Managing Cybersecurity in Healthcare during a pandemic

Ivan Sanchez Lopez
CISO Sanitas
12/05/2021

About me

- CISO Grupo Sanitas Europe & LatAm (part of Bupa Group)
- 13+ years experience in InfoSec:
  - Consulting
  - Telco
  - Logistics
  - Insurance & Healthcare
- CISA, CISM, CISSP, ISO 27001 Lead Auditor

Session topics

- Healthcare industry overview
- How disruption is affecting the Healthcare sector
- The evolution of the threat model
- How Sanitas has responded and adapted the cybersecurity model during Covid
- The role of regulation
- Pillars for an effective Healthcare security
- Future challenges

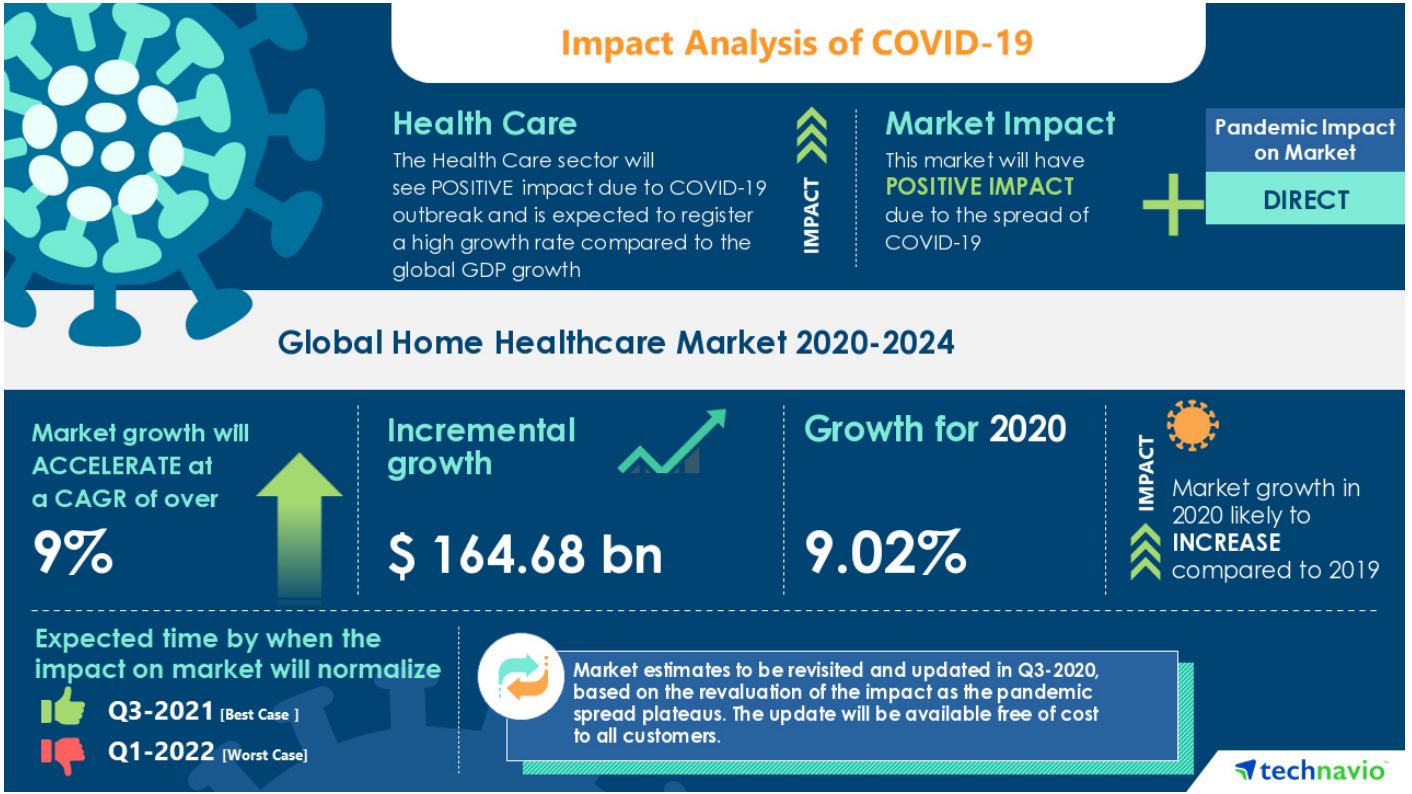
Healthcare market overview

- Global market for Private Healthcare estimated at US$4.7 Trillion in the year 2020, is projected to reach a revised size of US$7.

- Global market to reach $7.4 Trillion by 2027, with U.S. market estimated at $1.3 Trillion and China forecasted to reach a projected market size of US$1.6 Trillion.

