A Systems Perspective on Security Risk Identification: Methodology and Illustrations from City Councils

SmartCities

Smart Cities Research Brief
No.9

Abstract

This paper takes a system theoretic perspective to the process of security risk identification in the context of city councils. Based on this approach, we construct a framework that helps to identify risks. We analyze why this methodological framework is suitable for the risk identification process. Research in fifty Flemish city councils reveals the usefulness of our approach of combining a perceived vs. objective perspective with a technical vs. organizational one. We believe such a framework offers a workable tool for dealing with IS security risks in a systems thinking way.

1 A Systems Perspective on Security Risk Identification

1.1 Introduction

Today, city councils increasingly handle sensitive information of their citizens. Therefore the way in which this data is stored, retrieved and processed, becomes more and more important. However, the question arises how well this information is protected from unauthorized manipulation. To find answers to this question, we were asked to conduct an audit in fifty city councils in Flanders (Belgium) in view of identifying the risks these administrations face when handling sensitive data. (Note that for the purpose of this paper and because of a general acceptance in everyday language, we will refer to 'risk' where we technically speaking mean 'threat').

Our research question consists of two components. The first is to clearly identify the latent and manifest risks (Reason 1997) that subsist in the context of city councils, the second is to establish an identification methodology that takes a system theoretic (Forrester 1961) perspective towards risk.

The assumption we put forward relates to the feasibility of the framework we will develop in view of risk identification: we assume that taking a system theoretic perspective is a valuable strategy for identifying a broader and deeper range of risks than by taking a one-dimensional perspective (Gerber and von Solms 2005; Van Den Eede and Van de Walle 2006). Indeed, while conducting the audits in the city councils, we learned that using a strictly regulated method for analyzing risks is not sufficient. This observation is explained more in detail in the next sections. We experienced that when using an approach that includes system thinking and constructivist triangulation helps the auditor in analyzing IS security

risk. Hence our choice for an inductive research approach and the data collection to validate it.

What triggered our research is the finding that, even though the importance of information security is acknowledged, city councils have limited time, budgets, knowledge and awareness of information security and the corresponding threats (Berghmans et al.). To raise awareness, it is important that the risks are described in their context. If the context is ignored, the justification of the risk will be hampered, leading to mitigation guidelines that may not be acknowledged. Such will negatively influence awareness (Siponen 2000). For this reason, placing the risks in their context and as such explaining cause-effect relations, will positively influence the justification of the risks and the methods to mitigate them. Justification will result in a change in attitude and motivation towards mitigation guidelines (Siponen 2000). As such the need for a particular risk identification methodology imposes itself.

In this respect we take a system theoretic perspective towards risk identification, which will lead us to a methodology that combines a technical and an organizational point of view on the one hand, and an objective and perceived reality viewpoint on the other hand. When combining these perspectives, four quadrants emerge. In the remainder of this paper we will first focus on the methodological foundation by describing the relevance of system theory for this purpose and the four quadrants of our framework. Next we will show some illustrative cases which are built based on the experience in the city councils. In the subsequent section we will explain how the illustrative cases and the methodology relate and contribute to a better way of identifying risk. Finally we will conclude our findings and indicate possibilities for future research

1.2 Methodology

In this section, the risk identification process will be discussed in relation to the risk management process. The importance of using a system theoretic perspective when identifying risks will be explained. In the last part, the four quadrants model will be constructed. This model helps to identify cause and effect relationships between distinct identified risks in the context of the organization.

1.2.1 Risk Identification

Risk can be defined as the probability of an exposure and the cost (or loss) associated with the exposure (Courtney 1977). Risk management is the process in which an organization tries to identify, analyze (assess) and control risks (the risk strategy). The goal of the risk identification is to surface major risks before these badly influence the organization. By conducting a risk assessment, the risks will be prioritized against criteria relevant for the organization. To control risks, the organization has to decide which risks will be accepted and which will be avoided. Although these phases in risk management are not always distinctive in nature, this paper mainly focuses on the first part of the risk management process: identifying the risks, in this case of Flemish city councils.

As studied by Dhillon and Backhouse (2001), there is a growing disillusionment with the formal rational and overly mechanical conception in the analysis of Information Systems. As technical concepts become more embedded in the organizational structure, there is a growing demand to adopt social aspects. Current IS research addresses both man and machine and organization and technology (Dhillon & Backhouse 2001), but this is not yet reflected in the way risk analysis is conducted (Rutkowski et al. 2006). By using strictly regulated methods to conduct a risk analysis, the focus on risk remains incomplete and narrow: checklists of controls and mechanistic security engineering methods (Baskerville 1993).

