Cybersecurity & Patient Safety: What they don't teach you at medical school

Richard Staynings

Healthcare Security Luminary
Chief Security Strategist, Cylera
Faculty, University of Denver

CYLERA

UNIVERSITY OF DENVER

C-TM
COUNTER-TERRORISM MEDICINE

In Emergency Medicine Triage can be critical

What is Important?

What is Urgent & Critical?

In National Defense, most countries have identified what is critical to them.

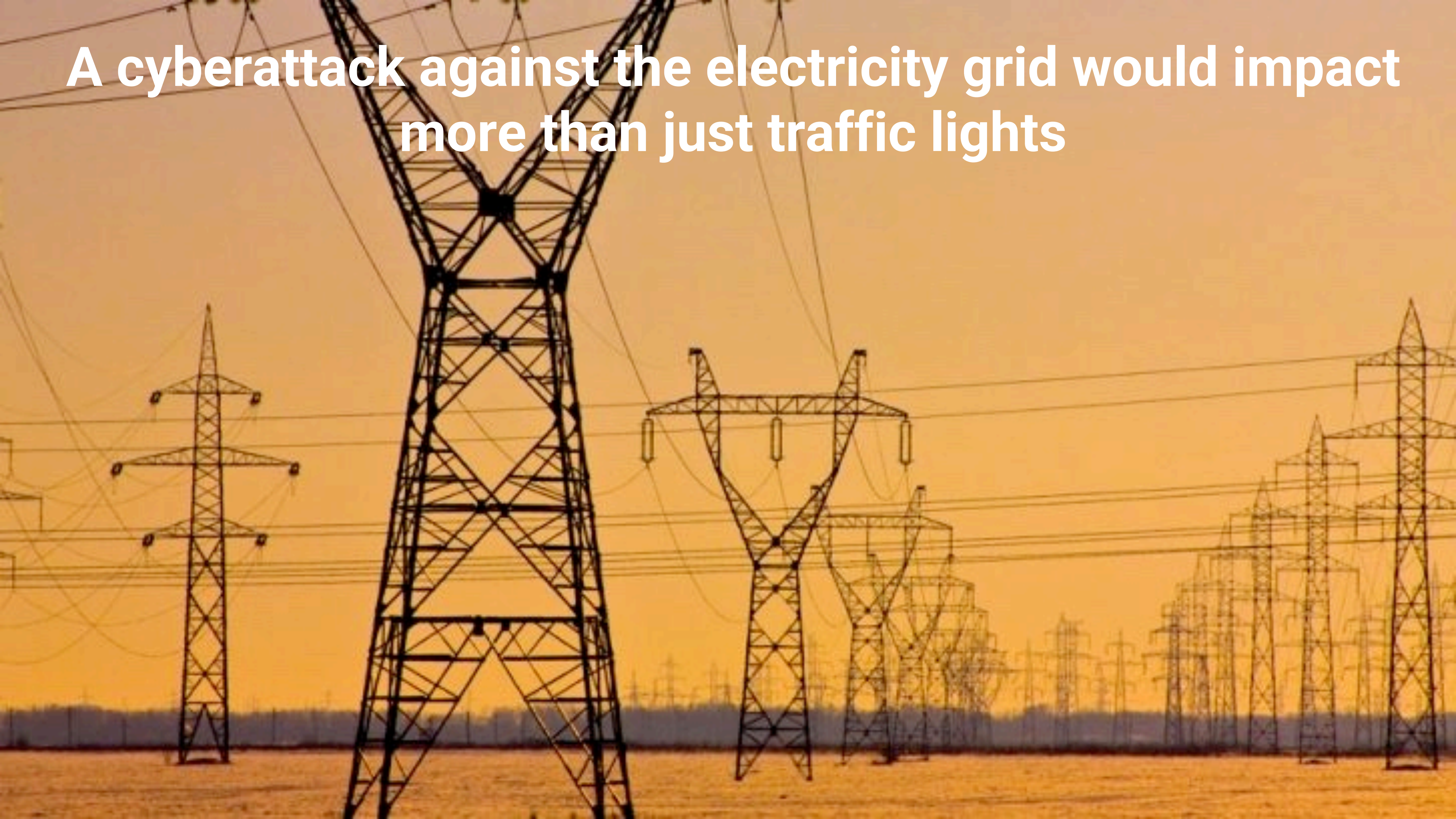
Healthcare is one of 16 national US critical infrastructure sectors.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation
- Water and Wastewater

National Critical Infrastructure

Our society is reliant upon these critical sectors

A cyberattack against the electricity grid would impact more than just traffic lights



A cyber attack against just one critical industry could be utterly devastating

A Public Health crisis could kill millions

New York City before sanitation

What happened when the power failed in New Orleans?

This is the abandoned Charity Hospital New Orleans USA. When in August 2005, Hurricane Katrina shut off the power and backup generators ran out of fuel, mold quickly took over, making the hospital unfit to treat patients.

But what if the disaster had been caused by a cyber attack, one that opened all the floodgates to the New Orleans basin?

A cyberattack that overloaded pumping stations?

Cyber-Kinetic attacks against critical infrastructure

ICS infrastructure is highly vulnerable

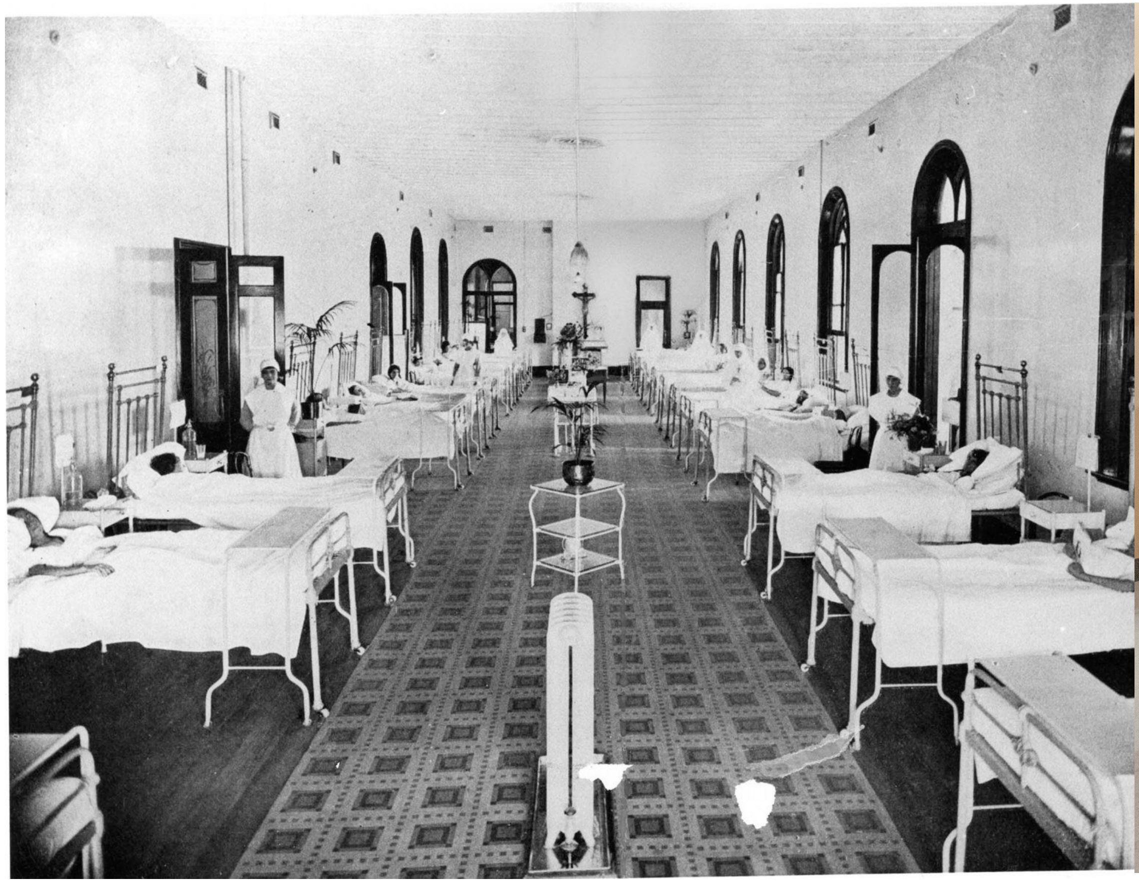
Russia reportedly GRU blew up

Baku-Tbilsi-Ceyan pipeline in 2008

(by cyber attack)

