

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

Anton Holmström<sup>a</sup>

*Institution of System and Space Science, Luleå University of Technology, Luleå, Sweden*

**Keywords:** Cyber Resilience, Information Security, Cyber Security, Incident Management, Ransomware, Business Continuity, Crisis Management, Cyber Crisis.

**Abstract:** As cyber threats grow in complexity, organizations must rethink their approach to information security, moving beyond technical solutions to focus on building organizational resilience. Previous research has primarily relied on a technical perspective, often overlooking the broader interdependencies between different organizational departments. This case study examines how a ransomware attack impacted a Swedish municipality by conducting semi-structured interviews with key individuals from IT, social services, and management, supplemented by internal documentation, police reports, and news coverage. The findings underscore the crucial role of cross-departmental collaboration and coordination in managing cyber incidents. Specifically, the study highlights how IT, social services, and management were interdependent in handling the crisis, demonstrating the need for their inclusion in the overall information security planning. This case provides valuable insights into the challenges public-sector organizations face during a cyberattack, offering a detailed understanding of how one municipality responded, recovered, and adapted to such an incident.


## 1 INTRODUCTION

At the end of 2021, the small Swedish municipality of Kalix gained national attention after being subjected to a large-scale ransomware attack that severely disrupted its operations and tested its overall resilience. This event presents a valuable opportunity to examine how different parts of an organization respond to cyberattacks, revealing the interconnectedness of technical, social, and managerial processes in incident handling. The attack forced the entire social services department to revert to analog operations, required the IT department to rebuild its infrastructure from scratch, and placed significant political and media pressure on the municipal leadership.

As cyber threats continue to rise globally, ransomware remains one of the primary concerns for organizations. According to recent reports by Verizon (2024) and ENISA (2024), the number of cyberattacks is increasing, with ransomware attacks still among the most prevalent. Ransomware typically involves threat actors taking control of a target's assets and demanding a ransom to restore access (ENISA, 2024). In response to this evolving threat land-

scape, organizations invest heavily in security solutions, such as technical tools, employee training, and security personnel (Carpenter and Roer, 2022; Shaikh and Siponen, 2023). While these proactive investments are crucial, they must be supplemented with reactive measures, which prepare organizations to respond effectively when preventive security controls fail (Baskerville et al., 2014). Incident and risk management provide a structured approach to responding to cyber incidents. However, as Benoît Dupont (2019) notes, reactive measures alone are insufficient for ensuring an organization's long-term resilience. The concept of cyber resilience—the ability to withstand, recover from, and adapt to digital disruptions—has emerged as a critical factor for organizational survival in the digital age (Seyedehsaba Bagheri et al., 2023; Björck et al., 2015; Linkov and Kott, 2019). Cyber resilience involves a continuous cycle of activities, from planning and detection to response and adaptation, to strengthen defenses against future threats (Benoît Dupont, 2019).

This paper aims to provide a detailed account of how a ransomware attack impacted a Swedish municipality, demonstrating how technical, social, and managerial responses were interdependent throughout the crisis. An organizational crisis is a low-probability,

<sup>a</sup>  <https://orcid.org/0000-0002-0498-4858>

high-impact event that threatens an organization's continuity, and its cause, effect, and resolution are clouded with uncertainty, alongside the perception that rapid decision-making is necessary. (Pearson and Clair, 1998). The study views the case by following the cyclical approach of preparedness, response, recovery, and lessons learned principles, often found in crisis and incident management frameworks (Boeke, 2018). Applying this cyclical approach to different organizational perspectives allows for a view of the systemic approach necessary to plan for, respond to, and recover from such an incident. Highlighting the importance of collaboration and coordination when facing adversity provides valuable insights for future research on how organizations can enhance their preparedness and resilience against similar cyber incidents.

## 2 METHODOLOGY

### 2.1 Case Study

This study employs a case study approach to examine the widespread effects of a ransomware attack on a Swedish municipality (Yin, 2018). Over several weeks, the attack disrupted IT, social services, and core business operations. The case study focuses on the municipality's responses, strategies, and adaptations during the crisis. This approach is well-suited for capturing the complexity and dynamics of real-world incidents (Walsham, 1995).

