulatory compliance



Ability to Provide
Patient Care

Failure to Manage Risks:

- Patient Impact
- Business Ops Impact
- Fines
- Lawsuits
- Reputation

Preventing Shark Attacks?

All About Them

Grow Your Business by Focusing on Others

Bruce Turkel

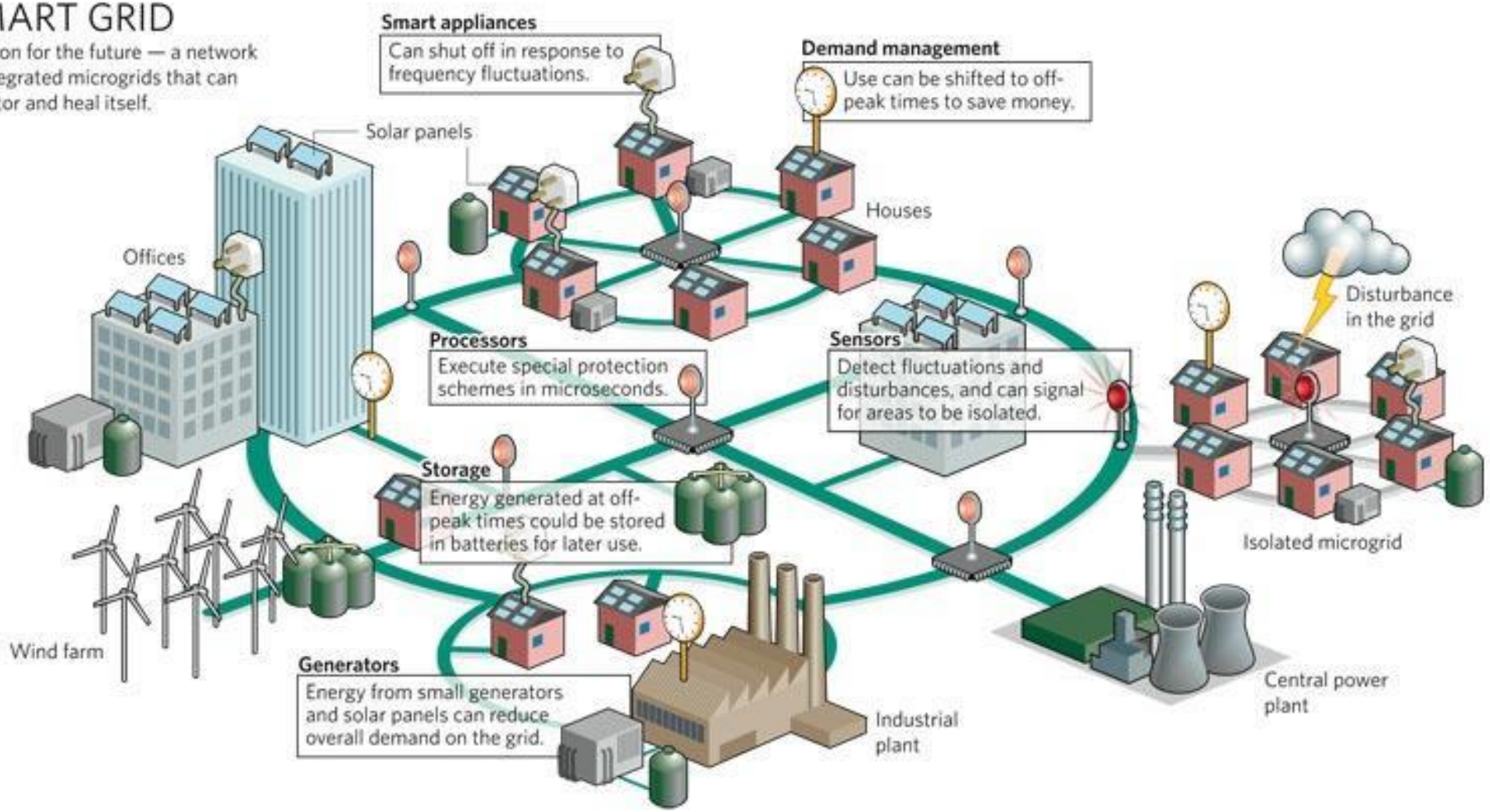
Shark Attack

Some brands use too much jargon or rely on fear. The Australian company Shark Attack Mitigation Systems (SAMS) makes wetsuits, including some that are designed to protect surfers and divers from shark attacks. The firm hired scientists to help it design camouflage in patterns likely to repel sharks. But in reality, shark attacks are rare – resulting in only four or five deaths worldwide each year. But, “SAMS is not investing all its money out of a desire to keep people safe from shark attacks; they’re hoping to profit from people’s fear of being killed in one.”

Principle of Resilience
(the capacity to react and recover quickly)

SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.



Resiliency – from Military Aircraft to the Smart Grid

The Six Security Properties

Property	Description
Confidentiality	Data is available and used only by those who need it for its intended purpose
Integrity	Assets (data and system resources) are changed only within defined use cases by authorized people
Availability	Assets are ready for use when needed
Authentication	User identity is established (you may choose to accept anonymous users)
Authorization	Users access levels and privileges are explicitly defined
Nonrepudiation	Specific users and their actions are documented

What is the threat type associated with each of these properties?