1.2.2 Systems thinking and constructivist triangulation

Referring to Reason's Swiss Cheese model we could say that traditional risk identification is about finding the holes in the cheese (Reason 1997). Then, about estimating their importance in terms of impact and frequency, and finally, plugging them by effectuating the appropriate response.

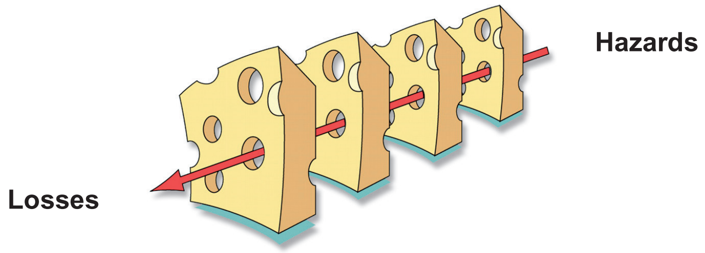


Figure 1

Swiss Cheese Model (Reason 1997)

The mainstream risk frameworks and best-practices, evangelized by consultants and business schools alike, propagate this same approach as sanctifying. Guaranteeing tomorrow's reliability by managing today's risks is at best a partial solution for the foreseeable problems, but at worst, tells nothing about the future reliability in terms of the management of the unforeseeable ones. The cure for this deeply rooted practice can be best described as systems thinking. It forms the backbone of this paper.

Systems thinking suggests that when we understand the structure of a system, we are in a much better position to understand and predict the behavior of the individual elements (people) and their relationships and can therefore make better decisions (Siponen 2000, p. 279): "Being restricted by living space, the frog living in a well cannot talk about the sea; being restricted by life-span, the worm living in the summer cannot talk about ice."' In other words, everybody's consciousness is limited by space and time, which presumes that a human being is necessarily unable to know the world in its entirety. In this respect, systems thinking can serve as an antidote for prejudice.

As important as the holistic view offered by the systems thinking perspective, is the constructivist triangulation approach we adhere to. In our philosophical assumption of the ontological and epistemological character of security, risks cannot be treated as a physical attribute 'out there' that can be measured (Oscarson 2007). Risk identification based on this worldview assumes risks to be mediated through social experience and interaction. (Renn 1998) This stems with a constructivist view which – in contrast to the objectivist approach – sees risk as a social artifact, produced by social groups or institutions, and determined by structural forces in society (Oscarson 2007). The audit technique used for this study reflects this world view.

1.2.3 Four quadrants

To help organizations in taking the difficult hurdle of risk identification, we propose a framework that consists of two perspectives only, but they are perspectives that are at the heart of security risk identification:

The first perspective is the difference between reality (risks identified based on objective measures) and perception (risks identified based on perceptions of individuals). This distinction is a basic component of systems thinking (Sterman 2000) as we have made clear. It implies thinking beyond the boundary of the obvious and the immediately observable. As we will explain below, the interpretation of risks can lead to new risks or can identify risks that would not be found when using objective measures.

The second perspective is what is generally dealt with in Information System (IS) literature as components of a system's reliability, namely the technical and the organizational component (Butler and Gray). Organizations become more and more dependent on Information Systems (Car 2003). This triggered the evolution from a narrow technical view on Information Systems (IS) towards an integrated view of organizational and technical concepts (Baskerville 2005). The distinction between the technical and organizational perspective in our model will prove to be essential for the understanding of the system under research. We argue that a perspective that sees procedure as the consequence of technology (and the other way around) is wrong in essence. The advantage and value of the approach we suggest is precisely that these should be viewed as two distinct aspects of the IS security paradigm. First we make this distinction (analysis phase) and subsequently we combine the emerging insights (synthesis phase) into risks. To do so, we first rely on a univocal interpretation of mutually exclusive categories. Indeed, when one does not take a system theoretic approach, technology is distinctive from organization and vice versa. And an observation is either objective or perceived. As such, risks will be identified in this first place distinctively, hence, positioning them in one of the four quadrants. The advantage is that in this analysis phase there are no grey areas, which eases and purifies the thinking about risk.

