Lessons Learned for Local Cybersecurity: Practical Implications of a Public Sector Cyberattack for Small and Medium-Sized Municipalities

Johanna Maria Schmidt [a*], *Stanislav* Mahula [b], *Joep* Crompvoets [c]

[a] Faculty of Social Sciences, Katholieke Universiteit Leuven (KU Leuven), Leuven, Belgium, johanna.schmidt@student.kuleuven.be, 0009-0009-9530-3832

[b] Faculty of Social Sciences, Katholieke Universiteit Leuven (KU Leuven), Leuven, Belgium, 0000-0003-0568-9604

[c] Faculty of Social Sciences, Katholieke Universiteit Leuven (KU Leuven), Leuven, Belgium, 0000-0003-1077-597X

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 21 May 2025

Abstract. Cybersecurity is an integral part of digital public governance and aims to ensure the confidentiality, integrity and availability of sensitive citizen-, business-, and government-related data. Given the increasing complexity of cyberthreats, driven by the digital transformation of the public sector and emerging technologies, local governments need robust and resilient cybersecurity strategies. This exploratory study examines the October 2023 cyberattack on Südwestfalen IT (SIT), an IT service provider for over 70 municipalities, cities and districts in Germany. As a result of this ransomware attack, for several months, public services were severely disrupted for over 1.6 million citizens. Against the backdrop of the particular challenges that local governments face in managing their cybersecurity, this study identifies lessons that small and medium-sized municipalities and cities derive from this cyberattack. The paper adopts a multi-method qualitative exploratory research approach, combining key informant interviews and document analysis through reflexive thematic analysis. Key findings highlight the importance of thorough implementation of cybersecurity standards such as network segmentation, tighter monitoring practices and two-factor authentication. To mitigate cluster risks, other key lessons include increased focus on top-down decision-making to enforce non-negotiable cybersecurity standards, given the need for IT service collaboration and the use of economies of scale resulting from the resource constraints of smaller local administrations. Further practical implications include an increased focus on staff training and implementing change management strategies to reduce resistance to reform at various stakeholder levels. This exploratory study of the SIT's recent cyber incident also serves as an example for small and medium-sized municipalities that are not part of cooperation networks, encouraging them to reconsider their cost-benefit analysis of independent cybersecurity strategies versus collaborative frameworks. Overall, the study offers valuable insights into the implications of cyberattacks for local administrations of small- and medium-sized municipalities. As such, it aims to contribute to developing more equitable and resilient cybersecurity strategies.

Keywords. Cybersecurity, local cybersecurity strategy, local digital governance, public sector cyberattack.
Research paper, DOI: https://doi.org/10.59490/dgo.2025.994

1 Introduction

Cybersecurity is an essential aspect of digital public governance, encompassing the confidentiality, integrity and availability of data and information (Möller, 2023). Its societal relevance can be illustrated by the direct impact cybersecurity incidents might have on the daily operations of public administration and citizens respectively, including the disruption of critical public services, the loss of sensitive data of citizens, governments and businesses, as well as financial damage and the erosion of public confidence in government (Roumani & Alraee, 2025; Shandler & Gomez, 2022). The landscape of cyber incidents is broad, including data breaches, ransomware attacks, phishing, and denial-of-service (DoS) attacks. It extends further with the advancements of emerging technologies, such as artificial intelligence, which pose unique and novel risks to data and information security (Ndumbe & Velikov, 2024; Savaş & Karataş, 2022). Therefore, considering various types of cyberthreats is crucial to ensure a comprehensive – adaptive and resilient – cybersecurity strategy for any organisation, and thus, adequate incident response and risk mitigation activities.

Local governments are people's first point of contact: the services they provide can have a significant impact on citizens' satisfaction with, for example, democracy, thereby influencing social cohesion and reducing inequalities (Hunter et al., 2016; Masuku et al., 2022; Meza, 2015; Sabbi et al., 2024). For small and medium-sized municipalities (SMMs) and districts, cybersecurity resilience is particularly important. However, while local governments have formal cybersecurity policies, they fail to integrate cybersecurity practices into their day-to-day operations (Hatcher et al., 2020). Researchers have also found that SMMs lack cybersecurity awareness among staff and officials at all levels (Norris et al., 2019; Norris & Mateczun, 2022).The issue is exacerbated further because SMMs, in particular, struggle to maintain human and financial resources to provide quality services (OECD, 2023). While lack of funding and inadequate training have been identified as key challenges, local governments also face a unique set of institutional, political, historical and cultural barriers that influence their ability to prevent and respond to cyberthreats (Hossain et al., 2025; Preis & Susskind, 2022).

