Current Situation Analysis of Information Security Level in Municipalities

Rose-Mharie Åhlfeldt, Marcus Nohlberg, Eva Söderström, Christian Lennerholth and Joeri van Laere
University of Skövde
[rose-mharie.ahlfeldt, marcus.nohlberg, eva.soderstrom, christian.lennerholth, joeri.van.laere]@his.sel

Abstract

Municipalities manage a significant part of society's services, and hence also handle a vast amount of information. A municipality's activities include managing a significant part of society's services, and the municipality's supply and management of information are, therefore, critical for society in general, but also for achieving the municipality's own operational goals. However, investigations show weaknesses in the municipalities' work on information security, and there is a need to study and identify the current level of security. This paper presents the result from a GAP analysis mapping the Swedish municipalities' current situation for systematic information security work, based on the demands made on municipalities from both research and social perspectives. The result shows that the information security level regarding the systematic security work is generally low and that there is a need for adapted tools for Information Security Management Systems in order to support municipalities.

Introduction

Information is a valuable working tool for all types of business, including business in municipalities. Municipalities manage a significant part of society's services, and hence also handle a vast amount of information. There is a pressure on municipalities to become digital, but they cannot simply move online and not rethink the way information is handled, stored, processed, etc. (Li and Yang, 2016). Municipalities' information supply are a critical part of society's information security. Secure information management is an activity issue and therefore encompasses the entire municipality's activities. However, investigations show weaknesses in the municipalities' work on information security, and there is a need to study and identify the current level of security.

A municipality's activities include managing a significant part of society's services, and the municipality's supply and management of information are, therefore, critical for society in general, but also for achieving the municipality's own operational goals. Therefore, Information security covers the entire municipality's activities and includes all information regardless of where in the business it is used, stored or processed. However, information security work in Swedish municipalities has been shown to be of low priority (MSB, 2015) and hence, there is reason to review this work and analyze the current level of security protection regarding information among municipalities.

The municipalities' activities are primarily aimed at the citizens of the municipality, but a large part of the business is also important to society as a whole. The municipalities' tasks include everything from being responsible for the daily care of children and the elderly to ensure that sensitive infrastructure works. Therefore, secure information management becomes a key issue for the municipalities to be able to perform their tasks satisfactorily (MSB, 2012). Information Security Management System (ISMS) is defined in ISO/IEC 27000 standard as part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

This system is applicable for all types of organizations, also for public administration units (ISO/IEC, 2014; MSB, 2015).

Although municipalities handle a significant part of socially essential services, several investigations and studies indicate that the municipalities have not come so far in their information security work (De Lange et al., 2015; MSB, 2015; SOU, 2015). Work in the municipalities is ongoing to protect critical business information highly due to the strong legal requirements that exist to manage the information at a certain level for the various areas of business. However, information security work is often carried out unstructured and not coherent much due to the complexity of different branches of activity in a municipality. Information security work needs to be lifted at the strategic management level in the municipalities for the work to be more coherent and systematically implemented. Successful e-government must, according to Hwang and Choi (2017) entail both technical changes and holistic organisational and administrative innovation.

This paper aims to present results from a study intended to develop practically useful methodological support for strategic information security work in municipalities. This is done by mapping the municipalities' current situation for systematic information security work, based on the demands made on municipalities from both research and social perspectives.

Background and Related Work

Information is an important tool in any organization. It's hard to imagine one day without information but in practice, one day without information becomes impossible. Information should be seen as an asset just like many other important assets that are crucial to an organization's activities and therefore need to be adequately protected. In order to carry out their duties, the information needs to be collected, stored, communicated and processed in different ways. In addition, there may be information in an activity that is extra sensitive or valuable. The consequence of losing such information can be devastating to both organizations and individuals. The organization's information security requirements are based on internal business requirements, but also external requirements from stakeholders, legal and contractual requirements as well as industry requirements. The information must therefore be protected in order to always be accessible when needed (availability), that it is correct and is not manipulated or destroyed (integrity) and that no unauthorized have access to it (confidentiality), these important characteristics that defines information security (ISO/IEC, 2014).

Municipalities in Sweden are organizationally relatively large, but they usually lack the financial resources of comparable private companies to invest in security. The investigated municipalities are small and medium-sized municipalities, which have between 300 and 5500 employees, and turnover from 30M Euro to 280M Euro. These would be fairly large companies, but are considered to be small for municipalities. In Sweden there are 290 municipalities in total.