In the next, synthesis phase, however, the System Theoretic component comes into play when combining quadrants into a Sensemaking (Weick 1995) exercise of finding storylines that reveal formerly hidden risks. In this second phase, those risks will be interconnected, clarifying the cause-effect relationship between them. This creates a dynamic flow, which improves the understanding of the risk. “The propagation of effects linked by causative mechanisms, is essential in the improvement of information security” (Gonzalez and Sawicka 2002).

Figure 2 illustrates the double entry matrix we use in this paper. On the vertical axis, there is a differentiation between the perception of risk and the risks identified by procedures. The horizontal axis differentiates the technical and organizational risks. In each quadrant a method of the analysis of information security risks is situated. Quadrants I and II represent the risks perceived, respectively from an organizational and technical point of view. Quadrant III represents identified organizational risks and Quadrant IV represents identified technical risks.

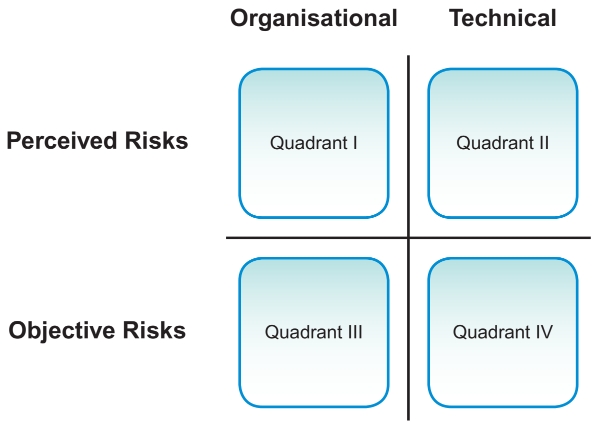


Figure 2

The four quadrants of risk identification

1.2.4 Perceived risks

During the risk management process, the perception of the possible threats influences the outcome. Risk perception is inherently subjective. Many cognitive and psychological processes influence an individual’s perception of risk (Slovic 2000). Also on the level of the organization as a whole, the perception of risk differs between professional groups. Previous research by Rutkowski et al. (2005) revealed that the perception of IT risks of the IT staff differs from the perception of the business managers. More specifically, when the concept of business continuity is considered, the business managers thinks in terms of time and cost of an IT failure, but have no feeling for what actually may go wrong in this respect. The IT managers on the other hand know what IT systems are running, but have insufficient knowledge of the business consequences. The research also suggested the need for more collaboration and awareness of both professional groups of the same organization.

The subjective nature and the need to combine the perceptions of risks emphasize the need to develop a methodology of risk analysis that involves different stakeholders in the risk identification process. In our proposed research methodology, interviews from both technical and organizational perspective are conducted to provide for a comprehensive risk assessment.

The purpose of the perspective of perceived risks in our framework is to appreciate the opinion of organization stakeholders in view of IS security risk detection. Their view on the situation is invaluable for detecting possible pitfalls concerning Confidentiality, Integrity and Availability (CIA).

Quadrant I: Perceived organizational risks

To detect perceived organizational risks, we used the method of Value Focused Thinking (VFT), as described by Keeney (1992) and applied by Dhillon and Torkzadeh (2006) in the area of IS security. By using VFT in the context of IS security, we can learn about the objectives of a stakeholder regarding IS security risks. The study of these objectives gives the researcher insights in the perception of risk in their organization. The method of VFT also learns how IS security differs among different stakeholders.

The interviewees for the detection of perceived organizational risks are the security officer, an IS user, a member of the board of directors and the person responsible for IT. The interviewee is asked to prepare the interview by describing ten objectives of IS security for his or her organization. These objectives will be discussed in depth during the interview. To conclude, the interviewer translates the objectives to risks for the organization. Hence, the detected risks can be used as perceived organizational risks.

Quadrant II: Perceived technical risks

With respect to the technical viewpoint, two respondents are interviewed: a member of the IT staff and an IS user. The interview with the IT staff member consists of two parts. First, the respondent answers questions about the context of IT in the city council and the technical implementation of the IS. Next, based on a technical scheme of the IT infrastructure, critical components are identified. The aspects of availability, integrity and confidentiality of the network components are discussed. The interview with the IS user is on a less technical level and focuses on the use of software tools and how to handle critical data. The perceived risks associated with the use of those tools and data are discussed.

