SIMULATION OF A CYBERATTACK IN A HOSPITAL PHARMACY: DEVELOPMENT OF TOOLS TO ENSURE CONTINUITY OF CARE

RIGAUD A.[1], ROUSSEL A.[1], DETREE J.[1], COLIN M.[1], CORNEAU H.[1], LEGARDIEN E.[2], KRUG E.[1], COLLET C.E.[1]
[1]*Pharmacy Departement;* [2] *Information technology departement*
Flers hospital center, Flers, Normandy, France
Email : collet.charles.edouard@gmail.com

5PSQ-016

Background & Objectives

Healthcare establishments are **increasingly vulnerable to cyber attacks** which can **compromise the continuity of care**, particularly in the pharmacy sector. In our hospital pharmacy, we carried a cyber attack simulation in order to identify the critical points and to find alternative tools to ensure the continuity of pharmaceutical tasks.

The aim of this study is to highlight the needs in order to develop **alternative tools or specific procedures to guarantee the continuity of pharmaceutical activities** in case of a cyber incident.

Materials and Methods

A cyber-attack simulation in a form of a complete informatics system failure was carried out for one afternoon.

Pharmacy staff were involved **to identify the critical points** that **prevented the provision of services and continuity of care following the cyber attack**.

Results

Pharmacists, pharmacy assitants, secretary, store keeper, ….

3 working groups

Supply / order

Prescription

Dispensing

Many tools were developed to ensure the continuity of pharmaceutical care during a cyberattack

Automated order form based on an extraction of current data

Binder listing services supplies (medicines, medical devices, gases, narcotics, antidotes, etc.)

Development of a downgraded sterilisation procedure

Paper registers for managing narcotics, outpatients and blood-derived medicines

'Back-up' computer, offline, was set up with all the back-up documents

Excel file containing protocol references to automate chemotherapy prescriptions, while generating production sheets and the corresponding labels

Conclusion

This study has highlighted the need for **tools and organisational measures** to ensure the **continuity of pharmaceutical care during a cyber attack**. A new cyber-attack simulation will be carried out to test the robustness of the tools developed.

The results of this simulation underline the importance of establishing tailor-made continuity plans as well asregular testing of their effectiveness

29th EAHP congress, 12 - 14 March 2025, Copenhagen, Denmark