At the same time, according to the European Agency for Cybersecurity (ENISA), the majority of cyberattacks in the EU target public administration organisations (European Agency for Cybersecurity, 2024). In addition, ENISA is seeing an increase in the number and advancement of cyberattacks. These developments could become increasingly relevant for SMMs, given their structural vulnerability in this respect. Still, local governments' cybersecurity strategies and incident responses have not been extensively researched (Hossain et al., 2025; Preis & Susskind, 2022). Therefore, this exploratory research aims to answer the following question: *What lessons may small and medium-sized municipalities derive from cyberattacks?*

This paper focuses on a single case study to explore the experiences of SMMs in Germany, where their municipal IT service provider Südwestfalen IT (SIT), a network cooperation owned by 72 municipalities, cities and districts, recently suffered a massive cyberattack (Südwestfalen IT, 2024a). The SIT's owners are also its customers; thus its strategic development is driven by representatives of the SIT's members (Südwestfalen IT, 2024c). Accordingly, SIT is governed by its association assembly, which is made up of elected officials representing the local governments of its member entities.

Based on key informant interviews (KIIs) and document analysis, this paper aims (1) to identify key lessons learned from the SIT cyberattack, (2) evaluate how they impact cybersecurity strategies, and (3) draw practical implications for cybersecurity strategies of small and medium-sized administrative entities.

This study's relevance is twofold: as the SIT cybersecurity incident is relatively recent, mostly journalistic and forensic assessments have been conducted to date (Brockhues & Boeselager, 2024; r-tec, 2024). Drawing on this recent data, this paper examines the real-world strategies of SMMs to address the evolving cyberthreat landscape. As the cyberattack on SIT can be seen as a high-profile incident, examining its strategic implications is directly relevant for other small and medium-sized administrations and can help improve the robustness and resilience of their cybersecurity strategies.

The remainder of the paper is structured as follows: Section 2 presents an overview of related research, followed by Section 3, which introduces the conceptual framework of this study. The methodology is outlined in Section 4 and the key results are presented in Section 5. Section 6 provides a discussion of the main findings, followed by the conclusion in section 7.

2 Literature review

2.1 Key cybersecurity concepts

The term *'cybersecurity'* generally refers to the protection of internet-connected systems, including both hardware and software, as well as data and information, from threats, i.e. cyberattacks (Srinivas et al., 2019). Cyberattacks can have different intentions, such as compromising the confidentiality, integrity and availability of data and

information of public and private organisations (Möller, 2023). Various types of cyberattacks are commonly identified, including spyware that tracks information or a replicating virus that attaches itself to other software. Other examples include ransomware attacks, which encrypt data on devices and offer decryption upon payment of a ransom, and a zero-day attack, which exploits a vulnerability in software before a security patch can be applied. Data can also be threatened by a brute-force attack, which is a trial-and-error method of gaining access to information such as passwords. According to ENISA ransomware attacks rank among the primary cyberthreats (European Agency for Cybersecurity, 2024). The agency also states that cyberweapons targeting zero-day vulnerabilities are a growing concern.

2.2 Cybersecurity in the public sector

While certain aspects to cybersecurity are common across sectors, peculiarities of the public domain make the issue even more acute. The importance of public cybersecurity has increased significantly over the last decades, mainly due to the increasing interconnection between IT and critical public infrastructure (Wirtz & Weyerer, 2017). While this development leads to many positive effects, the public sector represents an attractive target for cyberattacks: public organisations deal with a wide range of sensitive data of citizens, private sector organisations and public infrastructure (Trautman et al., 2024; Wirtz & Weyerer, 2017). Given this field of tension, public governments and administrations are urged by practitioners and researchers to address the evolving cyberthreats through strategic management of cybersecurity (Wirtz & Weyerer, 2017).

Some authors find that municipal governments need to invest in resources and technical capacity building to prevent cyber incidents; others identify leadership in public administration as critical to implementing up-to-date cyber protection measures (Frandell & Feeney, 2022; Wirtz & Weyerer, 2017). In addition, researchers find that local governments of all sizes have significant gaps in their cybersecurity policies (Hossain et al., 2024b). Other research is mainly concerned with structuring the complex landscape of (public) cybersecurity frameworks, with the aim of helping policymakers and practitioners identify gaps and challenges in framework implementation (Hossain et al., 2024a; Srinivas et al., 2019).

While public sector cybersecurity challenges are generally faced by both smaller and larger administration entities, local governments, as the primary bodies politically and administratively in charge of SMM cybersecurity, may face unique obstacles (Hossain et al., 2025; Preis & Susskind, 2022). Based on a study of US local governments, researchers attest that local governments have significant shortcomings in managing their cybersecurity, such as unawareness of security best practices as well as lacking individual risk audits and implementation of existing measures and policies (Norris et al., 2019). These shortcomings are generally linked to limited financial resources and underinvestment, leading to a self-reinforcing cycle of technological vulnerability that ultimately discourages the innovative efforts needed to keep pace with evolving cyberthreats (Fusi et al., 2023).