Threat Matrix – STRIDE Model

Security Property	Authentication	Integrity	Non-Repudiation	Confidentiality	Availability	Authorization
Design Elements:	*Spoofing*	*Tampering*	*Repudiation*	*Information Disclosure*	*Denial of Service*	*Elevation of Privilege*
Data Flows		X		X	X	
Data Stores		X		X	X	
Processes	X	X	X	X	X	X
Interactors	X		X			

The Eight Security Failure Modes

1. Execution of unauthorized code
2. Gain privilege / assume ID
3. Data disclosure
4. Unreliable execution
5. Resource consumption
6. Bypass protection mechanism(s)
7. Hide activities
8. Other

Which is most common on medical devices?

Applying Resilience to Healthcare Cyber Security

- Apply threat-based design practices
- Robust designs - Expect “unintended uses”
- Integrate controls to reduce likelihood of adverse events
- Design to mitigate the impact of adverse events

Principle of Respect

(have due regard for rights, avoid harming or interfering)

25 March 2018

What are the allegations against Cambridge Analytica?
The data analytics firm used personal information harvested from more than 50 million Facebook profiles without permission to build a system that could target US voters with personalised political advertisements based on their psychological profile, according to Christopher Wylie, a former Cambridge Analytica contractor who helped build the algorithm.

How is Facebook involved in the scandal?
The social media company has received a number of warnings about its data security policies in recent years and had known about the Cambridge Analytica data breach since 2015, but only suspended the firm and the Cambridge university researcher who harvested user data from Facebook earlier this month. A former Facebook manager has warned that hundreds of millions of users are likely to have had their private information used by private companies in the same way.

19 March 2018

…a professor at Cambridge University built a Facebook app around 2014 that involved a personality quiz. About 270,000 users of the app agreed to share some of their Facebook information, as well as data from people on their friends list. As a result, tens of millions ended up part of this data-mining operation…Consulting firm Cambridge Analytica, which paid for the research, later worked with the Trump campaign to help them target advertising campaigns on Facebook, using the data they'd gathered on users

In 2012, the Obama campaign encouraged supporters to download an Obama 2012 Facebook app that, when activated, let the campaign collect Facebook data both on users and their friends…when you installed the app, "it said it would grab information about my friends: their birth dates, locations, and 'likes.' "

The campaign boasted that more than a million people downloaded the app, which, given an average friend-list size of 190, means that as many as 190 million had at least some of their Facebook data vacuumed up by the Obama campaign — without their knowledge or consent. This Facebook treasure trove gave Obama an unprecedented ability to reach out to nonsupporters. More important, the campaign could deliver carefully targeted campaign messages disguised as messages from friends to millions of Facebook users…The campaign readily admitted that this subtle deception was key to their Facebook strategy. "People don't trust campaigns. They don't even trust media organizations," Teddy Goff, the Obama campaign's digital director, said at the time. "Who do they trust? Their friends.“ …Obama…was collecting live data on active users right up until Election Day…

More important, the vast majority of people involved in these data-mining operations had no idea they were participating. And in the case of Obama, they had no way of knowing that the Obama campaign material cluttering their feed wasn't really just political urgings from their friends.

Applying Respect to Healthcare Cyber Security

Transparency: Personal data shall be collected and/or used only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Individual Control: The data subject must give explicit consent to the processing of personal health data for specified purposes

Data Minimization: Personal data collection shall be limited to what is necessary in relation to the purposes for which they are processed

Accuracy: Personal data shall be accurate and corrected if inaccurate

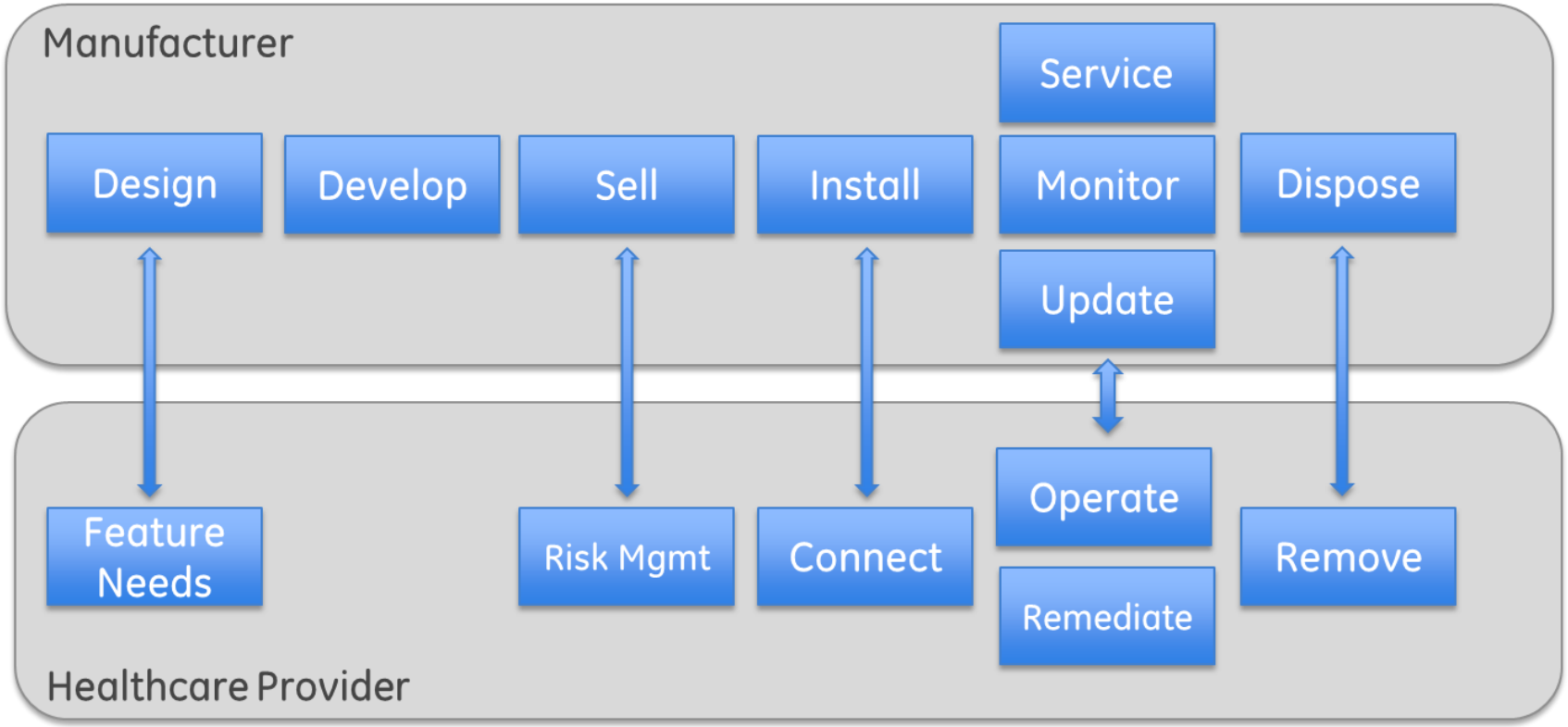
Timeliness: Personal data shall be kept for no longer than is necessary for the purposes for which the personal data are processed

