Transformation, Security & Cyber resilience in Healthcare

Ivan Sanchez Lopez
CISO Grupo Sanitas
19/May/2022

For Business Purposes only

About me

Ivan Sanchez
CISO Grupo Sanitas Europe & LatAm

15 years experience in InfoSec:

- Consulting
- Telco
- Logistics
- Insurance & Healthcare

CISA, CISM, CISSP, ISO 27001 Lead Auditor

Key Take aways of the session

❑ Showcase how the Healthcare industry is reshaping itself completely by applying data-centric technologies and creating new business models.

❑ Analyze the increasing attack surface as IoT and medical devices are on the rise.

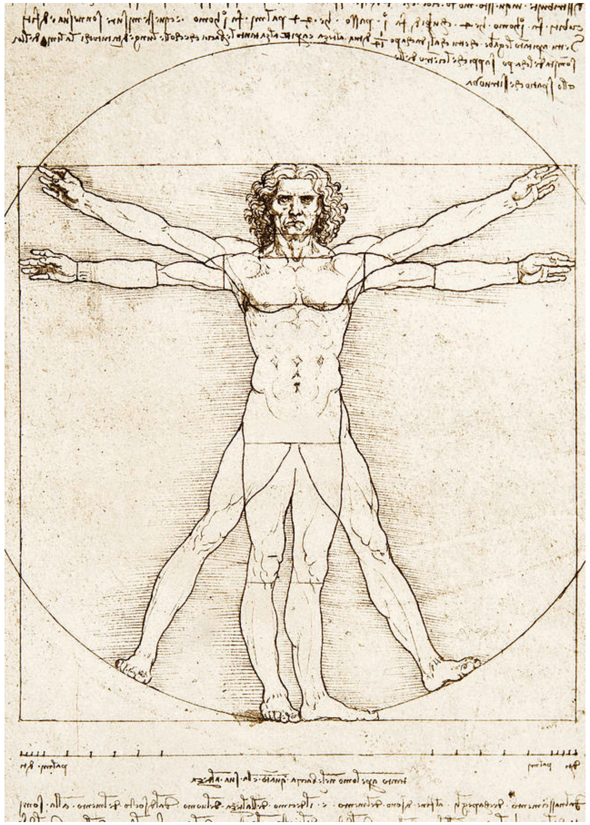
❑ Propose 4 fundamental pillars of an Information Security model to build resiliency for the current and future threats in Healthcare.

The inherent value of data

How lifestyle generates data

The inherent value of data

Body as a data generator



“Healthcare is not a science problem, it’s an information problem"

Thomas Goetz

The informational challenge

❑ The amount of data to collect and analyze is huge but technology is already available.

❑ Unlocking insights from medical records would be of high value and benefit to all key stakeholders in the health care ecosystem — patients, health care providers, payers, pharmaceutical companies and medical device manufacturers [1]

❑ Increasing costs from an aging population in developed countries creates pressure on National Healthcare systems: cost efficiencies through data management.

❑ Dr. Peter Diamandis (Health Longevity Inc): “*We’re going to see Apple and Amazon and Google and all the data-driven companies that are in our homes right now become our healthcare providers* “

❑ Amazon Alexa is compliant with U.S. HIPAA laws. There are more than 2,000 health wellness skills on its platform

[1] Source: *EY: Realising the value of health care data: a framework for the future*

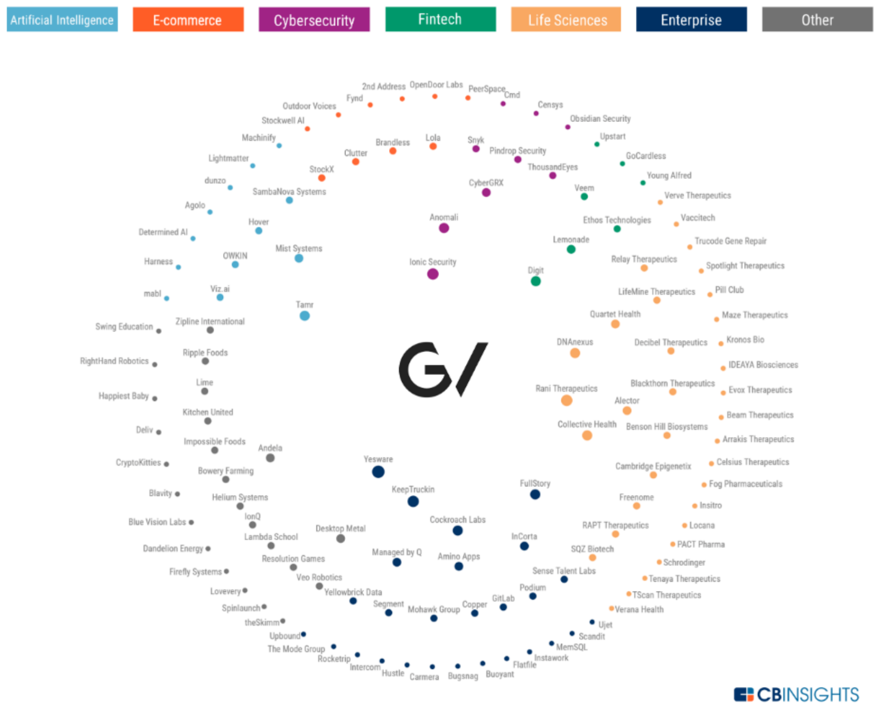
And the business opportunity

Investment in Healthcare is dramatically increasing

- ❑ Google Ventures has backed more than 30 health and life sciences companies since January 2018 (GV largest investing team) [1]
- ❑ Amazon, Berkshire Hathaway and J.P. Morgan partnership on “Project Haven”.
- ❑ Global End-User Spending on Wearable Devices to Total $62 Billion in 2021 (vs $32b in 2018) [2]
- ❑ Digital Health is expected to be the industry with the biggest growth in digital driven by mHeath initiatives.
- ❑ Internet of Medical Things (IoMT), 5G roll-out, advances in AI, blockchain for EHR,… will create multi-billion business opportunities.

WHERE GV INVESTS

Bubble size corresponds to total number of GV-backed investments in a company.
Companies included have had a GV-backed round since 1/1/2018 – 2019 YTD (11/8/2019).