### 2.2 Data Collection

Data collection incorporated multiple sources to understand the incident and the municipality's response. Using Walsham (1995) interpretive approach, I explored the subjective experiences of stakeholders. Nineteen semi-structured interviews (Kvale, 2012) were conducted with IT personnel, management, and social services employees (see Table 1). Interviews covered preparation, actions taken, and lessons learned from the crisis, with most lasting about an hour. While most were recorded and transcribed, some were not due to the topic's sensitivity.

To complement the interviews, I collected and analyzed various types of related data sources. This included:

- **Police Report.** Detailed the investigation and provided insights into the legal and procedural aspects of the attack.

- **Internal Documentation.** Included security policies, project reports, and internal communications related to the incident.
- **Media Coverage.** National and international news articles highlighted public narratives and external perceptions of the municipality's crisis response.
- **Consultancy Reports.** Updates from consultancy firms offered external perspectives on the technical and strategic measures taken during the crisis.

This combination of interviews and other relevant sources provided a solid foundation for analyzing the incident from multiple perspectives, ensuring a comprehensive understanding of the municipality's response.

### 2.3 Data Analysis

I employed a reversed root cause analysis to systematically trace the effects of the ransomware attack across the municipality, following the method outlined by Andersen and Fagerhaug (2006). This technique allowed me to work backward from the observed consequences of the attack, identifying the underlying factors and connecting them to the initial technical incident. By focusing on the impact rather than the cause, I could map how different departments—IT, Social Administration, and Management—were affected and how their responses were interrelated.

This analysis highlights the interdependencies within the organization and demonstrates how technical, social, and managerial factors combined to shape the response to the attack. By identifying these connections, the root cause analysis helped reveal the systemic nature of the incident, emphasizing the importance of cross-departmental coordination and collaboration in managing such crises. This systems overview forms the basis for the case description, providing a comprehensive understanding of the organizational response to the ransomware attack.

## 3 RESULT

### 3.1 Kalix: A Swedish Municipality

Kalix municipality is a Swedish municipality located in Norrbotten County, with the major city being Kalix. With around 15,480 inhabitants, it is a small municipality (Statistics Sweden (SCB), 2024). Swedish municipalities consist of a political function

Table 1: Interviews Conducted During the Incident Investigation.

Interviewee	Role and Description
IT-Consultant	External consultant working with incident handling.
IT-Consultant	Working as incident manager and forensic lead.
IT Manager	Current head of the IT Unit. Initial and follow-up interview.
Security Manager	Head of Security. Initial and follow-up interview.
IT-Controller	Quality assurance and monitoring. Initial and follow-up interview.
Staff Manager (Stabschef)	Manager for the IT unit during the crisis.
Head of Communications	Responsible for communication and information.
Head of Social Administration	Senior official in the social services department. Initial and follow-up interview.
Head of Unit	Manager for a work unit in elderly care.
Area Manager	Manager for ordinary housing at the social administration.
Assistant Nurse	Working at an elderly home care service unit.
Coordinator	Digital locks and vehicle coordinator at social administration.
Information Security Coordinator	Working with information security at social administration.
Area Manager	Working with information security questions at social administration.

and an administrative organization. The elected municipal council (kommunfullmäktige) sets the overall direction and budget, while the administrative organization implements these decisions (Kalix Kommun, 2024). Municipalities are divided into areas and units responsible for various local governance and public services (Rabe and Lidskog, 2024). Swedish municipalities have significant autonomy and responsibility, implementing national policies locally in areas like climate adaptation, sustainability, and public welfare. Their decentralized governance structure enables tailored approaches to local needs while aligning with national objectives (Rabe and Lidskog, 2024). This autonomy also makes municipalities central to local governance and crisis management, allowing for flexible and responsive strategies with minimal hierarchical oversight (van Laere and Lindblom, 2019).

### 3.2 Narrative of the Incident: The Cyber Crisis

In the early hours of December 16th, night shift employees in elderly home care found their planning and business systems unexpectedly unavailable. Initially dismissed as a routine disruption, it soon became clear that a more significant issue was unfolding within the municipality’s IT infrastructure. When the head of the social administration arrived at work later that morning, she received reports from different units also facing unavailable systems, indicating that the situation had escalated. Down at the IT department, similar reports came through from other administrative units.

At this point, the IT manager realized that it was more than a routine disruption, started an investigation, and contacted external consultants for support.

