CYBERSECURITY RISKS IN THE MEDICAL DEVICE NETWORK: ARE FRENCH HOSPITALS PREPARED ?

evachoulet@hotmail.fr

Eva CHOULET[1], Anne-Marie BELLIARD[1], Névine BELKAID[1], Emmanuelle CAUCHETIER[1], Jean-Luc PONS[1]

1 : Pharmacy departement , Hospital Center Victor Dupouy, 69 Rue du Lieutenant Colonel Prudhon, 95100 Argenteuil

2SPD-022

INTRODUCTION

Increase in cyberattack risk in the healthcare sector

The medical device (MD) supply chain represents a particularly exposed target

Significant impact on patients' safety and continuity of care.

Objective: Analyze the organizational and technical measures implemented by healthcare institutions (HIs) to prevent, detect, and respond to the risk and impact of a cyberattack on the medical device management process.

MATERIALS & METHODS

Audit conducted over a 3-month period (07/07/25 to 10/10/25)

Online questionnaire:

- 22 questions
- 4 sections : General information, history of cyberattacks, organization of medical device management and cyberattack preparedness, needs and perspectives.

Distribution of the questionnaire by email to public and private hospital pharmacies across France.

Descriptive quantitative and qualitative analysis of the responses collected in an Excel® spreadsheet → Identification of trends, differences in practices, and shared limitations among the various hospitals

RESULTS

30 HIs responded, including 1 ETS with a history of a cyberattack.

Average number of MSO beds: 589 beds

(MSO = Medicine, Surgery, and Obstetrics)

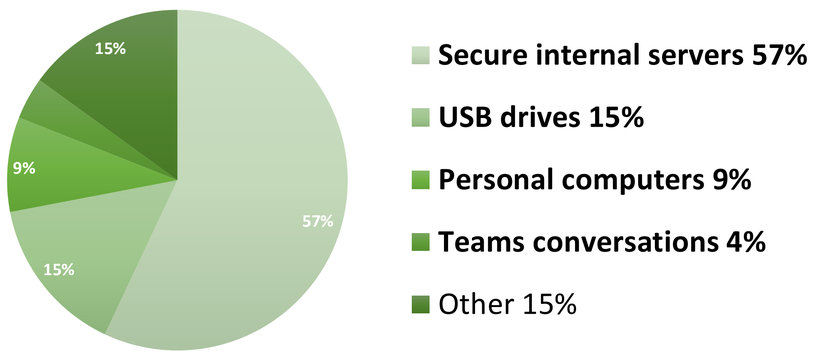
Type of establishments: Military hospital, University hospital, General hospital, ESPIC (Private non-profit healthcare institution), Private clinic

Loss of communication with departments and suppliers, untracked stock, traceability issues, and billing problems with manufacturers/National Health Insurance.

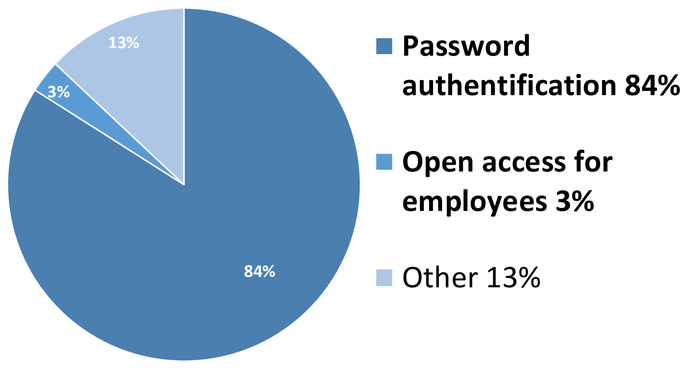
Operations resumed on Day 150, but payment delays persisted even 3 years later.

52% (n=15) of pharmacists were able to define the BCP/DRP (Business Continuity and Disaster Recovery Plan)

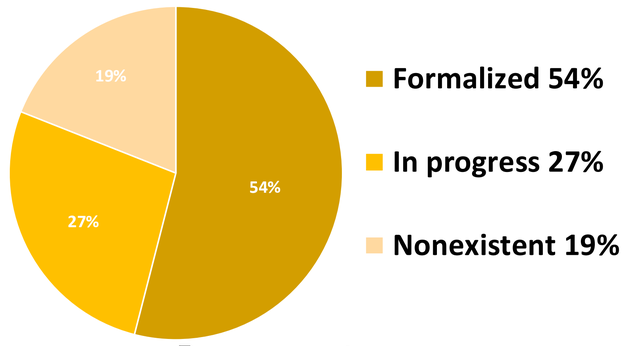
Data storage of the MD



Access to data by staff



Cyberattack procedures



➔ Among the 54%, 18% tested it

Strenghts

Implementation of a « crash box »
Territorial cooperation
Sufficient stock of MD available

Improvement Opportunities

Lack of training (practical and theoretical)
Difficulty performing daily backups

Limitations

Lack of support from the Information Systems Department (IT) and lack of regular training, time, and financial resources
Understaffing

CONCLUSION

Need for a harmonized national logistics resilience strategy with support from central purchasing bodies

Limited practical implementation despite finalized procedures

Key levers to strengthen continuity of care: team training and improved coordination between logistics and IT departments