Managing a Ransomware Attack: The Resilience of a Swedish Municipality – A Case Study

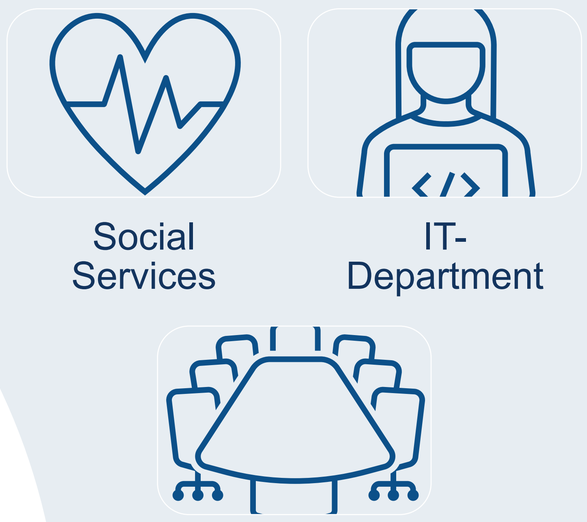
Overcoming cyber attacks through collaboration and coordination across all departments

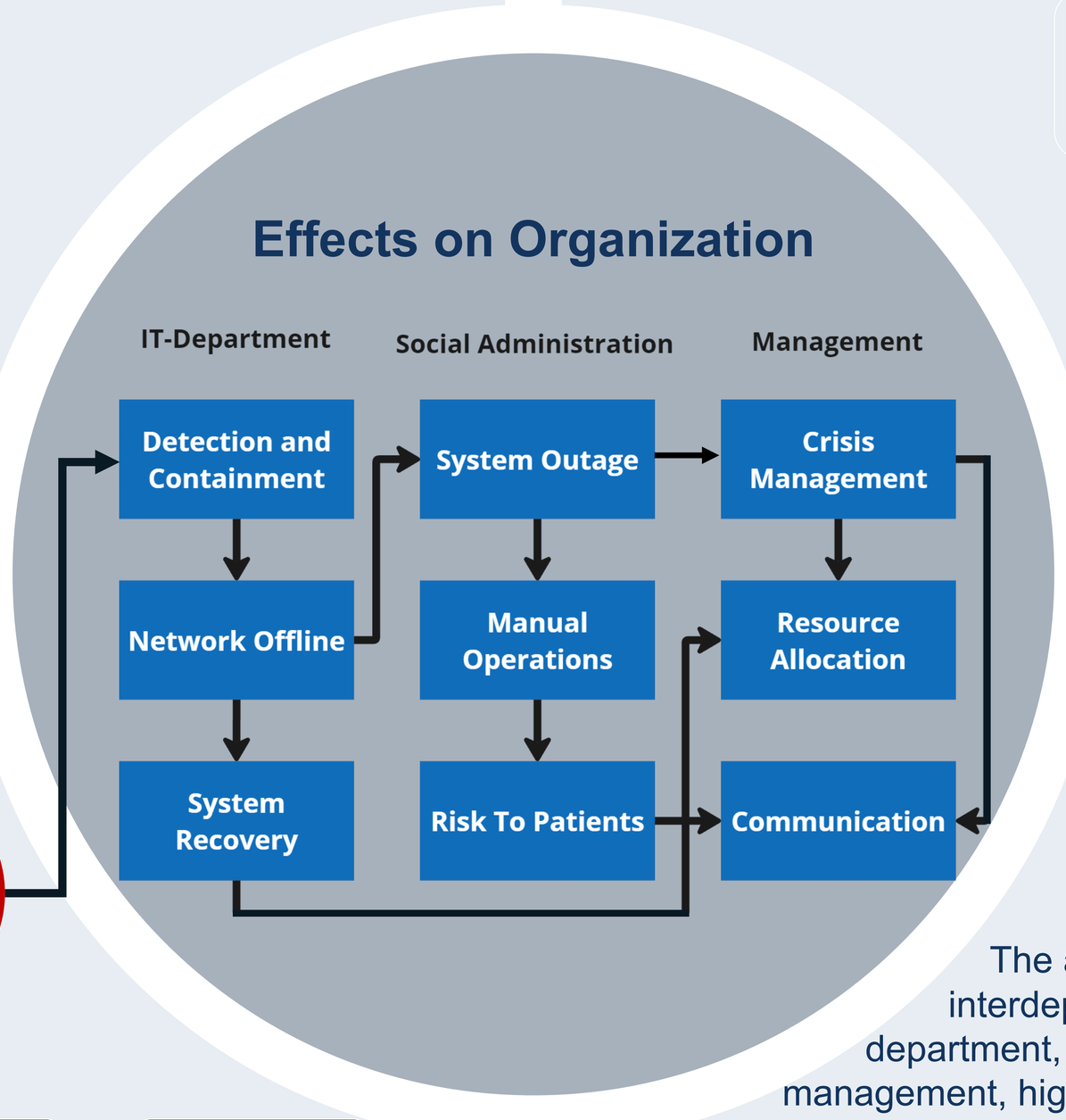
Main Finding

Effective cyber organizational resilience requires a holistic approach, leveraging collaboration and coordination across departments to ensure recovery and adaptability.

