CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

Live Web Event

A Patient Safety - Cyber Risk Discussion with Benoit Desjardins, M.D., Ph.D., FAHA, FACR, CISSP, C|EH

October 8, 2020

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Webinar Logistics

1. Slide materials – Link In Chat Box
2. All attendees are in “Listen Only Mode”
3. Please ask content related questions in “Q&A”
4. In case of technical issues, use / check “Chat”
5. Please participate in all polls
6. Please complete Exit Survey when you leave our session
7. Recorded version, final slides, and Certificate of Attendance will be shared with you within 24 hours

Introduction to Clearwater

- Leading provider of cyber risk management and HIPAA compliance software and solutions for healthcare
- 100% success rate when deliverables submitted to the Office for Civil Rights (OCR)
- Approximately 400 customers, including 68 IDNs, many with multi-year Enterprise Cyber Risk Management (ECRM) programs
- Founded in Nashville in 2009, colleagues in 20+ states, growing rapidly
- Portfolio company of Altaris Capital Partners, a healthcare PE firm with $4.8B under management

BLACK BOOK 2017 BLACK BOOK 2018 BLACK BOOK 2019 BEST IN KLAS CYBERSECURITY ADVISORY SERVICES 2018

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Your Presenters:

Bob Chaput, MA, CISSP, HCISPP, CRISC, C|EH, CIPP/US, NACD CERT Cyber Risk Oversight

Executive Chairman & Founder, Clearwater

- Executive | Educator | Entrepreneur
- Leading authority on healthcare compliance, cybersecurity, and enterprise cyber risk management
- 40+ years in Business, Operations, Technology & Cyber Risk Management
- 25+ years in Healthcare
- Contributing author to Wolters Kluwer’s *Health Law and Compliance Update* and the American Society of Healthcare Risk Management (ASHRM)’s *Health Care Risk Management Fundamentals*
- Global Healthcare Executive: GE, JNJ, HWAY
- Responsible for some of largest, most sensitive healthcare datasets in world
- Industry Expertise and Focus: Healthcare Covered Entities and Business Associates
- Member: NACD, IAPP, ISC^2, CHIME/AEHIS, HIMSS, ISSA, IAPP, ISACA, HCCA

Your Presenters:

Benoit Desjardins, MD, Ph.D., FAHA, FACR, CISSP, C|EH

Associate Professor of Radiology at the Hospital of the University of Pennsylvania

- 20+ years in Diagnostic Radiology
- Associate Professor of Radiology and Medicine, University of Pennsylvania
- Funded by National Institute of Health
- Ph.D. in Theoretical Artificial Intelligence
- Expertise in Cardiovascular Imaging, Artificial Intelligence and Cybersecurity
- Consultant for FBI in matters of cybersecurity
- Member (Medical): ACR, RSNA, NASCI, ISMRM, SCMR, AHA, HRS, AHA
- Member (Cyber): ISC2, HIMSS, HSCC, SIIM
- Black Belt (Tae Kwon Do), Wood Badge (BSA), Competitive Marksman

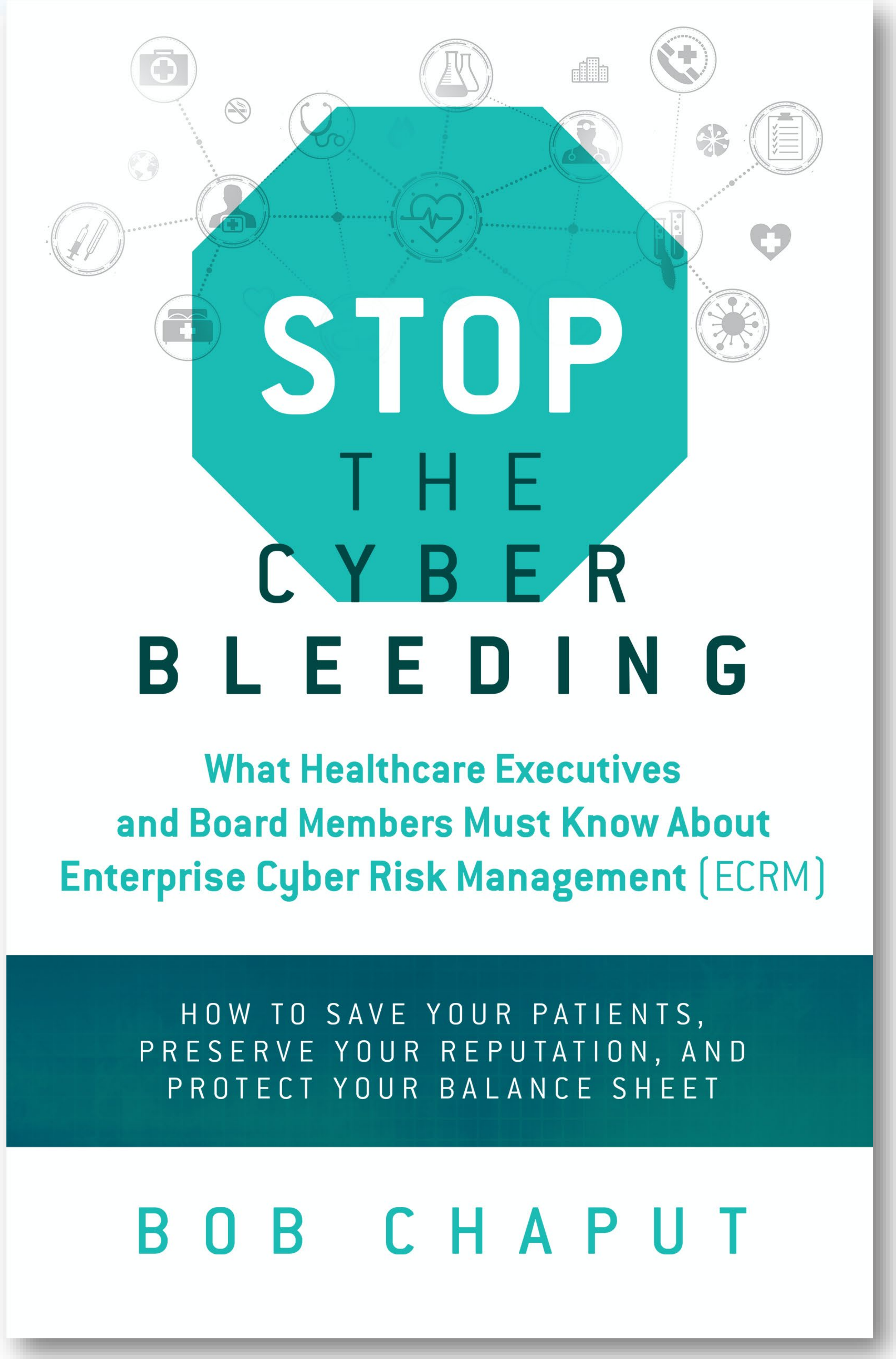
Pause and Poll

1. What type of organization do you represent?

- ❑ Hospital / Health System / IDN
- ❑ Other Covered Entity
- ❑ Business Associate
- ❑ Hybrid
- ❑ Don’t Know

Discussion Flow

- Introduction
- A View from the Front Lines
- Patient Safety / Cyber Risk Discussion
- Q&A



STOP THE CYBER BLEEDING

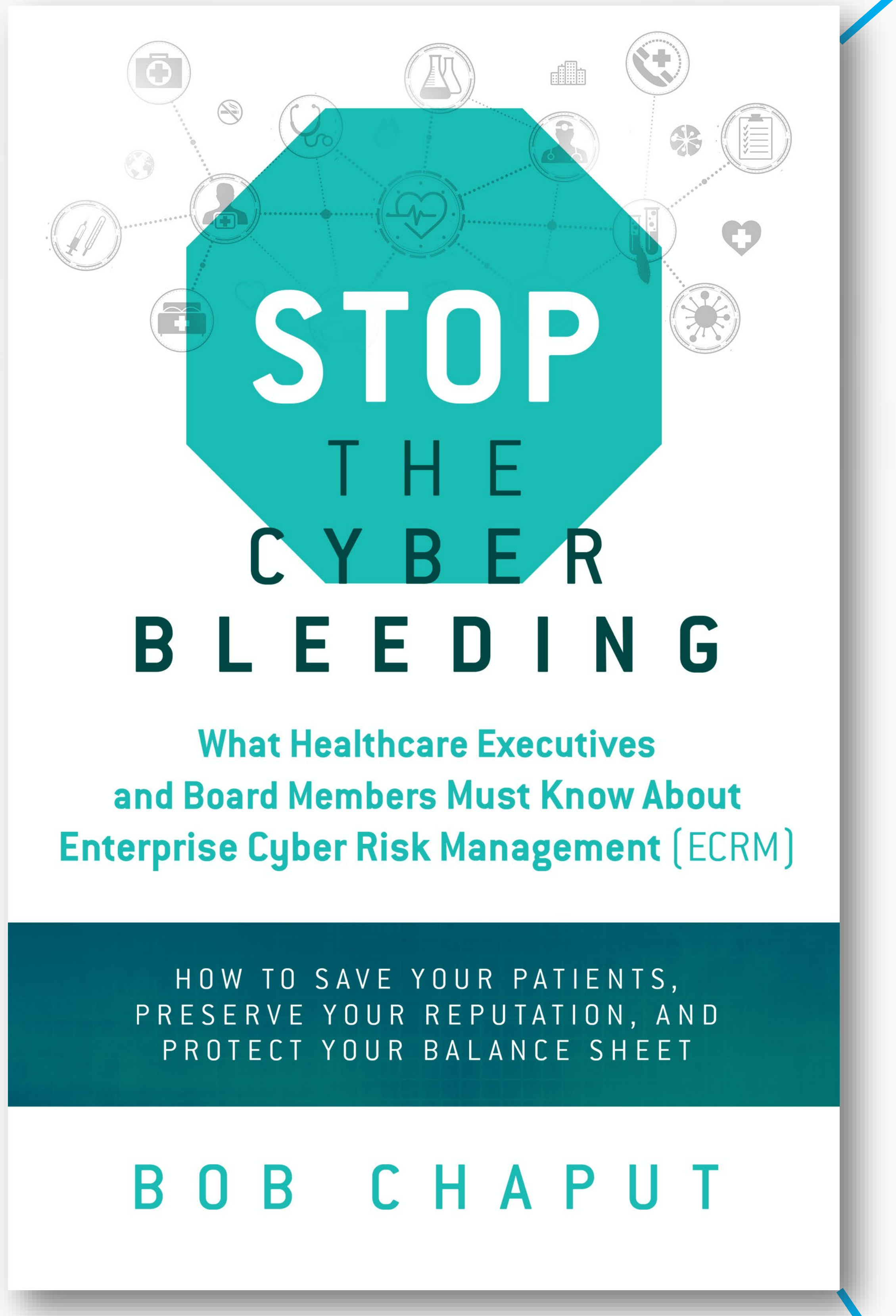
What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)

HOW TO SAVE YOUR PATIENTS, PRESERVE YOUR REPUTATION, AND PROTECT YOUR BALANCE SHEET

BOB CHAPUT

https://www.clearwatercompliance.com/stopthecyberbleeding

When Something “Cyber” Happens

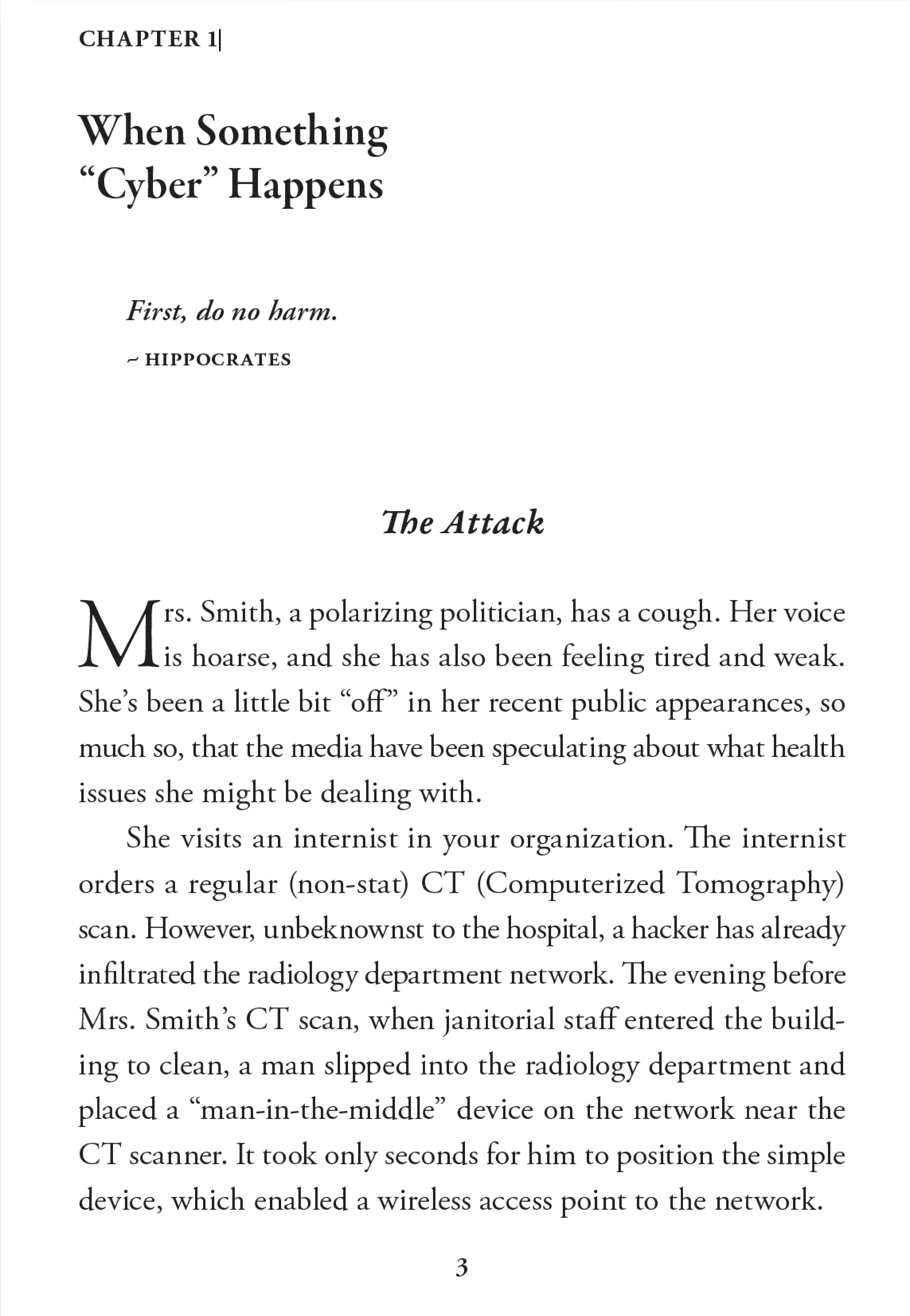


STOP THE CYBER BLEEDING

What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)

HOW TO SAVE YOUR PATIENTS, PRESERVE YOUR REPUTATION, AND PROTECT YOUR BALANCE SHEET

BOB CHAPUT



CHAPTER 1|

When Something “Cyber” Happens

First, do no harm.