1.2.5 Objective risks

The auditor's view (i.e. the perspective taken by the researcher, external auditor, third party) is equally important because it offers a complement to the perspective of the internal parties (See: Perceived risks). This view adds insights from literature, best practices, expert knowledge and an open mindedness towards the organization. Many procedures to objectively identify risks are available today (Aven and Kristensen 2005). The procedures used for this purpose, are briefly discussed below.

Quadrant III: Objective organizational risks

The organizational detection procedure consists of the detection and the research of formal procedures and policies. By assessing their maturity, possible risks can objectively be identified.

In the first procedure, the respondent answers a questionnaire based on topics of ISO 17799:2005. The questions are selected by a group of experts affiliated with Flemish city councils and are structured in the domains mentioned in Table 1. The possible answers reflect the maturity of their implementation in the organization. This questionnaire is then used as a basis for the interview. During this interview, the researcher asks more in depth questions concerning the security domains of the ISO norm.

In a second procedure, the interviewer tries to identify risks by conducting a 'social engineering' research. The input for the social engineering process is done together with the respondent. Some examples of the social engineering process are: trying to get critical data by using public search engines, phone calls to achieve passwords and physically trying to enter a secure zone.

Security policy
The organization of IS
Asset management
Human resources security
Physical and environmental security
Communication and operation management
Access control
Information systems acquisition, development and maintenance
Information security incident management
Business continuity management
Compliance

Table 1

The security topics of ISO 17799:2005

Quadrant IV: Objective technical risks

In order to detect objective technical risks, we conducted an audit in five technical areas: detection of network components, detection of configuration weaknesses, investigation of network traffic, the computer of an IS user and application testing.

The purpose of the first procedure, the detection of network components, is the mapping of both the internal and external structure of the network by using common open source tools, like Ping, Traceroute, Nmap, Wireshark and Netstumbler.

A second procedure is constructed to detect common configuration weaknesses in mainly critical network components. Besides common open source tools like Nmap, Telnet, Dig, and Wikto, a vulnerability scanner is used to achieve this. In this procedure, special attention is given to the firewalls, mainly the firewall protecting the internal network from the internet.

The third procedure guides the exploration of the internal network traffic. This is accomplished by using Wireshark. The goal of this procedure is to detect encrypted and unencrypted network traffic. Also the broad- and multicasting streams of network devices is inspected, to detect configuration issues.

In the fourth procedure, the computer of an IS user is examined. In contrast to the second procedure, local configuration settings will be explored under supervision of the IS user. Besides a more technical investigation, the researcher asks questions about the usage of the IS.

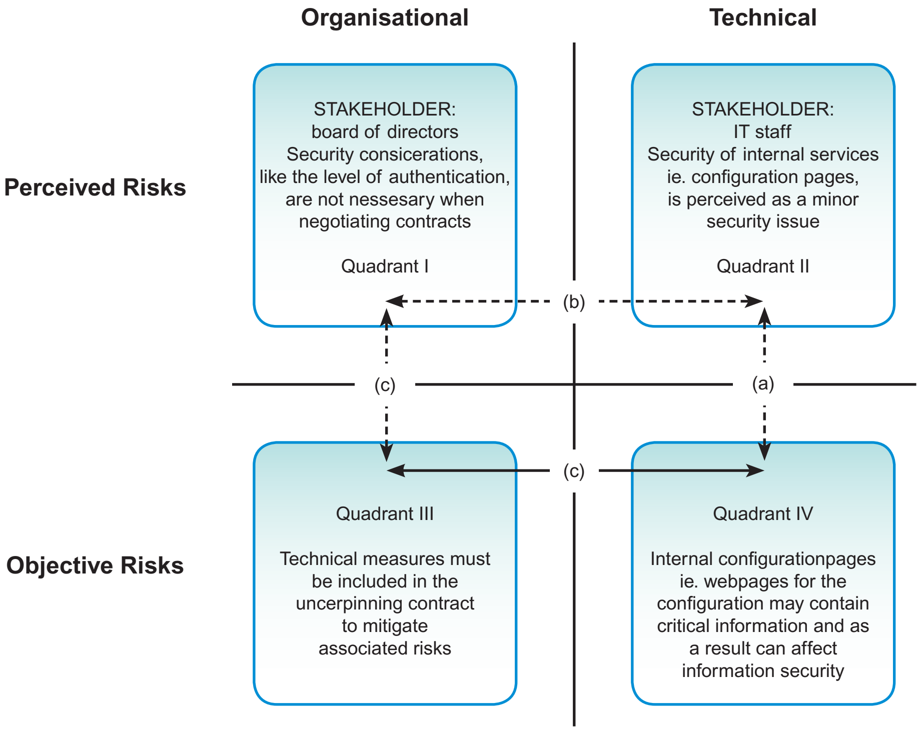
In the fifth and last procedure, some basic application testing is done. It is, however, important to notice that, due to the specific nature of applications used in city councils, application testing has not to be done on the level of city councils. It is better to accomplish this task on national level.