Source: *The Future According To GV (https://www.cbinsights.com/research/gv-google-ventures-investments/)*

Source: *https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev*

Source: *https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev*

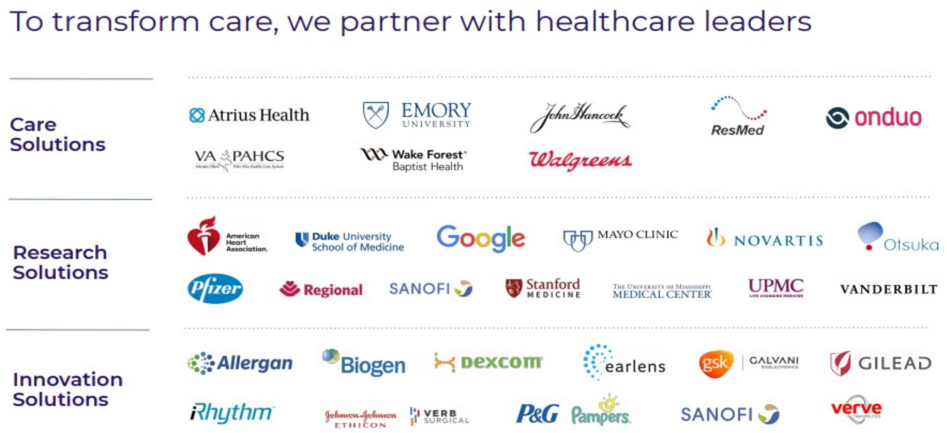
Sanitas
PARTE DE Bupa

Verily Life Sciences

formerly Google Life Sciences, est. Dec 2015

verily

Our mission is to make the world's health data useful so people enjoy healthier lives.



To transform care, we partner with healthcare leaders

Care Solutions
Atrius Health, EMORY UNIVERSITY, John Hancock, ResMed, onduo, VA PAHCS, Wake Forest Baptist Health, Walgreens

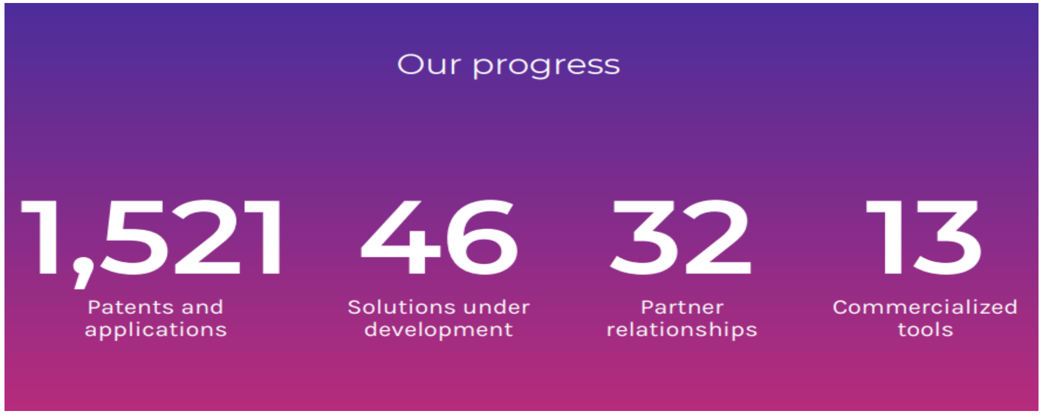
Research Solutions
American Heart Association, Duke University School of Medicine, Google, MAYO CLINIC, NOVARTIS, Otsuka, Pfizer, Regional, SANOFI, Stanford MEDICINE, The University of Mississippi MEDICAL CENTER, UPMC, VANDERBILT

Innovation Solutions
Allergan, Biogen, DEXCOM, earlens, gsk, GALVANI, GILEAD, Rhythm, Johnson & Johnson ETHICON, VERB SURGICAL, P&G, Pampers, SANOFI, verve

World-class investors

Alphabet, CAPITAL GROUP, ONTARIO TEACHERS' PENSION PLAN, SILVERLAKE, TEMASEK, T.RowePrice

$1.8B
External capital raised to date

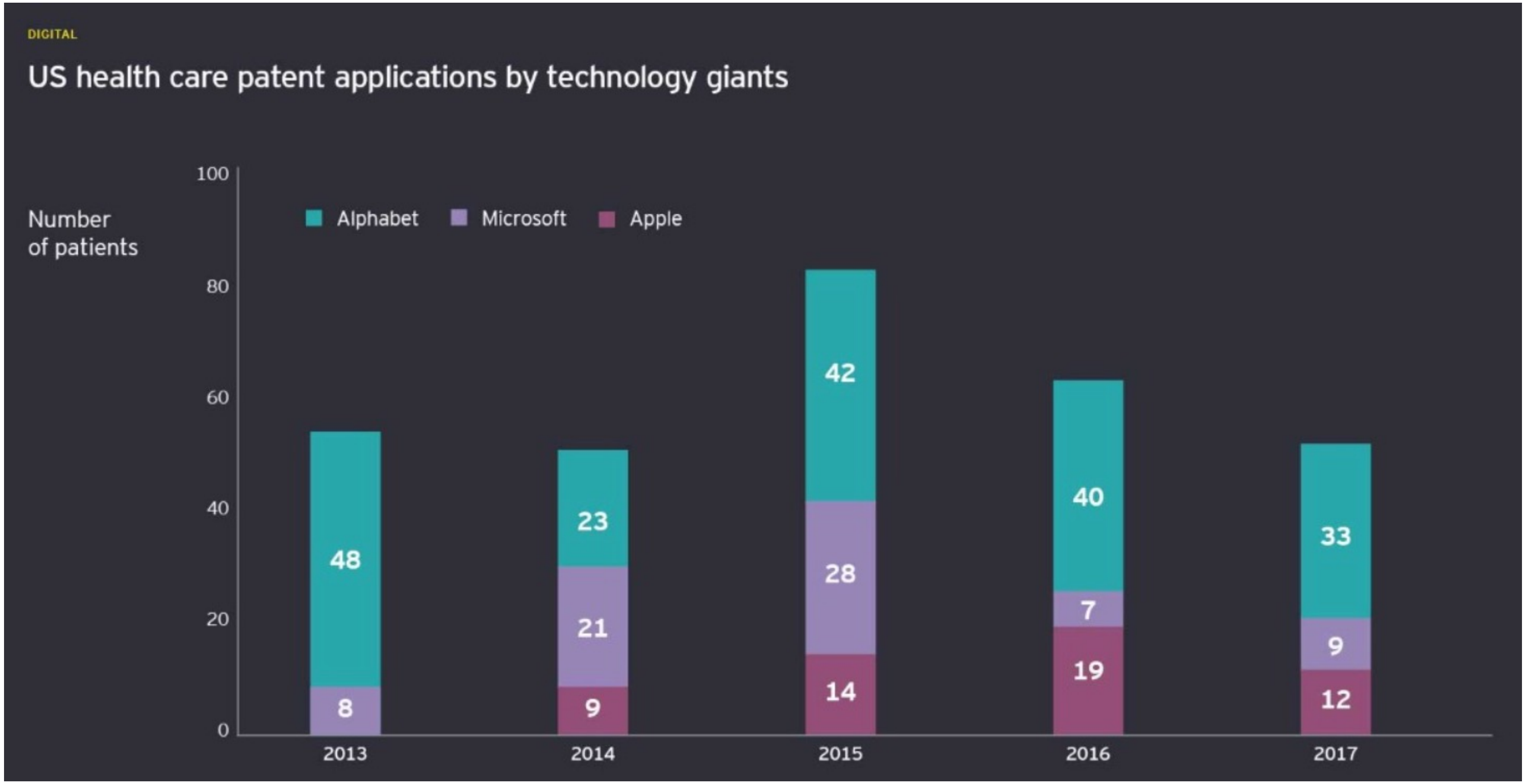


Our progress

1,521	46	32	13
Patents and applications	Solutions under development	Partner relationships	Commercialized tools