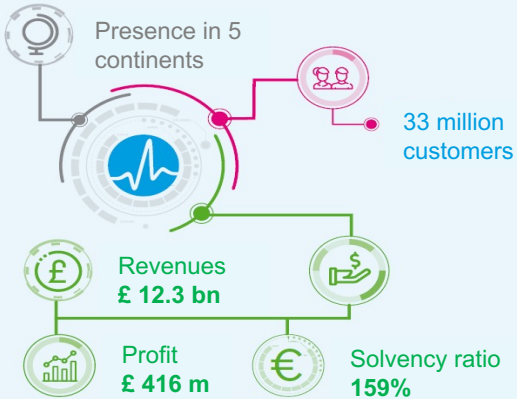
- Global market growth over 9%: China is forecasted 10.1% CAGR (2020-2027) with Europe grow at approximately 4.3% CAGR

Covid impact on healthcare predictions



About the Bupa Group

Healthcare has no boundaries



Australia & New Zealand

- Bupa Health Insurance
- Bupa Health Services
- Bupa Aged Care Australia
- New Zealand Care Services

United Kingdom

- Bupa UK Insurance
- Bupa Care Services
- Bupa Health Clinics
- Bupa Cromwell Hospital
- Oasis Dental Care
- Bupa Global North America
- Bupa Global Business Unit
- Bupa Global European Economic Area

Europe & LATAM

- Sanitas Seguros
- Sanitas Hospitales y NN.SS
- Sanitas Dental
- Sanitas Mayores
- LUXMED
- Bupa Acibadem Sigorta
- Bupa Chile
- Bupa Global Latin America

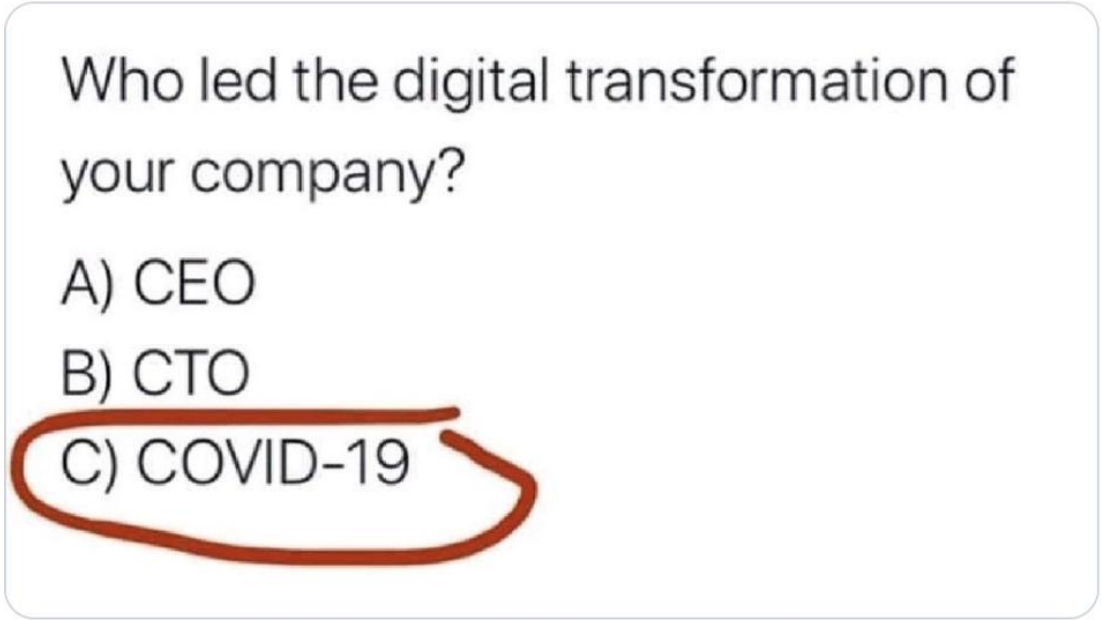
Other Markets

- Bupa Arabia
- Bupa Hong Kong
- Quality HealthCare (Hong Kong)
- Max Bupa (India)

Spanish healthcare market

Financing model	100% financed by Goverment taxes	Full coverage for primary and specialized medicine	60% of the price of medicines subsidized
Health provision	Dedicated network of public centers (ambulatory and specialized)	Good level of professionals in quantity and quality	Few contracts with the private system
Handicaps	“Bureaucratic” model	Limitation of public funds	17 regional health policies
	Aging population	Chronic disease growth	

Disruption in the Healthcare industry



Disruption in the Healthcare industry

- The Healthcare sector has probably been at the bottom of the different transformations that occurred in other industries
- Very intensive in human capital, long-term expenditures and often subjected to government bureaucracy, the appetite for digital investment has been low.
- Until now: changes in technology, consumer demands, an aging population and health predictions in a post-CoVid environment have pushed the industry into a radical (and accelerated) transformation