Security: Personal data shall be processed in a manner that ensures appropriate protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Collaboration
(working with others to achieve a desired result)

The Flip Flop Man

Applying Collaboration to Healthcare Cyber Security



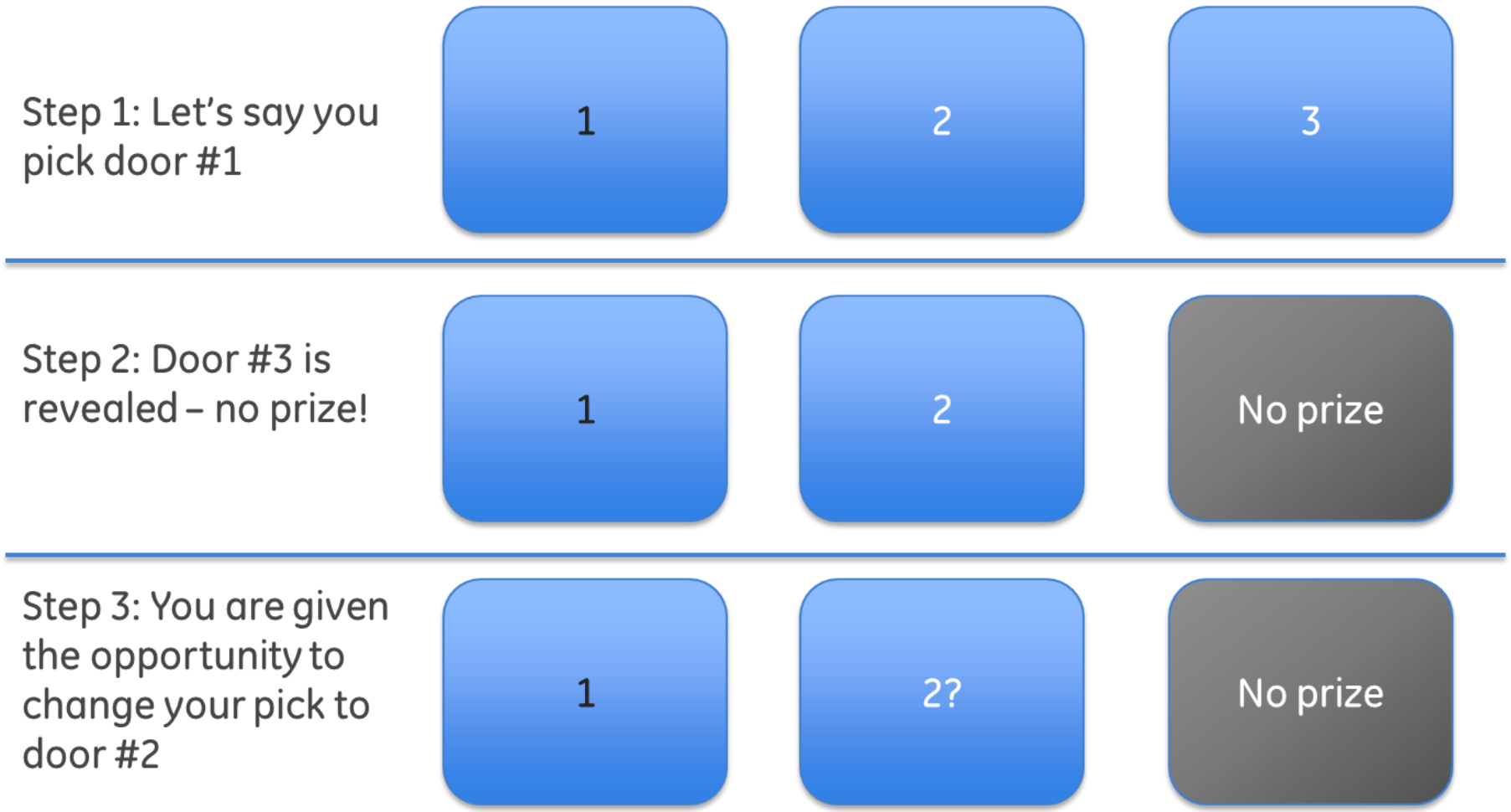
Systems Thinking

Security Incident Root Cause Analysis

Let’s Make a Deal – an Exercise in Probability Theory

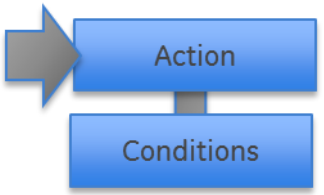
Which door hides the grand prize?