Source: *Verily's Corporate presentation at 38th JPMorgan Healthcare Conference, 13th Jan 2020*

Tech Giants entering into Healthcare



Source: EY Report: *When the human body is the biggest data platform, who will capture value?*

The technology is here already

Source: *Philips Lumify*
(https://www.usa.philips.com/healthcare/sites/lumify)

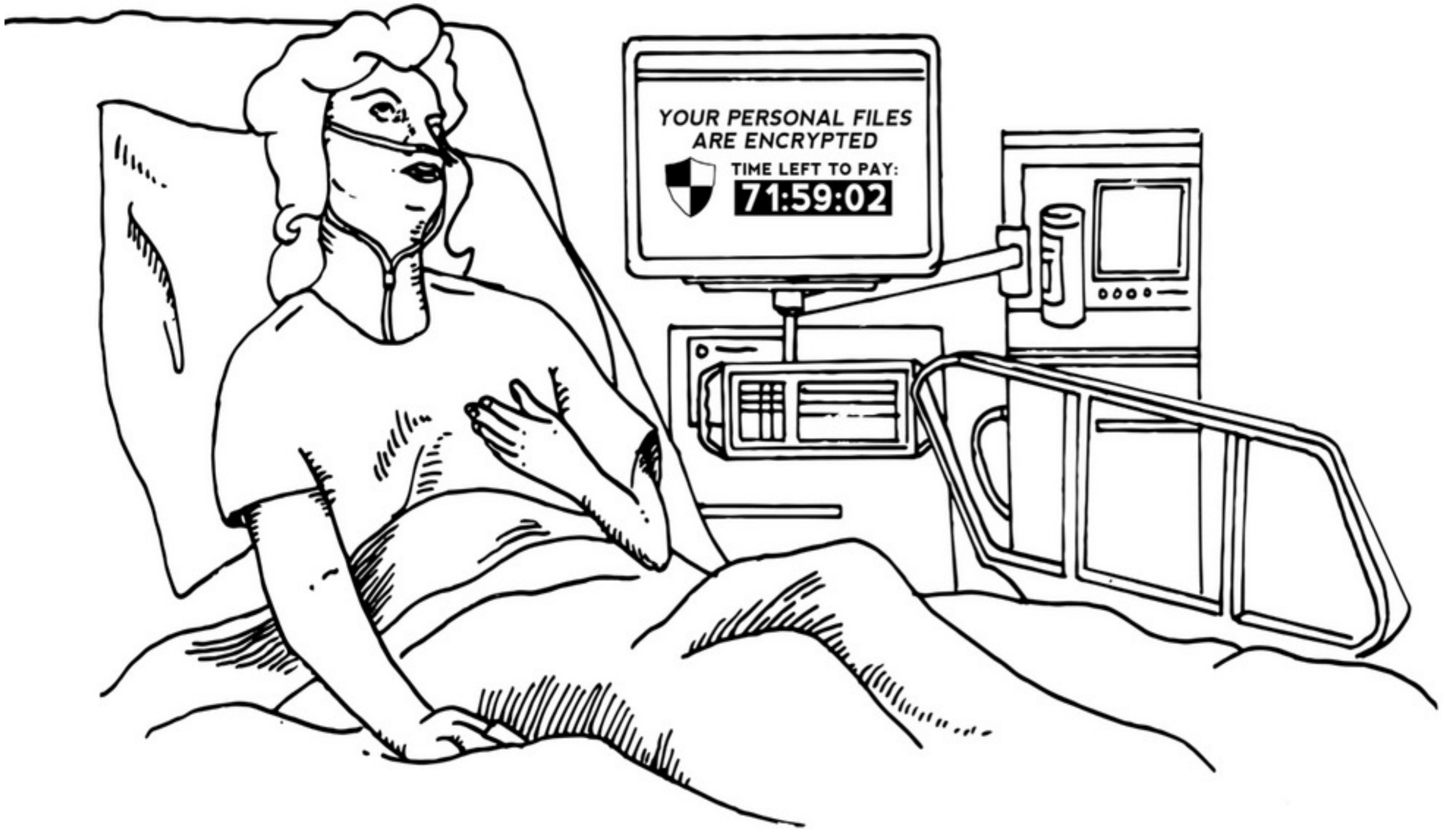
Information Security & Healthcare

A story of love & hate

- ❑ Information Security traditionally overlooked in Healthcare environments
- ❑ Huge dependency of unsecure third party equipment and legacy protocols (DICOM, etc) not subjected to regular updates
- ❑ Cultural approach still focused in Privacy rather than Cybersecurity
- ❑ Percentage of InfoSec investment not aligned with the increasing risk profile
- ❑ Traditional security solutions not fully suite to healthcare environments: **need to rethink our approach**

The battlefield

Always available?