~ HIPPOCRATES

The Attack

Mrs. Smith, a polarizing politician, has a cough. Her voice is hoarse, and she has also been feeling tired and weak. She’s been a little bit “off” in her recent public appearances, so much so, that the media have been speculating about what health issues she might be dealing with.

She visits an internist in your organization. The internist orders a regular (non-stat) CT (Computerized Tomography) scan. However, unbeknownst to the hospital, a hacker has already infiltrated the radiology department network. The evening before Mrs. Smith’s CT scan, when janitorial staff entered the building to clean, a man slipped into the radiology department and placed a “man-in-the-middle” device on the network near the CT scanner. It took only seconds for him to position the simple device, which enabled a wireless access point to the network.

3

Evolving Focus is Required

c. 2010

Compliance

c. 2015

Security & ECRM

c. 2018

Patient Safety

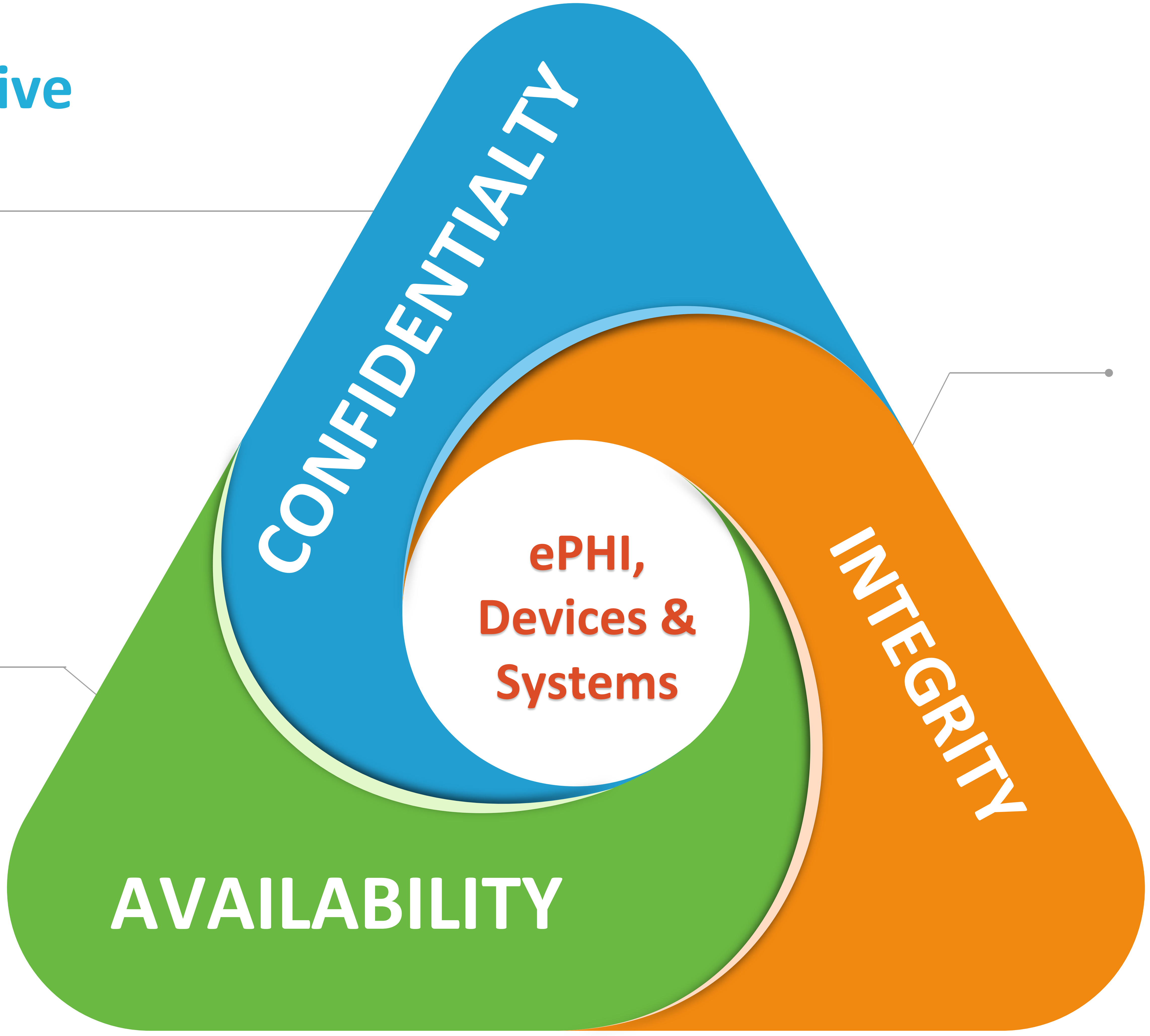
c. 2021

Medical Professional Liability

Our Core Responsibility

What if my Sensitive Information is shared?

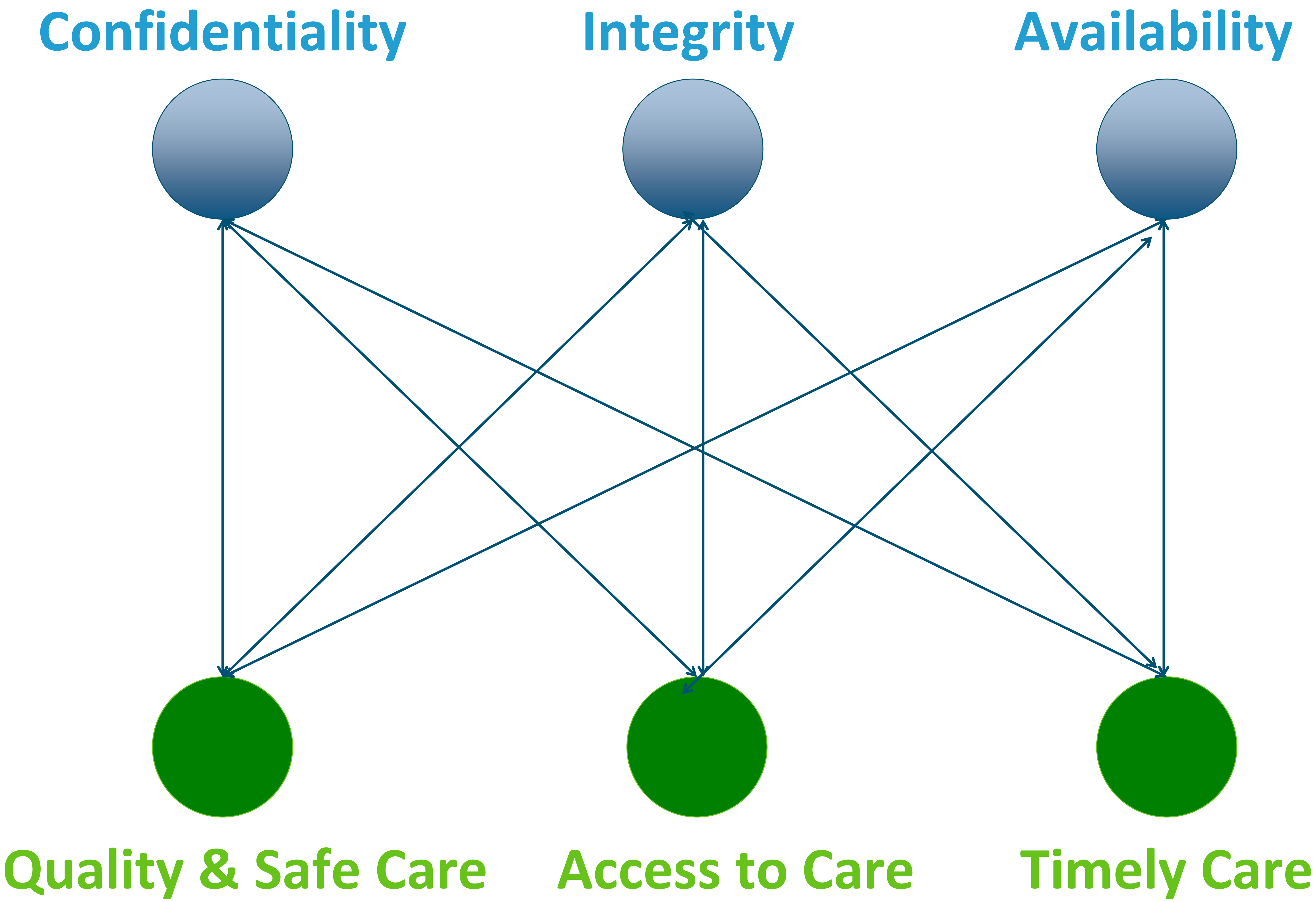
What if my Sensitive Information is not there when it is needed?



What if my Sensitive Information is not complete, up-to-date and accurate?

Don’t Compromise C-I-A!

Connect the Dots!



Patient Information & Patient Safety & MPL

Pause and Poll

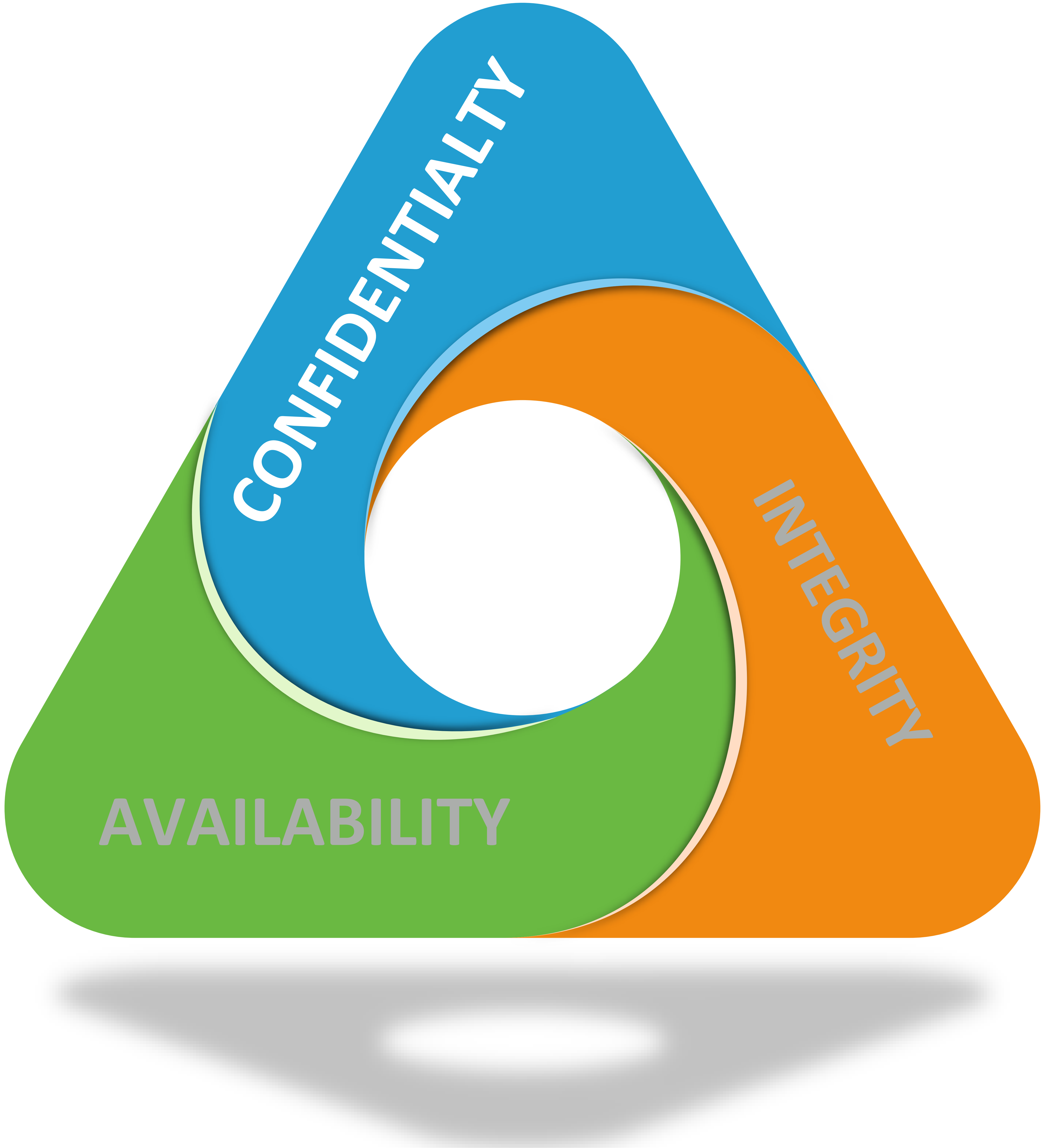
2. **What is the likelihood of a cyber event triggering a patient safety issue in your organization in the next 12 months?**

□ Greater than 20%
□ Greater than 40%
□ Greater than 60%
□ Greater than 80%
□ 100%

A View from the Front Lines

No one is going to die because of a confidentiality breach, they could however easily die as the result of an integrity or an availability cyber-attack.