In addition, researchers have found that rural municipalities with lower citizen demand for digital services also provide a smaller surface area for cyberattacks, although they note that these findings apply primarily to IT departments that manage their cybersecurity independently (Harry et al., 2025). However, other researchers recommend that local governments consolidate IT networks and form municipal collaborative partnerships to mitigate the cascading effects of budget constraints and reduce the fragmentation and complexity of cybersecurity measures (Hossain et al., 2025). On the other hand, research has shown that cybersecurity incidents can have a significant impact on the relationship between IT providers and local authorities, and that repairing trust is a complex process (Nowak & Distel, 2024). Given this complex and sometimes paradoxical landscape of considerations facing SMMs, it is highly relevant to explore the impact of an actual cybersecurity incident on local cybersecurity strategies.

3 Cybersecurity frameworks

In this section, we introduce and discuss how various available frameworks are operationalised and applied as heuristic lenses within the scope of this study (Abbott, 2004).

3.1 Cybersecurity frameworks overview

Various theoretical frameworks exist to cover and structure relevant aspects of this research topic, including the IT security compendium of the German Federal Office for Information Security (BSI), the international information security standard ISO 27001:2022, the US National Institute of Standards and Technology's Cybersecurity Framework 2.0 (NIST CSF 2.0) and the EU's NIS2 Directive.

NIST CSF 2.0 provides flexible, risk-based guidance for private and public cybersecurity management. Taking an outcome- and practice-oriented approach, NIST CSF 2.0 identifies six core functions of a cybersecurity framework: Govern, Identify, Protect, Detect, Respond and Recover. When compared with other frameworks, NIST CSF offers significant advantages for self-assessment, while at the same time, the framework would benefit from simplified

practical implementation (Ibrahim et al., 2018). Moreover, an earlier version of the NIST CSF has already been applied in a study of cybersecurity levels of local government organisations. Examining the cybersecurity levels of a local government organisation in Western Australia, several recommendations were formulated under the core functions of the NIST CSF, such as increasing cybersecurity awareness across the workforce and establishing a central inventory of assets, which serves as a basis for prioritising security measures based on their classification, criticality and business value (Ibrahim et al., 2018).

Ibrahim et al. (2018) also provide valuable insights into the application of the NIST CSF to a local government case, although this exploratory study can build on this by using a more recent version of the framework, i.e. NIST CSF 2.0, which additionally includes Governance as a core function of cybersecurity frameworks. As this study explicitly aims to identify the broader implications of the SIT cyber incident, it is essential to explore the development of governance approaches in this case of municipal collaboration.

In turn, the EU's NIS2 Directive complements this framework by adding a regulatory perspective, which is essential for analysing a municipal case in the EU. As an alternative, the IT security compendium of the BSI could be used (BSI, 2023). However, it may be considered too technical and detailed for the scope of this study.

3.2 Aggregated conceptual framework

In this study, a chosen heuristic lens comprises NIST CSF 2.0 and NIS2, as they are well-known and established cybersecurity frameworks with several strengths and include a wide range of aspects in a flexible way, which is particularly important for this exploratory study. They are also highly compatible and provide an international standard. Our conceptual framework is presented in the table below:

Tab. 1 – Conceptual framework

NIST CSF 2.0 core functions	NIST CSF 2.0 outcomes associated with core functions	NIS2 Directive focus measures
Govern (GV)	Establishing, communicating and monitoring the organisation's cybersecurity risk management strategy, expectations and policy	Appropriate management policies and clear accountability
Identify (ID)	Understanding the organisation's current cybersecurity risks	Regular and coordinated risk assessments
Protect (PR)	Safeguarding to manage the organisation's cybersecurity risks	Implementation of cyber hygiene baselines, practices and controls
Detect (DE)	Finding and analysing possible cybersecurity attacks and compromises	Early warning systems through appropriate technical measures
Respond (RS)	Taking action regarding a detected cybersecurity incident	Response obligations and reporting protocols
Recover (RC)	Restoring assets and operations affected by a cybersecurity incident	Ensuring process continuity and routine operations, as well as recovery measures

4 Methodology

4.1 Case description

SIT was founded in 2018, when two municipal IT service providers merged into the joint association SIT under the Municipal Cooperation Act of North Rhine-Westphalia, with the aim of consolidating their services for the benefit of their member municipalities, cities and districts. Due to SIT members' diverse size and structure, the cyberattack recovery process has been described as a balancing act (Brockhues & Boeselager, 2024). Within the scope of this paper, only SMMs that are members of the cooperation network SIT are addressed (Südwestfalen IT, 2024a).

During the night of October 29 to October 30 2023, the municipal IT service provider SIT detected a cyberattack on its systems, later described as the largest and most complex attack on the German public sector to date, with

over 1.6 million citizens affected (Südwestfalen IT, 2024d). In the following months, the digital public service landscape in this region in North Rhine-Westphalia was described as being thrown back into the Stone Age (Krischer, 2023). The most basic administrative operations, such as communication by telephone and mail, as well as the payment of social benefits, youth welfare services, the legal marriage of citizens and the issuing of driving licences, were unavailable (Brockhues & Boeselager, 2024). While some municipalities were more affected than others, all were severely hampered in their day-to-day administrative work by the SIT's remit: SIT provides comprehensive IT services such as e-government solutions, software development for administrative applications and network infrastructure (Südwestfalen IT, 2024b).