Disruption in the Healthcare industry

Sanitas
PARTE DE Bupa

Some of the digital trends in Healthcare are:

1. **Big Data and ML for predictive Health**
2. **Wearable medical devices**
3. **Video consultations and VR**
4. **Remote patient monitoring**
5. **Interoperability**

Information Security & Healthcare

- Information Security traditionally overlooked in Healthcare environments
- Huge dependency of unsecure third party equipment and legacy equipment and 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 inherent value of Heathcare data

- **PHI data is estimated 5x to 8x valuable than financial data**
- **Patient data is a desirable intangible asset: "*the value of the curated NHS data set could be as much as £5bn per annum*"**
- **According to Trustwave Global Security report, "healthcare data record may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card)"**

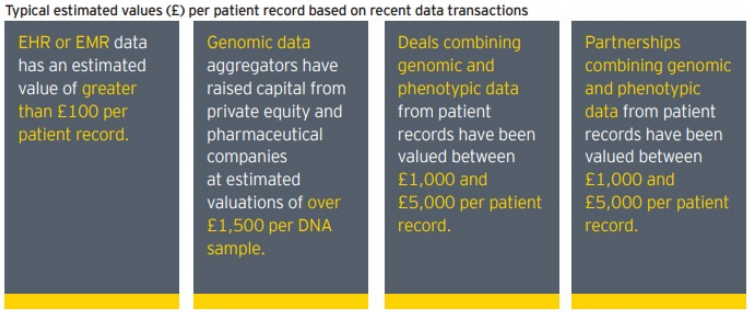


Figure 4. Observed values (£) per patient record based on recent data transactions (January 2019)

Source: EY: Realising the value of health care data: a framework for the future

2015: the year of Healthcare Data breaches (+100m records)

The New York Times

Today in Business | LIVE Latest Updates | Can Your Boss Make You Get Vaccinated? | Shedding Pandemic Pounds | Bonuses to Lure Workers

Millions of Anthem Customers Targeted in Cyberattack

Outside the Anthem facility in Indianapolis. Anthem said it detected a data breach on Jan. 29, and tha was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images

By Reed Abelson and Matthew Goldstein

Feb. 5, 2015

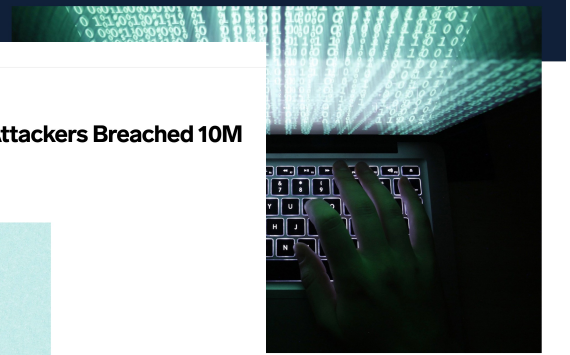
Anthem, one of the nation's largest health insurers, said late Wednesday that the personal information of tens of millions of its customers and employees, including its chief executive, was the subject of a "very sophisticated external cyberattack."

NEWS PLAN YOUR VACCINE COVID-19 POLITICS U.S. NEWS OPINION WORLD BUSINESS

SECURITY

Premera Blue Cross Hacked: 11 Million Customers Could Be Affected

One month after Anthem, another major health insurer announced it has been hit by a cyberattack: Premera Blue Cross.



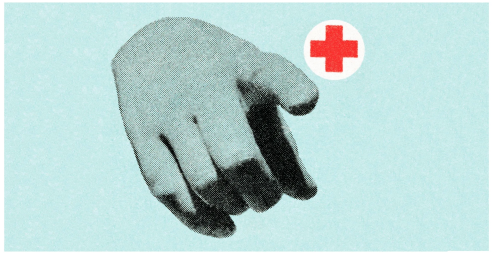
re. A barrage of damaging cyberattacks is shaking up the security industry, p hackers at bay, and instead turning to waging a guerrilla war from within

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

ANDY GREENBERG SECURITY 09.18.2015 12:48 PM

Hack Brief: Health Insurer Excellus Says Attackers Breached 10M Records

The breach represents the latest in a string of attacks on health insurance firms.