Richard Staynings
Chief Security Strategist
Cylera
Sept 18, 2019


CONFIDENTIALTY
INTEGRITY
AVAILABILITY

Confidentiality

- **Definition**
  - assurance that information has not been disclosed to unauthorized entities
- medical records and DICOM images contain PHI
  - HIPAA
  - fines
- most medical record **breaches**
  - breaches of confidentiality
  - can embarrass or financially hurt
  - will not physically harm or kill patients

pngfly.com

gettyimages.com

- **Anthem**: healthcare insurer
  - aka Wellpoint until Aug 2014
- Feb 2015: official email from Wellpoint HQ
  - link: `http://www.we11point.com`
- when clicked on link
  - downloaded keystrokes logging malware
  - recorded typed usernames and passwords
- **breach of 78 million medical records**

- **phishing** email from China!!
- fake: *we**11**point* (we11point)
- real: *we**ll**point* (wellpoint)

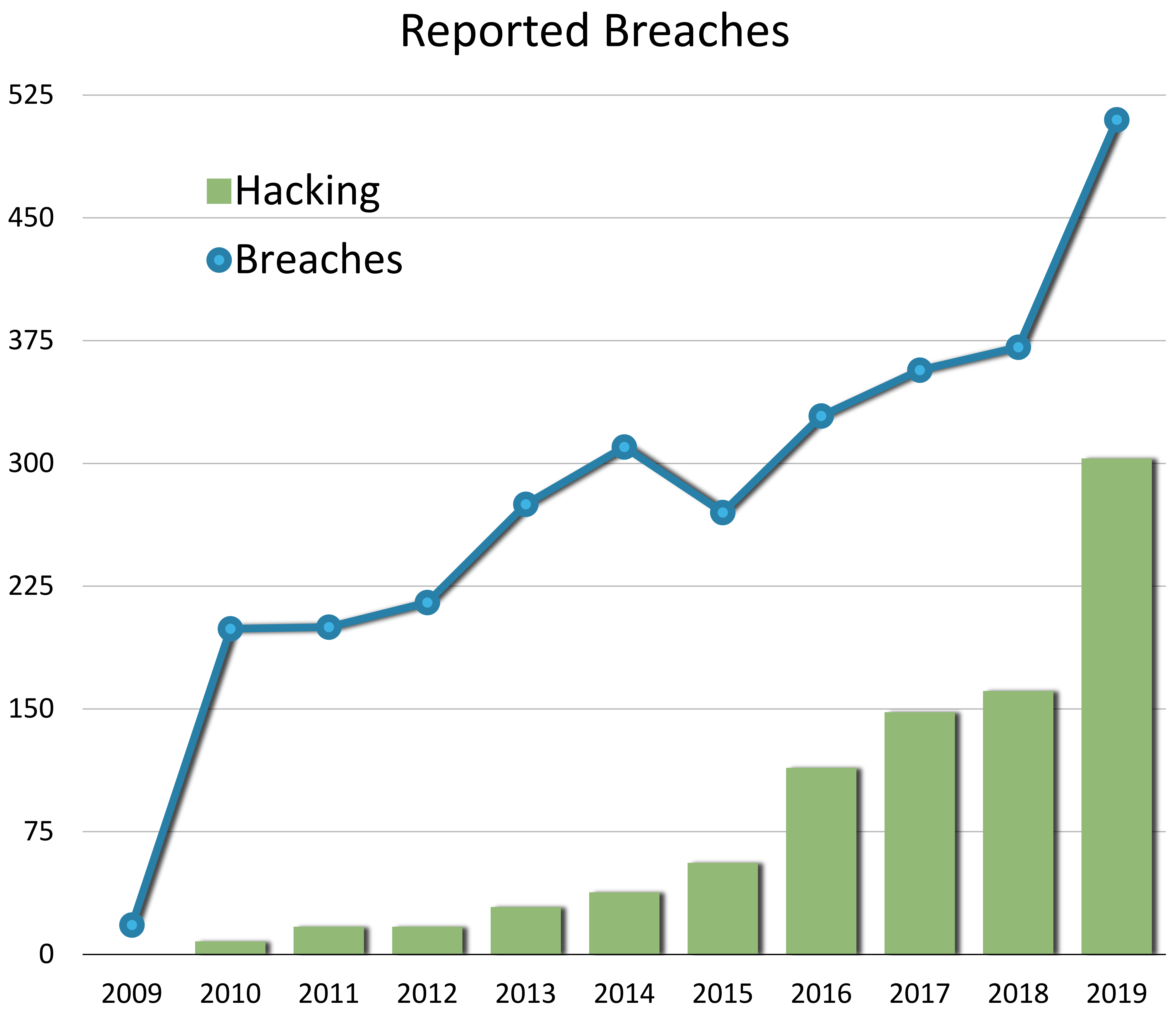
The Anthem Hack, ThreatConnect, Feb 2015, threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

US health care breaches

- **3143** healthcare data breaches
  - 94% of US hospitals affected
  - 70% of US population

- **231 million** records exposed
  - spike in 2015: 113 M
    - Anthem: 78 M
  - average other years: 11 M/yr

- breaches from hacking, theft or loss
- now mostly hacking
- breaches cost $4 billion in 2019



HIPAA Journal, 2020

Largest breaches

Date	Entity	#	Cause
2015	**Anthem**	78M	Hacking
2019	Quest Diagnostics	12M	Hacking
2015	Premera Blue Cross	11M	Hacking
2015	Excellus Health Plan	10M	Hacking
2019	Lab Corp	8M	Hacking
2014	Community Health Systems	6M	Hacking
2011	Science Applications International Corp	5M	Theft
2014	Community Health Systems Prof Services Corp	4.5M	Hacking
2015	UCLA Health	4.5M	Hacking
2013	Advocate Medical Group	4M	Theft

HHS breach report portal

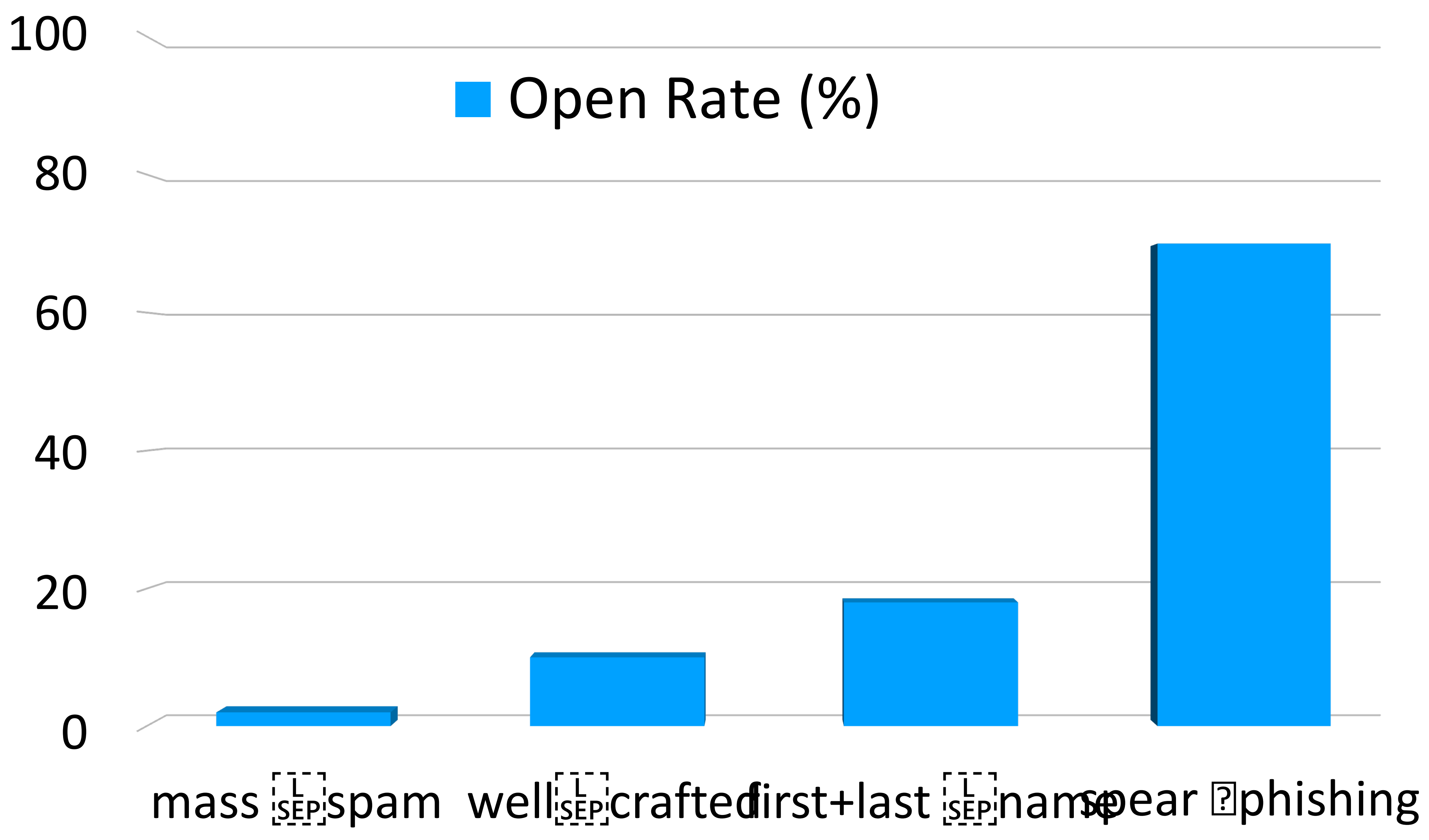
$115 millions settlement

$74 millions settlement

Cause of most breaches: phishing

fake emails

- induce individuals to reveal confidential information
- 23 attacks/min in 2018
- **top** cause of data breaches



Verizon DBIR Report, 2019

fake links

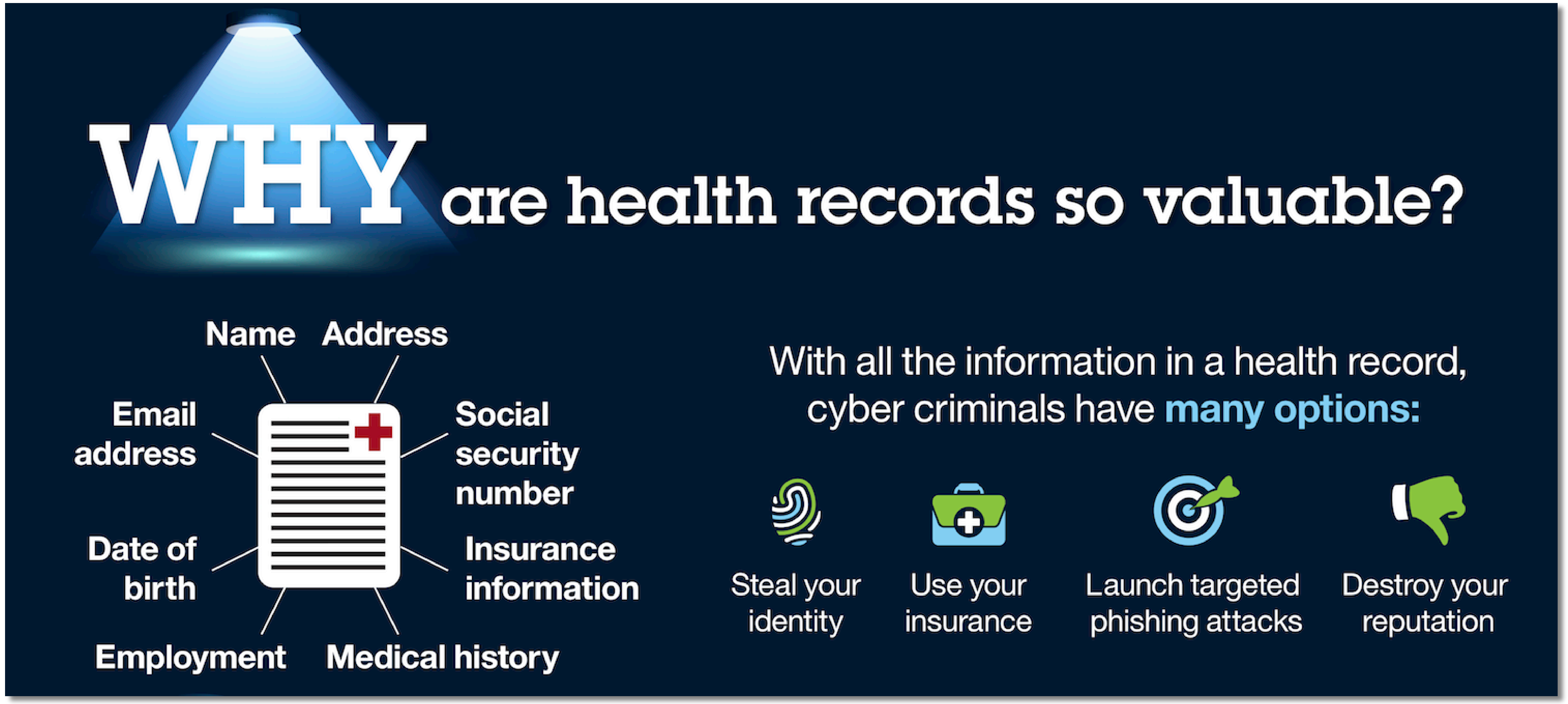
- spoofed URLs
  - www.acr.org → http://hacker.ru
- homoglyphs
  - wellsf**ɑ**rgo.com
  - instag**r**am.com
  - **apple**.com
  - **paypal**.com
- Anthem 78M records breach in 2015

Cyrillic	Latin
а с е о р х у	a c e o p x y
ԁ і ј ӏ ԛ ѕ ԝ	d i j l q s w

malicious file attachment

- office (38%), archive (37%), pdf (14%)
- virus or trojan
  - executes when opened by user
  - U Washington Med breach in 2013