These organizational problems are not only Swedish. For instance there are similarities in the research that De Lange (2015) describes about South Africa. It is also a challenge in the US (Morgan, 2017). Overall, a majority of countries appear to have organizational units similar to the Swedish municipality, although responsibilities and resources differ slightly.

Local municipalities are increasingly affected by information security incidents. One of the areas where this is often evident is in Ransomware, which has affected several municipalities globally, in some cases, such as San Francisco, very publicly (Rodriguez, 2016). In the general strive to become smart cities; municipalities become significantly more connected, while also potentially critical targets in cyber attacks.

Swedish authorities have carried out audits on municipal information security and found major challenges. For example, 170 out of 241 respondent municipalities currently do not work with a systematic information security work, 129 of 232 do not have incident management systems and 136 of 236 municipalities do not offer their employees education in information security (MSB, 2012). A joint review of information security in public Sweden further highlights the importance of raising the security level

within the municipalities in order for cooperation with other functions in the state to function well (SOU, 2015). The challenges for the municipalities are thus many, large and seem to internationally similar.

As far from the authors' knowledge, there is minor published academic research related to municipalities and information security management. Some work has been done (Lisiak-Felicka and Szmit, 2016; De Lange 2015) and it is essential to improve the understanding since municipalities have a critical role in the society today.

Research Approach

A qualitative approach was used to gather and analyse data related to municipalities' current situation for systematic information security work. A descriptive study (Williamson, 2002) has been conducted to establish current status of systematic information security work in 15 geographically close municipalities. A team of researchers worked together with the municipalities, with the intent of assessing how useful an existing GAP analysis technique is for systematic information security work. Since the goal was to assess the usefulness of existing techniques, the analysis was conducted over a selection of responsibility areas in the municipalities. The selected areas were healthcare, education, and social services, which are critical to society as well as having well established ties to information security issues. The GAP analysis technique consisting of three steps: Identify knowledge sources, document the current situation, and document improvements:

1. Identify knowledge sources: Identification of relevant policies, guidelines, instructions, system documentation etc that provide insight into what has already been implemented and documented, as well as identification of individuals and roles with insight into the way strategic information security work is performed.
2. Document the current situation: Use of a checklist originating from the ISO/IEC 27002 standard which was reviewed with the identified individuals and roles for whether or not they consider security measures to have been implemented or not. An analysis where each response is assessed on a scale between 0 and 3 (0 = no observance, 1 = inadequate observance, 2= acceptable observance, and 4 = high observance). Assessments are aggregated up for each heading level and ends up with a final assessment for each level.
3. Document improvements: After the assessment, a list is compiled over shortcomings, and an action list is construed in which priority, responsibility for implementation etc can be documented.

Before applying the GAP analysis, a review and update of the analysis checklist was conducted in which adaptations to municipal conditions was made. The adapted checklist consisted of 15 main headings, stemming from the updated version of the ISO/IEC 27002 standard (SS-ISO/IEC 27002:2014): Information security policy, Information security organisation, Personnel security, Asset management, Access control, Encryption, Physical and environmental security, Operation security, Communication security, Acquisition, Development and maintenance of information security systems, Supplier relations, Information security incident handling, and Information security aspects concerning organizational continuity.

Members of the research team visited each municipality and met with identified key roles in sessions lasting between 30 and 90 minutes depending on the amount of issues to cover. In this way, all areas of the checklist were covered and distributed between the relevant roles. The municipalities also identified and shared relevant documents with the research team beforehand. After completion of all 15 visits, the results were compiled into one report per municipality. The analysis leader went through the material and assessed the results from sub-sections to main headings in the checklist. The assessment was transferred to a template and visually in tables. Based on shortcomings identified in the material, a primary action list was constructed. A generalised report was also compiled in which the overall results from all 15 municipalities were documented and analysed in an anonymised form. Anonymisation was done as the GAP analysis is only intended for internal assessment and not for comparative purposes.

Results

This chapter presents the overall results of the fifteen participating municipalities in the survey. To make an exact comparison between the municipalities is not recommended for several reasons. In part, the mapping is based on self-estimation, which means that it depends entirely upon the respondents what the results are. Secondly, there are many roles that respond to different areas of responsibility and knowledge, which are not always directly comparable between the municipalities. In addition, there have been various analyst leaders in the respective municipalities, which can also lead to some differences in the assessments. However, it should be noted that the differences between the different analysts' assessments usually differ no more than 0.5 p for each subquestion (MSB, 2011). On the other hand, a comparison can be made in the sense of identifying trends in the result.