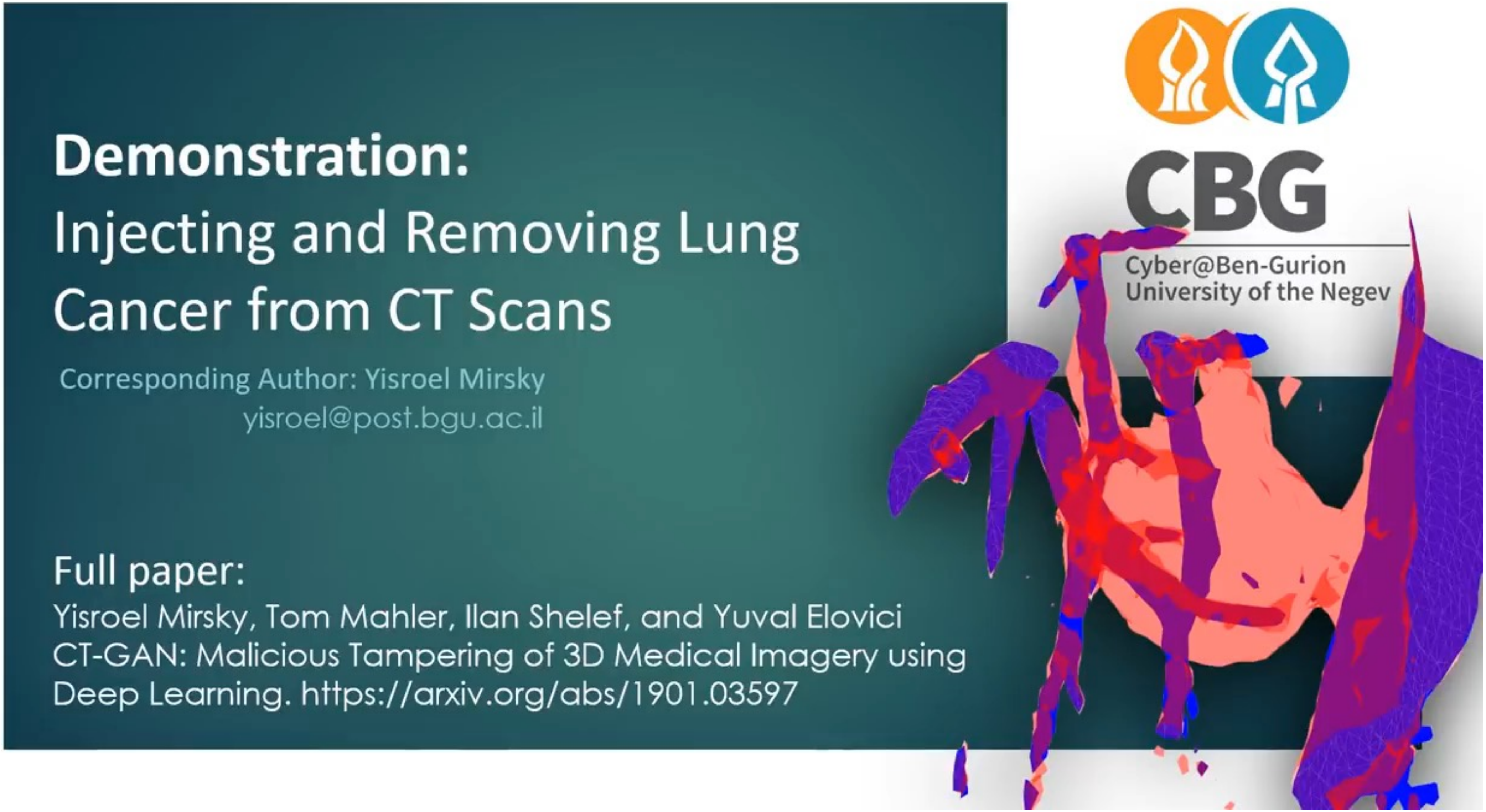


Source: *Engadget (https://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/)*

Always reliable?

Hackers manipulate lung cancer scans, fool radiologists and AI software in study

- ❑ Researchers at Ben-Gurion University (BGU) have developed malware to demonstrate vulnerabilities in CT (computerized tomography) and MRI (magnetic resonance imaging
- ❑ Medical scans were altered to add or remove images of tumours using a generative adversarial network (GAN) trained using medical images that are available for free on the internet.
- ❑ Radiologists and AI algorithms used to aid diagnosis misdiagnosed 99% of the scans that had been altered to add a tumour and 94% of those where cancerous cells were digitally removed.



Demonstration:

Injecting and Removing Lung Cancer from CT Scans

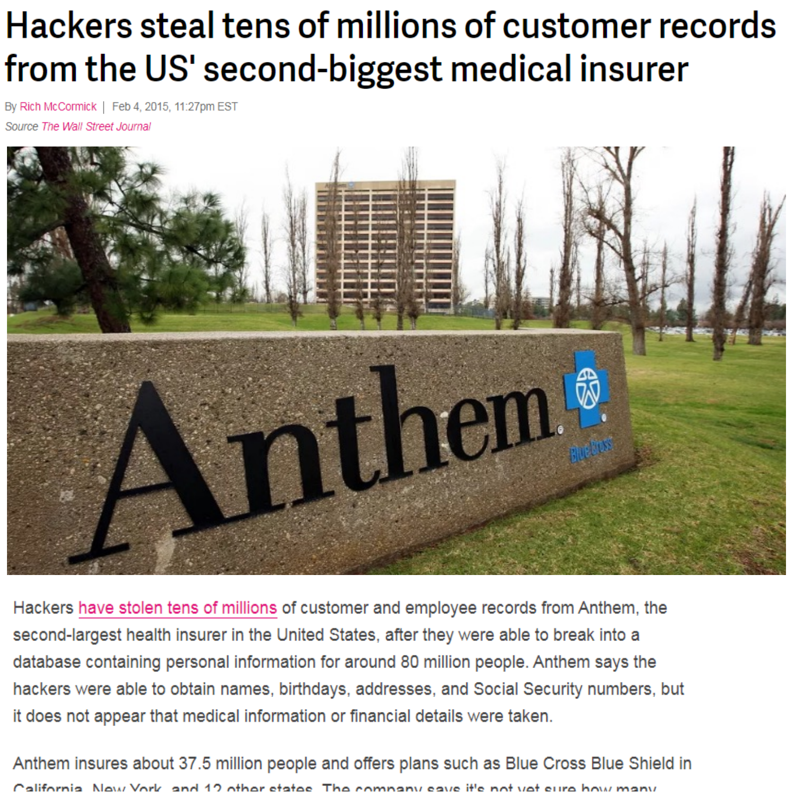
Corresponding Author: Yisroel Mirsky
yisroel@post.bgu.ac.il

Full paper:

Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici
CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. https://arxiv.org/abs/1901.03597

CBG
Cyber@Ben-Gurion
University of the Negev

Always private?