Medical records



highly valuable

- comprehensive record of identity
- immutable exploitable information

> 2 million victims of identity theft annually

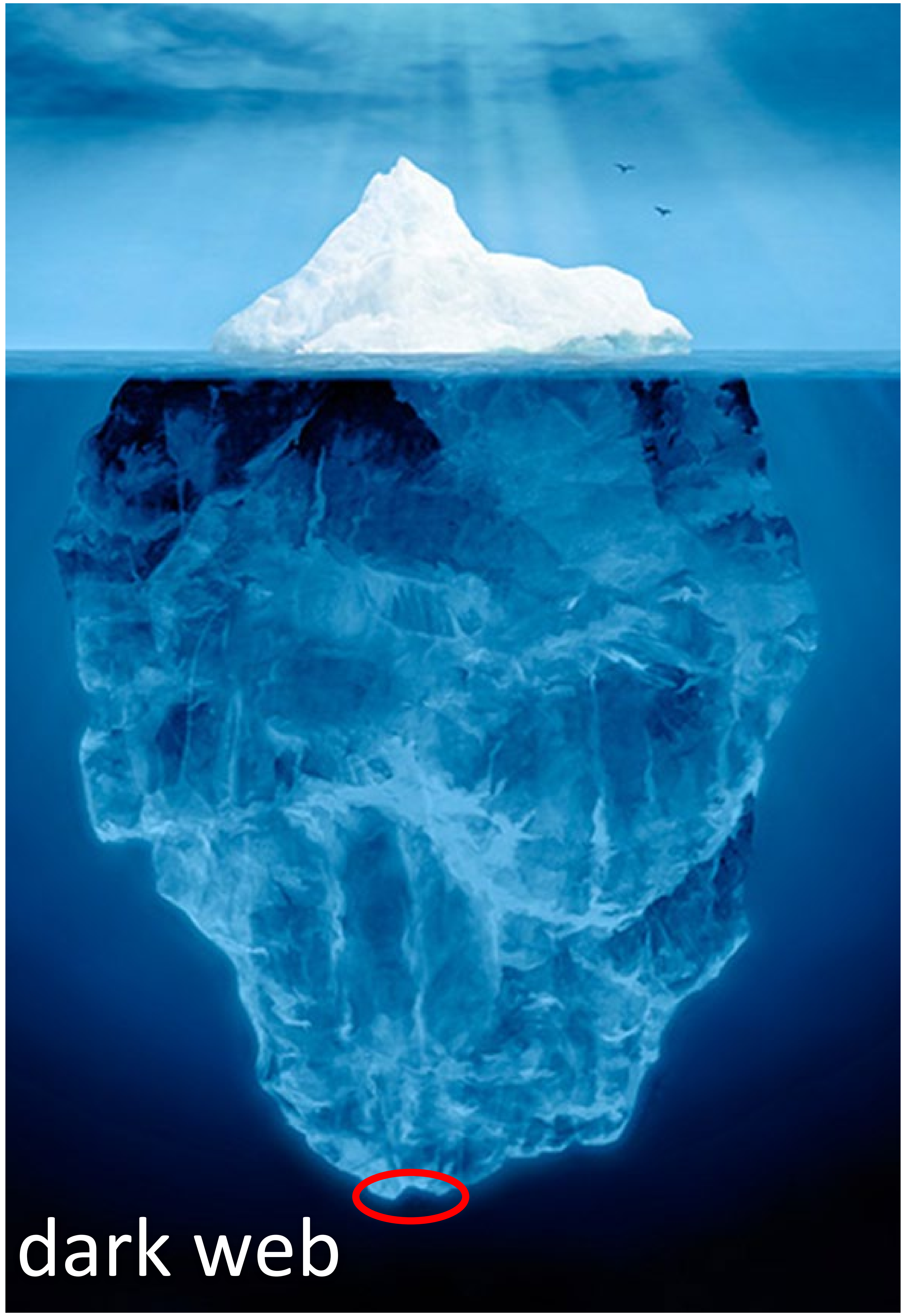
- $13K per victim to fix

Medical records

- hospitals have millions of medical records
- stored in secure data farms
- monitor hacks using threat intelligence feed
- Penn data farm
  - **6 million attacks / month**
  - Brazil, China, Ukraine

Where do stolen records go?

Porn
Ricin
Weed
Hitman
Uranium
Explosives
Stolen SSN
Powerful Drugs
Fake Passports
Human Trafficking
Rocket Launchers
Credit Card Numbers
Fake College Degrees
Stolen Medical Records
Hacked Government Data



surface web (4%)

deep web (96%)

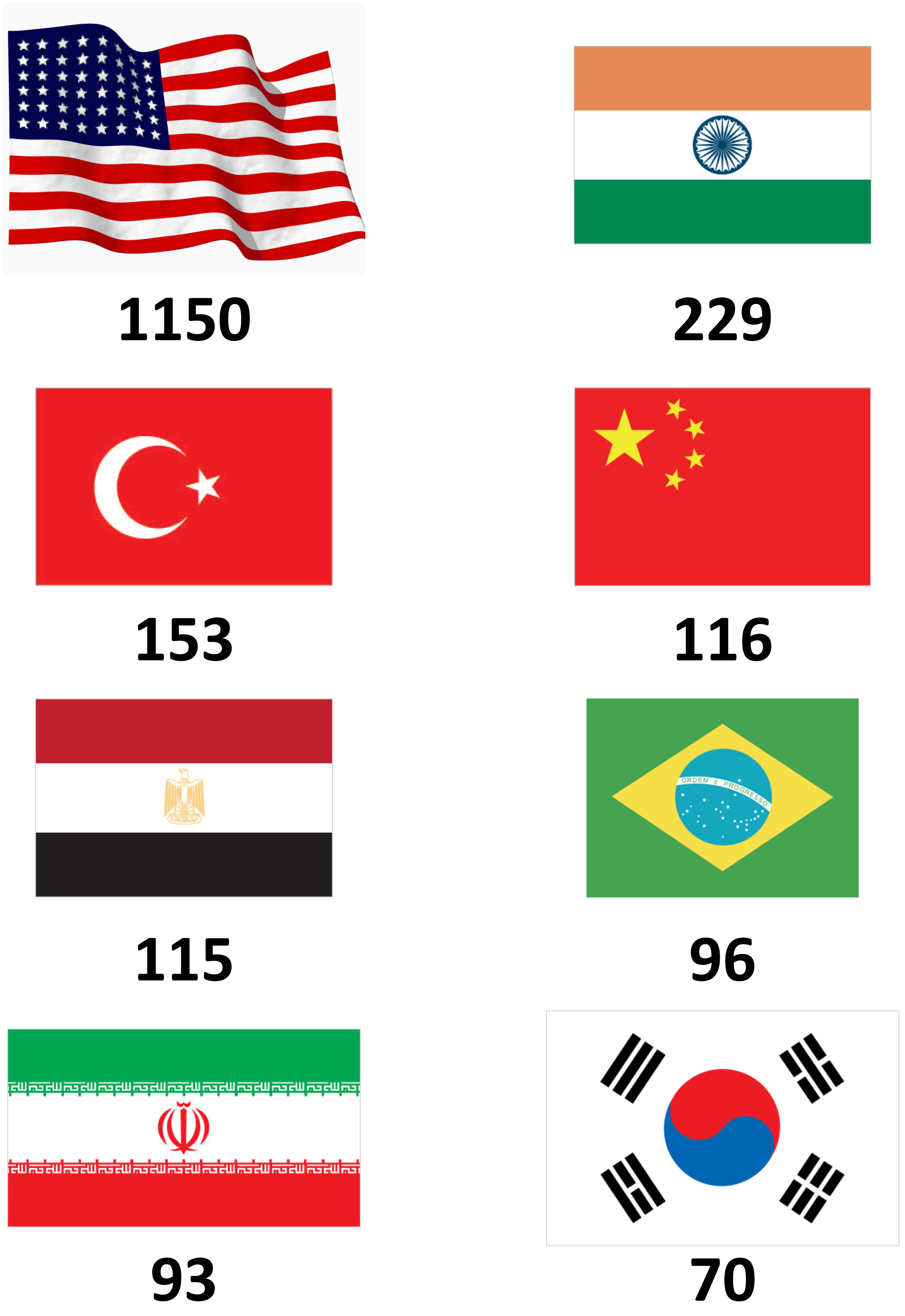
8416 active sites
(< 0.005%)

Recorded Future, 2019

Medical images can be breached too

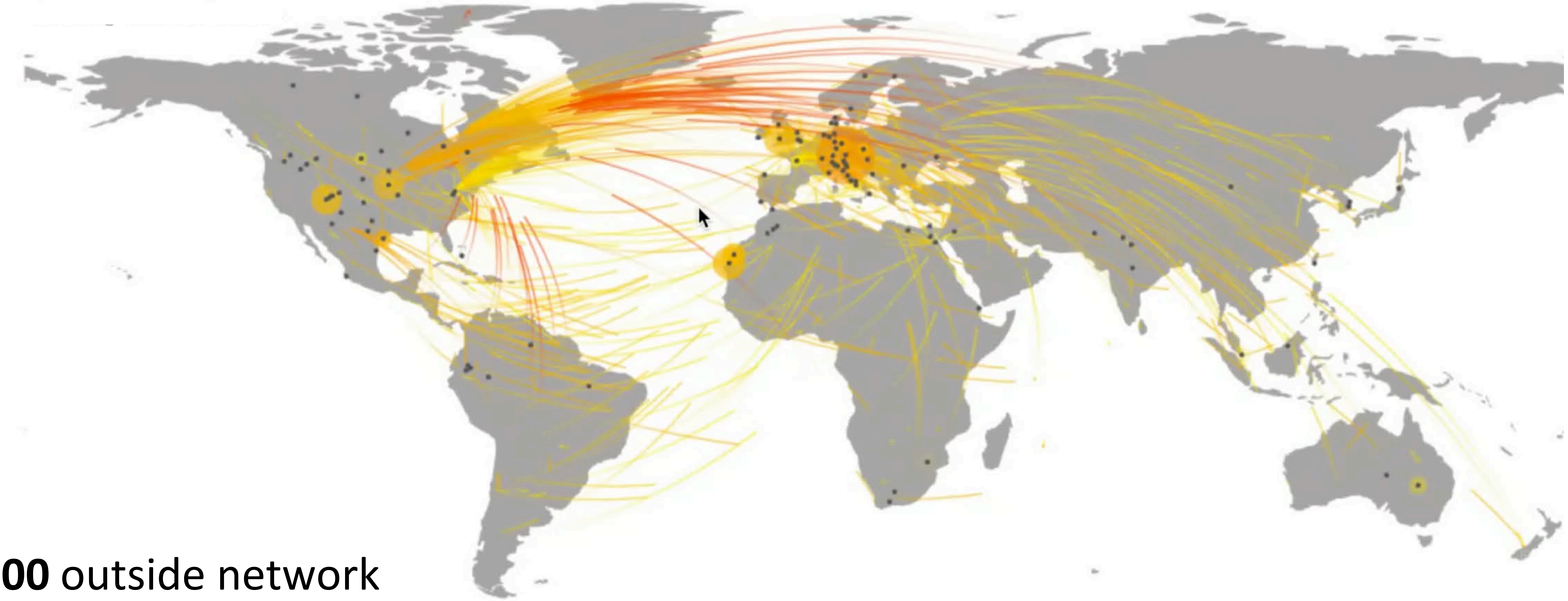
Recent breaches

- multiple security teams
  - MGH, McAfee, Greenbone Networks
- methods
  - manual scans of internet
  - search engine (Shodan)
- results
  - many unsecured networks
  - >36,000 medical devices discoverable on web
  - 1000s of **unprotected** image servers
  - 100s of millions of unprotected medical images
  - US is biggest culprit



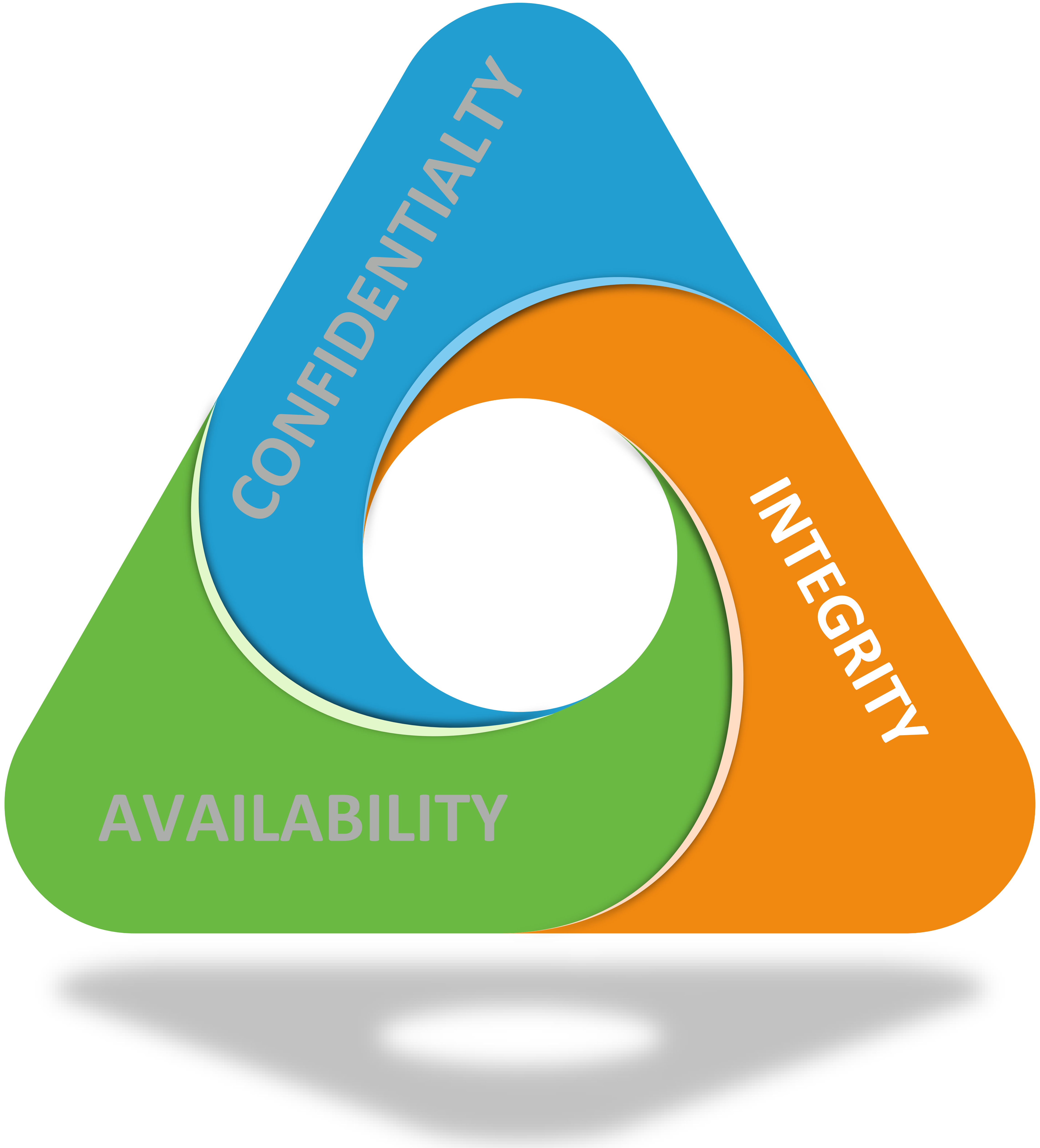
Pianykh, RSNA 2017

Breach of confidentiality



digitalattackmap.com

- at Penn: **250,000** outside network connection attempts blocked **daily**
  - vulnerability scanning
  - password spraying
  - web app testing