There is a clear trend that the level is generally low (1.2). There are also areas that clearly stand out where the shortcomings are commonplace.

Figure 1. presents the overall result of the survey for the fifteen municipalities. The rating levels are the same as those described in chapter 2.

Max value: 3
Norm value: 2
Average of municipalities: 1.2

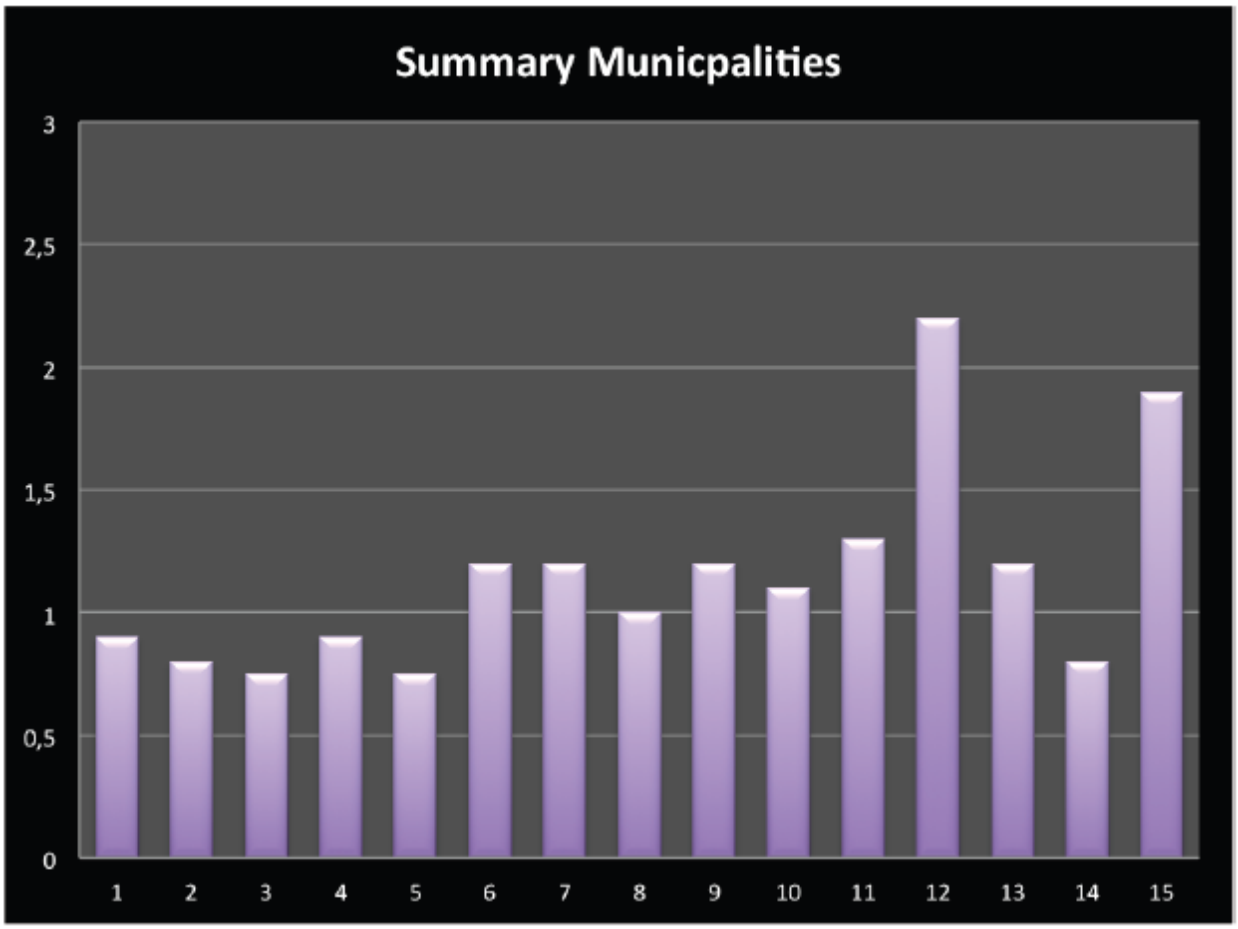

Figure 1: Compiled average result per respective municipality.