By 10:00, a couple of hours after the initial disruption, the head of social administration contacted the municipality director. After being informed of the situation, the municipality director called for the first crisis meeting to assess the scope and impact of the disruption. During the analysis, it became clear that disruption had impacted all administrative units. At this stage, the municipality director activated ‘stabsläge’ (staff mode). Staff mode can be described as the lowest or first level of preparedness for a crisis or resource-intensive operation. It is commonly used in healthcare and emergency services when a situation escalates beyond normal operations, requiring a more organized and centralized command structure.

At this point, the municipality still treated the disruption as an operational failure, adopting a 48-hour planning perspective. This perspective meant they were preparing for the disruption to last for the next two days, focusing on short-term solutions and stability.

The disruption affected the virtual private network (VPN) and operations across the municipality for example, the city library switched to analog lending, and the indoor swimming pool allowed free entry when its payment system failed.

At 11:30, the municipality informed the public on its website about the situation. Not knowing that it was a cyber-attack, the only information released was that a serious disruption had affected the entire munic-

ipality's operations. Further information was disseminated through the local TV channel around 12:00.

An hour later, at 13:00, the IT department and the consultants could confirm, through their analysis, that the municipality was under attack. A ransomware attack had infected almost all servers, affecting most business systems.

By 15:00, a second crisis management meeting confirmed the ransomware attack. The IT manager reported that most servers were encrypted, sensitive data may have been extracted, and a ransom note, signed "Nothing personal, just business," threatened to publish the data. The crisis team promptly decided against paying the ransom and filed a police report. The municipality's political leadership was briefed to ensure oversight.

By 15:30, a press release was issued, followed by a live press conference at 16:30, where the head of communications, alongside the municipality director, publicly acknowledged the ransomware attack and outlined the municipality's response strategy. Meanwhile, the IT manager engaged with the Swedish National Operations Department (NOA), providing critical information to aid the ongoing criminal investigation.

The following day, December 17th, the crisis management team gathered to review their response plan. At this stage, the impact of the attack was so severe that recovery would take longer than first estimated, forcing the team to switch focus from a 48-hour perspective to a longer crisis plan. Moving forward, the crisis management team would meet twice a day to assess the situation and update their response strategies.

Later in the day, on December 17th, the IT department decided, for security reasons, to take the entire internal network offline. This was to start the recovery and gather evidence for the police investigation. The network shutdown affected all assets relying on internet connectivity, including internal and external websites. By 12:30, the municipality held a digital press conference to update the public on the ongoing situation.

To summarize the steps taken as the situation unfolded and moving forward:

- **December 17th.** A temporary external website was launched to provide updates while email servers remained offline. Social media also played a role in disseminating information.
- **December 18th.** Cyber-attacks targeted the municipality director's personal accounts, likely in retaliation for refusing to pay the ransom.
- **December 20th.** Salary payments were manually processed with help from external financial con-

sultants, ensuring on-time payments despite system disruptions.

- **December 23rd.** All employee computers were collected for a full security overhaul, including reinstalling operating systems and endpoint protections—a process that took 3–4 weeks.
- **December 28th.** The original municipal website was restored, marking a major recovery milestone.
- **January 7th.** Employees changed account passwords using BankID, with alternative verification options provided.
- **January 10th–14th.** Schools reopened, requiring IT to check and reinstall 300 additional computers. A final press conference addressed questions on the attack, its impact, and associated costs.
- **January 17th.** Unpaid invoices and year-end financial processes were completed cautiously to avoid reintroducing risks. A new VPN with multi-factor authentication enabled remote work.
- **January 18th.** The new intranet was launched, restoring internal communications.
- **February 10th.** The preliminary police investigation closed due to insufficient evidence. Further attack attempts from the same and other IP addresses were blocked thanks to the strengthened security measures.

The full restoration of business systems took approximately three weeks, marking the end of an intense period of cyber crisis management. The incident highlighted the municipality's resilience and reinforced the importance of robust cybersecurity and transparent communication strategies.

### 3.3 Technical Analysis of the Attack

This section provides a detailed technical overview of the ransomware attack. While the details such as IP addresses and usernames remain confidential in the police report an attack sequence was developed based on the gathered data. Supplementary information was sourced from third-party forensic analysis of the malware identified on platforms such as VirusTotal and RecordedFuture (Recorded Future Triage, 2024; VirusTotal, 2024). Figure 1 illustrates the attack sequence.