Healthcare

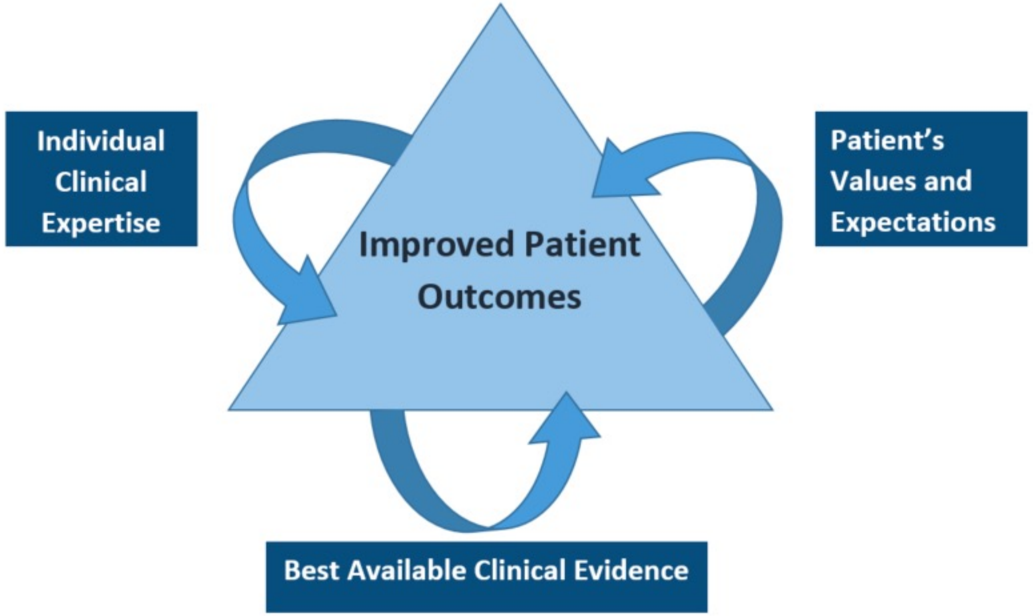
Healthcare has been transformed over the past century



Technology has fueled improvements in patient outcomes

Polio Patients in Iron Lungs before widespread vaccination

Modern Healthcare has enabled us to improve the human condition, to beat diseases that used to ravage families and communities and to live longer and better than ever before



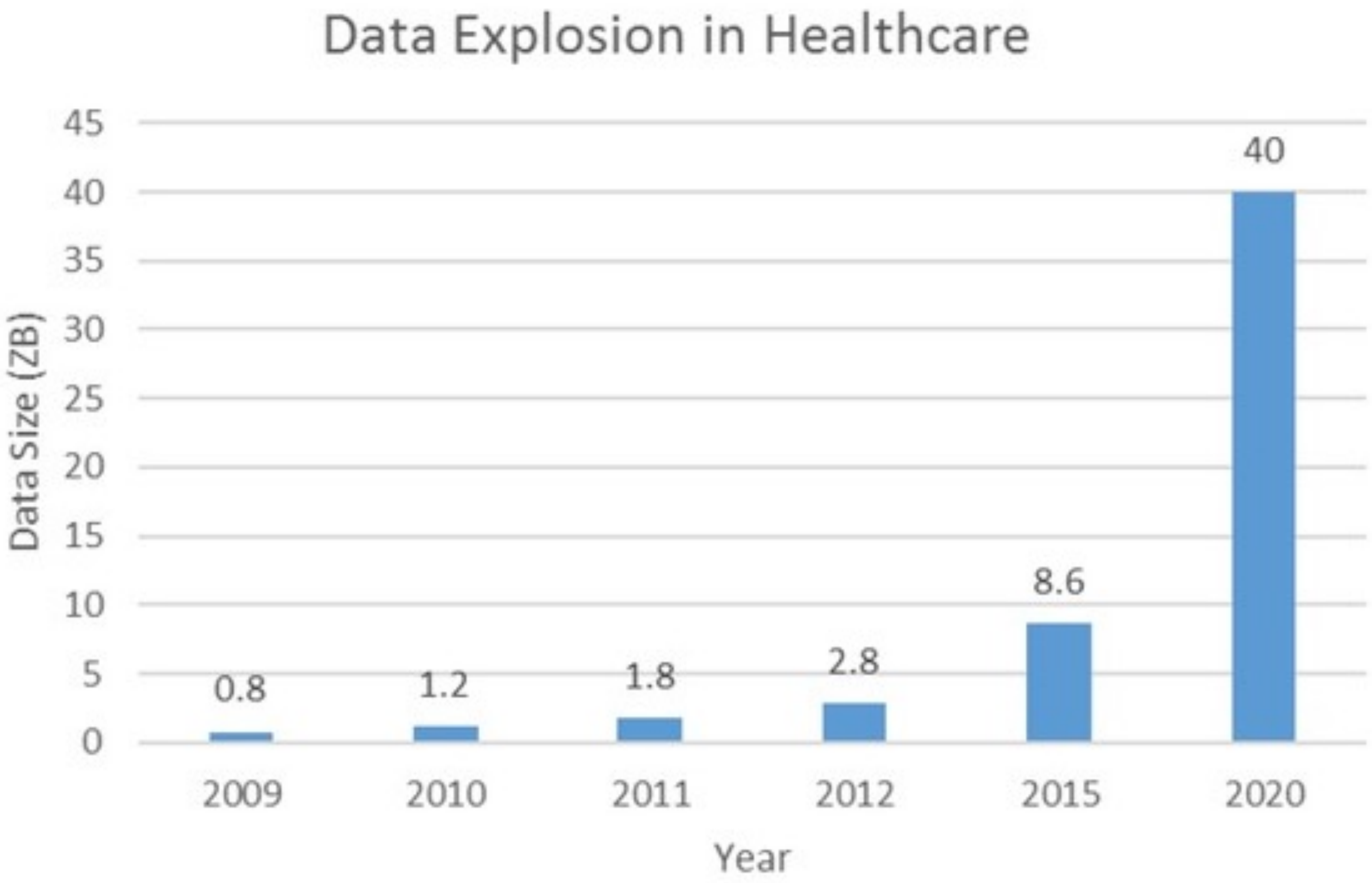
Improved Patient Outcomes

Individual Clinical Expertise

Patient's Values and Expectations

Best Available Clinical Evidence

Technology has resulted in an explosion of medical data



1 ZB = 1 billion TB

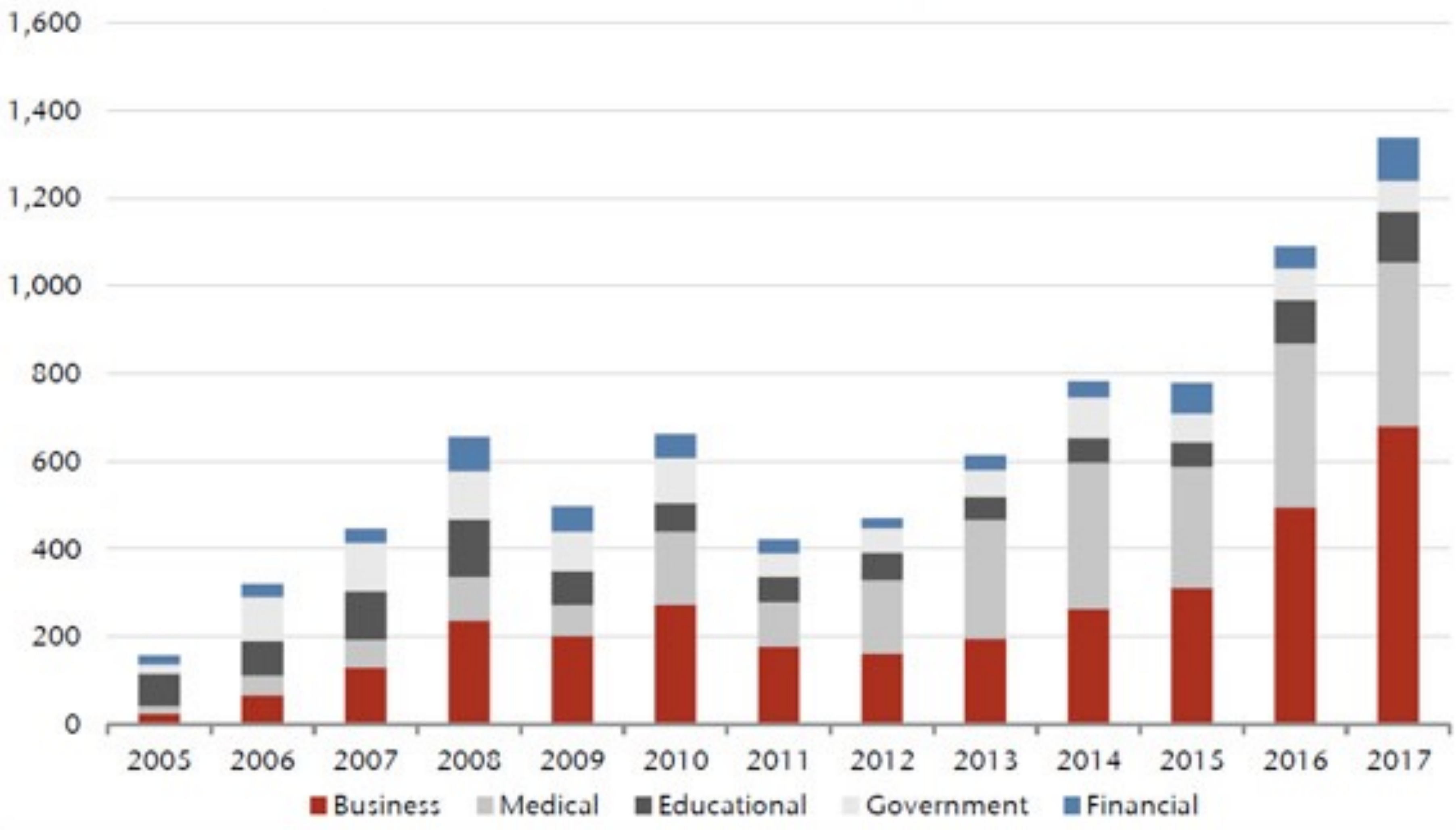
Hong, Big Data in Health Care, Data and Information Management 2 (3), Dec 2018

