hope

European Hospital and Healthcare Federation

# Looking beyond one's nose: how hospitals are dealing with cyber attacks and preparing for the worst-case scenario

AIM / EHFCN SEMINAR

12 DECEMBER 2024

SASCHA MARSCHANG, SENIOR ADVISOR

# HOPE at a glance

## Central Office

## Profile

- European non-profit organisation
- Created in 1966 in Rome
- Central office in Brussels

## Membership

- Covers almost 80% of hospital activity in the EU
- 37 organisations in all 27 EU Member States + UK, Switzerland and Serbia
- Public or private; public and private
- Three kinds of members: national hospital associations, federations of local and regional authorities, national health services/ministries of health

**Pascal Garel**
Chief Executive

**Marie Nabbe**
EU Affairs Officer

**Sofía Carbonell**
Project Officer

**Sascha Marschang**
Senior Advisor

# Main Activities

- **Influence and representation:** The EU has influence on hospitals and healthcare, however, impact is often produced at the national level. HOPE presents a common position before the EU
- **Comparative studies** produced internally or as part of EU projects
- **Publications:** Agora Report (detailed report on annual HOPE Agora summit proceedings; on specific topics across national health systems; Position Papers (on EU policy)
- **Other:** HOPE Exchange Programme, Conferences, Study Tours, EU projects

HOPE Board of Governors, June 2022, Brussels

HOSPITAL HEALTHCARE EUROPE

hospitalhealthcare.com

hope

HOPE HEALTHCARE DATA AND GOVERNORS' RESPONSES 2022

SAFEST

Health InnoFacilitator

dioptra

FLASH

TeNDER

RE-SAMPLE

LUCIA

periscope

XpanDH

HOSMARTAI

Participants of HOPE Exchange Programme 2019

# Cybersecurity: Knowledge vs action

- Are hospitals more aware of cybersecurity threats than other institutions?

  Possibly

- Are they well-prepared and able to cope with powerful cyber-attacks?

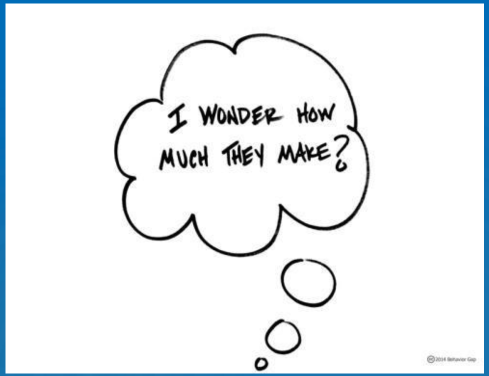
  Rarely

# Why hospitals are on alert

## Cybercrime is an everyday occurrence…

- Highly connected internally & externally – potentially much wider impact
- Very diverse user base, constantly in flux: management, healthcare professionals, administration & other staff, partner institutions, supply chain, patients / carers….
- Lots of entryways: digital hard- and software, mobile & IoT devices, portals, data storage...
- Sectoral transformation – old & new systems side-by-side (e.g., EHDS, AI deployment)
- High possibility of poor security practices, inadvertent errors, misconfigurations
- Hackers can access networks & systems, steal, manipulate, extort, store, release data
- Different threats: ransomware, malware, denial of service, supply chain, intrusion, etc.
- Perpetrators can be criminals, hacktivists, spies, insiders, competitors, skilled individuals…

# Healthcare data
# = particularly lucrative



- Important resale value of electronic health data (individual / bulk), other medical data, payment data, authentication data, strategic healthcare information, etc.
- Often interconnected with other personal data, e.g. civil status, DOB, social security / ID number, insurance coverage, etc.
- Darknet important facilitator of identify theft & fraud
- Victims can be targeted immediately and long-term
- Not only hospitals / healthcare providers affected, but all healthcare actors (health insurance providers, pharma companies, public health, research institutes, etc.)

# High stakes

- Individuals: risk to patient safety (physical & mental harm), personal data theft, privacy loss, extortion, potentially long-term impacts
- Healthcare professionals: impact on ability to perform job / give care, changing routines, confidentiality, liability, dismissal (…)
- Hospitals & healthcare organisations: impact on quality & continuity of care, business operations (incl. suppliers)
- Loss of public trust & confidence, reputation, economic viability, etc.