All in all, the fifteen municipalities are found to have significant shortcomings regarding their systematic information security work. Two municipalities are around acceptable levels while the others gather

around level 1. It is important to note that the content of the survey includes only the critical actions from the checklist which are considered necessary to have confidence in the information management organisation. In addition, there is also a great variety of municipalities' stronger and weaker areas which are for example, the fact that two municipalities received the same value on the assessment does not mean that their situation is comparable. They can be strong and weak in entirely different areas.

When analysing each chapter area (for analysis details, see Chapter 3), the average values in the analysed municipalities are shown in Table 1.

Table 1: Generalized result per chapter area

Information security policy	0,8
Organisation of information security	0,9
Human resource security	1,1
Asset management	0,9
Access control	1,7
Cryptography	0,2
Physical and environmental security	1,6
Operations security	1,4
Communication security	1,9
System acquisition, development and maintenance	1,3
Supplier relationships	1,2
Information security incident management	0,8
Information security aspects of business continuity management	1,1
Compliance	1,2

A more detailed discussion of these shortcomings and strengths is presented below.

Information Security Policy, Organization and Responsibility

More than half of the municipalities lack an information security policy that demonstrates management's direction of information security, as well as further guidelines and instructions. There may be documents that cover parts, but it is unusual to have a policy that clearly highlights the leadership's will and commitment. There is also a formal organisation around information security with responsible roles at both the top management level and delegated regarding the activities of most municipalities. Hence, the

foundation for a systematic information security work is lacking since the work is not at a sufficiently high strategic level, which is a prerequisite for quality. There is also uncertainty about who will drive this type of work in a politically managed organisation. However, this does not mean that no work is done in the area of information security in the municipalities, but the work is not based on formal documents and is not systematically implemented, which makes work more dependent on the individual's involvement.

Management of Information Assets

There is often some awareness about managing information in the municipalities as they work with communication in general, and have certain types of categorisations such as privacy, document management plans, archiving, etc. However, identification and classification of information assets are missing from an information security perspective. What information needs protection and what level of protection is needed? Awareness is needed for managing all critical information to achieve availability, integrity and confidentiality. As an example, it is stated that in the municipalities, system owners often are designated but not information owners, which is a hint that the municipalities focus more on the digital information (system thinking) instead of including all information in the responsible role regardless of digital or manual management.

Low Level of Competence in Information Security

Many of the identified shortcomings have a clear link to the lack of awareness and competence in the field of information security as a whole. This applies to all levels of staff and entities, ranging from executive roles to employees, as well as specific areas of activity in IT. As mentioned earlier, there is some awareness in the field of health and social care, especially regarding personal data management and confidentiality issues, but moreover, security awareness is low in terms of information management. In the case of education, it is largely exclusively in the form of training for newly employed, but often absent from internal promotion / change of service and as a continuous element in broadcasting skills. A thorough training plan for building an information security competence and, in the long run, a security culture within the municipality's activities is therefore necessary.

Roles for Cryptographic Controls

Cryptography is the subarea that has obtained the lowest assessment level. The area can be seen as highly technical and difficult to comprehend, but what the result shows is whether the organisations have understood and decided on what information, or not, needs to be encrypted and the consequences of this. Encryption as a security control is closely linked to the management of information assets to determine what protection the information needs. Encryption is a crucial security control in information security work, and it is of great value for the municipalities to have an understanding of what the consequences of encryption or lack of encryption are. For example, a lack of key management within the encryption area may mean that all information that is encrypted becomes permanently unavailable. Thus, not carefully scrutinising what is encrypted and how can potentially be behind a substantial level and irrevocable loss of information, even though the encrypted information remains.

Management of Information Security Incidents

Even if information security incidents occur, many municipalities have shortcomings in responsibility and routines for such incidents. This applies in particular to reporting routines, competence issues and contact questions. Employees are not sure who they should report to and which contact point, while there are often no uniform procedures for how the incidents are handled and addressed. This also includes shortcomings in common procedures for evaluating information security incidents.

Continuity Planning for Information Security

A systematic and comprehensive continuity plan for information security is lacking in most cases. If it exists, it is only as part of the general continuity or crisis plans for the municipalities, but in most cases there is a general stumble in which information security is an integral part of such plans. The same applies

to compliance and verification that the work is done as provided for in the plans. Here it is important to emphasize that continuity planning is not just about formal documents. There is also an area where practice must be done to ensure that it really works when something happens.