The cyberattack on the SIT in October 2023 exploited a zero-day vulnerability via a brute-force attack and is furthermore classified as a ransomware attack (r-tec, 2024). While the ransomware group that attacked SIT – a Russian collective called Akira – offered to coordinate modalities for recovering the data in exchange for a ransom, SIT chose not to do so due to valid backup copies of the data and the lack of evidence of data leakage (r-tec, 2024).

4.2 Data collection

This exploratory study adopts a multi-method qualitative research approach by relying on KIIs, complemented by archival and desk research (Bryman, 2012). Data gathered through desk and archival research include primary sources such as official records, reports and legislation, as well as secondary data such as academic journals, online databases and press outputs, providing a detailed description of the context of the study (Bryman, 2012). Two key complementary resources are the evaluation report conducted by the external company r-tec on behalf of SIT and a journalistic podcast series published by publicly-funded news broadcasts (Brockhues & Boeselager, 2024; r-tec, 2024).

By drawing on different data sources, theories and research methods, this study aims to fulfil the data, theory and method triangulation principle originally developed by Denzin (Bryman, 2012; Denzin, 2017). This approach not only allows for cross-comparability of findings but is particularly appropriate for this research topic as it involves different stakeholders with different perspectives and priorities (Bryman, 2012). By combining data from different key informants and sources with two different lenses, i.e. NIST CSF 2.0 and NIS2, triangulation provides a more comprehensive view of the research topic and increases the validity and credibility of the findings (Bryman, 2012).

In order to be able to ask open-ended and follow-up questions, the KIIs adopt a semi-structured approach (Magnusson & Marecek, 2015). As the single case study has not yet been widely researched, while preparing the interview questions guided by our conceptual framework, we remained open to new data and aspects that were not anticipated (Bryman, 2012). Potential interviewees were identified through desk research and network referrals, leading to two interviews in December 2024. The overview of informants is presented below:

Tab. 2 – Key Informant Interviews.

Interview	Role	Relevance	Format	Duration
1	Official of one of the districts affected by the cyberattack	Responsible for managing the district's administrative operations Involved in the SIT's strategic development	Online	45 minutes
	Leading member of the SIT's association assembly	The district consists of several SMMs and holds a total population of approx. 260.000		
2	Member of a city council	Represents the city's interests in the SIT's association assembly	Online	30 minutes
	Member of the SIT's association assembly	The city holds a total population of approx. 31.000, of which 15.000 live in the town centre and the rest in the surrounding villages		

The preliminary questions, which were sent to the interviewees in advance for the purpose of preparation, were developed and worded to cover the themes conceptualised by the aggregated framework consisting of the NIST

CSF 2.0 and the EU's NIS2 Directive. Hence, they were structured into the following blocks: implications for cybersecurity strategies and governance; current cyberthreats and protective measures; and threat detection, response and recovery. For instance, the questions asked what specific cybersecurity risks the attack revealed for SMMs, what specific challenges SMMs face in this regard, what impact the cyberattack had on cooperation between the SIT and its owners, and questions about strategies and actions beyond the SIT.

4.3 Data analysis

The data gathered from the interviews and archival and desk research was examined using Reflexive Thematic Analysis (RTA) (Braun & Clarke, 2006). While thematic analysis (TA) generally entails identifying, analysing and reporting on patterns, called '*themes*', within the data at hand, RTA takes a more interactive research approach. In RTA, themes are (re)developed based on analytical and interpretative reflection on the collected data (Braun & Clarke, 2006). Hence, themes emerge from an organic and reiterating coding process that includes review and reflection cycles during the whole data analysis process (Braun & Clarke, 2021a, 2021b). This iterative reflection on the data collected is particularly suited to the exploratory nature of this research, as the interviews, for instance, led to the identification of further resources.

Although RTA does not usually follow a strictly theory-driven approach or involve a priori coding, both cybersecurity frameworks form the initial basis for the data analysis process (Abbott, 2004). Braun and Clarke argue that research cannot be conducted in an atheoretical environment, so RTA aligns with this approach (Braun & Clarke, 2022). In addition, due to the flexible development of themes, (R)TA can be seen as more interpretive, whereas Qualitative Content Analysis is generally more descriptive (Braun & Clarke, 2021a). According to Braun and Clarke, this distinction arises since most TA methods explicitly rely on a discussion of the research's theoretical background. Given the heuristic lenses used, RTA is a better fit for this research.

The interviews were conducted in German, recorded in an audio format and transcribed with Microsoft Edge software (Bryman, 2012). The transcripts were manually cleaned by correcting transcription errors, but no content was edited (Bryman, 2012). Afterwards, the interviews were translated into English, and the correct information conversion was manually reviewed. The data analysis process was supported by the software NVivo 15 (Bryman, 2012).