Digitalization has transformed patient outcomes

But it has also introduced new risks

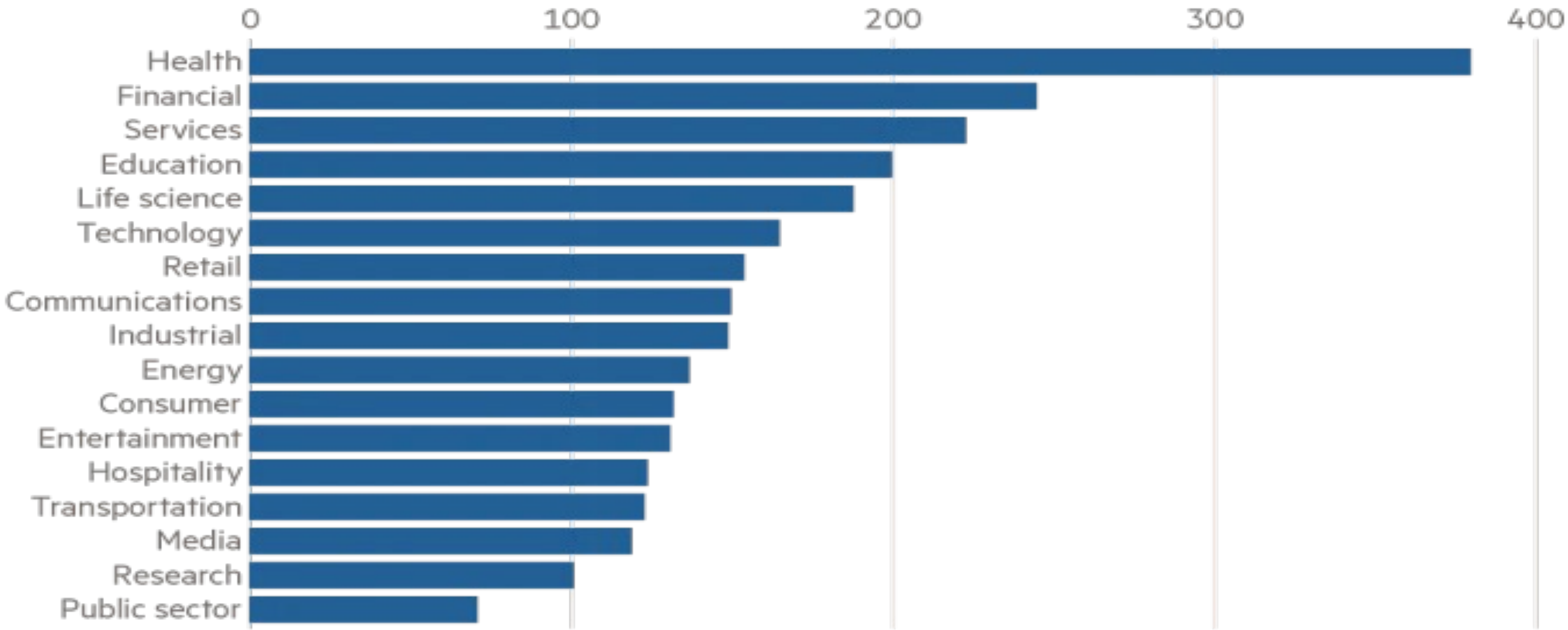
… that our PHI and PII maybe breached

Chart 9: Increasing number of data breaches (by entity)



Source: Jefferies, Identity Theft Resource Centre

…and Cyberattacks against Healthcare are very expensive



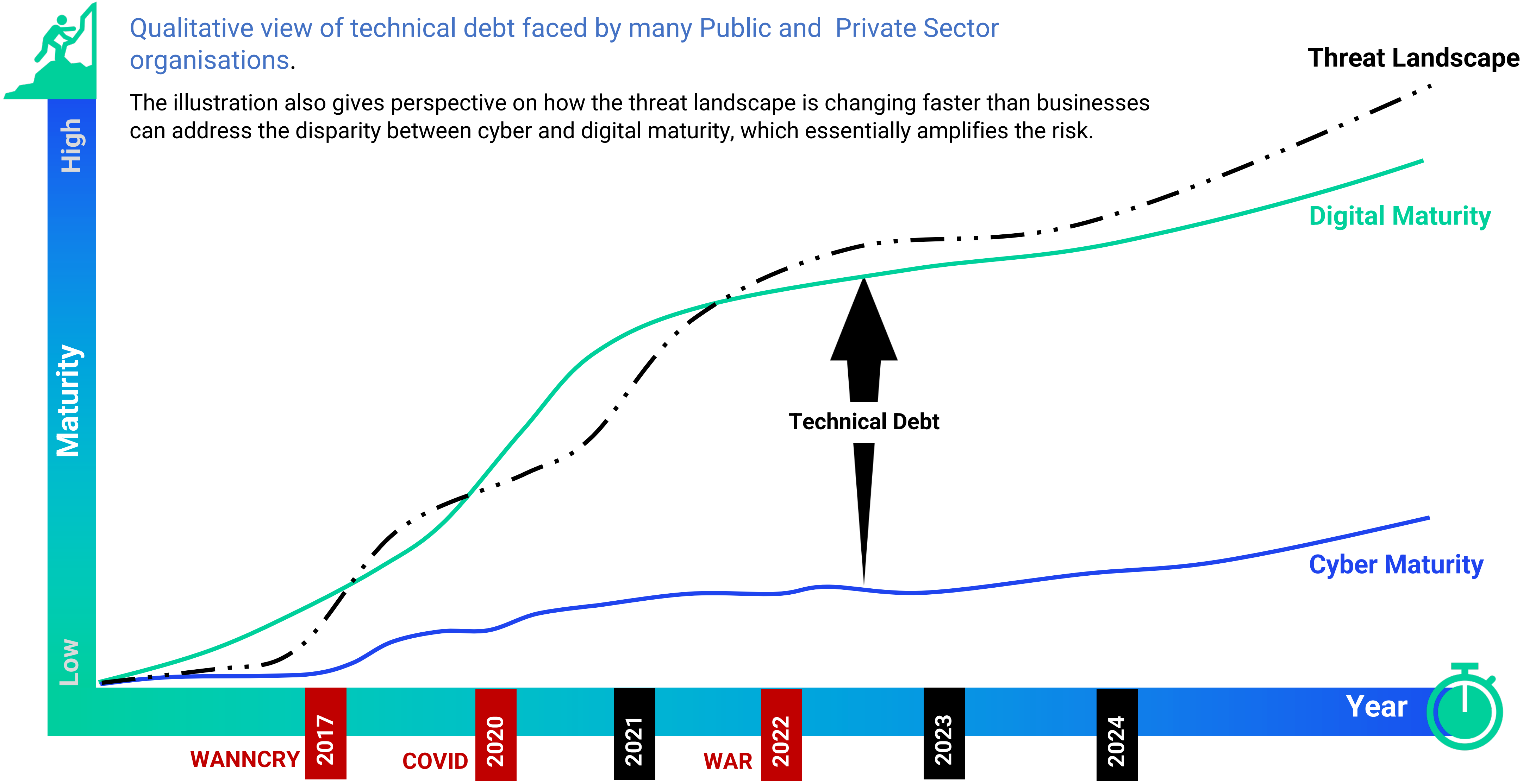
Source: Ponemon Institute

Cost of a data breach per capita

Maturity Paradox

Qualitative view of technical debt faced by many Public and Private Sector organisations.