Supplier Relationships

Each municipality needs to handle a large number of supplier relationships. The result shows that many municipalities are experiencing shortcomings in the process of managing supplier relationships. In many cases, for example, no background checks are made, or checks on the suppliers' security levels. There is uncertainty about, for example, whether operating systems purchased are on cloud services or not, how personal data provided by the vendors is managed and where the servers are located. The question about where the information is located, physically, affects the warehouse concerned and ownership of information. In many municipalities there is no follow-up to the fact that the work ordered has actually been carried out, ranging from small local suppliers who handle parts of municipal operations for a very long time, to very large foreign multinational companies. This means that there are also shortcomings in compliance with security requirements in the supplier agreements, such as rules for the permitted use of information and any requirements for supplier background checks, the supplier's obligation to regularly report the impact of security measures and the obligation to comply with the municipality's defined safety requirements. It is clear that the municipalities with their multifaceted business and many employees have an uneven relationship with many of their system vendors. They are left to the features that suppliers want to offer in their systems, rather than the requirements the municipalities have being met by the suppliers. This is an issue that is difficult to address for the individual municipality, but with the wider use of structured information security work at the municipalities, demands can be made from more and more municipalities, thus balancing the relationship with the suppliers somewhat.

Outsourcing Functions but not Responsibility

Many of the municipalities involved are smaller and therefore need to collaborate with other municipalities to facilitate, for example, the operation of IT, in order to gain and increase the quality of work, but also to make the resources available. However, it is important to note that their own responsibility for the information can not be handed away to another organization, as regulated by law. Information management remains a strategic and important issue in the municipality. The municipality maintains responsibility for the information even though the actual management is chiefly managed by someone else. This requires a great deal in the contractual writing between the municipalities and between the municipalities and their other partners. What's included, what's not included? Again, security requirements need to be lifted in the agreements so that the information and its infrastructure can reach the same level of security that would have been required within the organization. The municipalities can choose to trust someone else, but every municipality needs to ensure what is included in that trust, and what is not.

Existing Systems Control the Work

The products and services purchased from suppliers often control the security requirements of the systems. The municipalities do not usually have enough skills to require differently. In addition, many of the municipalities are too small to get their security requirements from suppliers met if the requirements are solely set by one municipality.

The Gap between IT and Business

Another shortcoming that has been clearly identified during the survey is the gap between IT and business. The various business areas in municipalities often consider and expect the IT unit to take care of, and take responsibility for, many of the security issues that are connected to the business. At the same time the IT department claim that they are solely IT service providers and have not the knowledge to understand the business requirements and needs in the way that the business expects. In addition, the IT department often find that they are not authorised to actually make these decisions. This is a general

problem and not specifically for information security, but it becomes clear that this type of understanding of IT and business has a specific impact on the level of security work.

Communication Security

The subarea where the municipalities actually have an acceptable level, is the communication security and, more specifically, the network security. This is mainly because several of the municipalities have worked with "Basic IT Security Level", which was the previous Swedish guidance for information security from MSB. "Basic IT Security Level" was a feature that emphasises system thinking more than information in general. For example, the formal organization regarding information security with responsibilities at both overhead management levels and delegated down in business is not clarified. Nor is it defined how to handle information assets. However, it is interesting to note that such guidance has nevertheless yielded results in the IT security work, as these areas in the survey generally give municipalities higher values in these areas.

Control of Access to Systems and Applications

Many of the municipalities have an acceptable level of control of access to systems. This is mainly due to that the systems offering features for applying different levels of access. This strength is partly double-grounded, since management partly relates more to the system's capabilities than the business's need for access control, and varies depending on the scope of operations. For example, systems for health and social services have significantly more opportunities for managing access while, for example, systems in the field of education do not have the same extent. Again, it is the business that will set the requirements for controlling access based on the value and protection needs of the information, thus setting these requirements when acquiring systems.