5 Results

The following results section is structured according to the aggregated conceptual framework introduced in Section 3, which combines the core functions of NIST CSF 2.0 and focus measures of the NIS2 Directive. Due to the exploratory nature of this research, the developed framework served as a heuristic lens and provided a starting point for the data analysis, in order to systematically organise the findings from both the KIIs and the archival and desk research. The first part of this section presents insights related to the functions Govern and Identify, while the second part covers the functions Protect, Detect, Respond and Recover.

5.1 Key lessons learned on Governance and Identification

When it comes to cybersecurity governance, a key takeaway is the introduction of more top-down decision-making: "*And that was one of the lessons we learned: certain things cannot be discussed democratically within such an organisation. Once the necessity of a measure has been recognised, it must be decided top-down*" (Interview 1). This change in the SIT's approach to governance also includes the following measures identified through the themes of this analysis. The governance structure of the SIT does not provide for the network's leadership to be full-time, which is seen as a weakness, especially in times of crisis. In addition, political oversight of the SIT's strategy development through the association assembly is still quite strong due to its make-up, potentially hindering a quick implementation of reforms. However, the interviewees observe a growing understanding of top-down measures.

Cost considerations have also been identified as an obstacle to governance and decision-making: The SIT is supported by levies, meaning the members bear additional costs, e.g. for the implementation of new measures aimed at achieving minimum security standards. Regarding membership policy, the SIT leadership intends to demand minimum security standards: *"[…] SIT's primary focus is, of course, on securing its services and network. To ensure this, minimum standards will be imposed on members in the future. Only those who implement certain measures will even be allowed access to the network*" (Interview 1). Cost considerations and organisational structures, such as resistance of employees, were named as potential barriers to this membership requirement.

The analysis revealed several different risks identified by the interviewees. In terms of understanding the cybersecurity risks of SMMs within the SIT, the cyberattack has particularly highlighted a cluster risk arising from the nature of a cooperative association, where entities pool resources and data. However, this risk was exacerbated by the lack of network segmentation. In addition, the lack of basic security practices, such as two-factor

authentication and password requirements, was also uncovered. Furthermore, the cyberattack underlined the lack of human and financial resources as a particular risk for SMMs. According to the interviewees, this risk can only be mitigated by taking advantage of economies of scale, i.e. by cooperating in networks such as SIT. Additionally, the support of external parties in identifying individual cybersecurity risks is seen as positive, such as a situation analysis provided by the federal state or the involvement of r-tec in identifying immediate, medium-term and long-term measures.

5.2 Key lessons learned on Protection, Detection, Response and Recovery

To protect organisations from cybersecurity risks, the cyberattack has reinforced and revealed the need for several further measures. Regarding cyberthreat monitoring, network segmentation should be increased, especially against the background of the intention to widen cooperation between SMMs. Furthermore, SIT aims to de-complicate the applications it offers to simplify monitoring and updating security standards. Related to this, when evaluating the recovery, the respondents stated that processes varied from city to city and were complicated by the complexity and customisation of applications. During this phase, most cities learned that consolidating IT services can likely reduce the long-term complexity of daily monitoring and future recovery processes, while some cities also restored functionality on their own.

Two key lessons have been learned about future cybersecurity threat detection: (i) Installing tighter cyberthreat monitoring solutions to prevent attackers from moving freely within the network, regardless of significant ongoing costs. Furthermore, (ii) analysing and prioritising security alerts appropriately, i.e. against the background of the individual security architecture.

Regarding the detection and analysis of security alerts, interview 1 revealed that security alerts received from official authorities should be thoroughly read and analysed to assess their risk to SIT's individual infrastructure. Furthermore, the representative of one administration entity names measures apart from SIT, namely educating employees in cyber hygiene, such as password requirements and auto-locking screens. However, the interviewee notes that administrative staff have a limited understanding of such additional protective measures. In addition, the interviewed member of the city council states that the city aims to build offline redundancies for their most crucial processes, particularly ensuring business continuity. For future responses to cybersecurity incidents, the immediate involvement of external experts such as r-tec would be helpful, as would a rapid system shutdown to prevent the worst-case scenario of data theft.

In addition to confirming the previously developed overarching conceptual themes of lessons learned, increasing centralisation and collaboration were identified as themes strongly connected to cybersecurity governance. Even though these measures are not predominantly driven by small and medium-sized administrative entities, they strongly impact their cybersecurity strategies. Furthermore, strategies leading to this goal are supported by the interviewees, such as a state programme to examine the state of cybersecurity in each municipality, city, and district and increasing top-down dictation of minimum requirements.

6 Discussion

6.1 Top-down approach to cybersecurity standards

Two key lessons from the SIT cyberattack include (1) an increased focus on top-down decision-making to ensure effective development and implementation of cybersecurity measures and (2) significant investment in robust and proactive monitoring and segmentation measures. This adjusted governance strategy appears especially relevant against the background of increased costs of additional measures, such as close meshed monitoring.