GETTY IMAGES

2015 IS QUICKLY becoming the year of the health insurance data breach. The latest

Most Popular


Wana Decrypt0r 2.0
English
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 decrypt some of your files for free. Try now by clicking <Decrypt>.
But 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.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Wannacry (May 2017)

NBC NEWS SECTIONS NIGHTLY NEWS MSNBC MEET THE PRESS DATELINE TODAY

NEWS > WORLD U.S. INVESTIGATIONS CRIME & COURTS ASIAN AMERICA LATINO NBCBLK

NEWS
MAY 17 2017, 9:39 AM ET

Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.

by ALEXANDER SMITH, SAPHORA

An ambulance worker at an NHS hospital in London on Friday

SHARE
Share
Tweet
Email
Print

LONDON — Why would doct

Last week's worldwide cyber computers at state-run medic discontinued Windows XP.

Thousands of operations and "WannaCry" malware threate and $600 were paid.

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO FEATURES MORE

TECH CYBERSECURITY

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brandom | May 12, 2017, 11:36am EDT

Peter O'Conner / Flickr

A massive ransomware attack has shut down work at 16 hospitals across the United Kingdom. According to *The Guardian*, the attack began at roughly 12:30PM local time, freezing systems and encrypting files. When employees tried to access the computers, they were presented with a demand for $300 in bitcoin, a classic ransomware tactic.

The Telegraph Coronavirus News Politics Sport Business Money Opinion Tech Life Style Travel Culture

Gadgets Innovation Big tech Start-ups Politics of tech Gaming

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled

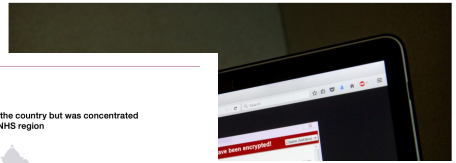
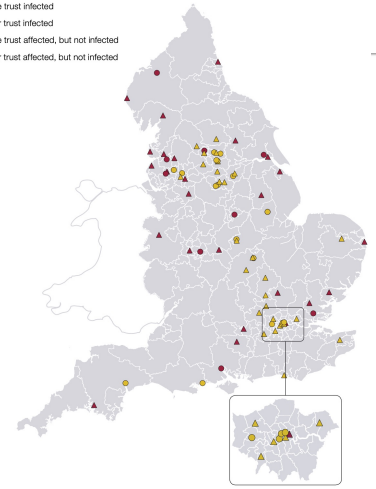


Figure 3
Trusts affected by the cyber attack

Disruption to front-line services affected all parts of the country but was concentrated in the North NHS region and the Midlands and East NHS region

- Acute trust infected
- Other trust infected
- Acute trust affected, but not infected
- Other trust affected, but not infected



Note
1 NHS England believes the concentration of infected trusts in the North NHS region and the Midlands and East NHS region does not reflect variations in cyber-security, but may be partially explained by these organisations becoming infected earlier in the day, before the WannaCry 'kill-switch' was activated.

Source: National Audit Office analysis of NHS England data

NL#TIMES TOP STORIES HEALTH CRIME POLITICS BUSINESS TECH

Hospital room - Source: Tomasz Sienicki / Wikimedia Commons at

CRIME INNOVATION HOSPITAL DUTCH HOSPITALS CYBER SECURITY RANSOMWARE
» MORE TAGS SHARE THIS:

MONDAY, JUNE 26, 2017 - 15:25

Ransomware attacks hit 15 Dutch hospitals

At least 15 Dutch hospitals were hit in ransomware attacks over the past three years, NOS reports based on a survey in which 25 hospitals participated anonymously. The hospitals insisted on staying anonymous out of fear of attracting hackers, according to the broadcaster. Another 20 hospitals refused to participate at all due to this concern.

In most cases ransomware blocks access to files on a computer and then demands money to reverse this. As most hospitals backup their data on an almost daily basis, little data was lost in a ransomware attack. In one case a hospital incurred delays in its outpatient clinic due to such an attack. One hospital had 75 computers infected with ransomware.

Sanitas
PARTE DE Bupa

Source: UK NAO (National Audit Office) Department of Health: Investigation: WannaCry cyber attack and the NHS

A profitable business model…

Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

▲ 'The quickest and most efficient way to restore our systems … was to pay the ra
president and chief executive of Hollywood Presbyterian Medical Center. Photogr

A Los Angeles hospital hit by ransomware swallowed t
the hackers.

Hollywood Presbyterian Medical Center had lost acces

BLEEPINGCOMPUTER

Search S

NEWS ▾ DOWNLOADS ▾ VIRUS REMOVAL GUIDES ▾ TUTORIALS ▾ DEALS

Home › News › Security › New Jersey hospital paid ransomware gang $670K to prevent data leak

New Jersey hospital paid ransomware gang $670K to prevent data leak

By Lawrence Abrams — October 3, 2020 — 10:15 AM

University Hospital New Jersey in Newark, New Jersey, paid a $670,000 ransomware demand this month to prevent the publishing of 240 GB of stolen data, including patient info.