The attack began when the attacker obtained a username and potentially a password. Although the precise acquisition method is unknown, plausible scenarios include retrieval from a leaked database or a social engineering attack, such as phishing. The attack-



ers likely employed brute force or password-spraying techniques to access the system.

The compromised account had domain administrator privileges, enabling the attackers to escalate their access quickly. They used these credentials to gain access to the organization's VPN. Once inside the internal network, the attackers achieved unrestricted access to critical infrastructure, including servers and databases, such as the Active Directory, which manages user accounts and permissions.

With administrative-level access, the attackers began preparations for the deployment of their ransomware payload:

- **Creation of Hidden Admin Accounts.** The attackers created a new domain administrator account, allowing them to operate with elevated privileges without raising suspicion. This step facilitated continued access and operational control within the network.
- **Neutralization of Endpoint Security.** They accessed the Group Policy Management system to disable all endpoint security policies. This critical step neutralized existing defenses and exposed systems to the subsequent malware deployment.

After compromising endpoint security, the attackers used PowerShell commands to download and execute the ransomware across the network. Forensic analysis of the malware revealed the following behaviors:

- **Shadow Copies Deletion.** The ransomware removed Volume Shadow Copies, eliminating a critical backup mechanism and preventing file restoration.
- **Boot Configuration Modification.** Using the `bcdedit` command, the malware altered the system's boot configuration data, complicating recovery by disrupting the startup environment.
- **System State Backups Deletion.** Through `wbadmin.exe`, the malware deleted system state backups, essential for restoring configurations and operational data.
- **File Extension Modification.** The ransomware encrypted files and changed their extensions to indicate compromise. These unique extensions rendered the files unusable without the decryption key.
- **Self-Deletion.** After encrypting files, the ransomware deleted itself to minimize forensic traces and evade detection.

As the encryption process unfolded, critical systems began failing progressively. The attack culminated in widespread disruption, rendering large portions of the

network inoperable. Significant damage had already occurred when the IT department detected the breach, leaving core business systems offline and operational capabilities severely compromised.

## 4 INTERPRETATION OF NARRATIVE

Three perspectives are directly relevant to the presented narrative: the IT unit, the social services administration, and the Management Administration. These three areas were particularly exposed during the cyber-attack and will be the study's perspectives.

### 4.1 IT-Department

The IT department, run by the IT manager, is tasked with supporting service delivery and is divided into different areas: operations, service and support, workplace, network and communication, data center, and business development and projects. The IT unit is also the system owner for the municipality's overall IT infrastructure, with each business unit responsible for its systems.

The IT department's role in managing the cyber attack was crucial, and its efforts can be understood by looking at the issue from a technical perspective.

When reports of disruptions began to pile up at the IT department. The technicians were already hard at work investigating the situation and trying to identify a root cause for the disruption. With a growing suspicion, the technicians could not yet confirm the cyber attack but could, based on their analysis, determine that this was no regular disruption. Feeling the growing weight of the situation, the IT department contacted external IT consultants to aid in the situation.

The IT department and consultants analyzed firewall and server logs, confirming a ransomware attack. Technicians calmly identified infected clients and discovered ransomware notes on most servers, realizing the encryption was already underway. However, they isolated one server while the malware encrypts a large file, capturing it before it could delete itself. Uploading the ransomware to VirusTotal revealed it was a novel strain, as it had not been analyzed before.

By this point, most servers were encrypted, except for some clients not connected to Active Directory (AD) or running older operating systems. Technicians reconstructed a timeline of events using server and firewall logs to understand the attack vector and methods, which formed the basis for the police report. The analysis revealed that attackers gained access via a VPN lacking multi-factor authentication (MFA) and