In addition, although cluster risks are inherent in the structures of cooperative networks such as the SIT, the financial and human resource limitations of SMMs require the use of synergies and economies of scale. Identifying resource constraints as a key factor driving local cybersecurity constraints is additionally underlined by further research (Hossain et al., 2025; Preis & Susskind, 2022). The cluster risks will be mitigated by increasing the segmentation of IT networks according to national and international standards.

Moreover, the cyberattack highlighted the severe deficits in basic cybersecurity practices at an operational level, such as the lack of password requirements or two-factor authentication and has therefore been identified as a focus area both at the individual and at the SIT management levels and will be addressed for example through employee training. This recognition of shortcomings in basic security practices correlates with previous research that identified these as key risks for local cybersecurity (Norris et al., 2019).

Evaluating key lessons derived from the cyberattack, SMMs are incorporating them into their cybersecurity strategies. While respondents support stronger governance frameworks and the enforcement of minimum security

standards – i.e. members will be excluded if they do not comply – other stakeholders not interviewed in this study may be more critical of this change in strategy. The same may be true for increased costs, which in the past have significantly impacted the strategic prioritisation of cybersecurity measures. Striking a balance between affordability and compliance with minimum standards could be crucial for implementing new measures and updated strategies, which correlates with other research that identifies public administration leadership and financial investment as critical factors in managing cybersecurity (Frandell & Feeney, 2022; Fusi et al., 2023; Preis & Susskind, 2022; Wirtz & Weyerer, 2017).

We found increased segmentation, monitoring, and simplification of services as likely cornerstones of an updated SIT cybersecurity measures. These aspects were already evident but became further exacerbated by the cyberattack. However, the withdrawal of individualised IT solutions could trigger further resistance among SIT members, confirming the need for change and expectation management as an additional strategic priority not mentioned in the interviews.

6.2 Greater centralisation and improved local implementation

Regarding practical implications for the cybersecurity strategies of SMMs, centralisation efforts appear to be the most prominent. This overarching strategic trend, such as centralising IT services and deepening collaboration between administrative units, is particularly supported by SMMs due to their limited financial and human resources to maintain an adequate level of cybersecurity. In this process, SMMs can likely be identified as potentially benefiting the most. As these entities depend on pooling resources, they should also strengthen protective measures, such as making certain standards non-negotiable within the network cooperation. They could also advocate for further centralisation at the federal and state levels, which could further increase benefits from economies of scale, such as redundancy and expertise.

This trend towards increased collaboration and consolidation of IT networks is consistent with the findings and recommendations of other research, which identifies cost savings and less complex cybersecurity measures as key benefits (Hossain et al., 2025). However, these findings are not aligned with the implications of other research, which suggests that IT service providers serving more citizens also provide a larger surface area for cyberattacks and a more attractive target (Harry et al., 2025). On the other hand, the respondents are aware of this increase in cluster risk and, therefore, support the introduction of the necessary cybersecurity standards to mitigate these risks and to be able to take advantage of the economies of scale on which they depend. Moreover, something that could be emphasised more by the SIT but is already being addressed at an individual level is cyber hygiene training for employees, which aims to reduce human-related cybersecurity risks. The need to improve and advocate for the implementation of cyber hygiene practices at a local level is also highlighted by previous research (Hatcher et al., 2020; Norris & Mateczun, 2022; Preis & Susskind, 2022).

6.3 Concluding reflections

While most of the key findings can be grouped according to the conceptual framework developed earlier, it becomes clear that they are highly interrelated. For example, reducing the complexity and customisation of IT services aims to significantly simplify Identification, Detection and Recovery, while it is also a key issue for the Governance of cybersecurity strategies. Therefore, effective change and expectation management measures and the involvement of all relevant stakeholders – such as political leaders, mayors and administrative staff – can be seen as crucial to achieving this strategic goal. A strategic change management approach was not identified during the data analysis but could significantly improve and speed up reform processes. As the specific implications of a complex service and governance landscape, such as the case of the SIT, have not been explicitly discussed in prior research, these findings provide new insights into developing cybersecurity strategies of collaborating local governments. However, researchers have previously found that local governments face a unique set of obstacles depending on their institutional, political and cultural context, which this case also confirms (Preis & Susskind, 2022).

Overall, the data analysis confirms the core functions and focal points of a cybersecurity strategy developed based on NIST CSF 2.0 and the EU's NIS2 Directive. In particular, proactive measures focused on preventing future cyberattacks are emphasised due to the accumulation of lessons learned within the themes of identifying, protecting and detecting cyberthreats. Furthermore, many of the consequences drawn were already observed before the cyberattack, but their urgency increased considerably. This increased sense of urgency against the background of evolving technology and public digital transformation is illustrated not only by the interview respondents but also by existing research (Ndumbe & Velikov, 2024; Roumani & Alraee, 2025; Savaş & Karataş, 2022; Wirtz & Weyerer, 2017).

