

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

¹Pharmacy Department; ²Information technology department

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**.



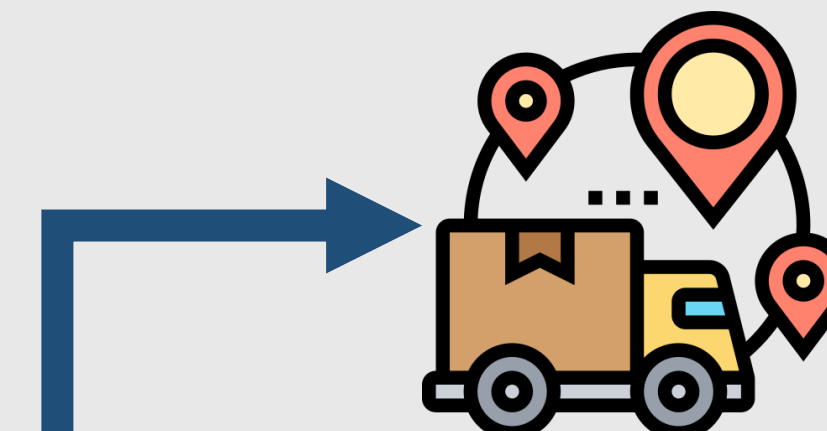
Results



Pharmacists, pharmacy assistants, secretary, store keeper, ...



3 working groups



Supply / order



Prescription



Dispensing



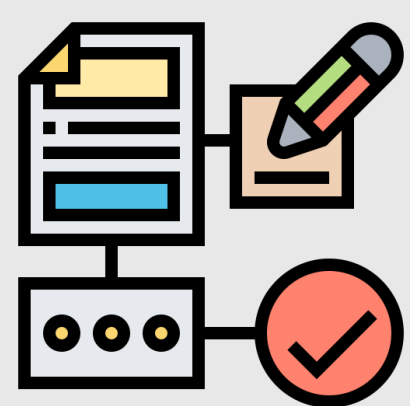
Many tools were developed to ensure the continuity of pharmaceutical care during a cyberattack



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 as regular testing of their effectiveness