The illustration also gives perspective on how the threat landscape is changing faster than businesses can address the disparity between cyber and digital maturity, which essentially amplifies the risk.

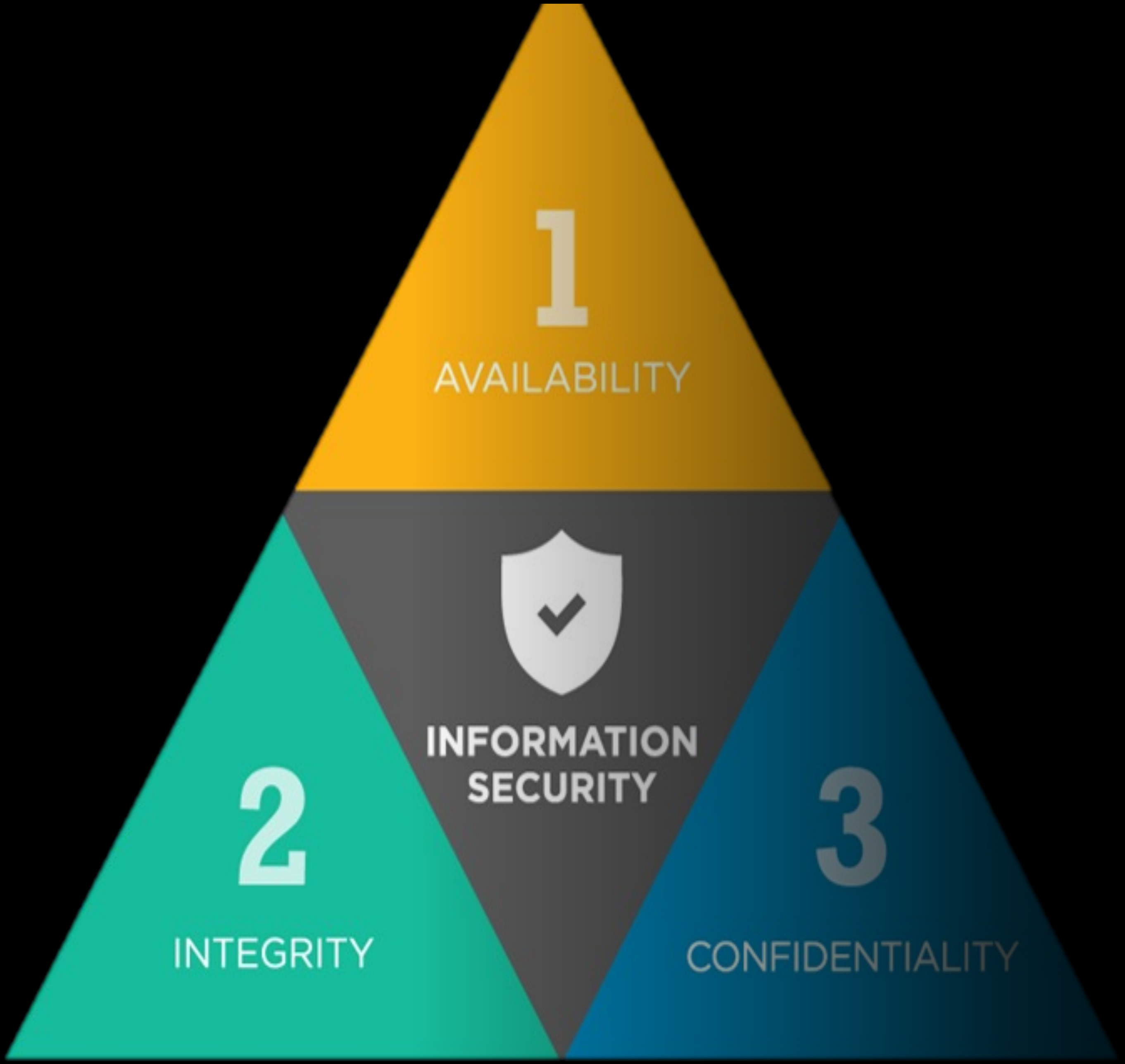


ATTACK SURFACE

CONCEPT, TYPES, TOOLS AND ATTACK SURFACE REDUCTION STRATEGIES

New Technologies Expand the Attack Surface

Cybersecurity



Cybersecurity
The CIA Triad

Protecting CIA data

Regulatory focus on CONFIDENTIALITY

BUT

What about INTEGRITY and AVAILABILITY?

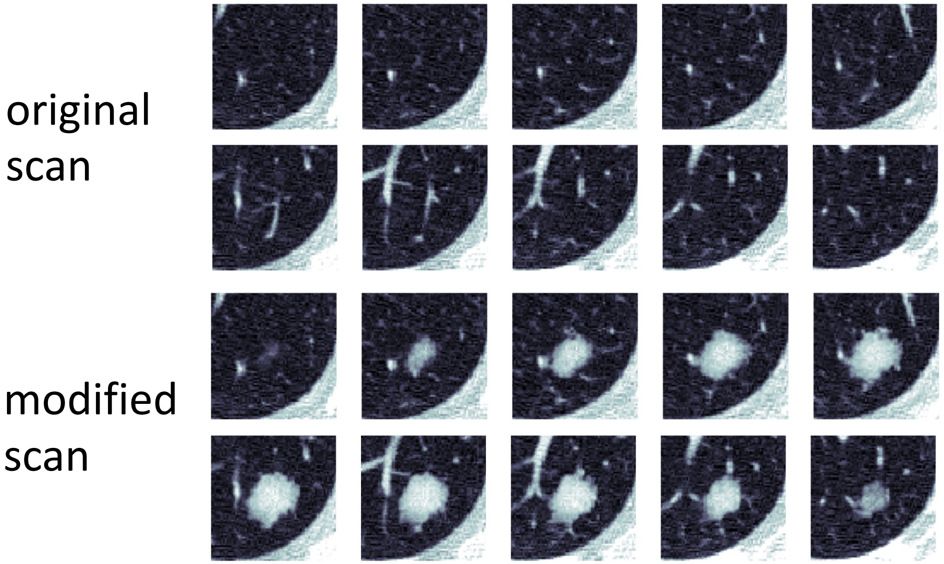
Integrity Attack

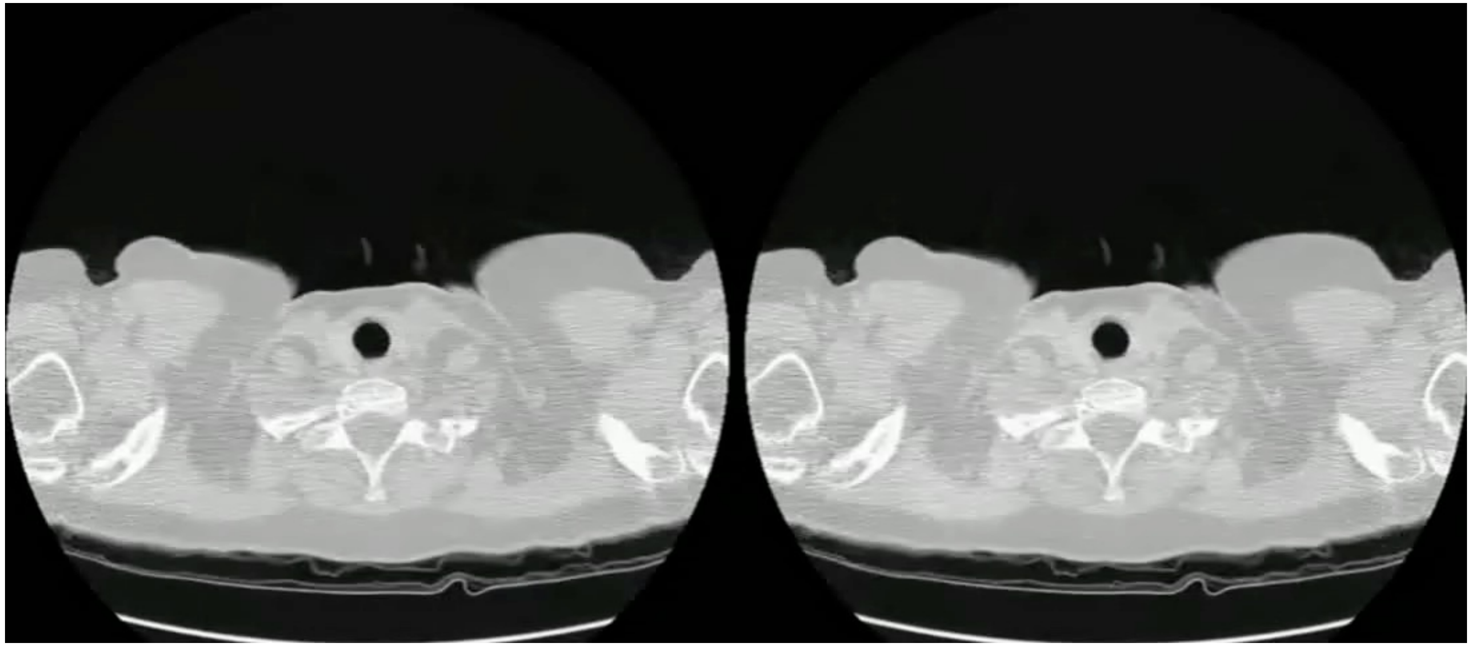
- What if a patient’s blood type or list of allergies was changed?
- Or their past medical history?
- Or their surgical instructions?