7 Conclusion

This exploratory qualitative research study finds that SMMs affected by the cyberattack on SIT have learned several

key lessons that ultimately affect the realignment of cybersecurity strategies. Overall, the urgency of implementing a proactive, centralised and standardised approach to IT services and cybersecurity strategies and measures was reinforced. In particular, as small and medium-sized administrations face budgetary and human resource constraints, they rely on a collaborative network, such as the SIT, with robust and up-to-date cybersecurity measures mitigating cluster risks. The SIT's cyberattack highlighted critical gaps in basic requirements, such as lack of monitoring, network segmentation, two-factor authentication and password requirements. Given the lengthy decision-making processes on such measures in the past, the interviewees concluded that there should be more top-down decision-making on implementing non-negotiable cybersecurity standards. Based on the analysis, practical implications include greater emphasis on employee training and developing change and expectation management strategies to mitigate resistance to reform. Other municipalities and local administrations not yet attacked might use these practical implications to evaluate their own state of cybersecurity, carefully ensuring the implementation of their national and international standards, such as segmentation and monitoring.

This case also illustrates the need to involve all relevant stakeholders, such as administrative staff through appropriate training, or political and administrative leadership in raising awareness of the need for action. In addition, this case could prompt other municipalities not involved in a cooperation network to reevaluate their cost-benefit calculation for maintaining cybersecurity standards on their own, and hence, likely improving redundancy, effectiveness, and cost-efficiency.

This study relies on two key informants, which may limit the breadth of perspectives. Nevertheless, for an exploratory analysis, the combination of interviews and document review offers a solid foundation. The interviewees can be considered representative of their own district and municipality, though further interviews and comparisons with other small and medium-sized administrative entities would improve the generalisability and validity of the findings.

Despite the limitations of representativeness, this research can be seen as revealing crucial implications for local cybersecurity governance of SMMs and thus providing a starting point for future research. Further research could explore and compare cybersecurity strategy and preparedness in rural and urban, or smaller and larger communities. For example, it would be interesting to further analyse the role of budgetary and human resource factors, as well as interoperability, in order to inform federal-state efforts to centralise IT services. Further research could also explore the role of change and expectation management measures, for example, by assessing the further implications of top-down governance models.

8 Acknowledgements

Contributor Statement*: Johanna Maria Schmidt: Writing – original draft, Conceptualisation, Data curation, Formal analysis, Investigation, Methodology; Stanislav Mahula: Writing – review & editing, Supervision, Visualisation; Joep Crompvoets – Project Administration, Supervision, Resources.

Use of AI*: During the preparation of this work, the author(s) used DeepL in order to translate the interview transcripts. After using this tool/service, the author(s) reviewed, edited, made the content their own and validated the outcome as needed, and take(s) full responsibility for the content of the publication.

Conflict Of Interest (COI): There is no conflict of interest

9 References

Abbott, A. (2004). Methods of discovery: Heuristics for the social sciences. Norton & Company.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021a). Can I use TA? Should I use TA? Should I (not) use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. Counselling and Psychotherapy Research, 21(1), 37–47. https://doi.org/10.1002/capr.12360

Braun, V., & Clarke, V. (2021b). One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE.

Brockhues, A., & Boeselager, F. (2024, June 17). Zero Day in Südwestfalen. Deutschlandfunk. https://www.deutschlandfunk.de/zero-day-in-suedwestfalen-folge-1-hackeralarm-bei- nacht-dlf-cab9c129-100.html

Bryman, A. (2012). Social research methods. (Fourth edition). Oxford university press.

Bundesamt für Sicherheit in der Informationstechnik. (2023, February 1). IT-Grundschutz- Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

Denzin, N. K. (2017). The Research Act: A Theoretical Introduction to Sociological Methods (1st ed.). Routledge. https://doi.org/10.4324/9781315134543

European Agency for Cybersecurity. (2024). ENISA THREAT LANDSCAPE 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

European Union. (2022, December 27). Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)Text with EEA relevance. https://eur-lex.europa.eu/eli/dir/2022/2555

Frandell, A., & Feeney, M. (2022). Cybersecurity Threats in Local Government: A Sociotechnical Perspective. The American Review of Public Administration, 52(8), 558–572. https://doi.org/10.1177/02750740221125432

Fusi, F., Jung, H., & Welch, E. (2023). Technological vulnerability and knowledge of cyber-incidents: threats to innovativeness in local governments? Public Management Review, 1–27. https://doi.org/10.1080/14719037.2023.2250362

Harry, C., Sivan-Sevilla, I., & McDermott, M. (2025). Measuring the size and severity of the integrated cyber attack surface across US county governments. Journal of Cybersecurity, 11(1). https://doi.org/10.1093/cybsec/tyae032

Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. Journal of Cyber Policy, 5(2), 302–325. https://doi.org/10.1080/23738871.2020.1792956