CONFIDENTIALTY
INTEGRITY
AVAILABILITY

Integrity

- **Definition**
  - verification that data has not been altered

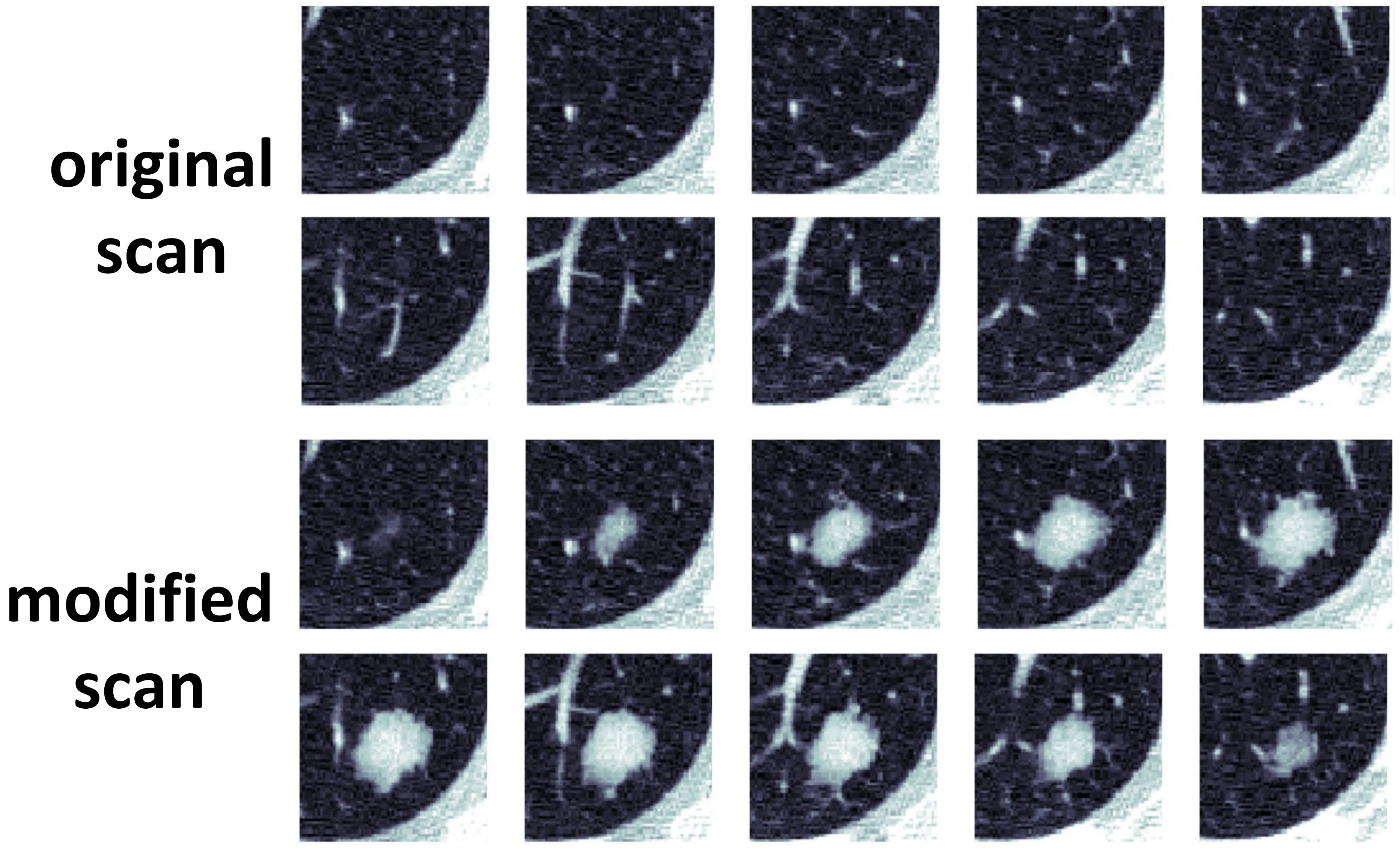
- **Breaches** of integrity
  - **not** obvious when they occur
  - less common but more dangerous than breaches of confidentiality
  - can affect management and could kill patients
  - e.g. breach that modifies lab results or imaging results

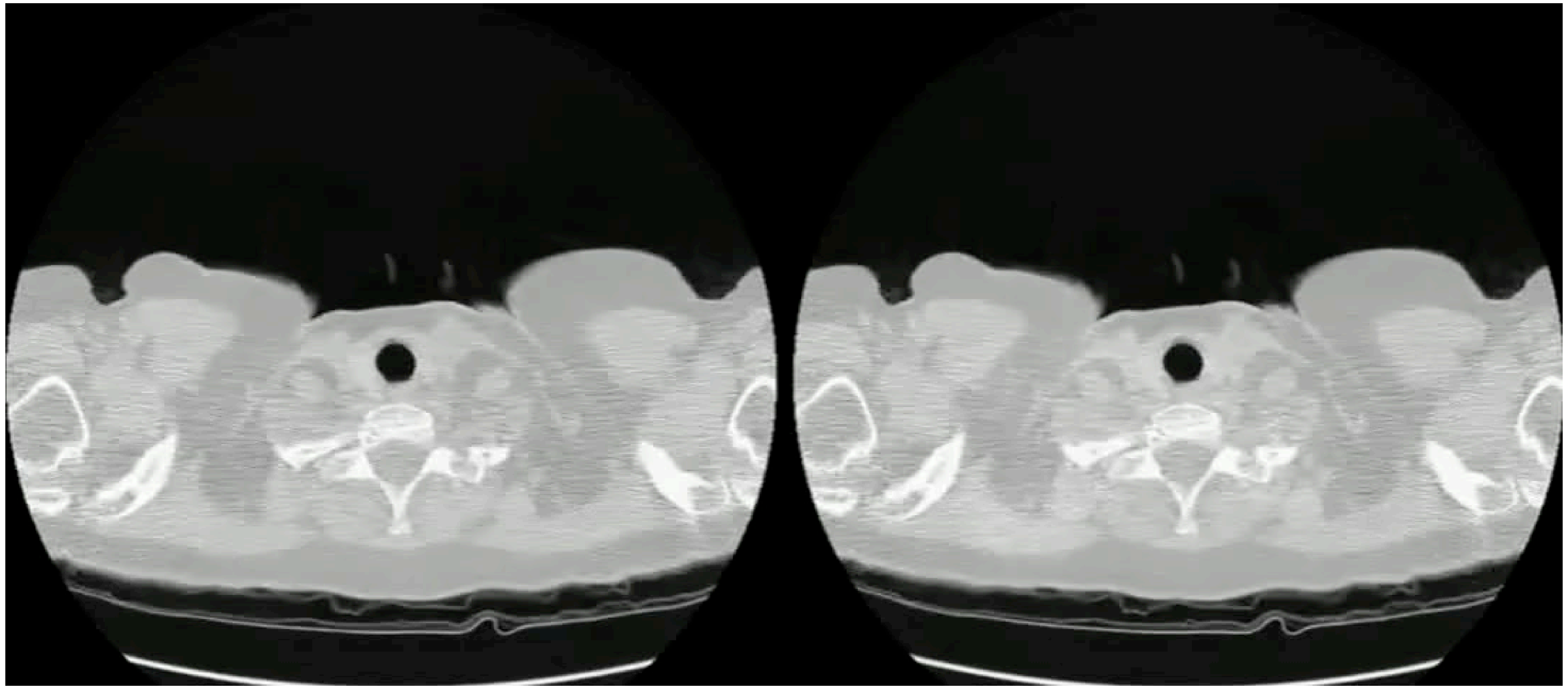
Avengers: Infinity War

Breach of integrity: images

hacking medical images

- intercept images on network between scanner and PACS
- add or remove nodules on CT images using deep-learning





original **fake nodules**

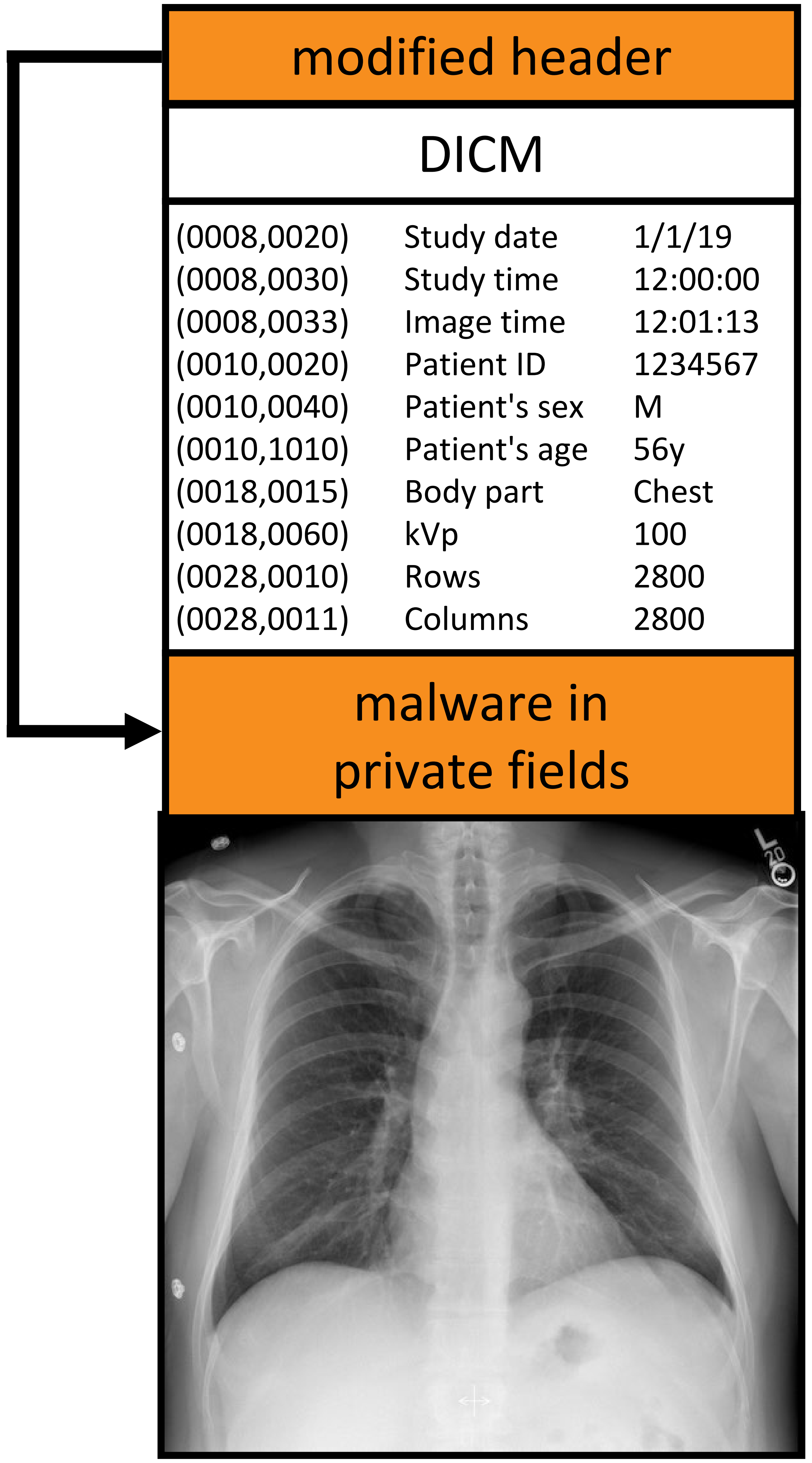
- radiologists fooled by:
  - added fake nodules (99%)
  - removed nodules (94%)

Mirsky, arXiv:1901.03597v2, Apr 2019

Breach of integrity: images

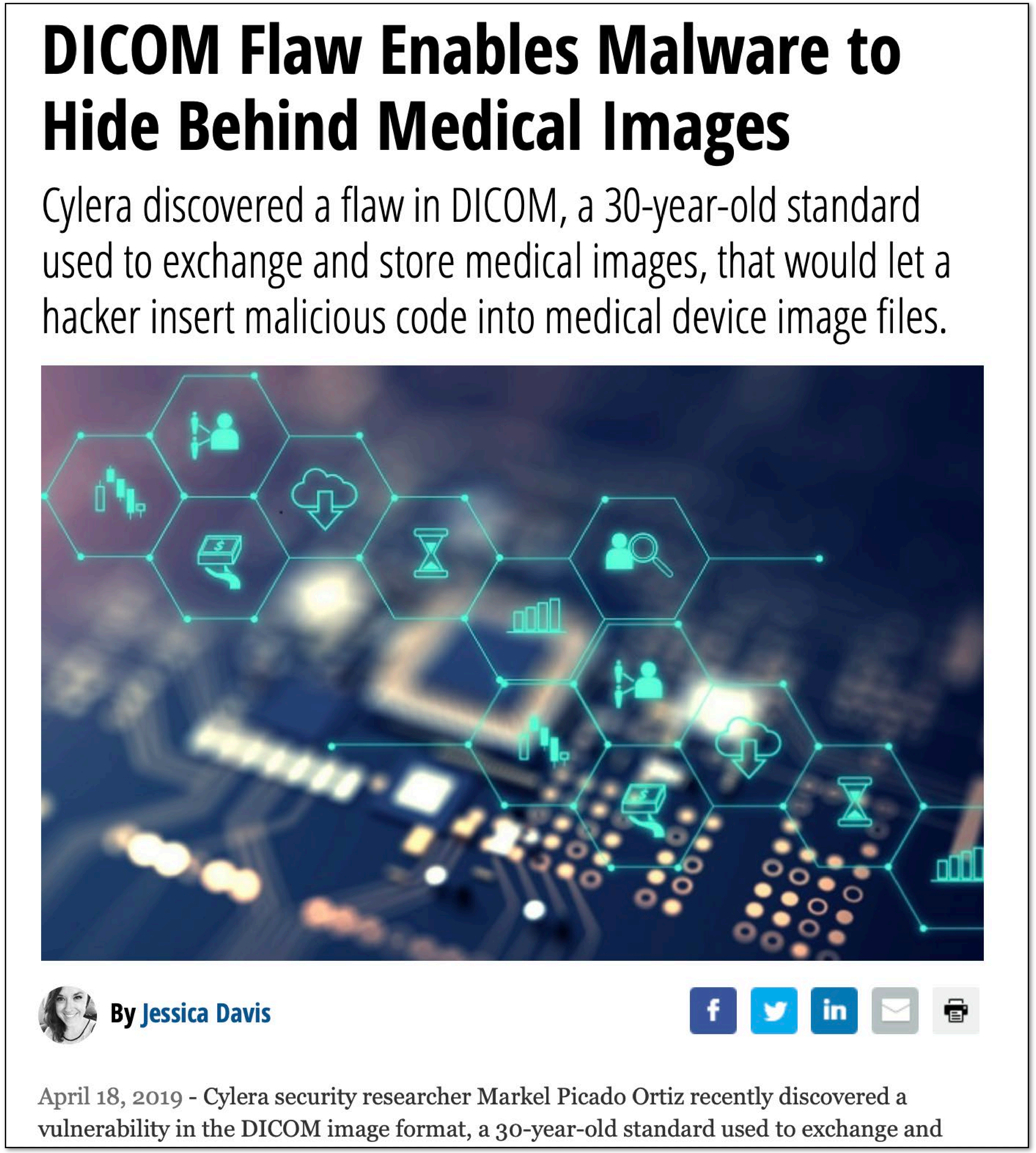
- modified medical images DICOM files
- header (preamble)
  - used for dual personality files
    - e.g. DICOM-TIFF
  - replaced by executable file header
- private fields
  - replaced by malware