Physical Security – Perimeter Security

The physical security of information has also had an acceptable level for many municipalities. This is largely due to the fact that physical protection includes not only protection of information but also persons and other resources at the municipality. Physical safety work is often handled at a more general level with responsibility for roles as security coordinators or technical management personnel who take overall responsibility for the physical protection of the municipality's resources. This also has an impact on the protection of information which is good, but it is important to point out that there are parts of the physical protection that directly affect information and which need to be considered specifically. For example, most municipalities have adequate physical protection with regard to server rooms, reserve resources, etc. whereas spaces such as switch cabinet for the networks may be exposed and accessible in a very exposed manner. Based on the above, the overall deficiencies and the areas in which the municipalities are better placed are listed below.

Overall shortcomings

- Absence of information security policy and other control documents in several municipalities
- Unclear organization and responsibility of information security
- Low level of competence in information security - formalized education is lacking
- Valuation and classification of information assets based on the confidentiality, accuracy and availability aspects are unclear or lacking entirely.
- Absence of rules for cryptographic security measures in large numbers of municipalities
- Incident handling processes are unclear or missing completely
- Unclear link with information security in municipalities' continuity management
- Non-compliance with compliance

Overall strengths

- Communication security and more specifically network security have an acceptable level.
- Control and access to systems and applications
- Physical safety - predominantly acceptable physical protection

The above results also mainly relate to the image of information security work in municipalities at a national level as MSB has developed in a survey published in November 2015 (MSB, 2015). It appears that many of Sweden's municipalities have shortcomings in their systematic work on information security. It defines shortcomings as policy and governing documents, responsibilities and roles, leading and coordinating information security work, information classes, education and skills development, in order to name some areas.

Analysis and Discussion

GAP analysis as a working tool can be a relatively complicated and resource heavy. It is based on an internationally agreed standard and therefore cannot easily be adopted to the specific domain. It also requires the analyst leader to have a solid basic knowledge and understanding of information security, in order to explain the background to the actions and what they are aimed for. Part of this is the complicated language, which several of the municipalities have highlighted as a problem area concerning the GAP analysis. The balance between what can be customised and what needs to be kept is difficult, in order to be in line with the standard while being customizable and understandable for those who use it. Managing the language is a challenge and not so easy to solve. The result of the survey shows that many of the municipalities have shortcomings regarding the work on information security. Only two out of fifteen municipalities reach an acceptable level. A primary reason is that there is no systematic work on information security at the municipalities. Although the result can be considered disappointing in general, it is important to note that the result does not mean that nothing is done in the municipalities regarding information security. There are apparently both enthusiasts and areas of activity in the municipalities that take great responsibility to ensure that the daily work works well. The survey using the GAP analysis focuses on systematic information security work, which requires formalised documents, procedures and processes for the entire municipality's information management.

In the survey, the main focus areas have been healthcare, social services and education. The areas of healthcare and social services tend to raise more awareness about information security and information management compared to education.

The level of systematic work on information security in the analyzed municipalities may be considered to be inadequate and much work remains. As mentioned earlier, a lot of work is being done in the area of information security in the municipalities, and the results of the survey can thus be surprisingly experienced for some. Therefore, it is important to emphasize that the survey shows the level of systematic work which requires organizational management and technical solutions to create information security that meets the needs of the business.

Below are the suggestions for improvement activities given to the municipalities and which can be seen as common based on the overall analysis. There is an excellent opportunity for cooperation between municipalities to facilitate the development efforts with information security in the municipalities.

- Establish information security policy and other management documents related to information security in the municipalities lacking these documents.
- Organize information security work by defining and assigning responsibility for information security.

- Provide education efforts in information security for both employees and management in order to raise security awareness and create a long-term security culture in the business. It is worth noting the importance of not only having some kind of education for new employees, but regularly training existing employees, especially when changing roles within the business.
- Evaluate and classify the municipality's important information assets based on the accessibility, accuracy and confidentiality aspects.
- Establish rules for using cryptographic security measures where applicable.
- Identify information security requirements and regulations for managing supplier relations.
- Establish regulations and processes for incident management.

The proposed suggestions to the municipalities for improvement measures, mentioned above, should be helpful in starting up the systematic information security work in the municipalities, primarily in the form of the introduction of an ISMS. This is also in relation to Soomro et al., (2016) and De Lange et al., (2015) which state that an holistic approach is needed in information security management. From a scientific view, following contributions can be addressed:

- No similar studies have been made where a complete number of municipalities participate in a specific region, meaning that the result is interesting and verifying important issues for further research.
- Empirical evidence showing the need for a systematic information security
- Empirical verifying a complex area and why not aim for a "quick fix."
- In addition to the survey, the work includes the development and use of an analysis technique that reflects the current situation and gives the municipalities a comprehensive picture of their information security work.