Attacks proven against Integrity of Medical Data

Hacking medical images

- Intercept images on network between scanner and PACS
- Add or subtract nodules on CT images using deep-learning





Original

Fake nodules

Radiologists fooled by:

- added fake nodules (99%)
- removed nodules (94%)

Ben-Gurion University of the Negev

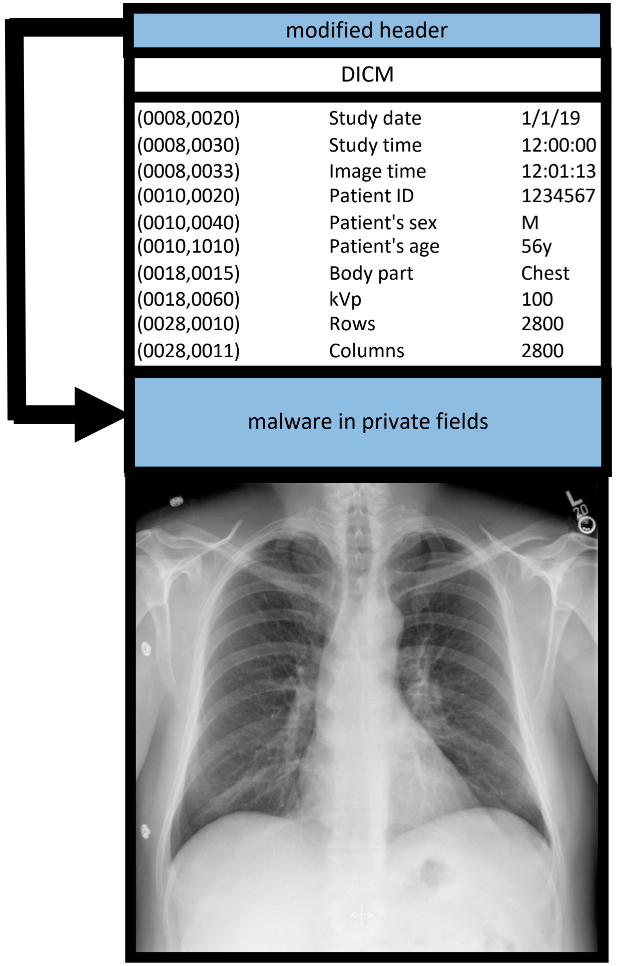
Mirsky et al, arXiv:1901.03597v2, Apr 2019

Medical data can be modified to contain malware

- Modified DICOM files
- Header (preamble)
  - used for dual personality files
  - replaced by executable file header
- Private fields
  - replaced by malware