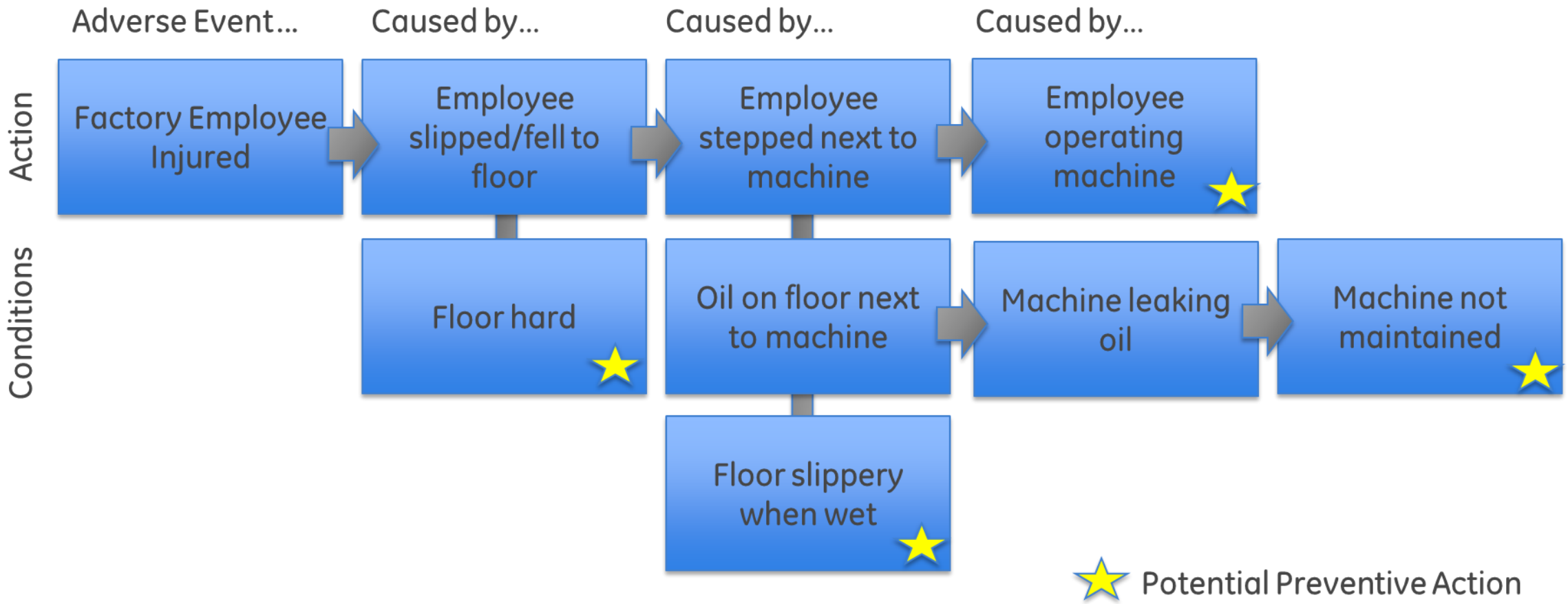
Now Let's Deal



What decision gives you the best chance to win?

Root Cause Analysis - Example





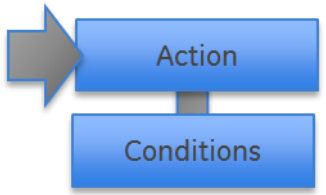
Note: Consider Action and Conditions - easier to fix conditions than to control actions!

Scenario

Hospital Operations are Shut Down Due to a Ransomware Attack

- All file on devices and in network storage are encrypted
- Malicious Threat Actors demand payment for key
- Hospital is forced to cease patient care operations until resolution

Root Cause Analysis – Actions and Conditions



Adverse Event…

Caused by…

Caused by…

Caused by…

Hospital Cannot Provide Patient Care

Files on devices encrypted

Hospital does not have encryption key

Devices rely on "electronic" files

Malware within hospital network

Flat network IT + OT

Devices connected to network

Vulnerability in device OS

1

Hospital employee downloaded malware

Device "use cases" involve network connectivity

Employee opened email attachment

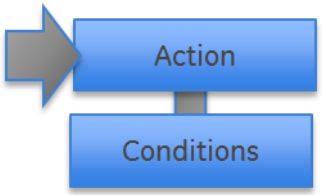
Attachment had malware

2

Attached files not screened prior to opening

Potential Preventive Action

1 Vulnerability in Devices



Adverse Event…

Caused by…

Caused by…

Vulnerability in devices

OS design defect ★

Defect (vulnerability) not patched

Patch not available (some devices)

OS not supported (EOL)