Picado Ortiz, Apr 2019, labs.cylera.com/2019/04/16/pe-dicom-medical-malware/



(0008,0020)	Study date	1/1/19
(0008,0030)	Study time	12:00:00
(0008,0033)	Image time	12:01:13
(0010,0020)	Patient ID	1234567
(0010,0040)	Patient's sex	M
(0010,1010)	Patient's age	56y
(0018,0015)	Body part	Chest
(0018,0060)	kVp	100
(0028,0010)	Rows	2800
(0028,0011)	Columns	2800

PE-DICOM file



DICOM Flaw Enables Malware to Hide Behind Medical Images

Cylera discovered a flaw in DICOM, a 30-year-old standard used to exchange and store medical images, that would let a hacker insert malicious code into medical device image files.

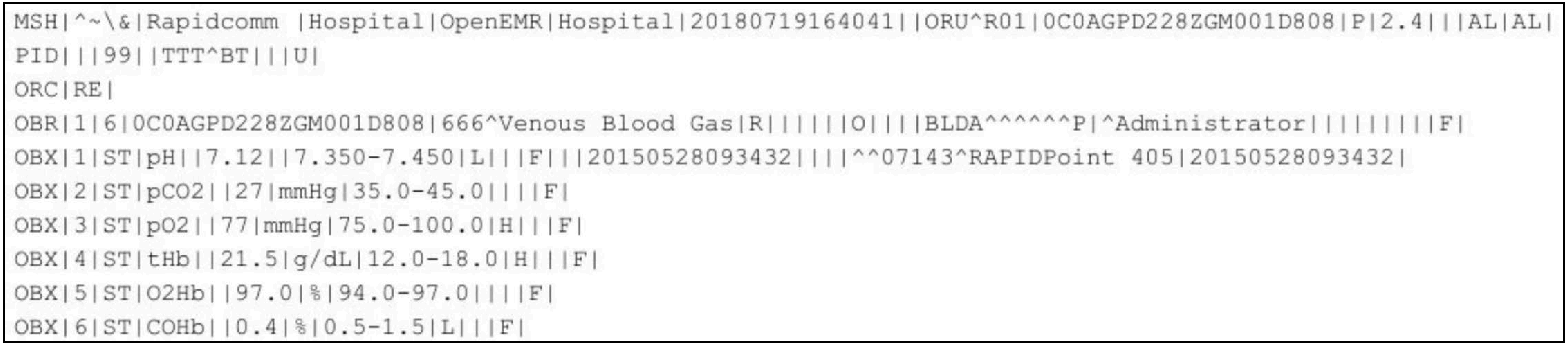
By Jessica Davis

April 18, 2019 - Cylera security researcher Markel Picado Ortiz recently discovered a vulnerability in the DICOM image format, a 30-year-old standard used to exchange and

Breach of integrity: HL7

data transmission protocol for clinical workflows

- lack of **authentication** and **encryption**



```
MSH|^~\&|Rapidcomm |Hospital|OpenEMR|Hospital|20180719164041||ORU^R01|0C0AGPD228ZGM001D808|P|2.4|||AL|AL|
PID|||99||TTT^BT|||U|
ORC|RE|
OBR|1|6|0C0AGPD228ZGM001D808|666^Venous Blood Gas|R|||||O|||BLDA^^^^^^P|^Administrator||||||||F|
OBX|1|ST|pH||7.12||7.350-7.450|L|||F|||20150528093432|||^^07143^RAPIDPoint 405|20150528093432|
OBX|2|ST|pCO2||27|mmHg|35.0-45.0||||F|
OBX|3|ST|pO2||77|mmHg|75.0-100.0|H|||F|
OBX|4|ST|tHb||21.5|g/dL|12.0-18.0|H|||F|
OBX|5|ST|O2Hb||97.0|%|94.0-97.0||||F|
OBX|6|ST|COHb||0.4|%|0.5-1.5|L|||F|
```

vulnerable to interception of data on networks

- proof of concept at Black Hat 2018 (ARP spoofing)
- inject false information
- disrupt care
- serious patient harm

Dameff, Black Hat 2018

Medical devices

15 million medical devices in U.S.

- from tiny pill-size devices
- to large stationary MRI scanners

typical hospital

- patient care dependent on technology
  - devices per ICU bed: 13
- thousands of medical devices
  - many devices **networked**
  - many **legacy** devices
    - can be in use for many years
    - not cyber-security oriented

Breach of integrity: devices

Proven attacks on generic devices

- muting alarms
- activating false alarms
- manipulate display data
- restoring system
- ransomware
- patient to image disruption
- mechanical disruption of motors
- disruption of results
- alteration of results
- leakage of PI
- denial of service

Nissim, RSNA 2017

Breach of integrity: devices

New York Times, March 2008

- team from U Wash and U Mass
- Medtronic's Maximo **pacemaker/ICD**
- hacked the device in a lab

McAfee FOCUS 2011 (Jack):

- wireless hack of **insulin pumps**
- repeatedly deliver maximum dose
- until reservoir depleted

BreakPoint Oct 2012 (Jack):

- assassinate victim from 50ft away
- wireless hack of **pacemaker/ICD**
- to deliver 830 volts shock

Black Hat 2018 (Rios and Butts):

- put malware on **pacemaker**
- wireless hack of **insulin pumps** (app in Jul 2019)

Barnaby Jack (RIP)

Breach of integrity: devices

Dick Cheney

- US Vice-President 2001-2009
- had wireless functions of pacemaker/ICD disabled in 2007
- even before NY Times article

Cheney, 60 minutes, Oct 2013

William Walden

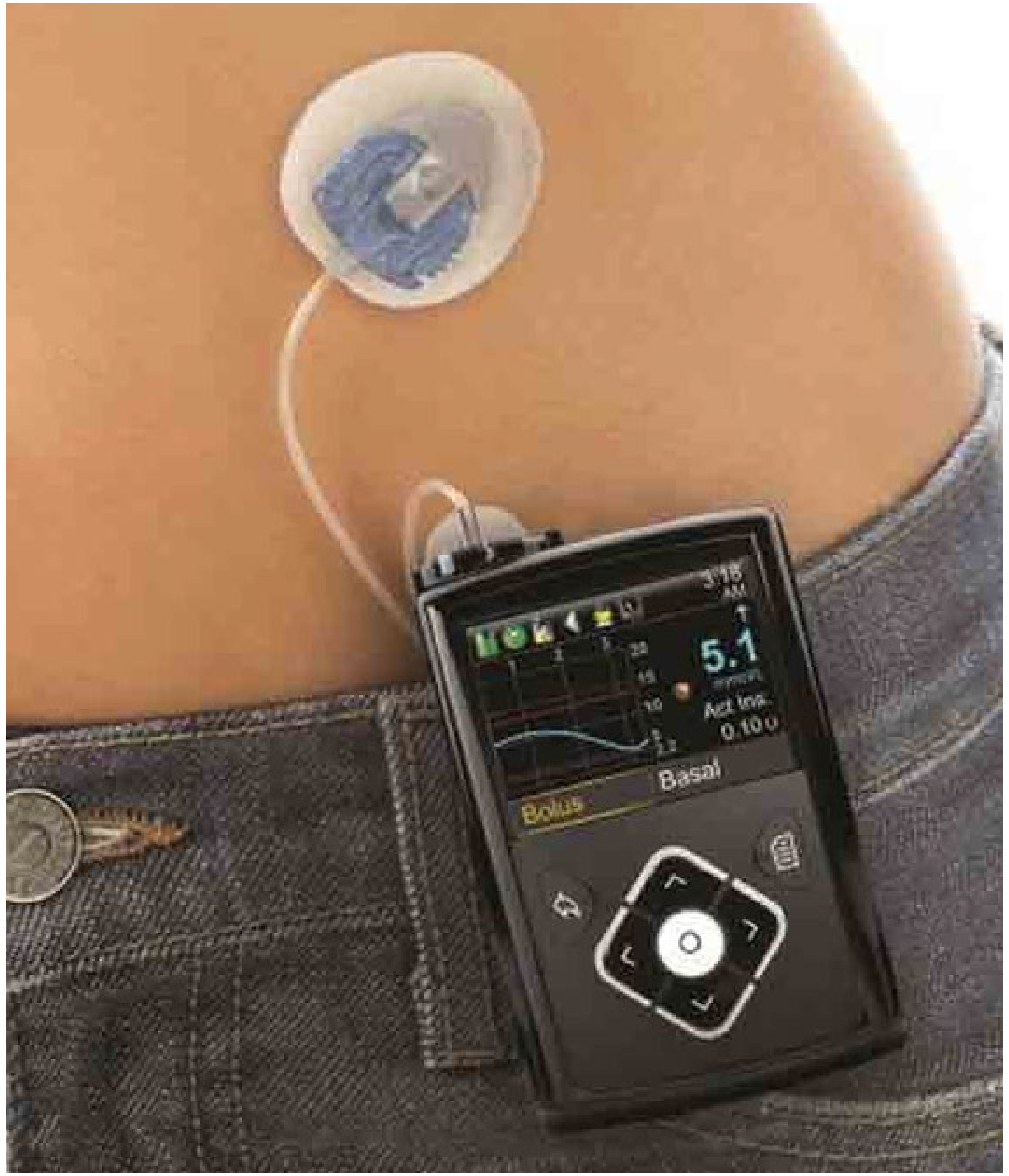
- US Vice-President on TV 2011-2012
- *Homeland: Broken Hearts* episode
- terrorists accelerate heart rate on pacemaker, killing him

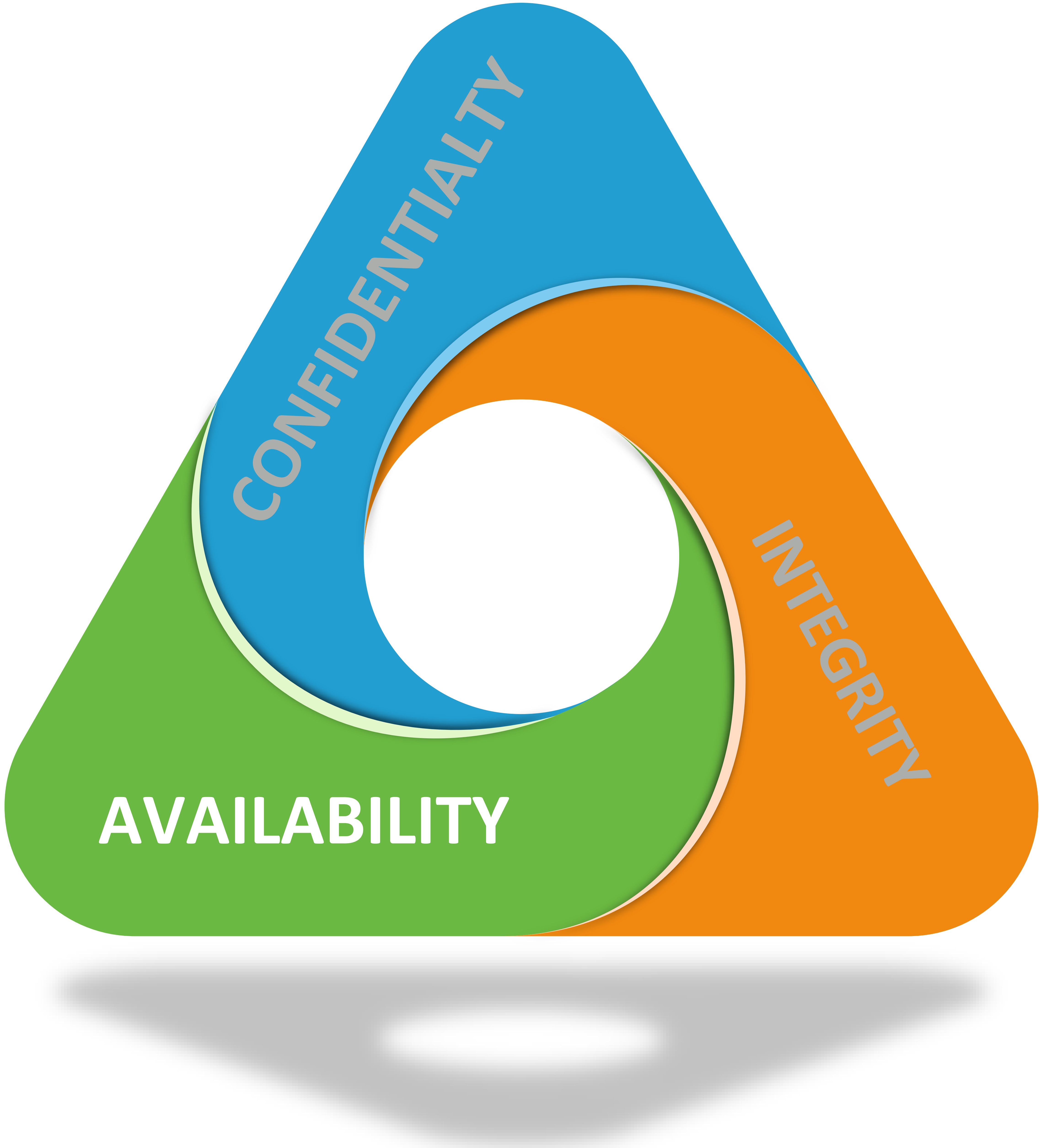
Breach of integrity: devices

- need to **keep perspective** here

- medical records
  - long history of breaches and thefts
  - **records need protection**