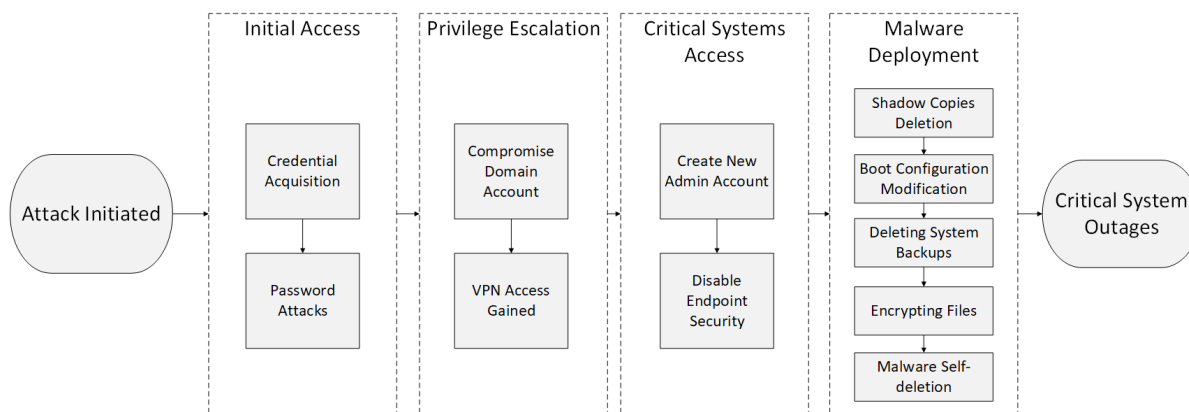


Figure 1: Attack Sequence.

exploited domain admin accounts to disable antivirus protections and deploy ransomware. Details of the attack are outlined in Section 3.3. The reconstructed timeline also guided the restoration process, helping technicians identify safe backups to avoid reintroducing malware.

The widespread impact of the attack exposed gaps in the existing IT infrastructure, prompting a complete rebuild. The team reconstructed the system using backups with Microsoft 365 cloud services and Microsoft Defender Security System. They manually restored and reinstalled all clients, ensuring they were clean by connecting them to Microsoft’s endpoint solutions via an isolated SIEM system. The network was rebuilt with segmentation and tiered user levels, and a VPN with geo-fencing was implemented to support remote work during the COVID-19 pandemic while restricting access to specific geographical areas. An infrastructure overhaul initially planned for three years was completed in just four weeks.

With the new IT environment, the IT team had to ensure the attackers were no longer present. They prompted every existing user to change their passwords by authenticating themselves using BankID, Sweden’s most widely used e-ID for digital identification, or identify themselves in person with physical ID (passport or driver’s license).

In the aftermath of the attack, the IT department was left with many lessons learned, a large list of upcoming less critical security changes that needed to be made, and an increased security awareness among the technicians. The insights and lessons learned led the technicians to review another part of their unit and identify new challenges, like establishing a forum for collaboration between IT, leadership, and the broader organization to drive security initiatives forward.

## 4.2 Social Services Administration

Social services are a central part of Kalix municipality’s core business. It manages various essential services related to residents’ welfare and care. The administration is divided into two main areas: individual and family, and elderly and disabled care. These areas cover everything from support and interventions for families, children, and young people to care for the elderly and support for people with disabilities.

The ransomware attack took all digital systems offline, forcing the elderly care home service—normally reliant on digital tools for scheduling, patient lists, and documentation—to revert to paper and pen. Experienced staff adapted quickly, drawing on prior manual work experience and close team cooperation. However, the transition posed significant challenges, as critical information had to be retrieved from old records or memory and transferred manually. The COVID-19 pandemic worsened the situation, increasing staff strain and patient safety risks. The Social Service Administration relied heavily on swift and decisive management. A home care unit manager described how crisis meetings and clear instructions helped guide staff through the disruption. Despite criticism over the lack of proactive planning, they were able to mitigate the crisis’s worst impacts with strong collaboration and effective communication.

As the crisis unfolded, frontline social service teams had to adapt rapidly. While flexibility and problem-solving were part of their routine, teams with experienced staff found the transition to analog methods easier, while newer employees faced greater challenges. Collaboration emerged as the key to maintaining critical operations. With meetings and planning conducted in person, many teams reported a strengthened collaborative culture, which proved vital during

the crisis and has since influenced departmental practices.

The head of Social Service Administration and the area manager highlighted how the attack fostered a new level of openness and transparency within the organization. Due to the attack, most digital communication channels, including internal and external web pages and email, were disrupted. Extra measures were taken to ensure everyone had access to the information they needed, such as holding frequent in-person meetings and sending information via SMS. This led to a more transparent communication culture.

Interviewees who had participated in crisis planning before the attack noted that this preparation helped them respond more effectively to the new situation. However, they also emphasized that no formal crisis planning or exercises specifically for cyber attacks had been previously done. For many employees, the scale of the attack and the previously unrecognized high reliance on digital systems came as a surprise, revealing their digital reliance as a vulnerability.