The attack on the hospital occurred in early September by a ransomware operation known as SunCrypt, who infiltrates a network, steals unencrypted files, and then encrypts all of the data.

DATAINSIDER — Digital Guardian's Blog — **Popular Topics:** Data Protection — Security News — Threat Research

FOLLOWING RANSOMWARE ATTACK INDIANA HOSPITAL PAYS $55K TO UNLOCK DATA

Chris Brook
Last Updated: Wednesday August 12, 2020

ital paid 4 BTC (Bitc

abc NEWS — VIDEO — LIVE — SHOWS — CORONAVIRUS

Report: Alabama hospitals pay hackers in ransomware attack

An Alabama hospital system that quit accepting new patients after a ransomware attack says it gotten a key to unlock its computer systems

By The Associated Press
5 October 2019, 21:08 • 1 min read

News headlines today: Dec. 23, 2020

Catch up on the developing stories making headlines.

TUSCALOOSA, Ala. -- An Alabama hospital system that quit accepting new patients after a ransomware attack said Saturday it had gotten a key to unlock its computer systems.

A statement from DCH Health Systems didn't say how the three-hospital

....that went uncontrolled

EL HOSPITAL DE TORREJÓN SUFRE EL PRIMER CASO DE RANSOMWARE A UN HOSPITAL EN ESPAÑA

Publicado por Equipo PSN Sercon | Ene 21, 2020 | Actualidad, Sector sanitario

DAN GOODIN, ARS TECHNICA SECURITY 09.18.2020 08:00 AM

A Patient Dies After a Ransomware Attack Hits a Hospital

The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.

PHOTOGRAPH: LUKAS SCHULZE/GETTY IMAGES

PART OF A ZDNET SPECIAL FEATURE: CORONAVIRUS: BUSINESS AND TECHNOLOGY IN A PANDEMIC

Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

One of the Czech Republic's biggest COVID-19 testing laboratories hit by mysterious cyberattack.

By Catalin Cimpanu for Zero Day | March 13, 2020 -- 17:36 GMT (17:36 GMT) | Topic: Coronavirus: Business and technology in a pandemic

Image via Google Street View

The Brno University Hospital in the city of Brno, Czech Republic, has been hit by a cyberattack right in the middle of a COVID-19

NEWSLETTERS

ZDNet Announce UK

ZDNet's Announcements newsletter offers a mix of stories, special offers and members-only benefits.

Your email address SUBSCRIBE

SEE ALL

RELATED STORIES

Security
Security updates released for Adobe Reader after vulnerability 'exploited in the wild'

Security
Microsoft brings Threat and Vulnerability Management capability to Linux

LATEST DEVELOPMENTS

FRANCE 24 LIVE

#COVID19 #ISRAELI-PALESTINIAN CONFLICT FRANCE AFRICA CULTURE SHOWS FIGHT THE FAKE

Coronavirus notice • View the recommendations and information for travellers issued by the French Government →

Europe

'Mafia-type' groups likely behind cyber attacks on French hospitals, minister says

Issued on: 25/02/2021 - 10:12

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

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

CORONAVIRUS Resources | INDIA VARIANT Q&A | LATEST UPDATES | INDIA TRAVEL BAN | MASKS Q&A | VACCINE DISTRIBUTION | STATE-BY-STATE VACCINE

BUSINESS

Cyberattacks Cost Hospitals Millions During Covid-19

Attack at Universal Health Services cost the company $67 million last year

The hospital industry, under strain of the coronavirus pandemic, is facing increased threats from hackers.

PHOTO: BRENDAN SMIALOWSKI/AGENCE FRANCE-PRESSE/GETTY IMAGES

MOST P

BRIAN BARRETT SECURITY 03.21.2020 09:00 AM

Security News This Week: Ransomware Groups Promise Not to Hit Hospitals Amid Pandemic

Plus: iPhone cracking, credit card skimming, and more of the week's top security news.