# Why cyber-resilience is so difficult to achieve in practice

Typically, only 2-5 % of hospital budgets dedicated to digitalisation in European hospitals, incl. cybersecurity measures

- Huge array of critical elements
- Continuous budget cuts affecting hospital services / departments in many countries and regions
- Cybersecurity competing with operational / staff costs
- Persistent staff shortages
- High workload & stress
- Digital literacy gaps
- Lack of cybersecurity & health data expertise / positions
- Outdated technologies, (lack of) interoperability
- Digital fragmentation across EU
- Impact of COVID-19
- (…)

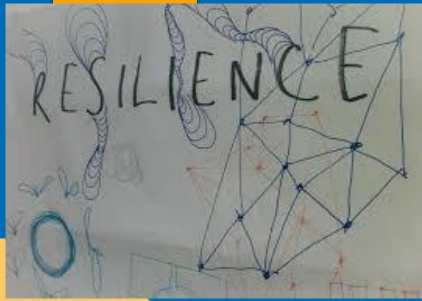
# What hospitals are/should be doing

- Leadership & preparedness – “Not if, but when”, “anywhere, anytime, anyplace”
- Establish cybersecurity teams to instigate change of mindset
- Risk / vulnerability assessments & information systems security policies
- Prepare & practise for worst-case scenarios (e.g., simulations), awareness-raising, reducing stress & building up confidence
- Detailed procedures for incident handling & recovery
  - Reaching / informing all staff, dealing with most urgent emergencies
  - Reverting to paper protocols, low-tech alternatives
  - Safeguarding inter-departmental communication

# What hospitals are/should be doing (cont.)

  - Plans for business continuity, crisis management, reinstatement: immediate vs. longer-term priorities of all services / clinics / administration
  - Co-operation with other HC providers
  - Informing patients / carers / suppliers / etc. (e.g., using landline phones)
- Investigation & incident response plan
- Data breach plan, incl. how to recuperate / retain data, redesign processes
- Adequate insurance coverage
- Information sharing (local, regional, national)
- Post-event assessment: ensure lessons learnt are known to all staff / partners

# Building resilience: What policies / measures should be in place?



## Staff

Passwords – strong identification, regular mandatory changes

Two / multi-factor authentication

Strict access controls, adopt principle of least privilege

Terminate access immediately upon leaving

Prohibit / restrict use of personal e-mail & other accounts

Awareness programmes (threats, common errors, scope of consequences, etc.)

Training - continuous data security / crisis exercises involving ALL staff, toolkits, guidelines

## Vendors / suppliers

Review all vendors' cybersecurity practices

Access - limit, control, monitor activities

Ensure support / assistance

## Systems / networks

Up-to-date software & OS patches

Anti-virus: advanced managed detection & response

Multi-layered firewalls

Robust backups (cloud-based / onsite)

Connected / IoT devices – limit access, intrusion protection, secure storage / key management

Data loss prevention: encryption of patient / operational data, information labeling and protection (e.g., tracking documents)

Secure internal directories

Advanced (AI) solutions to monitor / analyse user and device behaviours, detect abnormalities

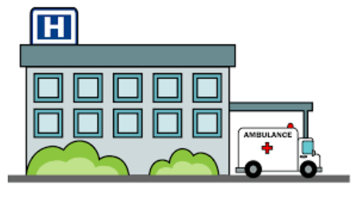
Regular audits (resilience / penetration testing, etc.)

# Cybersecurity

EU legislation – new safeguards & responsibilities

## NIS2 Directive

- Covers all dimensions of information systems security, applies to essential / important entities
- Prevention of health service disruption through mandatory technical, operational, organisational measures, proportional to risks affecting entities
- Risk assessment / management, clear incident reporting, identification / authentication, business continuity, securing communications, audits, training (...)
- Protecting patient data, incl. proper storage and handling practices
- Supply chain control (regular checks of contractual provisions)
- Senior management responsibilities
- Strict sanctions



# How to succeed?

- Ensure practical toolkits & protocols are available – outlining roles, tasks, processes, priorities, communication, etc.
- Make training concrete and personal: all staff / stakeholders need to feel relevance, progress, become emotionally involved (e.g., interactive, exciting, competitive…)
- Instill cyber hygiene through permanent improvement
- Involve staff in co-creation (identification of good practices, user-friendliness)
- Ensure balanced approach:
    - Acknowledge existing limitations & gaps
    - Pool resources with other sites / partner institutions
    - Maintain diversity of approaches
- EU Cybersecurity Action Plan for Hospitals / Healthcare Providers could provide comprehensive 'package' of existing information & guidelines, unleash new investments / funding, help clarify hospitals' responsibilities regarding the interplay of regulations

hope

European Hospital and Healthcare Federation

# THANK YOU.

**SASCHA MARSCHANG**

ADV@HOPE.BE

@euhospitals

www.hope.be