The incident highlighted the need for redundancy in critical assets, such as paper records and alternative systems like non-digital locks. In the long term, the attack prompted changes in working practices and a stronger focus on security. A key development was hiring a dedicated information security coordinator to oversee policies, crisis management plans, and collaboration with IT and municipal management on security issues.

### 4.3 Municipal Management Administration

Kalix Municipal Administration plays a central and guiding role in the municipality's activities. It is responsible for leading and coordinating the overall work of the municipality and ensuring that political decisions are implemented effectively and by laws and regulations. The department is responsible for the municipality's strategic planning and governance and controls finances, human resources, and communications. Here, the municipal director, the highest official in the municipality, sits and leads the administration.

When news of the incident reached the Municipal Management Administration, they initially considered it a severe operational disruption. However, as reports continued to arrive from different parts of the organization, it became clear that the situation was more complex than a routine technical issue. The management group swiftly decided to activate the central crisis management team, which included the municipality director, security manager,

and representatives from every administration. The security manager led the group to conduct a situational analysis to establish an overview of the disruption and determine which parts of the organization were affected, allowing them to allocate resources where needed. Since the disruption impacted areas delivering critical societal functions, such as elderly care and home care, health and safety became the top priority. Coordinating efforts across administrations was vital, along with maintaining open communication. Regular meetings with the crisis management group and administration leaders ensured information flowed steadily, keeping employees informed. When it became evident that the disruption was a comprehensive ransomware attack, the management group was informed that the attack had not only encrypted critical parts of the IT infrastructure but also threatened to steal sensitive data. Despite the attackers' threats, the management group remained firm in their decision not to pay the ransom and instead filed a police report. The IT department had already taken the entire network offline, affecting significant parts of the municipality's operations. To ensure that residents and employees remained informed and reassured, the management team provided continuous updates through available channels, including press conferences, announcements on the local TV channel, and a temporary website continuously updated with new information. The management group appointed two key media contacts: the Municipal Director and the Information Officer. The team also implemented a communication strategy, revising it before and after each statement as necessary. The group decided to take ownership of the information early to prevent rumors and mitigate the spread of false information. As the IT department worked to restore operations as quickly as possible, they realized the need to completely rebuild the existing IT infrastructure to minimize the risk of future attacks. The management team decided to proceed with this comprehensive rebuild despite the high costs, viewing it as a reasonable investment given their firsthand experience of the attack. While managing the immediate crisis, the management team also began assessing the financial impact of the attack. The analysis showed that direct costs amounted to nearly SEK 2.5 million, with consulting fees accounting for a significant portion. Other costs included investments in security tools such as Microsoft Defender and overtime expenses for staff involved in incident handling in the IT department and across the organization. The indirect costs of the incident remain speculative. However, it is reasonable to assume that long-term effects include rebuilding trust in the organization and

allowing recovery time for the employees involved. In summary, from the municipal management's perspective, the cyberattack represented a significant crisis that required swift decision-making, close cooperation between management and administration, and transparent communication with employees and the public. Municipal management acted as a central coordinating force, ensuring that residents and employees received the information and support needed while restoring and securing the IT systems that continued in the background.

#### 4.4 Cross-Analysis of the Three Perspectives

The ransomware attack demonstrated the interconnectedness of Kalix municipality's departments, revealing how actions taken by one part of the organization directly influenced the others. As the IT department responded by taking the network offline, this immediately affected the Social Service Administration, forcing them to switch to manual operations, which increased the risk to patient care during the COVID-19 pandemic. Concurrently, the Management Administration was tasked with activating crisis protocols, making critical resource allocation decisions, and ensuring transparent public communication to maintain trust.

The cause-and-effects represented in Figure 1 highlight the systemic impact of the attack across the organization. The cascading effects, from the IT department's technical containment measures to the Social Service Administration's operational changes, emphasize the need for continuous coordination between all departments. Each circle in the diagram shows how actions or disruptions in one area triggered responses in others, highlighting the importance of timely communication and strategic alignment.

This analysis shows that the organization's ability to respond effectively depended not on any single department but on the collective actions and communication between departments. The IT department's technical expertise was crucial in containing the attack. However, the close coordination of the Management and the cooperation and effort of the Social Service Administration ensured the continuity of critical services, such as elderly care. The incident demonstrated that resilience is a shared responsibility across the entire organization.