Device useful life > s/w support life ★

or

Patch not approved by manufacturer

Ineffective patch support from manufacturer ★

or

Available and approved patches not applied

Ineffective patch management by HDO ★

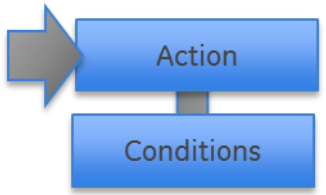
or

Vulnerabilities and patches not monitored

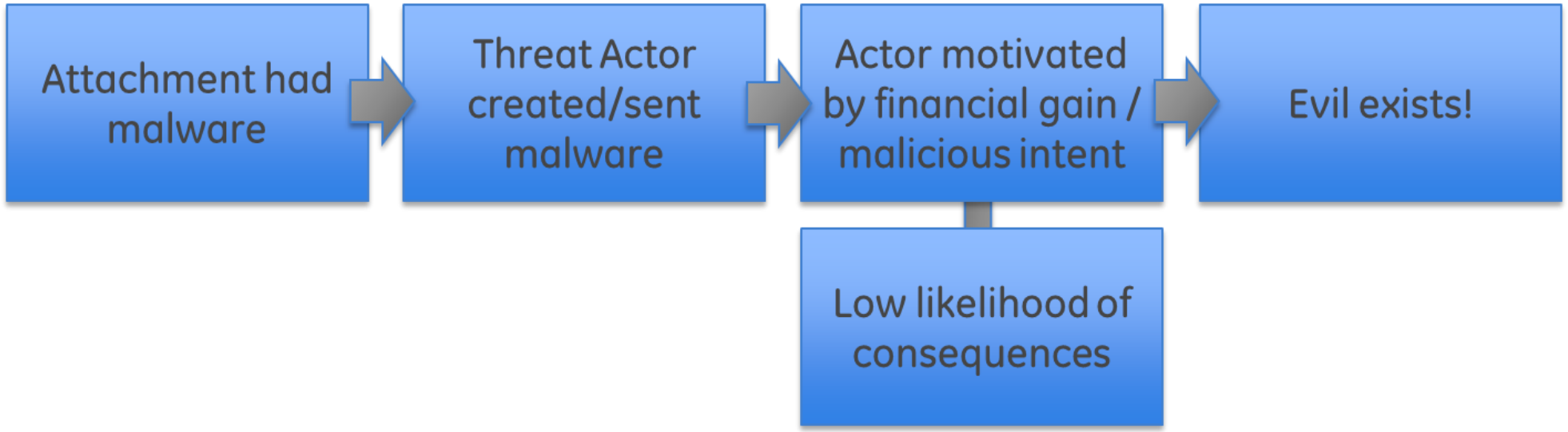
Ineffective:
- Process
- Documentation
- Communication
- Asset Management
- Resource Allocation
- Etc.

★ Potential Preventive Action

2 Attachment had Malware



Adverse Event… Caused by… Caused by…



Potential Preventive Action ?

05 April 2018

…a majority of security professionals in the healthcare and pharmaceutical industries admit that they have had a data breach because of an unpatched vulnerability for which a patch was available.

This was one startling finding of a survey of nearly 3,000 security professionals across industries and countries by the Ponemon Institute on behalf of ServiceNow.

A full 77 percent of respondents said that their organizations do not have enough staff to patch vulnerabilities in a timely manner, while 60 percent said they would hire more staff to help with patching in the next 12 months.

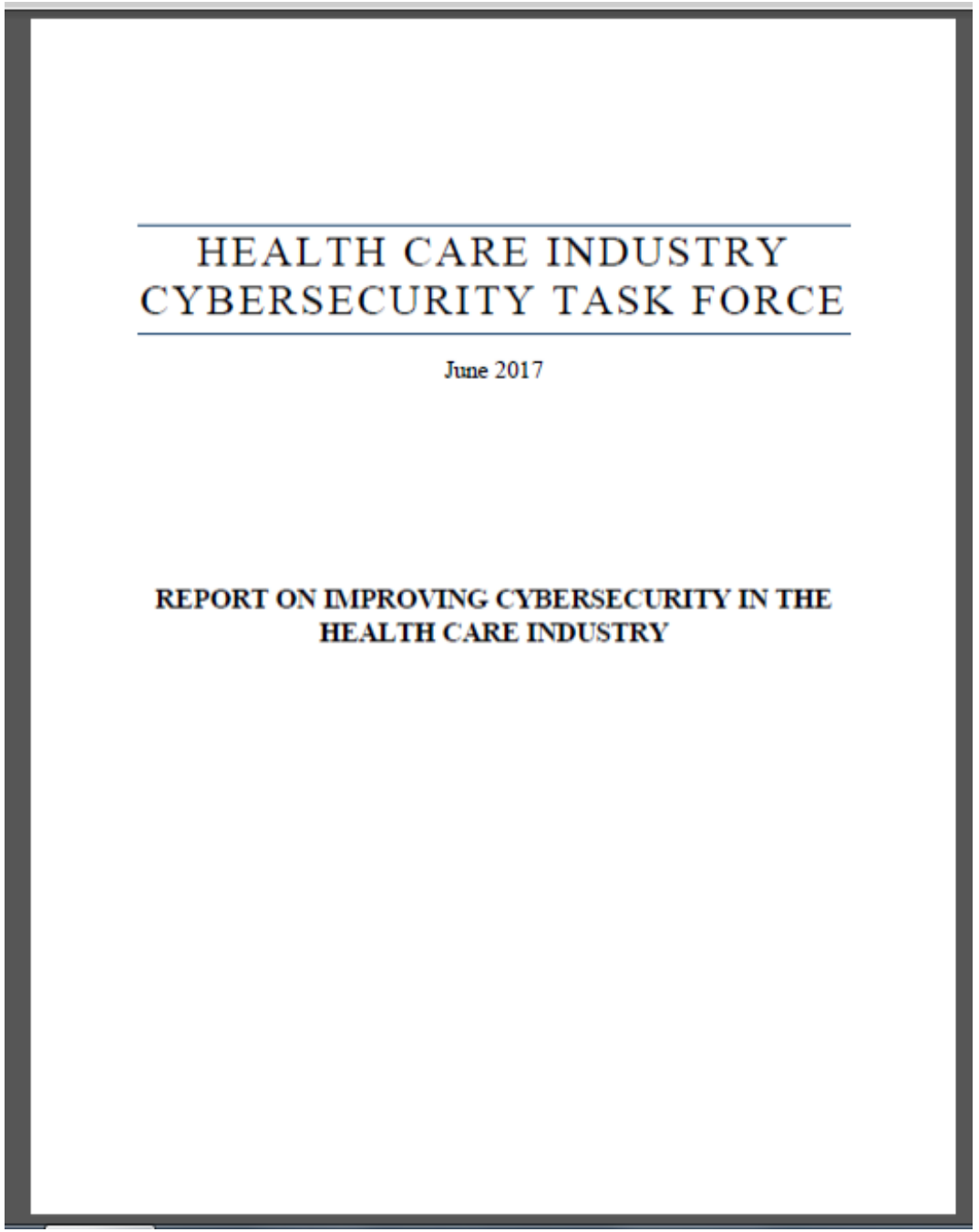
However, adding cybersecurity staff may not always be possible…According to nonprofit IT advocacy group ISACA, the global shortage of cybersecurity professionals will reach 2 million by 2019.

