HUMAN FACTOR IN CYBERSECURITY
ACCA 2025

Dusko Milojevic

22. Maj 2025

Cybersecurity Toolbox for Connected Medical Devices

CYLCOMED

KU Leuven: Legal and Ethical Partner in CYLCOMED Project

- **Role**: Ensures ethical and legally compliant use of innovative solutions to enhance the cybersecurity of connected medical devices (CMDs).
- **Expertise**: Develops an ethical and legal framework addressing privacy, data protection, CMD regulations, and cybersecurity legislation.
- **Track Record**: Renowned for expertise in AI, autonomous systems, data protection, eHealth, ethics & law, intellectual property, media, telecommunications, and cybersecurity. Longstanding partner in large international and interdisciplinary research projects.

CHARITÉ

MEDIACLINICS Wearable Health Applications

fib Niño Jesús

KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

EVIDEN an atos business

XLAB

RGB medical devices

MARTEL innovate

OSPEDALE PEDIATRICO Bambino Gesù

INOV

Scan to learn more:

Funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

CYBERSECURITY INCIDENTS ARE HITTING THE HEADLINES

CYBERATTACK

The cyberattack that has paralysed Barcelona's Hospital Clínic: "No ransom will be paid"

Major Catalan public hospital hopes to resume some activity progressively from Tuesday after serious ransomware attack

Nura Portella
Photo: ACN
Barcelona. Monday, 6 March 2023. 13:07
Updated Tuesday, 13 February 2024. 09:46
Reading time: 2 minutes

Cyber Security News

Home | Threats | Cyberattack News | Vulnerability | Zero-Day | Data Breaches | Cyber AI | What Is

Cyberattack News

Transport for London Faces Cyber Attack Operation Distributed

By Balaji N - September 3, 2024

Sections | THE IRISH TIMES | 3° | Subscribe

Health

HSE cyber attack: More than 470 legal proceedings issued against health service after ransomware hit

Leak by Conti, the Russia-based crime group, compromised personal data of almost 100,000 staff and patients

Expand

LATEST STORIES ›

Your top stories on Tuesday: Poll finds Fianna Fáil-Fine Gael the most popular new coalition; Irish troops return from Lebanon

Rod Stewart to play Glastonbury 2025 legends slot: 'I'm proud, ready and able to

Forbes | Billionaires | Innovation | Leadership | Money | Business | Small Business | Life

14,889 views | Jun 28, 2019, 05:28am

FDA Warns Of Dangerous Cybersecurity Hacking Risk With Connected Medical Devices

Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.

Type here to search

POLITICO

EU-US relations | War in Ukraine | Romania election | Poland election | Newsletters | Podcasts

NEWS > DEFENSE

Thousands of UK troops hit in suspected Chinese hack on defense ministry

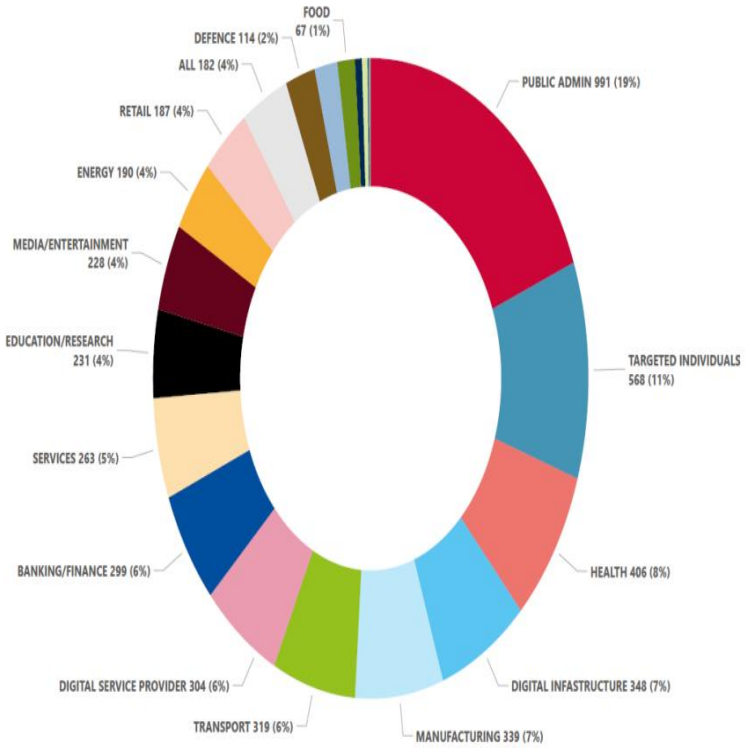
Defense Secretary Grant Shapps briefed the House of Commons Tuesday afternoon — but is avoiding publicly pointing the finger at Beijing.

Home / Tech / Security

First death reported following a ransomware attack on a German hospital

Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack.