The case study highlights how the growing complexity of crises, particularly in the digital age, means managing cyber risks is a key part of resilience (Sheffi, 2015). This aligns with Williams et al. (2017), who argues that crisis management and re-

silience are intertwined when facing adversity. However, while this case illustrates the organization's capacity to manage the immediate crisis, it remains difficult to pinpoint the exact characteristics that define organizational resilience in this context. Resilience is often a complex and multifaceted concept beyond technical or procedural measures (Benoit Dupont, 2019). Resilience in practice often involves a combination of formal crisis management protocols and informal, human-driven responses, making it difficult to operationalize and measure (Hillmann and Guenther, 2021). This is reflected in the Kalix case, where resilience was demonstrated, but the exact mechanisms—technical, cultural, or leadership-driven—remain challenging to isolate. Moreover, whether Kalix's response exemplifies resilience, robustness, or even antifragility remains open to interpretation. As Munoz et al. (2022) argues, resilience often overlaps with robustness (the ability to withstand disruptions without degradation) and antifragility (emerging stronger after adversity), making it challenging to differentiate between these outcomes.

## 5 CONCLUSIONS

In this paper, I describe an extensive ransomware attack that hit a Swedish municipality. Although the attack originated as a technical incident, its consequences spread throughout the organization, affecting various departments and functions. This study provides a comprehensive view of how information security should be treated as an organizational concern. Ensuring information and cyber security requires a systemic approach that integrates all interconnected parts of the organization into its security framework. The represented study of a unique case offers a rare, detailed look at the far-reaching impacts of a ransomware attack beyond the technical domain, underscoring the critical importance of social and managerial responses in recovery and resilience. The analysis illustrates that building effective organizational resilience against such attacks requires collaboration and coordination across all departments. The findings from this case offer valuable insights for both practitioners and researchers, emphasizing the importance of addressing cyber incidents from a holistic, organizational perspective. This case can serve as a foundation for further research in information security, particularly in exploring how organizational interdependencies affect incident response. It also offers a detailed scenario for crisis management and tabletop exercises, helping organizations simulate real-world cy-



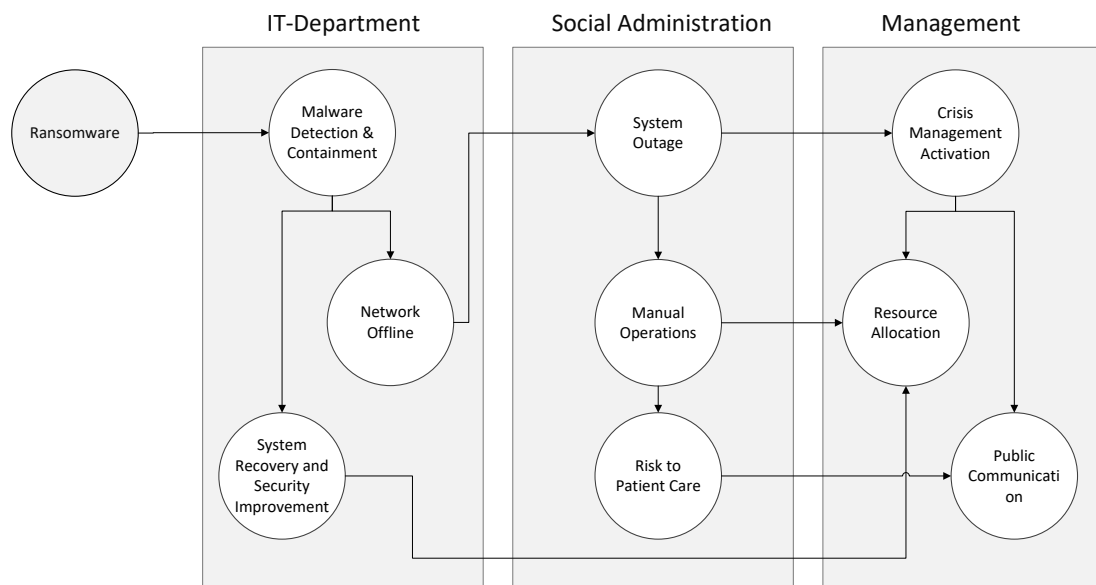


Figure 2: Chain of effect from the ransomware attack.

ber events and strengthen their preparedness strategies. Additionally, the case study can be used in higher education as a working example for students to analyze the complexities of cyber resilience, and in companies and public-sector organizations as a reference for improving cybersecurity frameworks and organizational preparedness. Future research could delve deeper into how organizations can foster the drivers of organizational resilience, such as redundancy, cooperation, transparency, and comprehensive communication, and explore practical ways to implement and operationalize these strategies.