Building System Maturity - Indicators

	Engaged	Proactive	Systemic	Industry Leader
Business Leadership	you know the business has a problem	the business knows it has a problem	the business solves the problem	solution is a model for industry
Resources	you know whom to invite to your meeting	people participate as volunteers	dedicated resources & resource planning	recognized Industry experts
Products	compliance controlled via stop ship orders	compliance controlled via design changes	compliance controlled within product planning	first to market with compliant products
Motivation	compliance viewed as a cost	compliance viewed as a need	compliance viewed as an advantage	compliance used as a selling point
Expertise	have a gap	have an SME	building DNA	organizational knowledge
Communications	op mechs once per quarter	op mechs once per week	what's an op mech?	publish
Program	meetings	changes	processes	invitations
Documentation	eMail	PowerPoint	released documentation	industry guidance
Customers	indifferent	asking	expecting	bragging

Building a System

June 2017



HEALTH CARE INDUSTRY
CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

From “Health Care Industry Cyber Security Task Force” (June 2017)

The imperatives are:

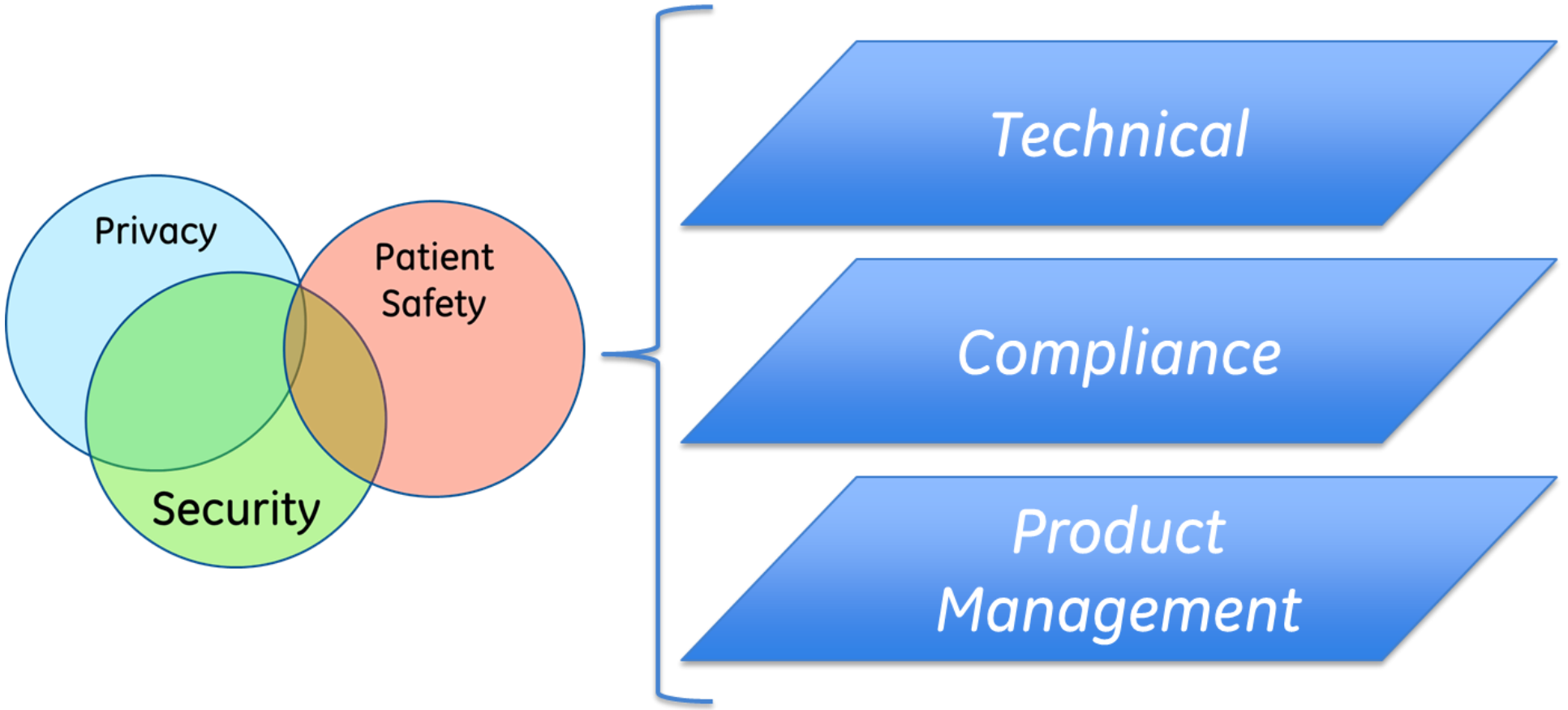
1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, weaknesses, and mitigations.