CYLERA

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



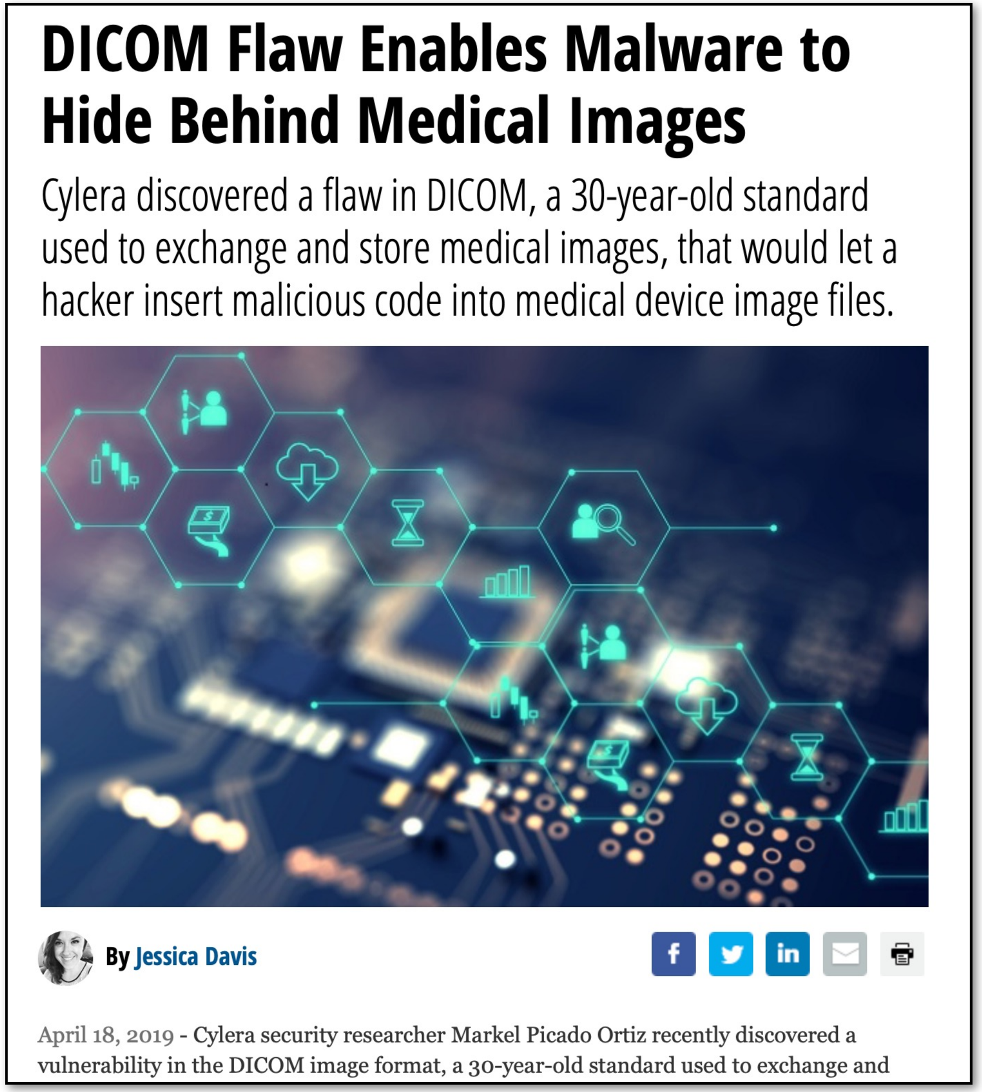
modified header

DICM

(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

malware in private fields

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

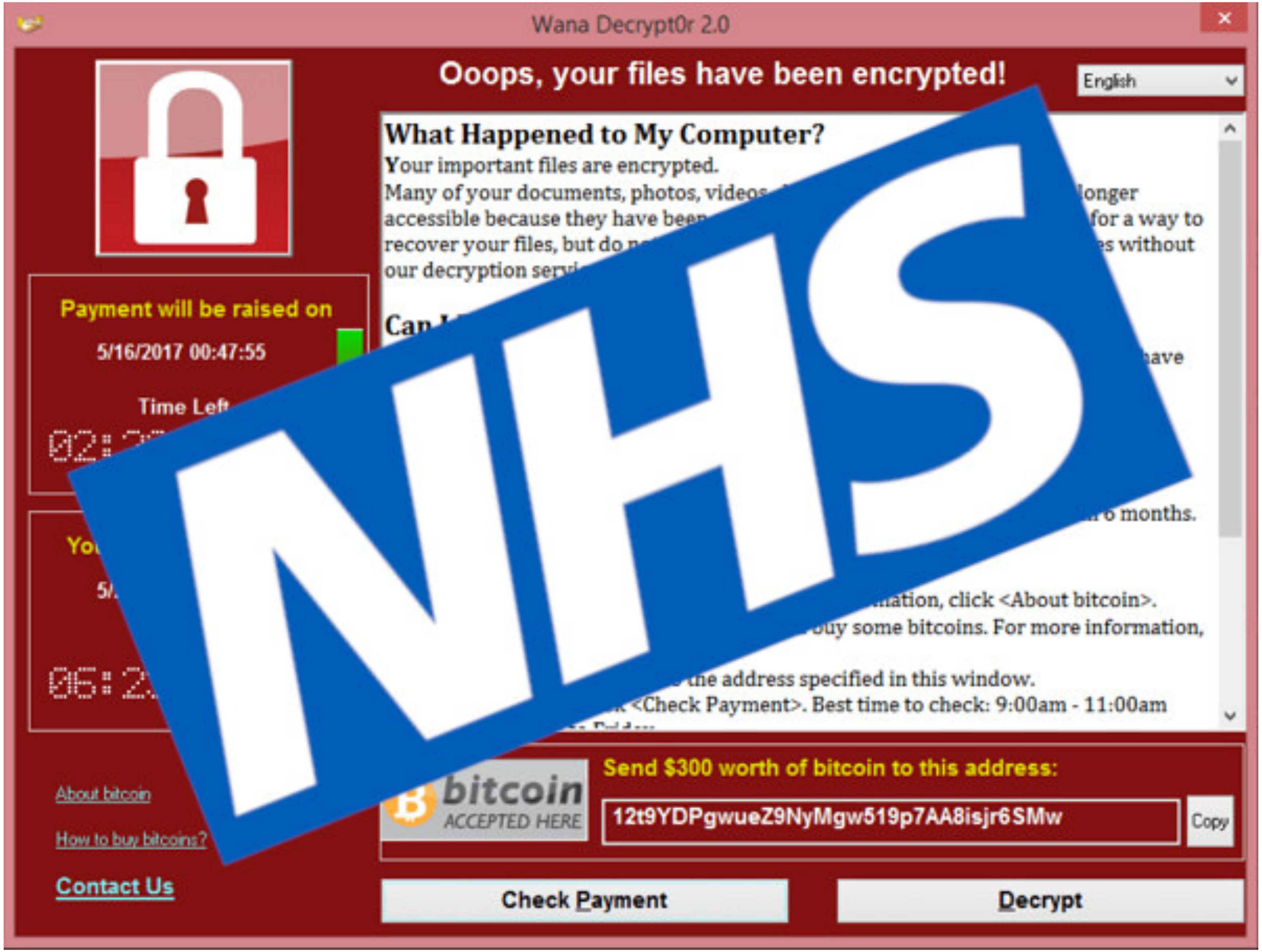
Availability Attack

What happens when IT goes down?

Ransomware – and other forms of cyber extortion

North Korean WannaCry attack shut down much of the UK NHS in 2017

WannaCry affected at least 81 of the 236 trusts across England - a third of NHS systems



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos longer accessible because they have been for a way to recover your files, but do n s without our decryption serv

Can I

ave

6 months.

mation, click <About bitcoin>.

uy some bitcoins. For more information,

the address specified in this window.

<Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:2

Yo

5/

06:2

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry Ransomware Costs Britain's NHS Approximately **$121M**

6 years later the NHS still has a massive elective surgery backlog

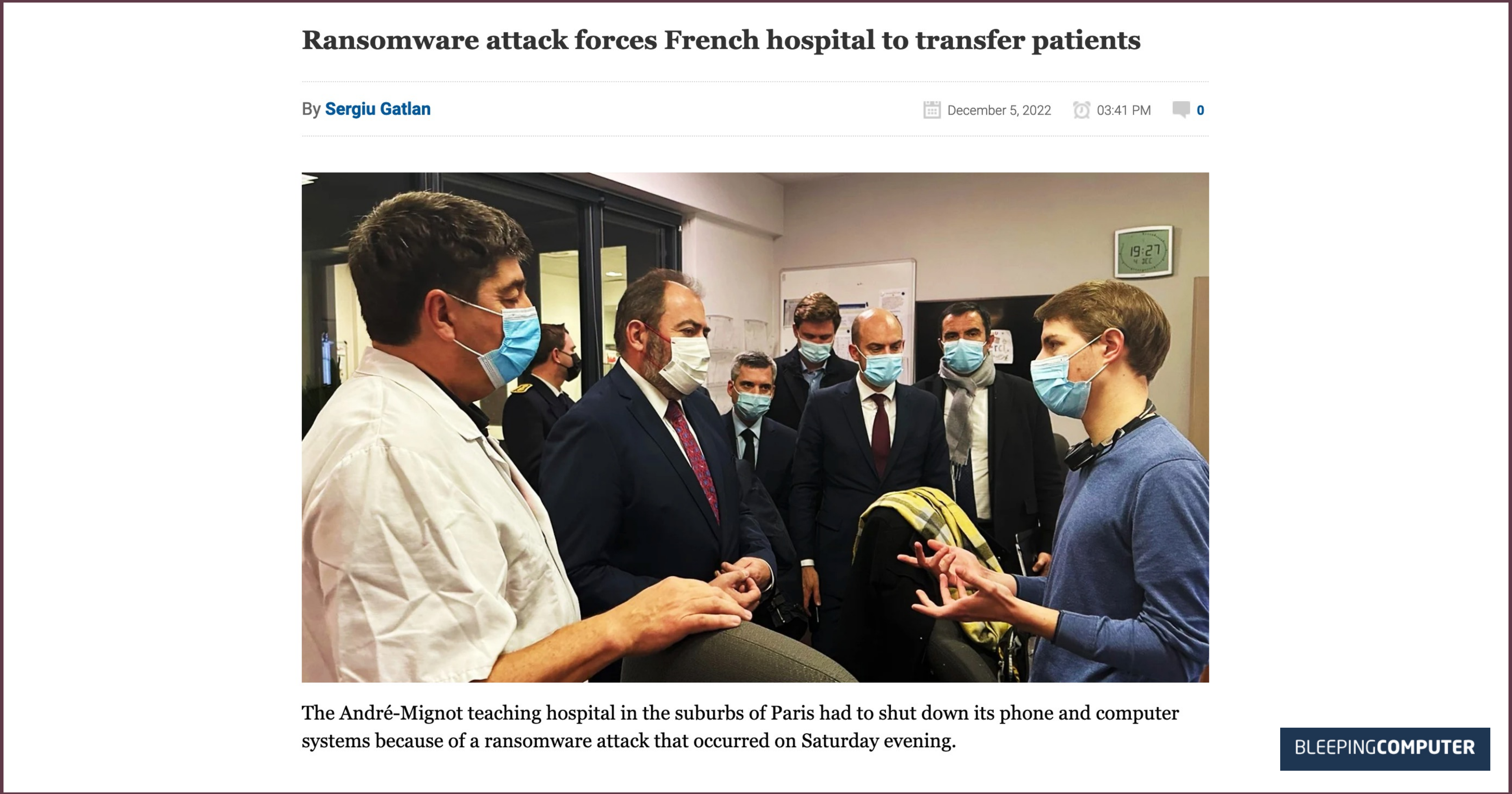
Irish Health System Executive attacked

CONTI

May 2021

Recovery costs for ransomware attack on Ireland's publicly funded healthcare system, is likely to total $600 million, says Paul Reid, HSE's director general.

What happens when someone needs to go to hospital, but the hospital has been hacked or held to ransom?