## REFERENCES

- Andersen, B. and Fagerhaug, T. (2006). *Root cause analysis*. Quality Press.
- Baskerville, R., Spagnoletti, P., and Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, 51(1):138–151. Publisher: Elsevier.
- Benoît Dupont (2019). The Cyber-Resilience of Financial Institutions: Significance and Applicability. *Journal of Cybersecurity*. <https://doi.org/10.1093/cybsec/tyz013>
- Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, 353:311–316. <https://doi.org/10.1007/978-3-319-16486-131>
- Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, 31(3):449–464. <https://doi.org/10.1111/gove.12309>
- Carpenter, P. and Roer, K. (2022). *The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer*. John Wiley & Sons.
- ENISA (2024). ENISA Threat Landscape 2024. Technical report, European Union Agency for Cybersecurity. Retrieved September 30, 2024, from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- Hillmann, J. and Guenther, E. (2021). Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews*, 23(1):7–44. <https://doi.org/10.1111/ijmr.12239>
- Kalix Kommun (2024). Kommunens organisation. Retrieved August 26, 2024, from <http://www.kalix.se/kommun/Kommunens-organisation/>
- Kvale, S. (2012). *Doing Interviews*. SAGE.
- Linkov, I. and Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In Kott, A. and Linkov, I., editors, *Cyber Resilience of Systems and Networks*, pages 1–25. Springer International Publishing, Cham. <https://doi.org/10.1007/978-3-319-77492-31>
- Munoz, A., Billsberry, J., and Ambrosini, V. (2022). Resilience, robustness, and antifragility: Towards an appreciation of distinct organizational responses to adversity. *International Journal of Management Reviews*, 24(2):181–187. <https://doi.org/10.1111/ijmr.12289>
- Pearson, C. M. and Clair, J. (1998). Reframing Crisis Management. *Academy of Management Review*, 23(1):59–76. <https://doi.org/10.2307/258633>
- Rabe, L. and Lidskog, R. (2024). Planning and Perceptions: Exploring Municipal Officials' Views on Residents' Climate Preparedness. *Sustainability*, 16(11):4698. <https://doi.org/10.3390/su16114698>

- Recorded Future Triage (2024). Malware Analysis. Retrieved December 10, 2024, from <https://tria.ge/220102-2q4ydaagf9>
- Seyedehsaba Bagheri, Gail Ridley, and Belinda Williams (2023). Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems*. <https://doi.org/10.3127/ajis.v27i0.4183>
- Shaikh, F. A. and Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-023-10404-7>
- Sheffi, Y. (2015). *The power of resilience: how the best companies manage the unexpected*. The MIT Press, Cambridge, Massachusetts London, England.
- Statistics Sweden (SCB) (2024). Folkmängd och befolkningsförändringar - Kvartal 2, 2024. Retrieved August 26, 2024, from <https://www.scb.se/hitta-statistik/statistik-efter-amne/befolkning/befolkningens-sammansattning/befolkningsstatistik/pong/tabell-och-diagram/folkmangd-och-befolkningsforandringar---manad-kvartal-och-halvar/folkmangd-och-befolkningsforandringar---kvartal-2-2024/>
- van Laere, J. and Lindblom, J. (2019). Cultivating a longitudinal learning process through recurring crisis management training exercises in twelve Swedish municipalities. *Journal of Contingencies and Crisis Management*, 27(1):38–49. <https://doi.org/10.1111/1468-5973.12230>
- Verizon (2024). Data Breach Investigations Report. Technical report. Retrieved February 26, 2021, from <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>
- VirusTotal (2024). VirusTotal. Retrieved December 10, 2024, from <https://tinyurl.com/y5xdb7jt>
- Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, 4(2):74–81. <https://doi.org/10.1057/ejis.1995.9>
- Williams, T., Gruber, D., Sutcliffe, K., Shepherd, D., and Zhao, E. Y. (2017). Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams. *The Academy of Management Annals*, 11. <https://doi.org/10.5465/annals.2015.0134>
- Yin, R. K. (2018). *Case study research and applications: design and methods*. SAGE, Los Angeles, sixth edition.