From “Health Care Industry Cyber Security Task Force” (June 2017)

In health care, security and cyber risk has historically fallen to IT. Information governance is a relatively new concept in the industry and should include not just IT and security stakeholders, but also information stakeholders. Governance structures should also include clinical and non-clinical leaders. Governance of information shifts the focus from technology to people, processes, and the policies that generate, use, and manage the data and information required for care.

Medical Device Cyber Security

Layered Execution across the Multiple Risk Domains



In the case of cybersecurity, some decision makers use the wrong mental models to help them determine how much investment is necessary and where to invest. For example, they may think about cyber defense as a fortification process — if you build strong firewalls, with well-manned turrets, you'll be able to see the attacker from a mile away. Or they may assume that complying with a security framework like NIST or FISMA is sufficient security —just check all the boxes and you can keep pesky attackers at bay. They may also fail to consider the counterfactual thinking — We didn't have a breach this year, so we don't need to ramp up investment — when in reality they probably either got lucky this year or are unaware that a bad actor is lurking in their system, waiting to strike.

The problem with these mental models is that they treat cybersecurity as a finite problem that can be solved, rather than as the ongoing process that it is. No matter how fortified a firm may be, hackers, much like water, will find the cracks in the wall. That's why cybersecurity efforts have to focus on risk management, not risk mitigation.

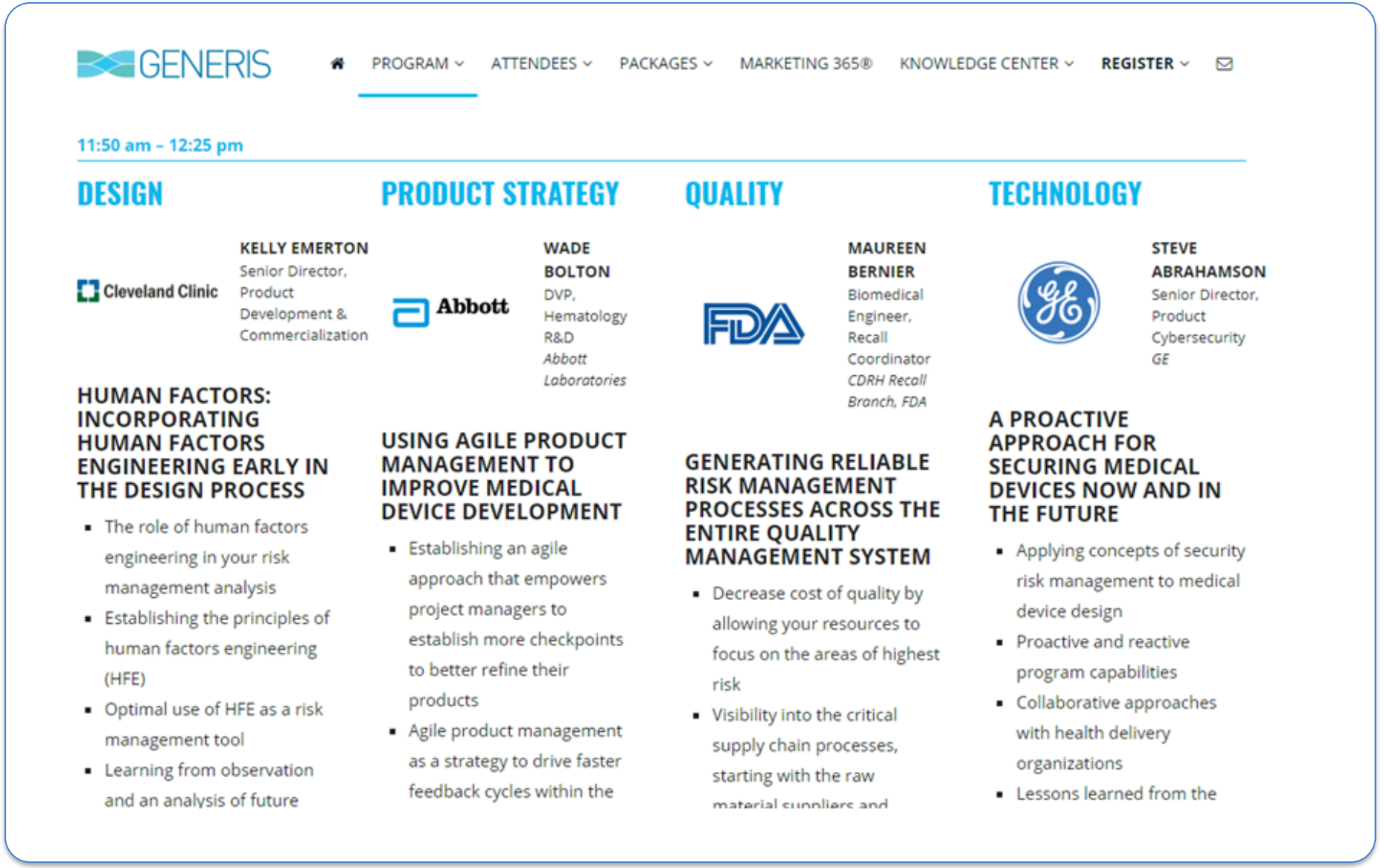
…security professionals should explain cyber risk by using clear narratives that connect to risk areas that high-level decision makers are familiar with and already care deeply about. For example, your company's risk areas may include customer data loss as well as the regulatory costs and PR fallout that can affect the company's reputation. It's not just about data corruption — it's also about how the bad data will reduce operational efficiency and bring production lines to a standstill.