1.3 Illustrative Cases

In this section, we present two illustrative cases of risk identification based on the framework presented above. In both cases, distinct risks are considered, the combination of which can result in a violation of Confidentiality, Integrity and Availability (CIA). By combining different risks, the cause and effect relationships will become clear. The method described in this paper and summarized in Figure 2 will help in detecting the relationships. The dotted lines from Figure 3 and Figure 4 illustrate the cause and effect relationship of identified risks. The full line illustrates the recommendation to mitigate the risks.

Case 1

In the first case, a city council outsourced the technical management of the print servers. For this purpose, a contract was signed between the contractor and the city council. However, no security considerations were applied. While conducting the technical research, the researchers found an unprotected webpage that was used to manage all the printers of the organization. The researchers gained full access to this page, which, off course, should be protected for unauthorized users. When taking a closer look to the webpage, a clear text username and password was found. After using the username and password in trying to access critical servers, administrator access was granted. To conclude, it took the researchers less than 10 minutes to obtain full access to the critical components of the IT infrastructure.



STAKEHOLDER: board of directors
Security consicerations, like the level of authentication, are not nessesary when negotiating contracts

STAKEHOLDER: IT staff
Security of internal services ie. configuration pages, is perceived as a minor security issue

Technical measures must be included in the uncerpinning contract to mitigate associated risks

Internal configurationpages ie. webpages for the configuration may contain critical information and as a result can affect information security

Figure 3

Case 1: The print server administrator page

This case shows that a combination of different risks results in a serious risk in case of an attack. The CIA of critical data is in danger. Figure 3 explains the application of our model in this case:

The IT staff is not aware of security consequences associated with unprotected configuration pages on the internal network. However they insist that those pages should be protected, the lack of authentication is not perceived as a high risk: they doubt the critical character of print servers regarding the overall information security (II). Our research has proved this perception to be wrong: the username and passwords are in readable format included on the configuration page (IV). In addition, the lack of diversity in usernames and passwords on different systems negatively influences the risk.

As a consequence of this technical perception (II), there was no awareness of the members of the board of directors for organizational (i.e. administrative) measures to control the risks associated with the outsourcing activity (I): the level of authentication of the configuration pages is not negotiated.

As a consequence of this organizational perception (I) the security issue was not introduced in the underpinning contract with the service supplier (III). Hence our conclusion and recommendation to take technical measures that mitigate the technical risks (IV) of CIA violation in the domain of print servers and to back this up with the necessary contractual guarantees at the side of the contractor (III).

Case 2

In the second case, the combination of different risks, found in many of the Flemish city councils, can be exploited by attackers. It was found that in many of the city councils, the firewall seems to protect the city council from attacks that are actively initiated from the Internet. The protection of the network traffic from the local network to the Internet was perceived as trusted, so no protection of the firewall concerning outgoing network traffic was implemented. Also, in a lot of cases, users were using their computer with administrator rights. Combining this with the lack of awareness of the IS users, which was found in nearly all of the city councils that were investigated and the insufficient practice of patch management, a scenario as described below is not inconceivable.