- medical devices
  - vulnerable, can be hacked
    - hacks are often proofs of concept
  - a hacker could hack them to harm patients
    - possible but unlikely
  - malware could randomly reach a device and cause havoc
    - has happened
    - **devices need protection**




CONFIDENTIALTY
INTEGRITY
AVAILABILITY

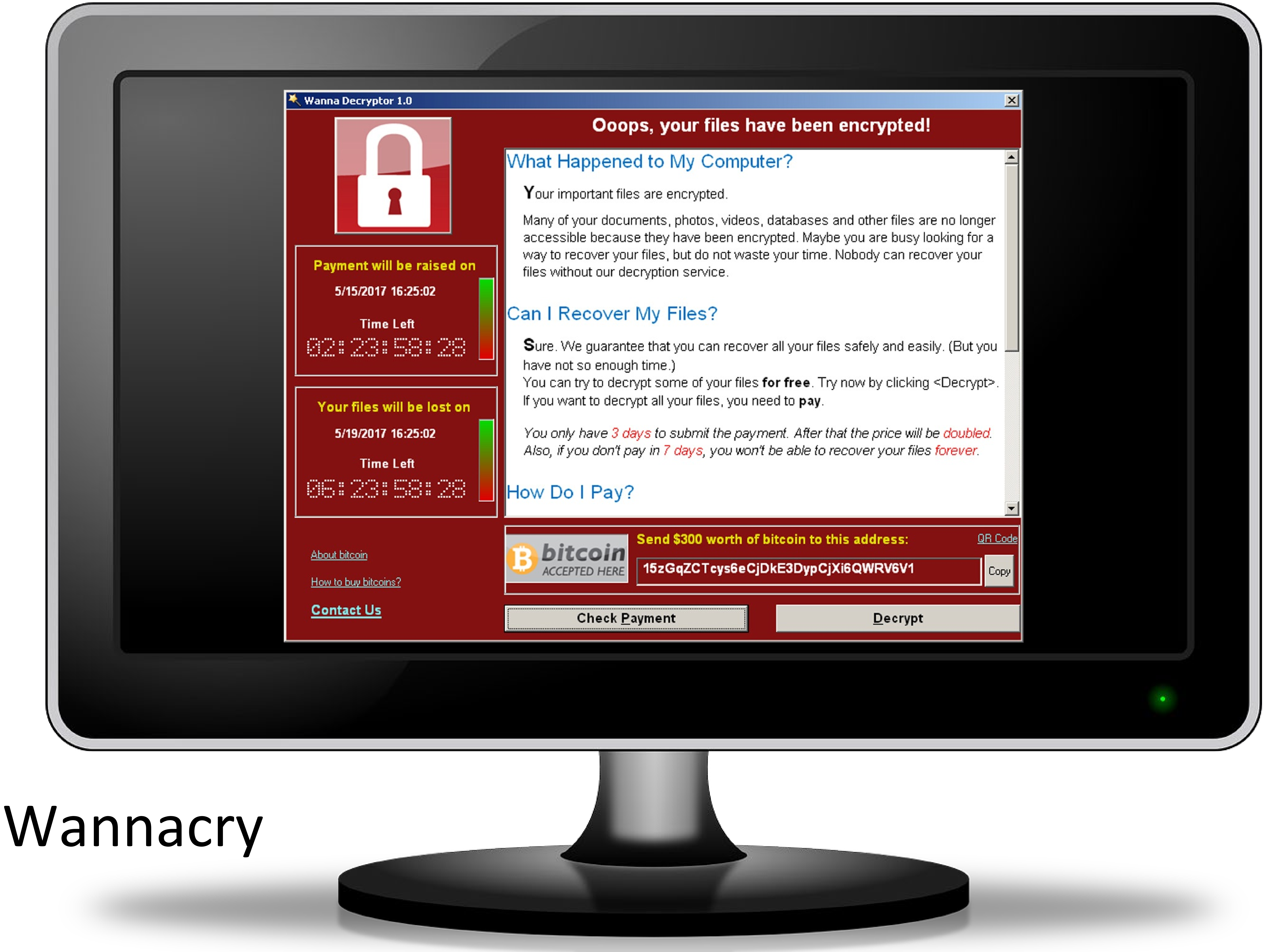
Availability

- **Definition**
  - guarantee of reliable access to information by authorized people

- **Breaches** of availability
  - **very** obvious when they occur
  - can harm patients
  - e.g. if surgeon loses access to patient's medical record before or during surgery, can harm patient

PoliticalCartoons.com

Breach of availability



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

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.

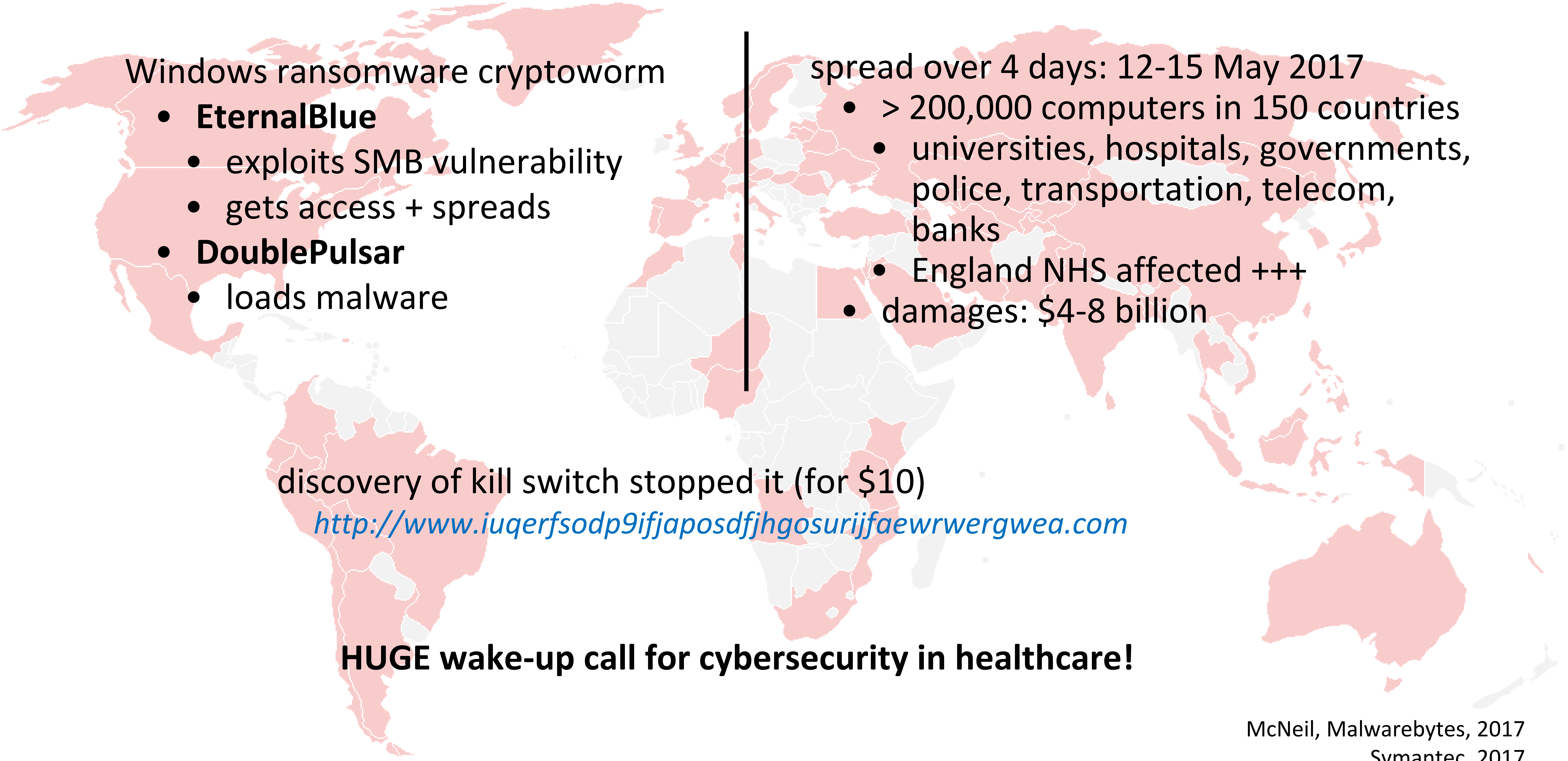
How Do I Pay?

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

May 2017 - Wannacry

Wannacry ransomware



Windows ransomware cryptoworm

- **EternalBlue**
  - exploits SMB vulnerability
  - gets access + spreads
- **DoublePulsar**
  - loads malware

spread over 4 days: 12-15 May 2017

- > 200,000 computers in 150 countries
  - universities, hospitals, governments, police, transportation, telecom, banks
  - England NHS affected +++
- damages: $4-8 billion

discovery of kill switch stopped it (for $10)

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

HUGE wake-up call for cybersecurity in healthcare!

McNeil, Malwarebytes, 2017
Symantec, 2017

bronsonhealth.com

Brookside ENT and Hearing Center

- medical practice in Michigan
- Apr 2019: **ransomware** attack
  - encrypted all medical records
  - $6500 ransom
- FBI advised **not** to pay ransom
  - doctors did not pay

→

- hackers **deleted all medical records**
- impossible to recover records
- doctors decided to shut down clinic and retire

Glaser, Newschannel 3, March 2019,
wwmt.com/news/local/west-michigan-doctors-office-hacked-doctors-held-for-ransom

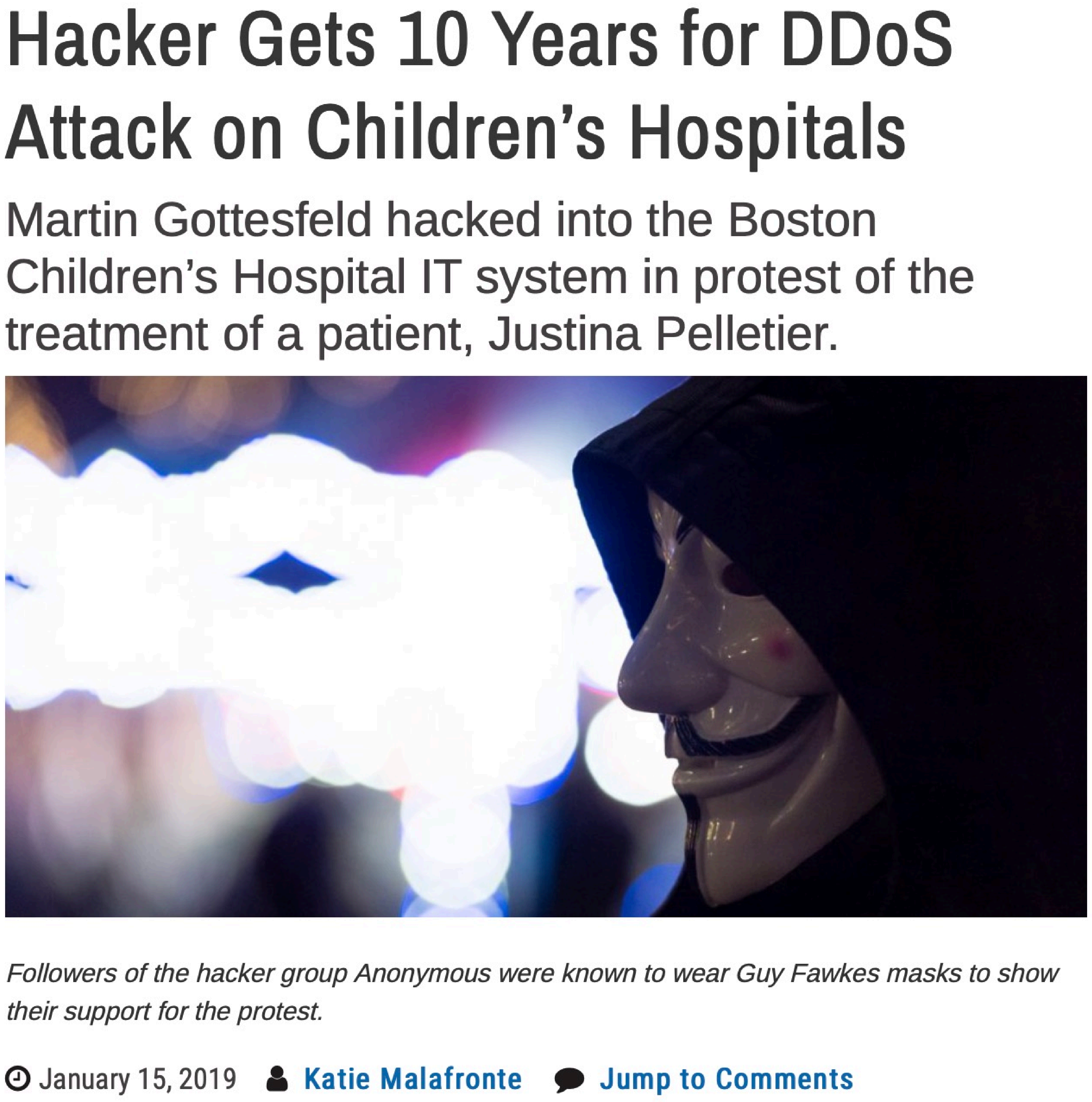
Breach of availability

denial of service (DoS, DDoS)

- send millions of DICOM messages to overwhelm DICOM server
- leads to denial of service
- DICOM server becomes too busy to perform basic tasks

Boston Children's Hospital (Apr 2014)

- malware on 40,000 routers
  - controlled by hacker
- flooded 65,000 IP adresses
- blocked online access for 2 weeks



Hacker Gets 10 Years for DDoS Attack on Children's Hospitals

Martin Gottesfeld hacked into the Boston Children's Hospital IT system in protest of the treatment of a patient, Justina Pelletier.