THE CYBERSECURITY THREAT LANDSCAPE



92%

of organizations in this research had at least one cyberattack over the past 12 months

$4.7M

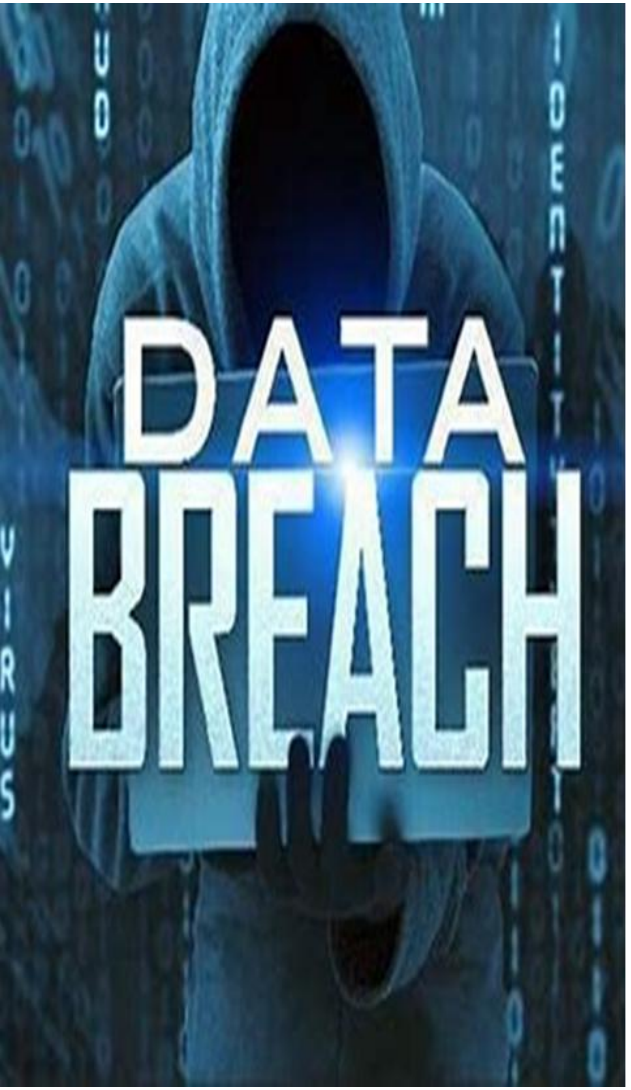
is the average total cost for the single most expensive cyberattack experienced over the past 12 months