PHOTOGRAPH: JOSEPH PREZIOSO/GETTY IMAGES

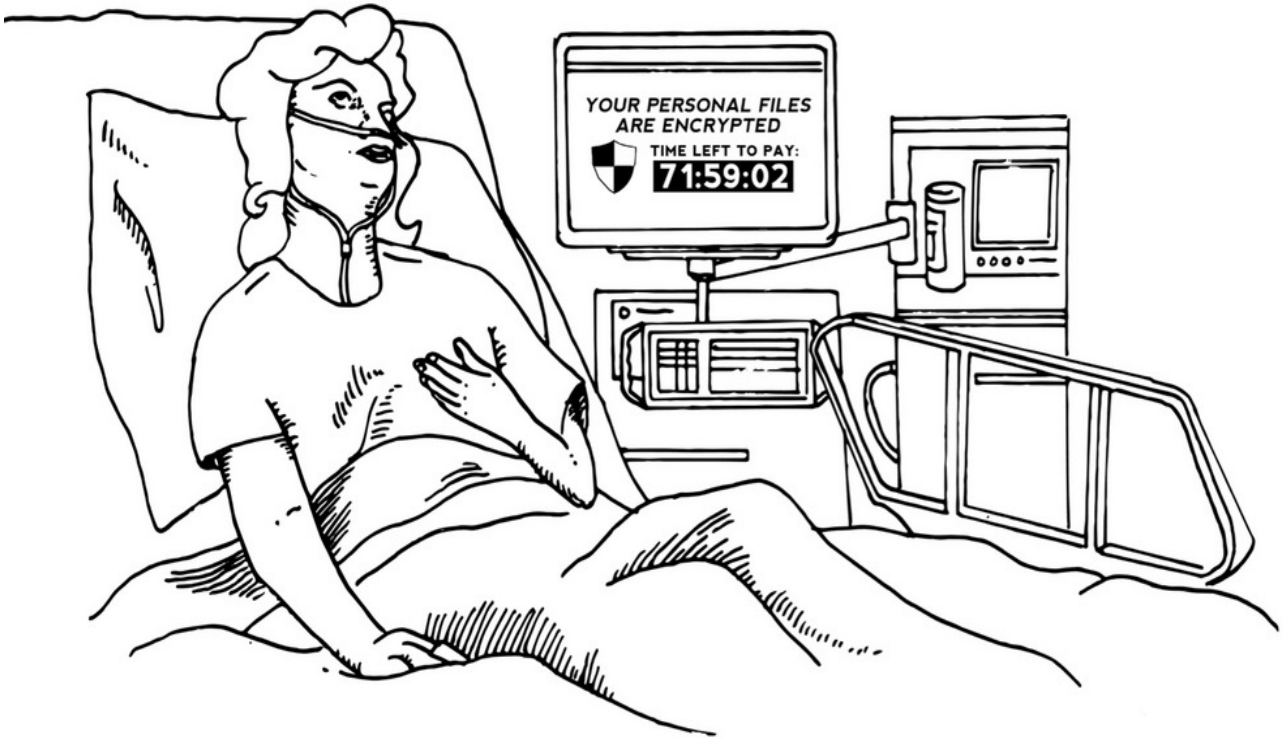
Healthcare Cybersecurity & CoVid: a wake up call

- The cyberthreat landscape became critical in the worst moment… while dealing with a global pandemic

- Pressure on hospitals and medical centres was increasing but there was no option but to deal with the “digital pandemic” and protect our crown jewels at the same time