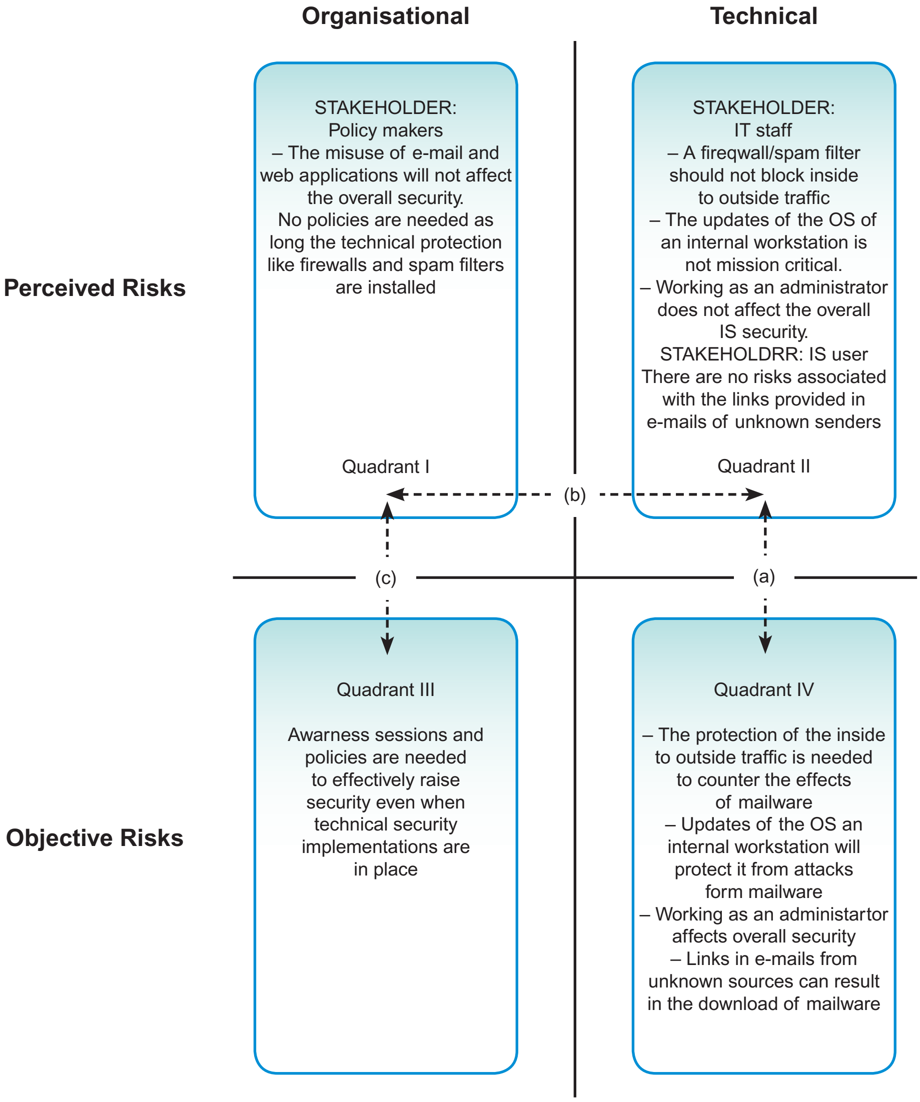
The IS user receives an e-mail from an unknown sender. The e-mail, (that was not intercepted by the spam filter) contains a link to an attacker's website. As the receiving IS user is interested in the subject of the e-mail and is not aware of the risks associated with e-mails from unknown senders, the user clicks on the link provided by the e-mail. By doing so, the user initiates the attack: a request to the web server will be initiated. After receiving the request, the web server (of the attacker) will generate an answer for the IS user. This answer contains the information the user requested. Additionally, the web server of the attacker is programmed to include exploit code in the answer of the request. The information and the exploit code is sent back to the IS user. When receiving the answer, the computer of the IS user processes it. The computer, which is not patched and is used with administrator rights, will not only show the answer in the browser of the user, but will also execute the malicious code that was included in the response. This code will infect the computer. As a result, the computer contacts persistently the attacker, without the interaction of the user. The firewall, which is not configured to distrust network traffic coming from the internal network, passes trough the connection and the attacker has been successful. The attacker can use this persistent connection to investigate the computer and in the worst case, the whole network. As most of the networks of city councils are not segmented and no boundaries between the IS user computers and the critical servers exist, the CIA of the IS are at risk.