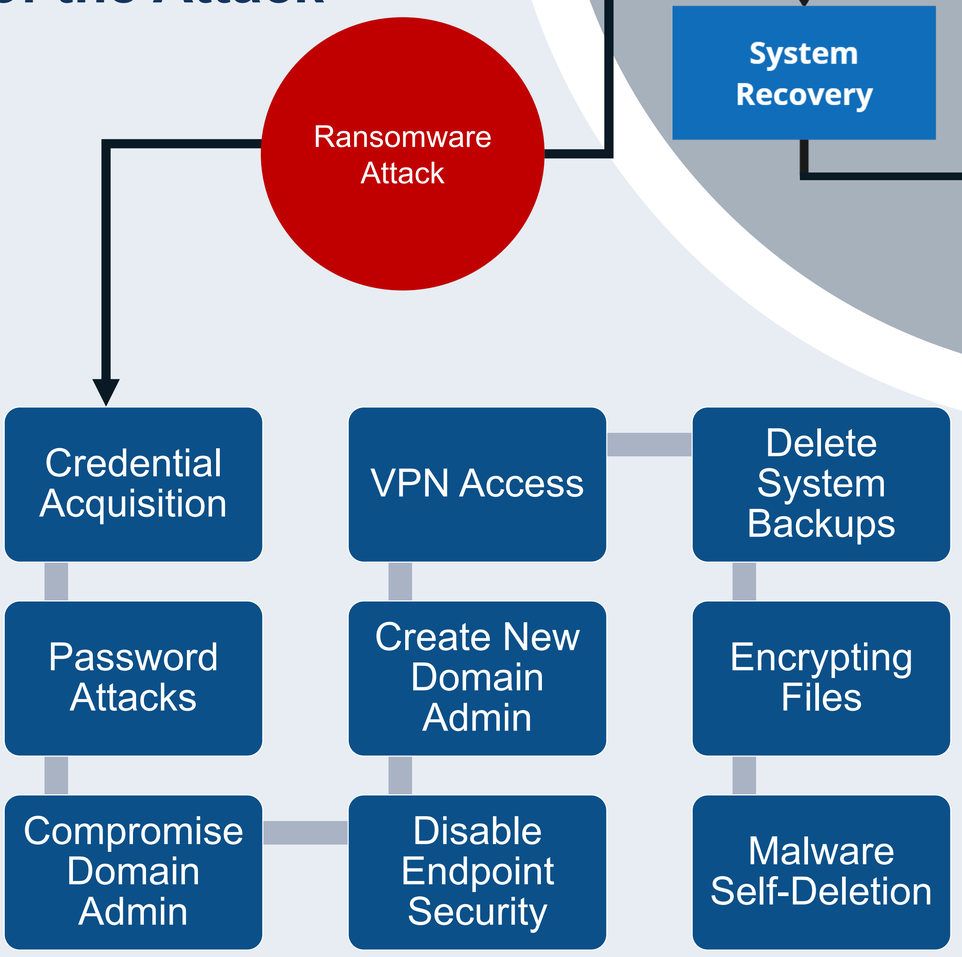
Method

This study adopts a case study approach, combining 19 semi-structured interviews with key stakeholders from IT, management, and social services. Supplementary data sources include police reports, internal documentation, and media coverage, analyzed through reverse root cause analysis to trace the systemic effects of a ransomware attack.





Technical Analysis of the Attack



Results

Coordination across departments was crucial for minimizing disruption.

The attack demonstrated the interdependence of the IT department, social services, and municipal management, highlighting how technical containment measures triggered operational adjustments and management-level decisions.

Conclusions

This case study underscores that building resilience against ransomware requires a holistic approach that integrates technical, managerial, and social responses. Effective recovery hinges on cross-departmental collaboration and systemic planning. These findings highlight the need to treat cybersecurity as an organizational concern, not just a technical challenge.

FIRST AUTHOR ANTON HOLMSTRÖM

Interreg Aurora ISSUES
Co-funded by the European Union
LULEÅ UNIVERSITY OF TECHNOLOGY