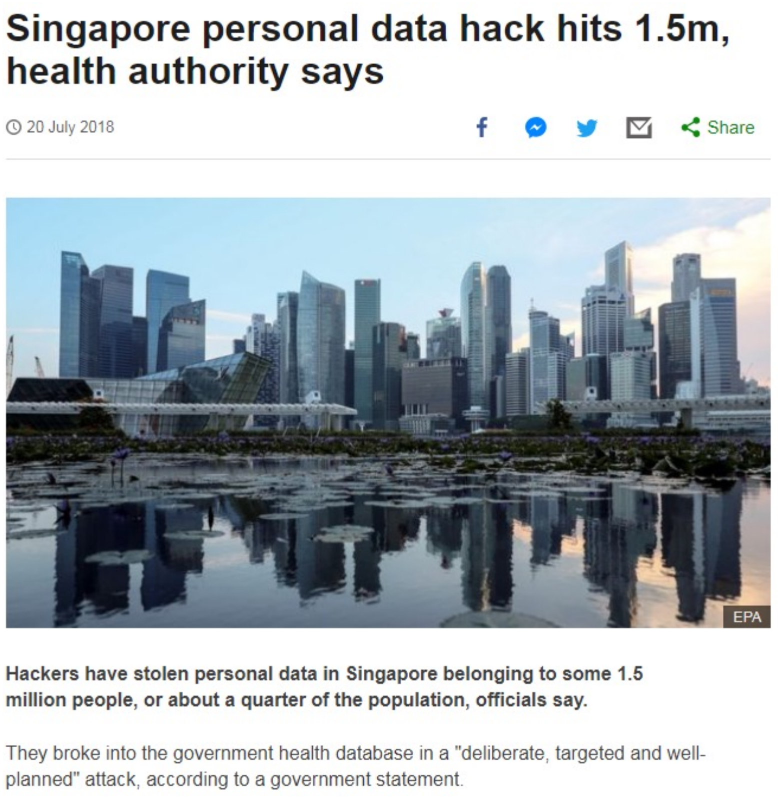
Hackers steal tens of millions of customer records from the US' second-biggest medical insurer

By Rich McCormick | Feb 4, 2015, 11:27pm EST

Source The Wall Street Journal

Hackers have stolen tens of millions of customer and employee records from Anthem, the second-largest health insurer in the United States, after they were able to break into a database containing personal information for around 80 million people. Anthem says the hackers were able to obtain names, birthdays, addresses, and Social Security numbers, but it does not appear that medical information or financial details were taken.

Anthem insures about 37.5 million people and offers plans such as Blue Cross Blue Shield in California, New York, and 12 other states. The company says it's not yet sure how many



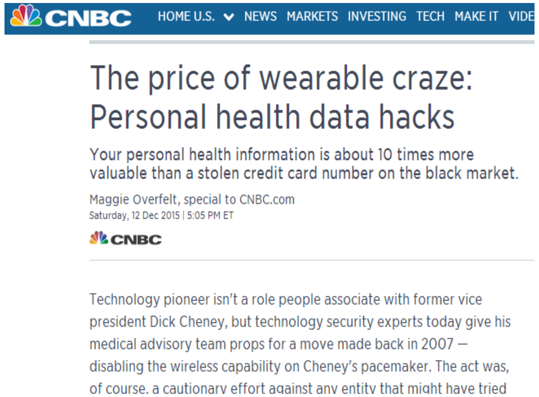
Singapore personal data hack hits 1.5m, health authority says

20 July 2018

Hackers have stolen personal data in Singapore belonging to some 1.5 million people, or about a quarter of the population, officials say.

They broke into the government health database in a "deliberate, targeted and well-planned" attack, according to a government statement.

PHI data is 10x valuable than financial data



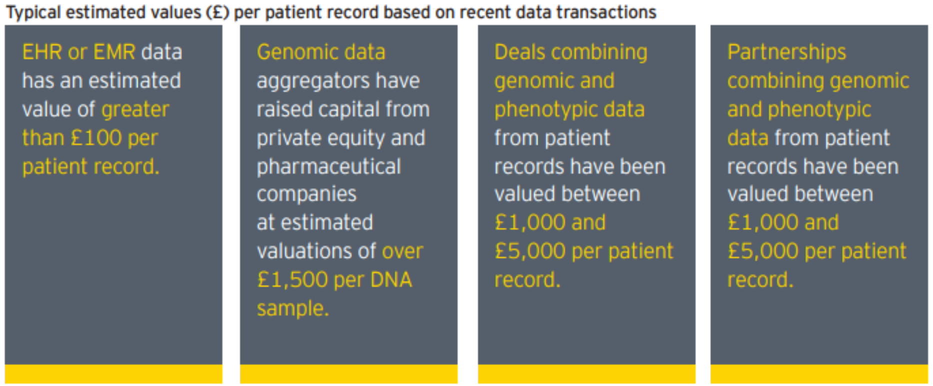
HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDE

The price of wearable craze: Personal health data hacks

Your personal health information is about 10 times more valuable than a stolen credit card number on the black market.

Maggie Overfelt, special to CNBC.com
Saturday, 12 Dec 2015 | 5:05 PM ET

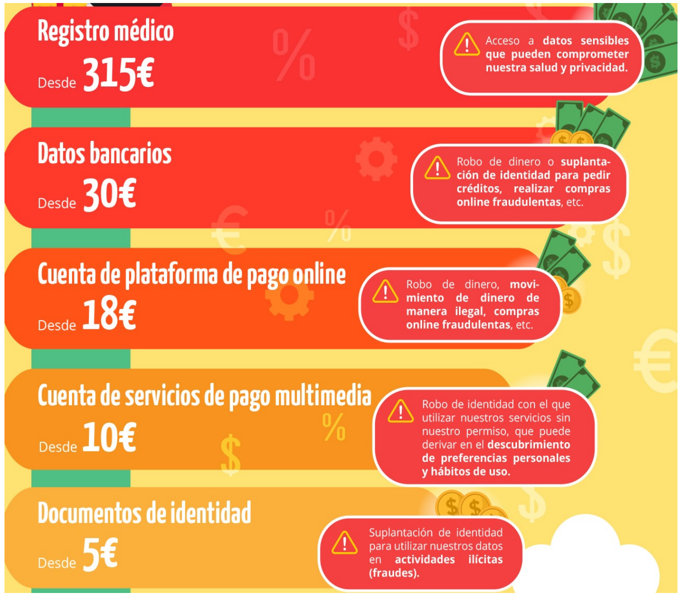
Technology pioneer isn't a role people associate with former vice president Dick Cheney, but technology security experts today give his medical advisory team props for a move made back in 2007 — disabling the wireless capability on Cheney's pacemaker. The act was, of course, a cautionary effort against any entity that might have tried



Typical estimated values (£) per patient record based on recent data transactions

EHR or EMR data has an estimated value of greater than £100 per patient record.	Genomic data aggregators have raised capital from private equity and pharmaceutical companies at estimated valuations of over £1,500 per DNA sample.	Deals combining genomic and phenotypic data from patient records have been valued between £1,000 and £5,000 per patient record.	Partnerships combining genomic and phenotypic data from patient records have been valued between £1,000 and £5,000 per patient record.