Followers of the hacker group Anonymous were known to wear Guy Fawkes masks to show their support for the protest.

January 15, 2019 Katie Malafronte Jump to Comments

com

Breach of availability

- **three weeks ago**, Düsseldorf , Germany
- ransomware attack
  - against Heinrich Heine University
  - affected affiliated University Hospital
  - encrypted about 30 hospital servers

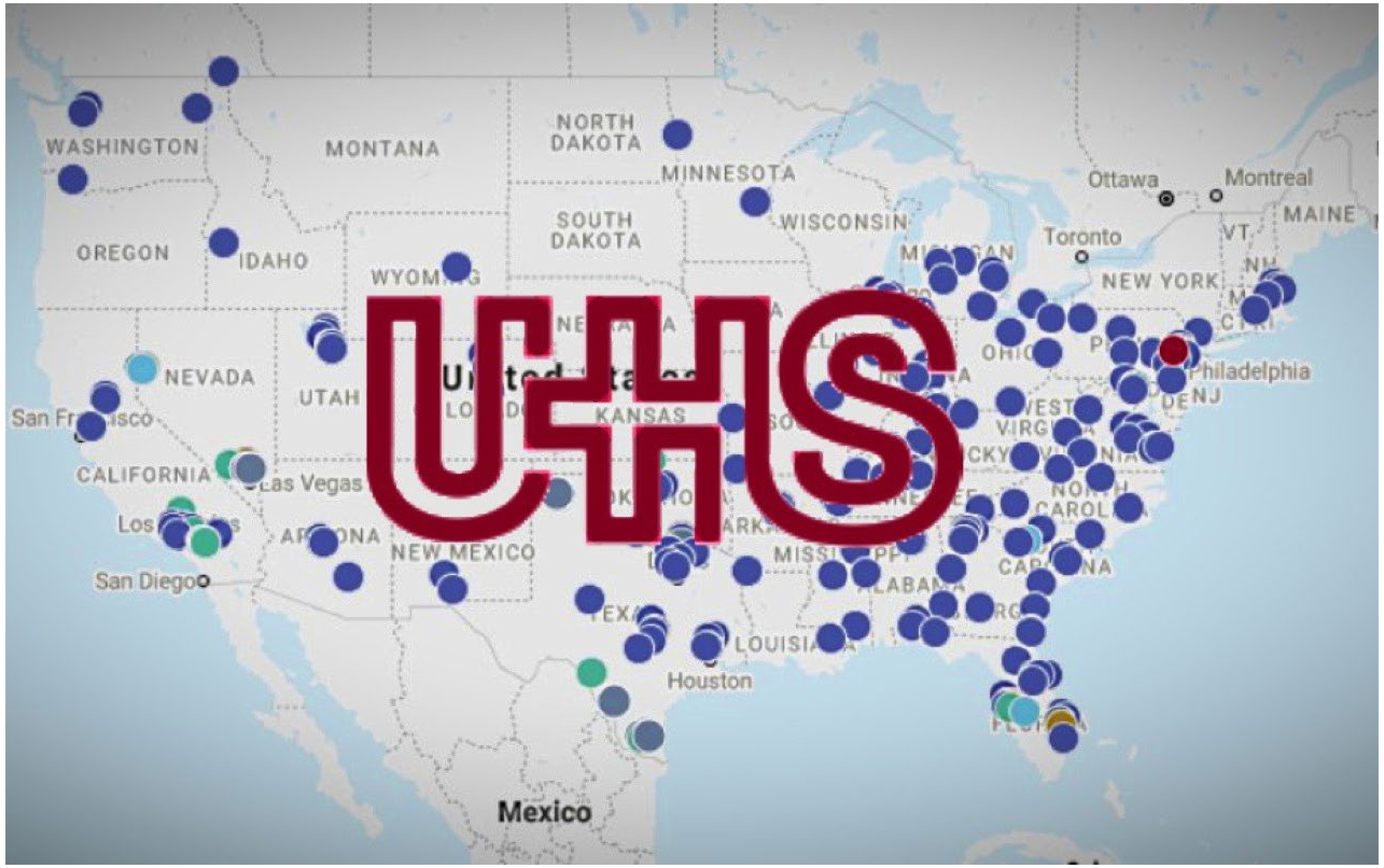
- woman suffered critical medical condition
  - went to that ER for treatment
  - turned away from hospital
  - rushed to a hospital 20 miles away
  - one-hour delay in treatment
  - woman **died**

UHS massive attack

- **Two weeks ago**, across USA
- Universal Health Services (UHS)
  - 400+ healthcare facilities US and UK

- ransomware attack (Ryuk)
  - lost access to computers and phones
    - labs, ekg's, radiology studies
    - no access to PACS system
  - redirecting ambulances
  - relocating patients

- **four deaths** reported??
  - caused by delays in lab results
  - unclear if related to attack



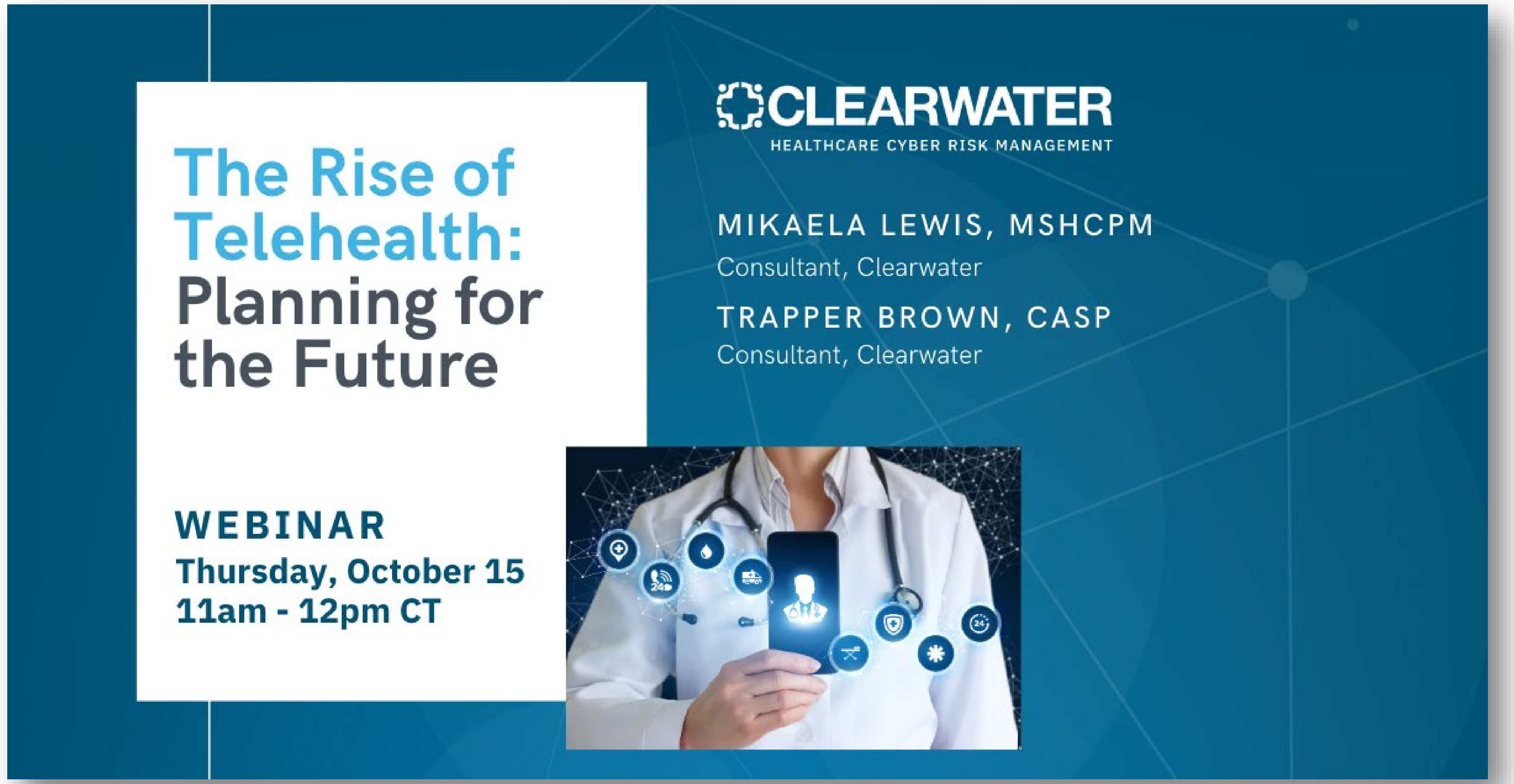
Discussion and Q&A

Pause and Poll

3. This session helped me better understand the unintended potential for patient harm due to the digitization of our healthcare system:

- ❑ Strongly Agree
- ❑ Agree
- ❑ Not Sure
- ❑ Disagree
- ❑ Strongly Disagree

Upcoming Clearwater Education



CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

The Rise of Telehealth: Planning for the Future

MIKAELA LEWIS, MSHCPM
Consultant, Clearwater

TRAPPER BROWN, CASP
Consultant, Clearwater

WEBINAR
Thursday, October 15
11am - 12pm CT

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

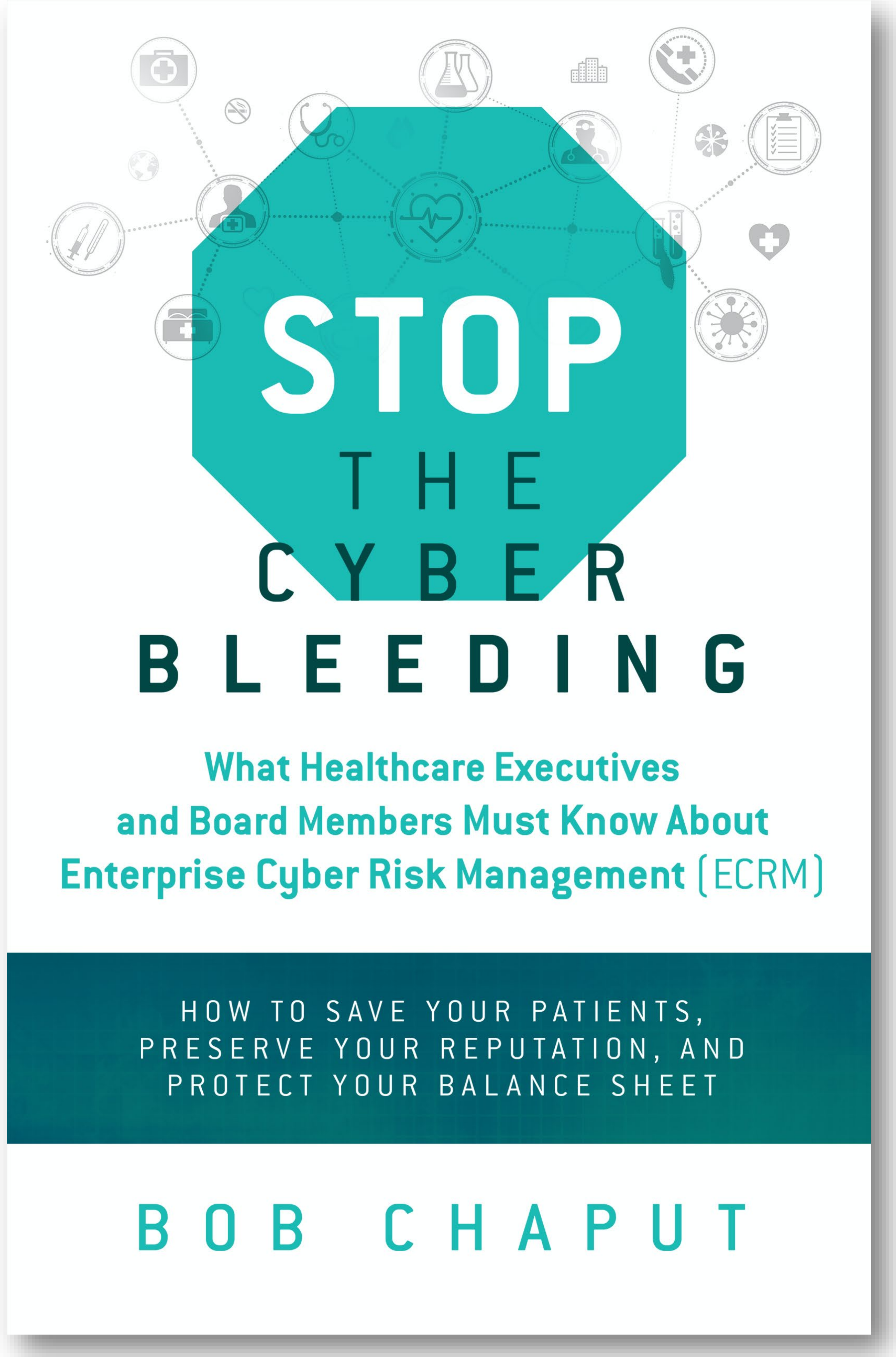
IRM | Analysis®

ENTERPRISE CYBER RISK MANAGEMENT SOFTWARE

LIVE DEMONSTRATION
Tuesday, Oct 27
@11am CT

See how an OCR-Quality®
Risk Analysis is done.

Learn more and register at https://clearwatercompliance.com/upcoming-educational-events/



STOP THE CYBER BLEEDING

What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)

HOW TO SAVE YOUR PATIENTS, PRESERVE YOUR REPUTATION, AND PROTECT YOUR BALANCE SHEET

BOB CHAPUT

INTERESTED IN A COPY?

https://www.clearwatercompliance.com/stopthecyberbleeding

Thank You & Questions

Bob Chaput
bob.chaput@clearwatercompliance.com

Benoit Desjardins
benoitd@upenn.edu

Thank you for completing the short survey when you leave the session.
We appreciate and use your feedback.

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

www.ClearwaterCompliance.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-compliance-llc/

Twitter | @clearwaterhipaa