Ransomware attack forces French hospital to transfer patients

By **Sergiu Gatlan**

December 5, 2022 03:41 PM 0

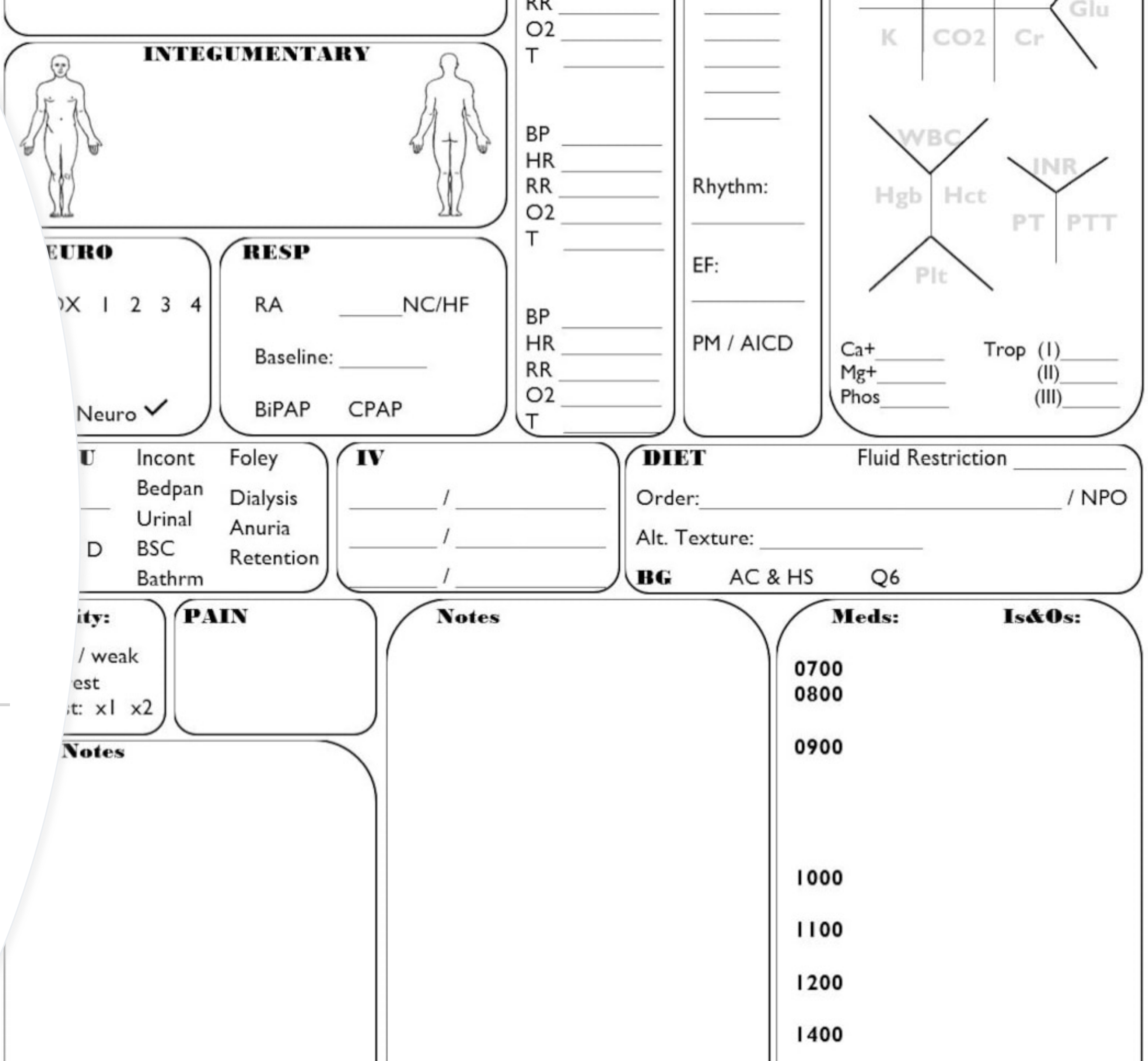
The André-Mignot teaching hospital in the suburbs of Paris had to shut down its phone and computer systems because of a ransomware attack that occurred on Saturday evening.

BLEEPING**COMPUTER**

Digital Health has turned the industry on its head.

Its totally dependent on IT and IoT

Few nurses under 45 can successfully revert to paper charts when tested



RR ______
O2 ______
T ______

K | CO2 | Cr | Glu

INTEGUMENTARY

BP ______
HR ______
RR ______
O2 ______
T ______

Rhythm: ______

EF: ______

PM / AICD

WBC | Hgb | Hct | Plt

INR | PT | PTT

EURO

X 1 2 3 4

Neuro ✓

RESP

RA ______NC/HF

Baseline: ______

BiPAP CPAP

BP ______
HR ______
RR ______
O2 ______
T ______

Ca+ ______
Mg+ ______
Phos ______

Trop (I)______
(II)______
(III)______

U

D

Incont
Bedpan
Urinal
BSC
Bathrm

Foley
Dialysis
Anuria
Retention

IV

______ / ______
______ / ______
______ / ______

DIET Fluid Restriction ______

Order: ______ / NPO

Alt. Texture: ______

BG AC & HS Q6

ity:

/ weak
est
t: x1 x2

PAIN

Notes

Notes

Meds: **Is&Os:**

0700
0800
0900
1000
1100
1200
1400

This places us at risk

Risk that if HIT / HIoT systems go down that patient treatment will suffer.

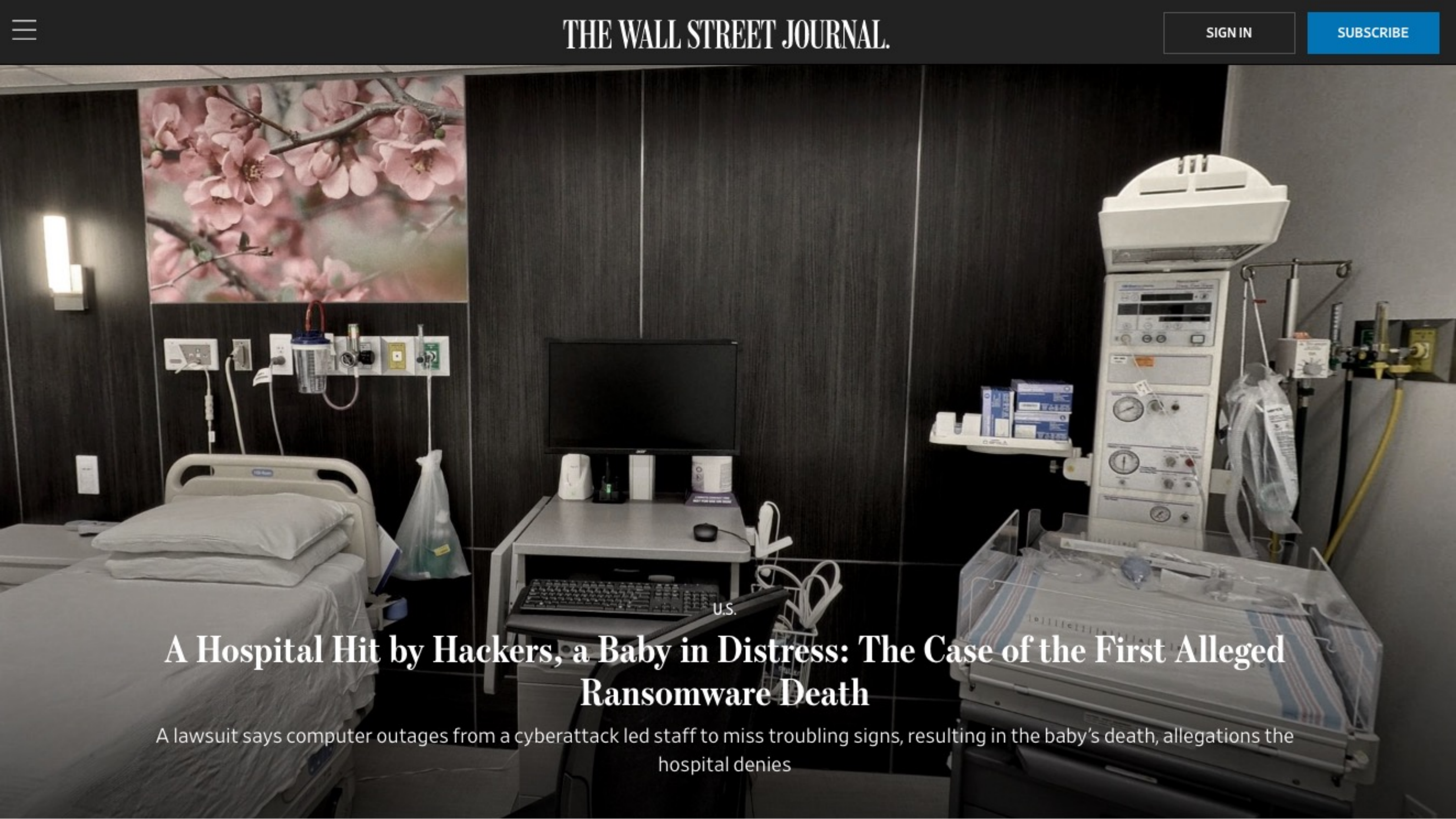
Failure of IT may also lead to patient safety concerns including increases in morbidity and even mortality.