Figure 4. Observed values (£) per patient record based on recent data transactions (January 2019)



Registro médico
Desde 315€
Acceso a **datos sensibles que pueden comprometer nuestra salud y privacidad.**

Datos bancarios
Desde 30€
Robo de dinero o **suplantación de identidad para pedir créditos, realizar compras online fraudulentas**, etc.

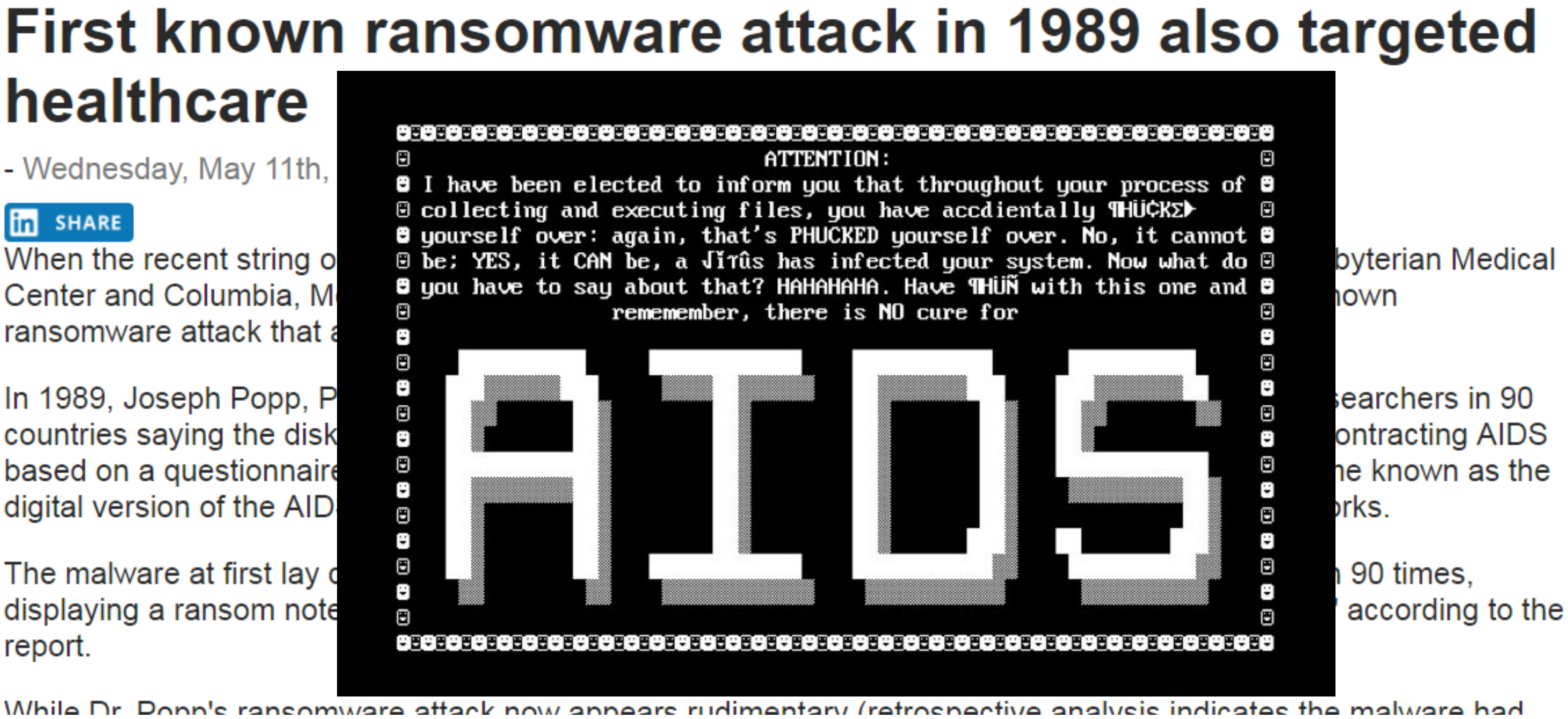
Cuenta de plataforma de pago online
Desde 18€
Robo de dinero, **movimiento de dinero de manera ilegal, compras online fraudulentas**, etc.

Cuenta de servicios de pago multimedia
Desde 10€
Robo de identidad con el que utilizar nuestros servicios sin nuestro permiso, que puede derivar en el **descubrimiento de preferencias personales y hábitos de uso.**

Documentos de identidad
Desde 5€
Suplantación de identidad para utilizar nuestros datos en **actividades ilícitas (fraudes).**

Did you know...

The first ransomware attack (1989)



First known ransomware attack in 1989 also targeted healthcare

- Wednesday, May 11th,

When the recent string o ... byterian Medical
Center and Columbia, M ... own
ransomware attack that a

In 1989, Joseph Popp, P ... earchers in 90
countries saying the disk ... ontracting AIDS
based on a questionnaire ... e known as the
digital version of the AID ... rks.

The malware at first lay c ... 90 times,
displaying a ransom note ... ' according to the
report.