Some CEOs may think that security investments are for building an infrastructure, that creating a fortified castle is all that's needed to keep a company safe. With this mental picture, the goals of a financial decision maker will always be oriented toward risk mitigation instead of risk management.

Creating an Executable System

- Principles & Policies
- Procedures & Practices
- Implementation Programs
  - Communication
  - Training
  - Operating Mechanisms
  - Metrics
- Assessment
- Continual Improvement

Medical Device Security – Where Does it Fit?



GENERIS

PROGRAM ATTENDEES PACKAGES MARKETING 365® KNOWLEDGE CENTER REGISTER

11:50 am – 12:25 pm

DESIGN

Cleveland Clinic

KELLY EMERTON
Senior Director, Product Development & Commercialization

HUMAN FACTORS: INCORPORATING HUMAN FACTORS ENGINEERING EARLY IN THE DESIGN PROCESS

- The role of human factors engineering in your risk management analysis
- Establishing the principles of human factors engineering (HFE)
- Optimal use of HFE as a risk management tool
- Learning from observation and an analysis of future

PRODUCT STRATEGY

Abbott

WADE BOLTON
DVP, Hematology R&D
Abbott Laboratories

USING AGILE PRODUCT MANAGEMENT TO IMPROVE MEDICAL DEVICE DEVELOPMENT

- Establishing an agile approach that empowers project managers to establish more checkpoints to better refine their products
- Agile product management as a strategy to drive faster feedback cycles within the

QUALITY

FDA

MAUREEN BERNIER
Biomedical Engineer, Recall Coordinator
CDRH Recall Branch, FDA

GENERATING RELIABLE RISK MANAGEMENT PROCESSES ACROSS THE ENTIRE QUALITY MANAGEMENT SYSTEM

- Decrease cost of quality by allowing your resources to focus on the areas of highest risk
- Visibility into the critical supply chain processes, starting with the raw material suppliers and

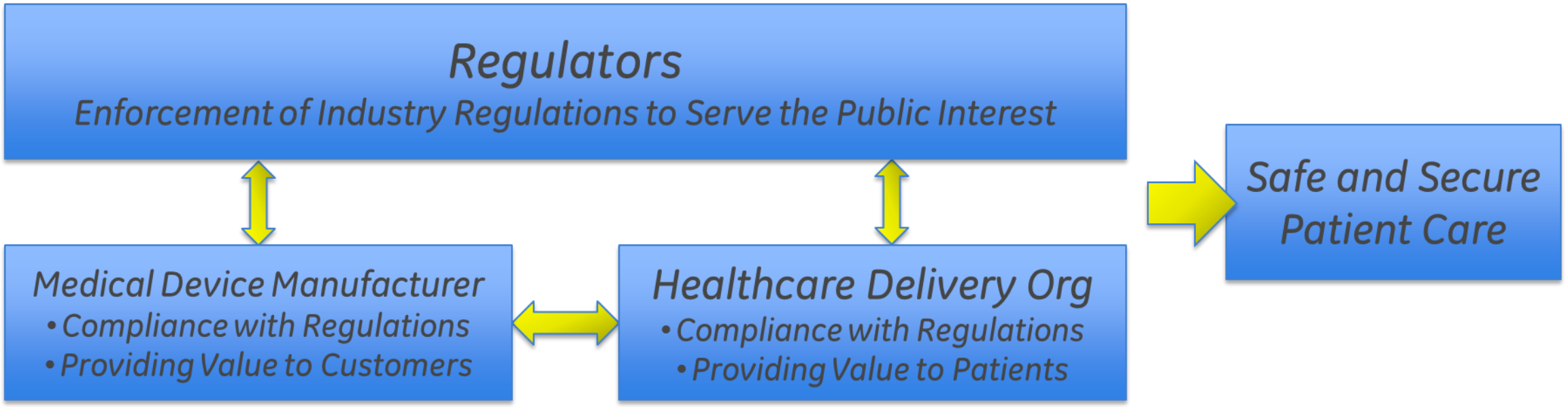
TECHNOLOGY

STEVE ABRAHAMSON
Senior Director, Product Cybersecurity
GE

A PROACTIVE APPROACH FOR SECURING MEDICAL DEVICES NOW AND IN THE FUTURE

- Applying concepts of security risk management to medical device design
- Proactive and reactive program capabilities
- Collaborative approaches with health delivery organizations
- Lessons learned from the

Building in Collaboration



INCOSE Healthcare Working Group

4th Annual Systems Engineering in Healthcare Conference

Imagination at work.

Discussion:
Building a System for Cyber Security in Healthcare

19 April 2018

Steve Abrahamson
Sr. Director, Product Cyber Security
GE Healthcare

Abstract

Healthcare cybersecurity is finally being recognized as critical to our ability to improve the quality of healthcare and access to healthcare. In May 2017 the initiation of the cyberattack known as "WannaCry" was a wake-up call to those who had been ignoring the problem. But what have we learned? What are the real risks? How can we best address this problem? Finding solutions to this challenge will involve systems thinking. While engineers are uniquely qualified to find solutions, this is not an engineering problem. A system involving different types of risks, the pervasive weak link of human interactions, threat actors ranging from trusted insiders to nation states, multiple regulators, and stakeholders with differing priorities, all contribute to the complexity of the system. Developing a system to manage security risks that includes secure device design, secure engineering and development, secure deployment, and life cycle support, all while working collaboratively across technology developers, manufacturers, and healthcare delivery organizations, poses a unique challenge and opportunity.