From a practical view, following contribution can be addressed:

- The result reaches out to a broad audience because the study has a municipal perspective, but also county councils, authorities and other organisations have an interest in how the situation is and how the work is done.
- An adaptive analysed tool for the municipality sector in order to identify the level of information security in municipalities.

Future Work

The study presented in this paper includes a significant group of municipalities in a specific local area. However, only the key areas of the municipalities' ordinary business were investigated. More research is needed in order to emphasize secure and efficient information management in other important areas as well, such as, property, operation and maintenance. Another important area highlighted in this study was crisis management. The municipalities have ongoing work connected with count administrative boards regarding crisis management from a civil defence perspective. This demonstrates the need for well-functioning information security work within the municipalities, since the civil defence includes secure information and communication. More research is needed on how this task can be integrated into the municipals' systematic information security work and how collaboration can be addressed and improved between municipalities and other authorities. Another area of improvement is the adaptation of the standard to other branches. In this study the mapping of a GAP analysis was addressed for municipalities.

Similar adaptation may be needed for other branches as well, for instance, healthcare, finance etc. A key issue is to get an adjustment that is not too detailed but still so general that it maintains an applied level.

Conclusions

This paper has presented results from fifteen municipalities in a local area in the west of Sweden. The results show that even if information security management is a crucial concern for municipalities, they do not meet the mandatory requirements set by the government. Municipalities is a crucial part of most societies today, with wide ranging areas of responsibilities. They are large and complex organizations, that often suffer from limited resources, and with different opportunities depending on their individual sizes. Even though there has been an increase in the demands put on them in regard to information security, they seem to be lacking in general. There are many reasons for why, but it might be more relevant to discuss how they can actually improve instead. Our suggestions include, among other, that they could benefit from having a ISMS adapted to their requirements in general, and specifically GAP-toolkits adapted for municipalities. Only through finding key metrics and useful tools, can managements support be ensured, and this is key in this domain, as in many other.

References

Behnia, A., Rashid, R.A and Chandry, J.A, (2012). A Survey of Information Security Risk Analysis Methods. Smart Computing Review, Vol.2, No.1.

De Lange, J., R. Von Solms and M. Gerber (2015). Better information security management in municipalities. IST-Africa Conference, 2015, IEEE.

Hwang, K. and Choi, M. (2017), Effects of innovation-supportive culture and organizational citizenship behaviour on e-government information system security stemming from mimetic isomorphism, Government Information Quarterly, 34 (2017), pp.183-198

ISO/IEC (2014) 27000:2014 Information technology -- Security techniques – Information security management systems -- Overview and vocabulary. ISO/IEC (2014).

Li, Z. and Yang, F. (2016), The e-govermnent information model based on GDR, Procedia Computer Science, 91 (2016), pp.193-200.

Lisiak-Felicka, D., & Szmit, M. (2016). Information security management systems in municipal offices in Poland. Information Systems in Management, 5(1), 66--77.

Lopes, I and Oliveira, P, (2015). Implementation of Information Security Olives: A Survey in Small and Medium Sized Enterprises, New Contributions in Information Systems and Technologies, Vol. 353, pp. 459-468.

Morgan, J. (2017). County and municipal cybersecurity, Part 1. CIO. Available online: https://www.cio.com/article/3184618/government-use-of-it/county-and-municipal-cybersecuritypart-1.html.

MSB (2015). En bild av kommunernas informationssäkerhetsarbete 2015. Myndigheten för samhällsskydd och beredskap (MSB). Advant Produktionsbyrå AB. Publ.nr: MSB943-december 2015. ISBN: 978-91-7383-619-7 (in Swedish). MSB (2012). Kommunernas informationssäkerhet – en vägledning. Myndigheten för samhällsskydd och beredskap (MSB). Danagård LiTHO. Publ.nr: MSB508 – December 2012. ISBN: 978-91-7383-304-2 (in Swedish).

Rodriguez, J. R. (2016). 'You Hacked' appears at Muni stations as fare payment system crashes. San Francisco Examiner, Nov 26, 2016. Available online: http://www.sfexaminer.com/hacked-appearsmuni-stations-fare-payment-system-crashes/.

Solms, R, (2012). Information Security Management: Processes and Metrics. Diss, University of Johannesburg.