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024a). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences, 14(13), 5501. https://doi.org/10.3390/app14135501

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024b). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. Information, 15(6), 342. https://doi.org/10.3390/info15060342

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in Local Governments: A Systematic Review and Framework of Key challenges. Urban Governance. https://doi.org/10.1016/j.ugj.2024.12.010

Hunter, D. J., Marks, L., Brown, J., Scalabrini, S., Salway, S., Vale, L., Gray, J., & Payne, N. (2016). The potential value of priority-setting methods in public health investment decisions: Qualitative findings from three English local authorities. Critical Public Health, 26(5), 578–587. https://doi.org/10.1080/09581596.2016.1164299

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. The Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

Krischer, H. (2023, December 29). Seit einem Hackerangriff ist in Südwestfalen nichts mehr, wie es einmal war. Welt. https://www.welt.de/regionales/nrw/article249275488/In-Suedwestfalen-hat-ein-Hackerangriff-mehr-als-70-Kommunen-getroffen-auch-zwei-Monate-danach-liegen-noch-Systeme-lahm.html

Magnusson, E., & Marecek, J. (2015). Doing Interview-based Qualitative Research: A Learner's Guide (1st ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781107449893

Masuku, M. M., Mlambo, V. H., & Ndlovu, C. (2022). Service Delivery, Governance and Citizen Satisfaction: Reflections from South Africa. Global Policy and Governance, 11(1), 96-. https://doi.org/10.14666/2194-7759-11-1-6

Meza, O. D. (2015). Local Governments, Democracy, and Inequality: Evidence on the Political Economy of Inequality-reducing Policies in Local Government in Mexico. State and Local Government Review, 47(4), 285–296. https://doi.org/10.1177/0160323X15627852

Möller, D. (2023). Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (1st ed. 2023.). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-26845-8

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Ndumbe, S.I., Velikov, P. (2024). Government Strategies on Cybersecurity and How Artificial Intelligence Can Impact Cybersecurity in Healthcare with Special Reference to the UK. In: Jahankhani, H., Bowen, G., Sharif, M.S., Hussien, O. (eds) Cybersecurity and Artificial Intelligence. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-52272-7_9

Norris, D. F., & Mateczun, L. K. (2022). Cyberattacks on local governments 2020: findings from a key informant survey. Journal of Cyber Policy, 7(3), 294–317. https://doi.org/10.1080/23738871.2023.2178319

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. Public Administration Review, 79(6), 895–904. https://doi.org/10.1111/puar.13028

Nowak, D., & Distel, B. (2024). Trust in Times of Cyber Crisis: Understanding Organizational Trust Repair in the Public Sector. In M. Janssen, J. Crompvoets, J. R. Gil-Garcia, H. Lee, I. Lindgren, A. Nikiforova, & G. Viale Pereira (Eds.), *Electronic Government* (pp. 134–149). Springer Nature Switzerland.

OECD. (2023). OECD Regional Outlook 2023: The Longstanding Geography of Inequalities. OECD. https://doi.org/10.1787/92cd40a0-en

Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. Urban Affairs Review (Thousand Oaks, Calif.), 58(2), 614–629. https://doi.org/10.1177/1078087420973760

Roumani, Y., & Alraee, M. (2025). Examining the factors that impact the severity of cyberattacks on critical infrastructures. Computers & Security, 148, 104074-. https://doi.org/10.1016/j.cose.2024.104074

r-tec. (2024, January 19). Abschlussbericht Security Incident Südwestfalen-IT. https://www.sit.nrw/fileadmin/user_upload/SIT_Incident_Response_v1.1.pdf

Sabbi, M., Osei, A., Wigmore-Shepherd, D., & Ahlin, E. (2024). Minding the local slot: municipalities as drivers of trust in public institutions. Canadian Journal of African Studies, 58(2), 301–325. https://doi.org/10.1080/00083968.2024.2339490

Savaş, S., Karataş, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int. Cybersecur. Law Rev. 3, 7–34 (2022). https://doi.org/10.1365/s43439-021-00045-4

Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks – undermining public confidence in government. Journal of Information Technology & Politics, 20(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Südwestfalen IT. (2024a). Das ist die Südwestfalen-IT. https://www.sit.nrw/sit

Südwestfalen IT. (2024b). Leistungen. https://www.sit.nrw/leistungen

Südwestfalen IT. (2024c). Unsere Gremien. https://www.sit.nrw/sit/gremien

Südwestfalen IT. (2024d, October 30). Ein Jahr nach dem Hackerangriff: Südwestfalen-IT zieht Bilanz. https://www.sit.nrw/detailansicht/ein-jahr-nach-dem-hackerangriff-suedwestfalen-it-zieht-bilanz

Trautman, L. J., Shackelford, S., Elzweig, B., & Ormerod, P. (2024). Understanding Cyber Risk: Unpacking and Responding to Cyber Threats Facing the Public and Private Sectors. University of Miami Law Review, 78(3), 840.

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration, 40(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614