Death by Ransomware

On the evening of 11 September 2020 paramedics in Düsseldorf, Germany, were alerted to an inbound ambulance and the deteriorating condition of a 78-year-old woman suffering from an aortic aneurysm.

Due to a ransomware attack and rapidly failing IT systems, the hospital was unable to accept the patient who was redirected to another facility 32km away in Wuppertal delaying the patient’s treatment by an hour. The patient died shortly after arrival in Wuppertal.

German authorities have yet to extradite the Russian suspects.



THE WALL STREET JOURNAL.

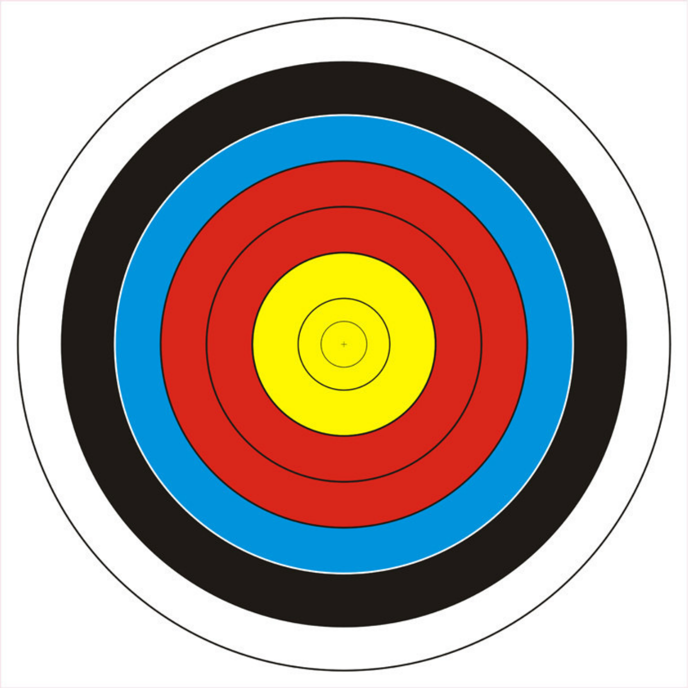
U.S.

A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death

A lawsuit says computer outages from a cyberattack led staff to miss troubling signs, resulting in the baby's death, allegations the hospital denies

Healthcare is being targeted

- Reported ransomware events against healthcare nearly doubled in 2020 Q3 (USA Today)
- Healthcare providers are typically more desperate to pay ransom to protect PHI and get their systems back up and running (Check Point)
- Healthcare networks typically require the use of older, unsupported software running on medical devices in particular



- UCSF reportedly paid $1.14M to recover their encrypted files in 2021
- UHS, one of the largest healthcare providers, suffered a Ryuk ransomware event, typically precipitated by commodity threats Emotet and Trickbot
- Events are not isolated to North America. India reported the second most ransomware attacks in Q3 2020

Between 2 and 3 US hospitals are being attacked by ransomware EVERY WEEK

That results in:

- Hospitals forced on divert
- Cancelation of appointments
- Patient safety concerns
- Loss of revenue
- Loss of reputation
- OCR investigation & fines
- Class Action Lawsuits

CYLERA

The average total cost of a breach in healthcare increased by 9.4% to **$10.1 million** in 2022.

IBM X-Force Cost of a Data Breach Report, 2022

According to HHS' Office for Civil Rights, cumulative healthcare breaches by 2021 have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records.

That equates to more than 94.63% of the 2021 population of the United States.

HHS OCR 2021

Cybercrime cost $6 Trillion USD in 2021

Cybersecurity Ventures Official Annual Cybercrime Report

By 2025 Cybercrime will cost $10.5 Trillion USD

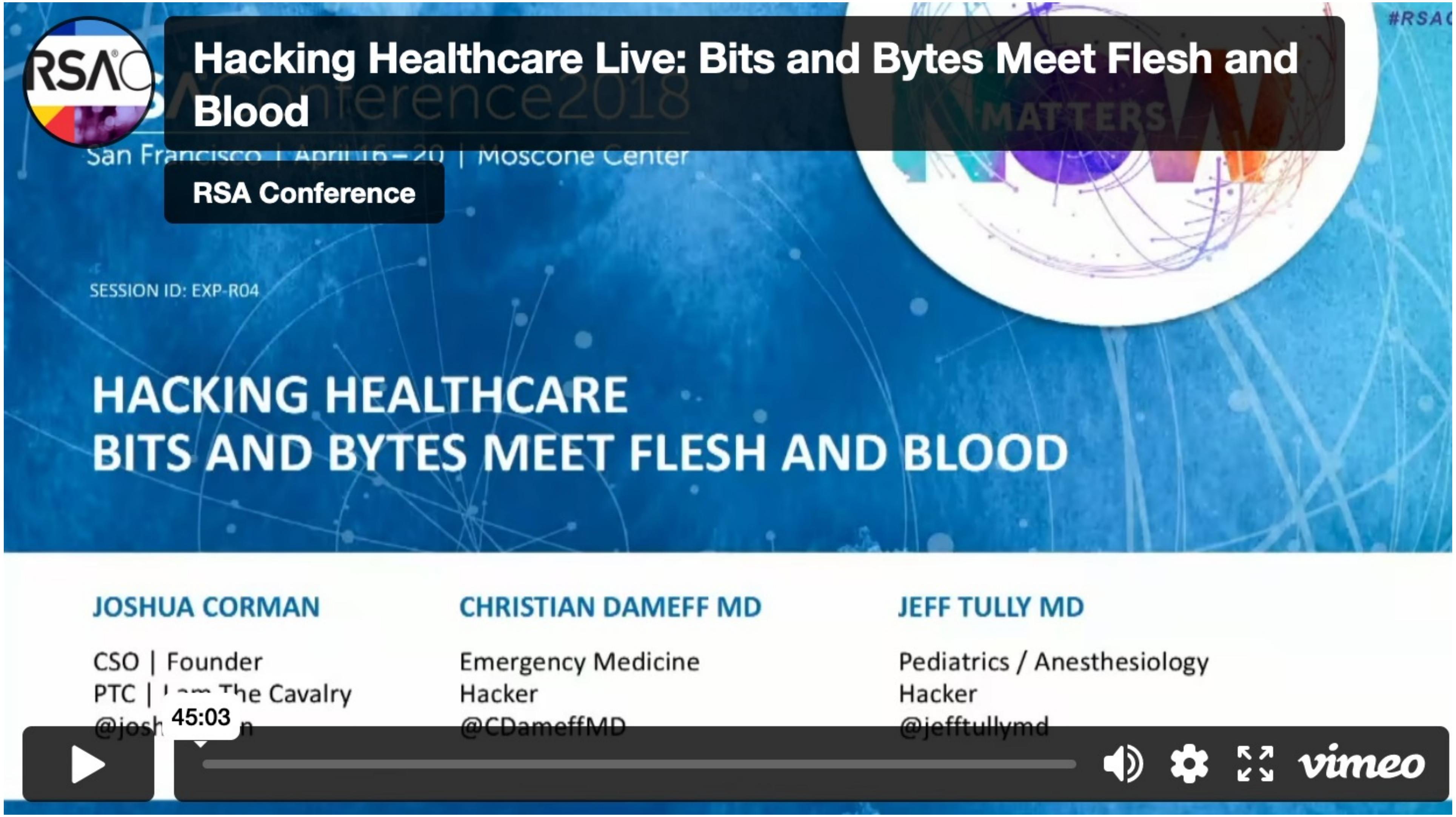
Cybercrime Magazine

A few departing thoughts to consider

Can you speak 'Cyber'?

Do clinicians know the right questions to ask?

Should we implicitly trust IT / IoT?



Hacking Healthcare Live: Bits and Bytes Meet Flesh and Blood

RSA Conference

RSA Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: EXP-R04

HACKING HEALTHCARE
BITS AND BYTES MEET FLESH AND BLOOD

JOSHUA CORMAN	CHRISTIAN DAMEFF MD	JEFF TULLY MD
CSO | Founder PTC | I am The Cavalry @joshcorman	Emergency Medicine Hacker @CDameffMD	Pediatrics / Anesthesiology Hacker @jefftullymd

Available to watch on my blog at https://cyberthoughts.org – search for ‘RSA’

Let’s Keep the Lights
on
&
Keep Patients Safe

Thank You

@rstaynings

richardstaynings

Richard Staynings

Chief Security Strategist, Cylera

https://cyberthoughts.org/

https://cylera.com

CYLERA

UNIVERSITY OF DENVER