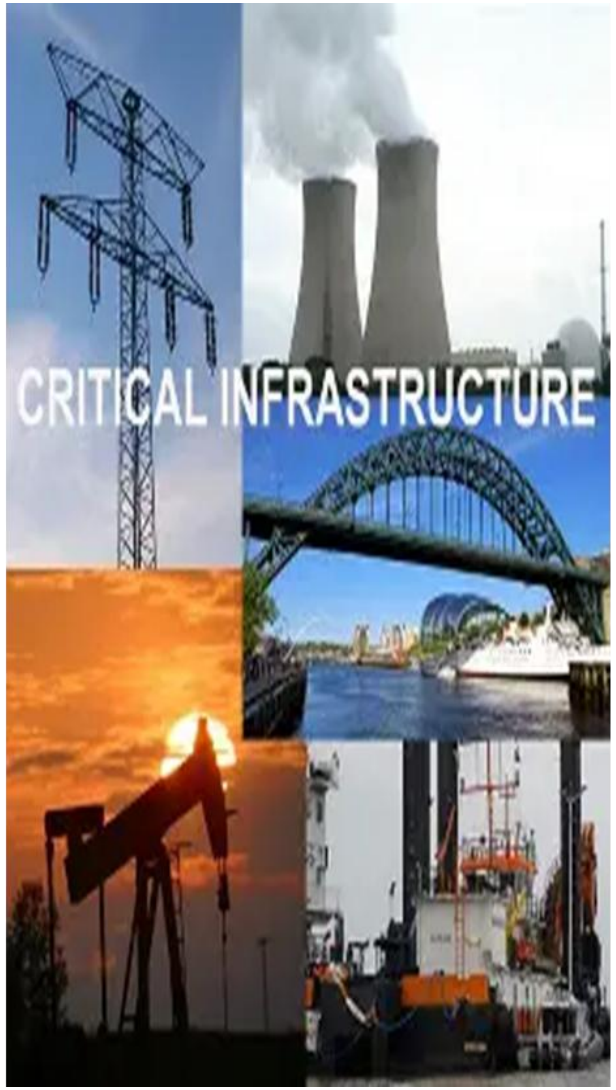
$1.47M

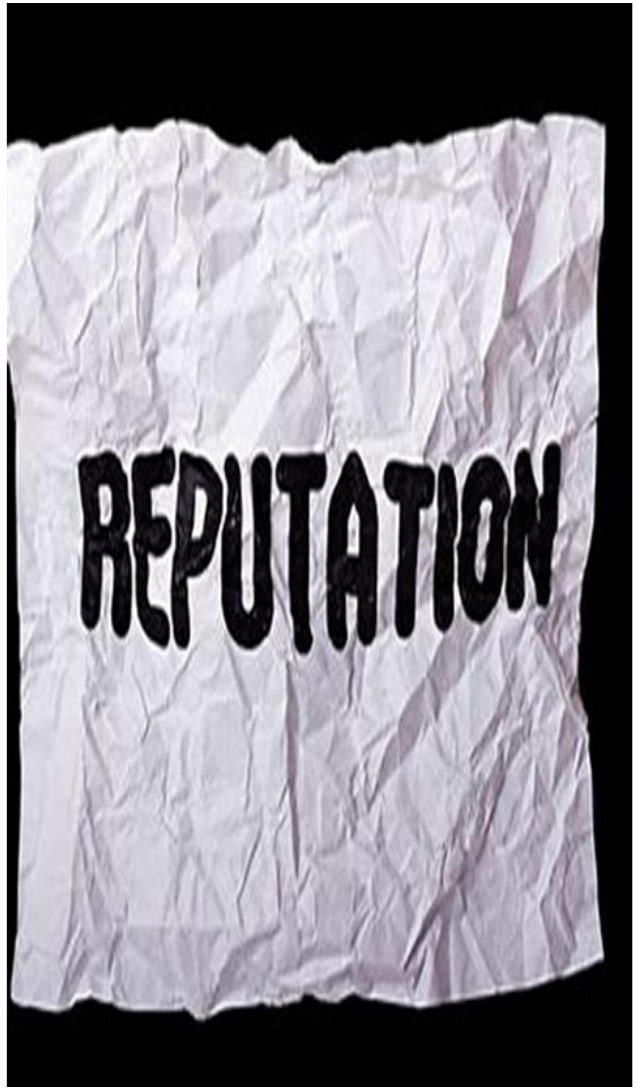
in disruption to normal healthcare operations was on average the most significant financial consequence from the cyberattack

WHAT IS AT STAKE? DIRE CONSEQUENCES OF CYBERATTACKS

CYLCOMED







“CURE” TO CYBERSECURITY CHALLENGES - POLICIES

- Cybersecurity Strategy for the Digital Decade
- European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers

“CURE” TO CYBERSECURITY CHALLENGES - REGULATIONS

- Cybersecurity Act (CA)
- Network and Information Systems Directive (NIS2)
- General Data Protection Regulation (GDPR),
- Cyber Resilience Act (CRA)
- Artificial Intelligence Act (AI Act)
- Regulation on the European Health Data Space (EHDS)
- Medical Device Regulation (MDR)
- …….

“CURE” TO CYBERSECURITY CHALLENGES – TECHNICAL MEASURES

- Encryption
- Anonymisation
- Patch Management
- Multi-factor authentication (MFA)
- Least privilege principle
- Firewalls (hardware or software-based)
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- …..

HUMAN FACTOR

HUMAN FACTOR

Human factor contributed to approximately 68% of breaches

Human error remains a critical threat area, consistently ranking highly, if not the top category

WHAT IS HUMAN FACTOR IN CYBERSECURITY ?

SCHOLARLY LITERATURE

- “human factor”
- “human element”
- “human dimension”
- “insider threat”
- “end-user”
- “human resources security”
- …….

REGULATIONS

- NIS2 explicitly mentions the “human factor” in its Recital 78, and “human resource security” (Recital 79)
- Recital 8 of the CSA points out that cybersecurity is not only an issue related to technology but also one where **human behavior** is equally important

HOW TO ADDRESS THE HUMAN FACTOR?

UNDERLYING FORCES SHAPING THE CYBERSECURITY ARCHITECTURE

LACK OF RESOURCES

- NIS investment report highlights significant disparities in investments across critical infrastructure, revealing a gap that threatens the collective goal of a cyber-secure EU
- Healthcare historically faces the underfunding, facing significant trade-offs

LACK OF CYBERSECURITY EXPERTS

- The ISC2 (2024) report estimated that 299,000 cybersecurity professionals are needed to meet EU workforce demands
- Eurobarometer survey highlights the growing cybersecurity talent gap across the EU
- Some sectors, such as healthcare, are even more under pressure

CHALLENGING REGULATORY LANDSCAPE

NIS2

- Risk management measures shall include at least, inter alia, “basic cyber hygiene practices and cybersecurity training”

- Member States shall ensure that the **members of the management bodies** of essential and important entities **are required to follow training**, and shall **encourage** essential and important entities **to offer** similar training to their employees on a regular basis (NIS Article 20)

GDPR, MDR, AI ACT…

TECHNICAL AND “**ORGANISATIONAL**“ MEASURES

OPEN QUESTIONS

- Should cybersecurity legal frameworks incorporate stronger enforcement mechanisms, accountability models, and proactive human risk management strategies to enhance human factor governance?

- Do we need more terminological clarity, coherence, and legal consistency between legal frameworks regarding the human factor?

CYLCOMED

THANK YOU FOR YOUR ATTENTION

cylcomed.eu

Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**