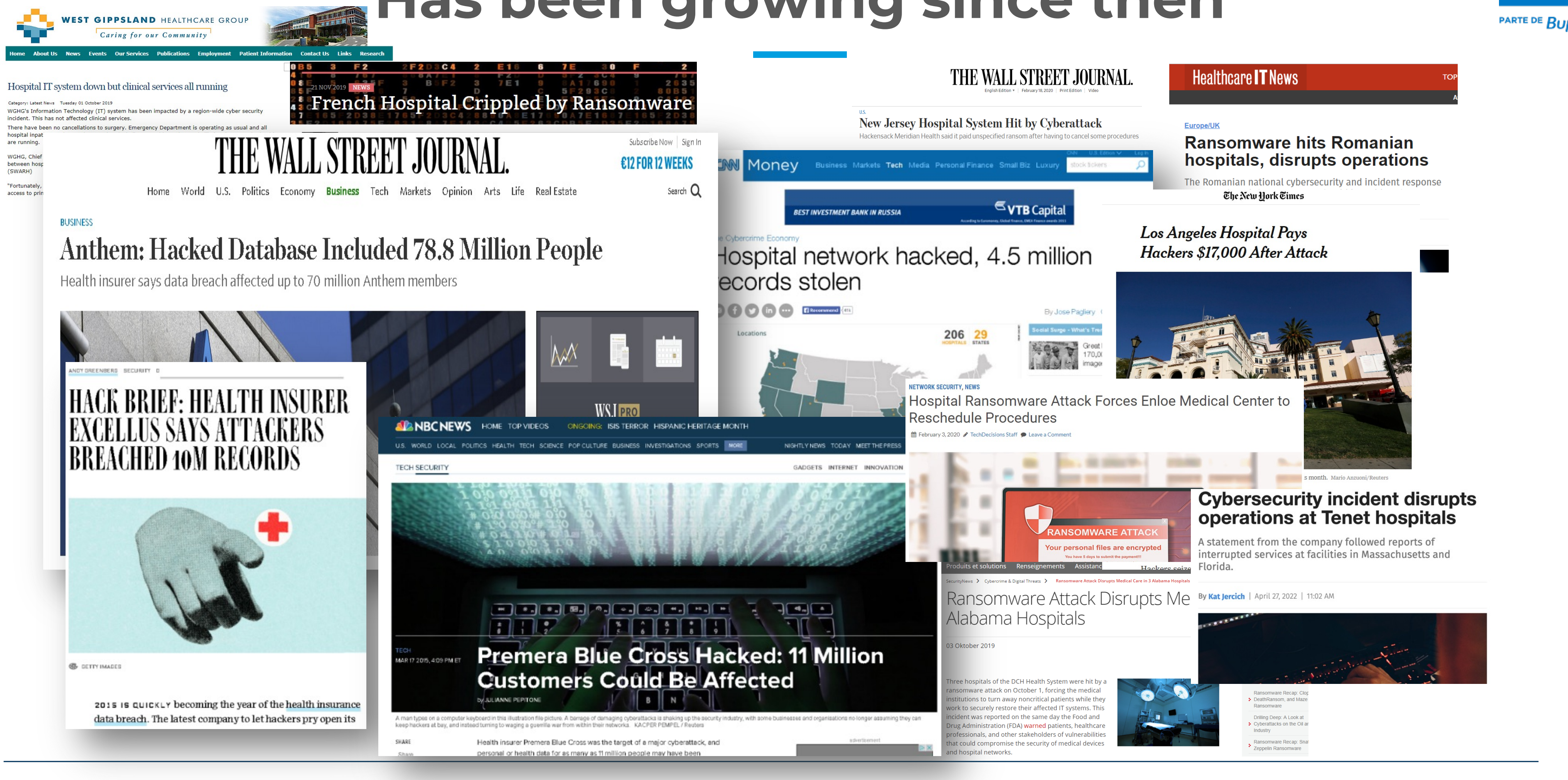
While Dr. Popp's ransomware attack now appears rudimentary (retrospective analysis indicates the malware had

```
                              ATTENTION:
 I have been elected to inform you that throughout your process of
 collecting and executing files, you have accdientally ¶HÜÇKΣ▶
 yourself over: again, that's PHUCKED yourself over. No, it cannot
 be; YES, it CAN be, a √ïrûs has infected your system. Now what do
 you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
           rememember, there is NO cure for

                               AIDS
```

Source: *https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)*

Has been growing since then



WEST GIPPSLAND HEALTHCARE GROUP
Caring for our Community

Home About Us News Events Our Services Publications Employment Patient Information Contact Us Links Research

Hospital IT system down but clinical services all running

Category: Latest News Tuesday 01 October 2019

WGHG's Information Technology (IT) system has been impacted by a region-wide cyber security incident. This has not affected clinical services.

There have been no cancellations to surgery. Emergency Department is operating as usual and all hospital inpat

are running.

WGHG, Chief

between hosp

(SWARH)

"Fortunately,

access to prin

21 NOV 2019 NEWS

French Hospital Crippled by Ransomware

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

€12 FOR 12 WEEKS

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate Search

BUSINESS

Anthem: Hacked Database Included 78.8 Million People

Health insurer says data breach affected up to 70 million Anthem members

WSJ PRO

ANDY GREENBERG SECURITY

HACK BRIEF: HEALTH INSURER EXCELLUS SAYS ATTACKERS BREACHED 10M RECORDS

GETTY IMAGES

2015 IS QUICKLY becoming the year of the health insurance data breach. The latest company to let hackers pry open its

NBC NEWS HOME TOP VIDEOS ONGOING: ISIS TERROR HISPANIC HERITAGE MONTH

U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATIONS SPORTS MORE NIGHTLY NEWS TODAY MEET THE PRESS

TECH SECURITY GADGETS INTERNET INNOVATION

TECH
MAR 17 2015, 4:09 PM ET

Premera Blue Cross Hacked: 11 Million Customers Could Be Affected

by JULIANNE PEPITONE

A man types on a computer keyboard in this illustration file picture. A barrage of damaging cyberattacks is shaking up the security industry, with some businesses and organisations no longer assuming they can keep hackers at bay, and instead turning to waging a guerrilla war from within their networks. KACPER PEMPEL / Reuters

SHARE

Share

Health insurer Premera Blue Cross was the target of a major cyberattack, and personal or health data for as many as 11 million people may have been

advertisement

THE WALL STREET JOURNAL.

English Edition ▾ | February 18, 2020 | Print Edition | Video

U.S.

New Jersey Hospital System Hit by Cyberattack

Hackensack Meridian Health said it paid unspecified ransom after having to cancel some procedures

CNN Money Business Markets Tech Media Personal Finance Small Biz Luxury

CNN U.S. Edition Log In

stock tickers

BEST INVESTMENT BANK IN RUSSIA VTB Capital

e Cybercrime Economy

Hospital network hacked, 4.5 million ecords stolen

Recommend 41k

By Jose Pagliery

Locations

206 HOSPITALS 29 STATES

Social Surge - What's Tre

Great 170,0 image

Healthcare IT News

TOP

Europe/UK

Ransomware hits Romanian hospitals, disrupts operations

The Romanian national cybersecurity and incident response

The New York Times

Los Angeles Hospital Pays Hackers $17,000 After Attack

s month. Mario Anzuoni/Reuters

NETWORK SECURITY, NEWS

Hospital Ransomware Attack Forces Enloe Medical Center to Reschedule Procedures

February 3, 2020 TechDecisions Staff Leave a Comment

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!

Produits et solutions Renseignements Assistanc

Hackers seize

SecurityNews > Cybercrime & Digital Threats > Ransomware Attack Disrupts Medical Care in 3 Alabama Hospitals

Ransomware Attack Disrupts Me Alabama Hospitals

03 Oktober 2019

Three hospitals of the DCH Health System were hit by a ransomware attack on October 1, forcing the medical institutions to turn away noncritical patients while they work to securely restore their affected IT systems. This incident was reported on the same day the Food and Drug Administration (FDA) warned patients, healthcare professionals, and other stakeholders of vulnerabilities that could compromise the security of medical devices and hospital networks.

- Ransomware Recap: Clop DeathRansom, and Maze Ransomware
- Drilling Deep: A Look at Cyberattacks on the Oil ar Industry
- Ransomware Recap: Sna Zeppelin Ransomware

Cybersecurity incident disrupts operations at Tenet hospitals

A statement from the company followed reports of interrupted services at facilities in Massachusetts and Florida.