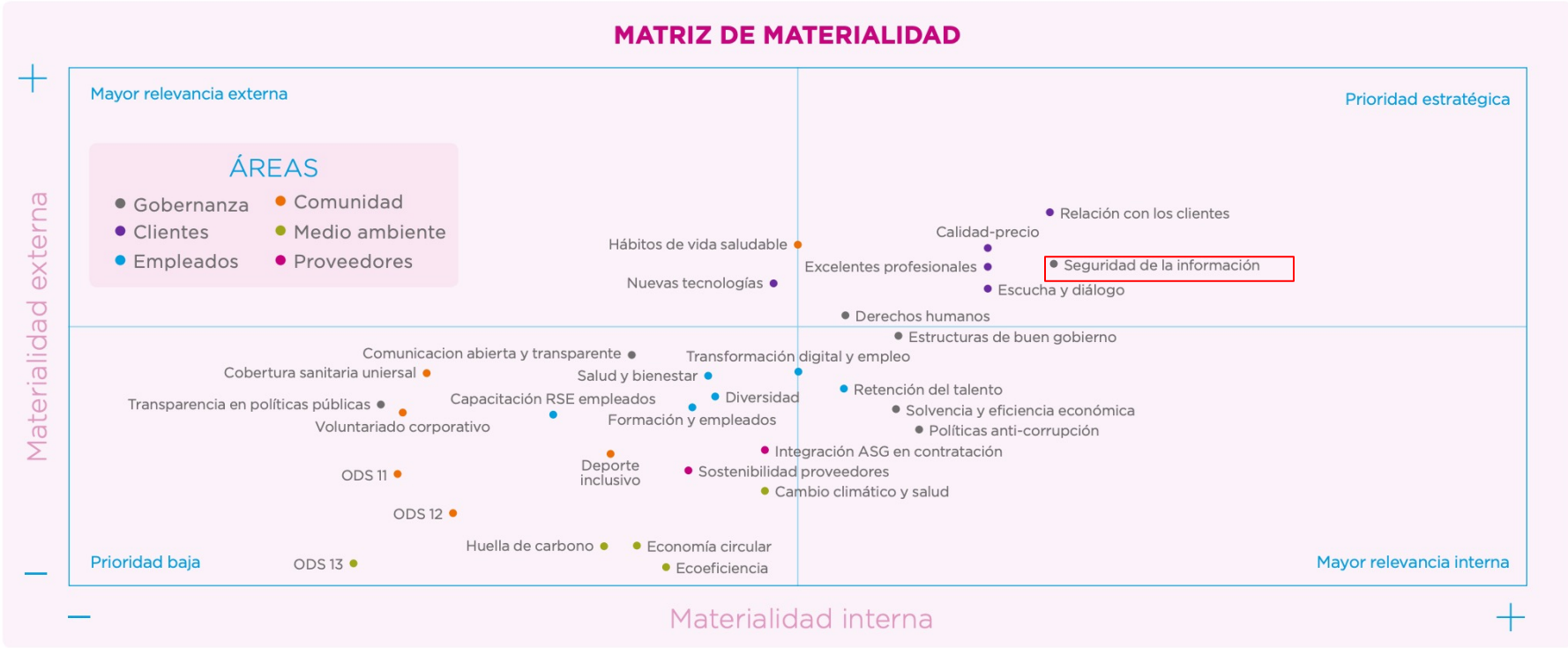
The battlefield

And the asset to protect



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

Sanitas approach to Information Security



Source: Sanitas 2019 Annual Corporate Report

How we tackled the situation

- One message was clear at the early stages of the pandemic: we need to take action IMMEDIATELY: we can't afford a cyberincident considering the occupation levels of the hospitals.

- Resources are limited: where to focus? As usual, let's start by the basics:
  - Hygiene controls
  - Attack surface review
  - Threat Intel
  - Ensure proper and 24x7 monitoring

- We will then evolve across different phases as the pandemic situation evolves

Phase I (February-May 2020): Ensure the basics

- A deep review of basic controls in our hospital's environment, such as:
  - Multi-Factor Authentication for all remote accesses
  - Network-Connected devices compliant with security policies
  - AV and EDR effectively deployed across all endpoints
  - Intensive in awareness
- In parallel, activation of our offensive security Red Team for an initial attack surface testing
- And looked for support: several cross-EU initiatives sponsored by the ECSO (European Cyber Security Organization)

Phase II (May-September 2020): Accelerate

- Phase I helped us to spot some weak points, so the InfoSec and IT Ops teams accelerated the remediation.
- Pressure in medical centres was increasing while state of emergency was declared in Spain.
- But we needed to move to the next stage and accelerate the deployment of controls such as:
  - Network segmentation to avoid propagation
  - Proxy Cloud for a secure mobility
  - Automation of attack surface tests on a 24x7 basis
  - Ethical phishing exercises: test the human firewall
  - Fine-tuning of EDR rules: test, learn and adapt

Phase III (September'20-February'21): Consolidate

- Controls deployed in Phase II showed good results, so we needed to consolidate and integrate them

- InfoSec teams where exhausted so we reviewed our sourcing model to increase our bandwidth: staff? contractors? both?

- We decided to change our traditional 50% staff-50% contractors and convert contractors into staff to capitalize all the knowledge acquired during the previous phases and move to a 70%- staff-30% contractors model

Phase IV (February'21 -): Evolve

- We entered into the pandemic having a defined structure… now we have a complete different one.

- But we need to stay ahead and recognize the need to evolve in certain areas:
  - Gain control of all IT-environments: unmanaged or unreachable environments are not acceptable.
  - Leverage cloud services: they provide scalability and the opportunity for integration heterogenous environments
  - Gain business support: we are moving towards a service based OPEX model.
  - And of course… champion the cultural change!

The role of regulation

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 p draft guidance details the agency's recommendations

NIST | NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index | Search

Information Technology Laboratory

About ITL | Publications | Topic/Subject Areas | Products/Services | News/Multimedia | Programs/Projects

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

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.

enisa

ICT security certification opportunities in the healthcare sector

V1.0
DECEMBER 2018

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

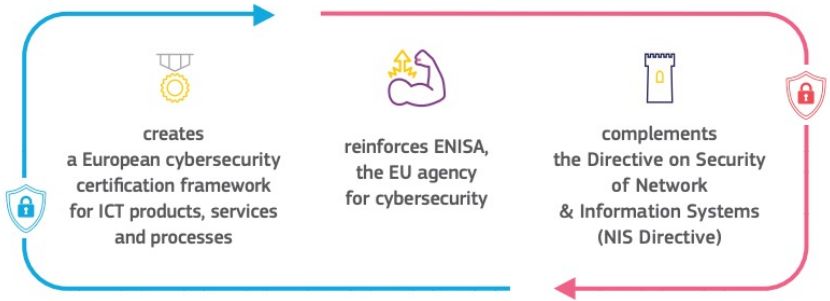
With a positive focus within the EU

https://project.securehospitals.eu/

EU CYBERSECURITY ACT

THE LATEST EU'S LEGISLATION TO ADVANCE CYBERSECURITY ACROSS EUROPE

THE EU CYBERSECURITY ACT AT A GLANCE



27th June 2019 the EU Cybersecurity Act comes into force:

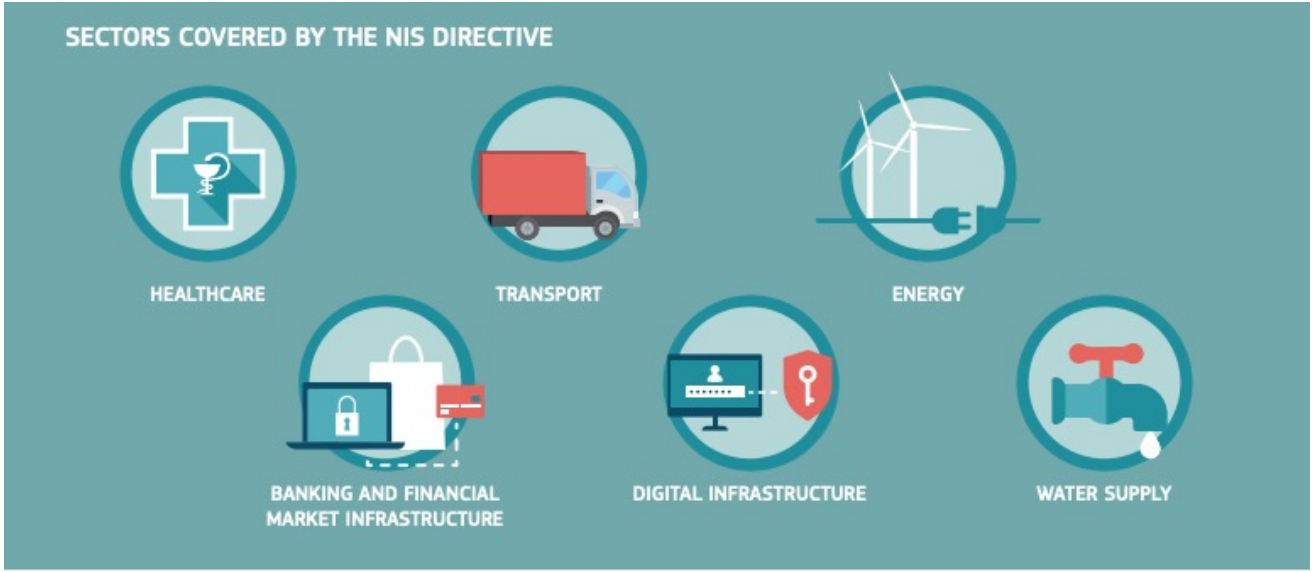
"*The Cybersecurity Act introduces for the first time EU-wide rules for cybersecurity certification. Companies in the EU will benefit from having to certify their products, processes and services only once and see their certificates recognised across the Union.*"

Source: EU Cybersecurity Act Infographic

The NIS Directive represent the first ever **EU-wide law on cybersecurity**. The Directive has assisted in stepping up the cybersecurity of network and information systems within the European Union.

Adopted by the European Parliament on 6 July 2016 and entered into force in August 2016.EU states have to transpose the Directive into their national laws by 9 May 2018

Source: EU NIS Fact Sheet



DIGITAL SERVICE PROVIDERS ARE ALSO COVERED BY THE NIS DIRECTIVE AND ARE SUBJECT TO SIMILAR OBLIGATIONS

Digital service providers are:

The new security provisions encourage consumers' trust and boost the digital economy.

What have we learned so far: pillars for an effective healthcare cybersecurity

Endpoint & Infrastructure protection

- Understand your threat profile and attack surface
- Identify key assets within the environment.
- Apply patching and avoid outdated SW versions.
- Consider advanced protection, far beyond traditional AV.
- Isolate environments. Apply network segmentation
- Secure methods for remote access (2FA as a minimum)
- 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.
- Cybersecurity as a regular Board discussion

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 & Industry

- R&D investment
- Promoting adoption of vulnerability disclosure policies
- Translating the Common Vulnerability Scoring System (CVSS) for medical devices
- Bug-bounty initiatives for medjacking
- Manufacturers liability for unsecure products
- Promote collaboration and information-sharing

Q&A? Thanks!

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


“Security is always too much until the day it is not enough”
William H. Webster. Former Director, FBI