By Kat Jercich | April 27, 2022 | 11:02 AM

With unexpected impacts

- ❑ On 14th May 2021, the HSE was subjected to a serious criminal cyberattack, through the infiltration of IT systems using Conti Ransomware.
- ❑ With over 80% of IT infrastructure impacted and the loss of key patient information and diagnostics, this resulted in severe impacts on the health service and the provision of care.
- ❑ The HSE employed the assistance of An Garda Síochána, the National Cyber Security Centre, Interpol and the Irish Defence Forces.

Conti cyber attack on the HSE

Independent Post Incident Review

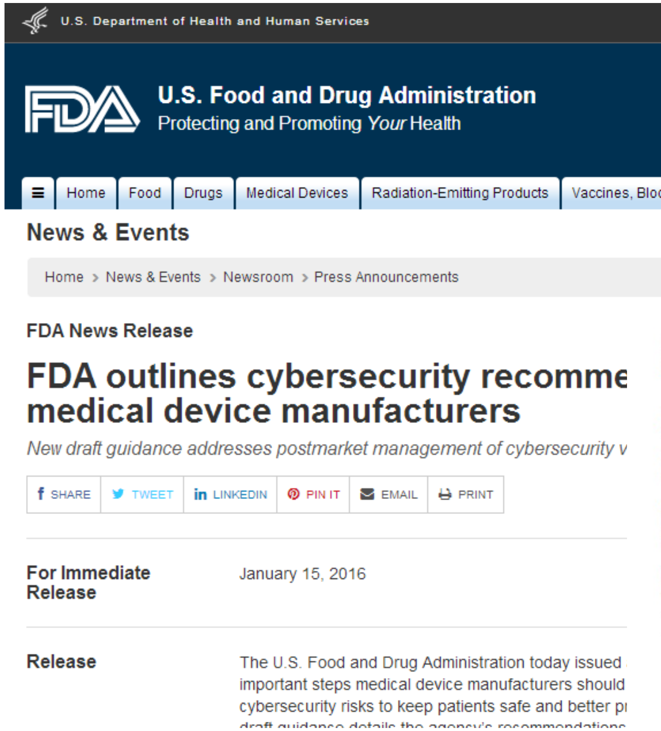
Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team

03 December 2021

Redacted

Conti cyber-attack on the HSE Independent Post Incident Review

Regulations still developing



U.S. Department of Health and Human Services
U.S. Food and Drug Administration
Protecting and Promoting *Your* Health
A to Z Index
Search FI
≡
Home
Food
Drugs
Medical Devices
Radiation-Emitting Products
Vaccines, Blood & Biologics
Animal & Vete

News & Events

Home > News & Events > Newsroom > Press Announcements

FDA News Release

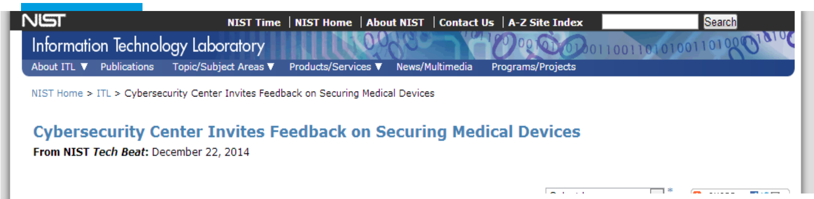
FDA outlines cybersecurity recomme medical device manufacturers

New draft guidance addresses postmarket management of cybersecurity v

SHARE
TWEET
LINKEDIN
PIN IT
EMAIL
PRINT

For Immediate Release January 15, 2016

Release The U.S. Food and Drug Administration today issued important steps medical device manufacturers should cybersecurity risks to keep patients safe and better pı draft guidance details the agency's recommendations



NIST Home > ITL > Cybersecurity Center Invites Feedback on Securing Medical Devices

Cybersecurity Center Invites Feedback on Securing Medical Devices

From NIST *Tech Beat*: December 22, 2014

Contact: Jennifer Huergo
301-975-6343

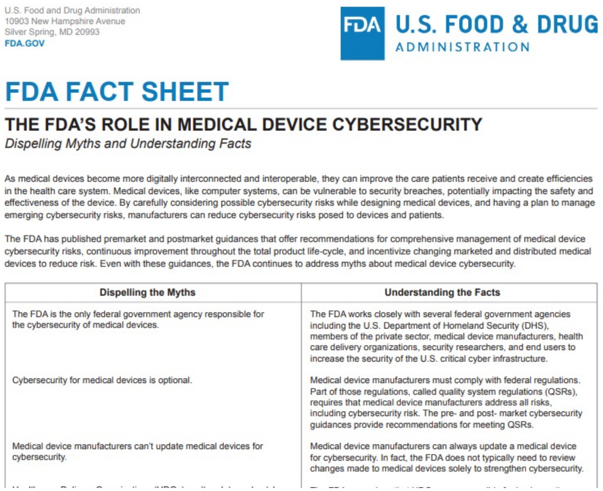
Hospitals are increasingly using networked technology to improve the accur system. A networked infusion pump—a device used to convey fluids, drugs a the device's programming as well as automated cross checks against pharm

e con

e Nat
lities t

ite of
manu
g the

enter
ogical



U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

FDA U.S. FOOD & DRUG ADMINISTRATION

FDA FACT SHEET

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.

ICT security certification opportunities in the healthcare sector

V1.0
DECEMBER 2018

www.enisa.europa.eu
European Union Agency For Network and Information Security

4 basic pillars for a Healthcare InfoSec model

Endpoint & Infrastructure protection

Understand your threat profile and attack surface

Identify key assets within the environment, focus on (m)IoT

Patching and avoid outdated SW versions.

Consider advanced protection, far beyond traditional AV.

Isolate environments. Apply network segmentation

Secure methods for remote access

Categorize and protect entry points to your infrastructure

Apply advanced network traffic analytics

Employee Awareness

The weakest factor is always the human factor: regular awareness programmes.

Understand employee motivations and help them to comply with security policies.

Issue guidelines to employees on Information Security.

Best practices and regulations

Industry guidelines and support for their implementation

Sponsor cyber measures within manufacturing community

Drive a collaborative approach and good Cybersecurity practices

Ensure strong end-to-end encryption for medical devices

No-trust policy by default when connecting devices

Firmware cryptographically signed as mandatory

Research

R&D investment

Promoting adoption of vulnerability disclosure policies

Translating the Common Vulnerability Scoring System (CVSS) for medical devices

Bug-bounty initiatives for medhacking

Manufacturers liability for unsecure products

Thanks

https://www.linkedin.com/in/ivansanchezlopez