By using the model, this situation can be explained as shown in Figure 4.

a. The combination of four technical perceptions is the basis of this case. Firstly, the IT staff perceived the combination firewall-spam filter as being a sufficient method to mitigate the risks associated with e-mail (II), however, fighting spam can't be fully effective (IV). Secondly, by updating the operating systems of the computers, the risk of unavailability of other software is perceived higher than risks associated with outdated software versions (availability) (II). This example shows, however, that by combining the risks associated with possible vulnerable computers, may harm the whole organization in the perspective of CIA (and not only availability). The third technical perception that is proven to be wrong, is that working as an administrator is safe. In many cases users grant this access because of the ease to install own software. By using Internet and e-mail as an administrator, exploit code can harm the computer CIA (IV). The last technical perception is the perception of the IS user that underestimates the risks associated with the use of links in e-mails from an unknown source.

b. As a consequence of the four technical perceptions above, the use of e-mail and Internet was perceived as being completely safe (II). The risks associated with the misuse of Internet and e-mail is considered low. As a consequence, the policy makers perceive no risks of the lack of awareness campaigns of IS users (I).

c. Hence our conclusion and recommendation to consider awareness sessions for both the end users and the IT personnel (I) to explain the risks associated with the usage of e-mail and Internet. By raising awareness of the end users, they can avoid risks that are difficult to counter by technical security implementations (III). The IT staff on the other end must be aware of the risks associated with a firewall that only blocks the incoming traffic.



	Organisational	Technical
Perceived Risks	STAKEHOLDER: Policy makers – The misuse of e-mail and web applications will not affect the overall security. No policies are needed as long the technical protection like firewalls and spam filters are installed Quadrant I	STAKEHOLDER: IT staff – A fireqwall/spam filter should not block inside to outside traffic – The updates of the OS of an internal workstation is not mission critical. – Working as an administrator does not affect the overall IS security. STAKEHOLDRR: IS user There are no risks associated with the links provided in e-mails of unknown senders Quadrant II
Objective Risks	Quadrant III Awarness sessions and policies are needed to effectively raise security even when technical security implementations are in place	Quadrant IV – The protection of the inside to outside traffic is needed to counter the effects of mailware – Updates of the OS an internal workstation will protect it from attacks form mailware – Working as an administartor affects overall security – Links in e-mails from unknown sources can result in the download of mailware

Figure 4

Case 2: Spam opened by an IS user

1.4 Discussion

The two illustrative cases in the previous section show that a risk identification method must span the four quadrants. As a consequence, risk identification methods that concentrate on objective measures overlook or ignore the context. When using only technical or organizational measures, the real cause of risks may be overlooked.

The use of objective measures stimulates the perception that risks are distinct. During our research, however, it became clear that risks aren't distinct in nature. By using the constructed framework, the researcher is stimulated to place the risks in the context of the organization. The consequence of this practice is that interrelationships between risks will become clear. As a result, this model helps to identify the best countermeasures to mitigate risks.

When considering the cases, it should also be clear that often, risks are at the intersection of the objective and the perceived level. This implies that the result of a risk identification process will be different depending on the organization. As a consequence, this framework can also be used to understand the importance of the organizational context when implementing security guidelines. When the context is omitted, new risks can be initiated. The perception of the risks will influence the construction and implementation of security guidelines.

When interpreting the illustrative cases, it becomes clear that risk is propagated on the boundary of the quadrants representing the perception of technical and organizational risks (quadrant I and II). Hence our recommendation that a committee, presented by all departments and levels of the organizations, must be implemented to detect possible risks due to different perceptions. This was one of the most frequent recommendations we made to Flemish city councils. It was found that in practice this guideline typically was only implemented for legal compliance reasons. This is a perfect example of how security guidelines, when implemented, can create a false feeling of being secure. The lack of awareness on all levels of the organization is a contextual factor that influences the implementation of this security guideline.

1.5 Conclusion

This paper shows that an identification procedure must have both technical and organizational measures to detect real risks. As the illustrative cases show, by using objective tools, various potential but distinct risks were discovered. This research showed that when those risks are placed in the framework from Figure 2, the cause and effect relationships between distinct risks become clear.

Our risk identification method may be applicable in other risk identification scenarios as well. Also, it can serve the process of constructing organizational guidelines.

When considering only a part of this framework while identifying risks, the real cause may be overlooked. The framework presented, showed that the analysis of both the perception of risks and objective risks, technical and organizational, helps to interpret the risk in the context of the organization. Hence, the risks are justified, which leads to a higher level of awareness of the risks. As a consequence, taking a system theoretic perspective may positively influence the risk assessment and the risk mitigation.

2 Further information

2.1 References

1. Aven, T. and Kristensen V. (2005) Perspectives on risk, Reliability Engineering and System Safety, 90, 1, 1-14.
2. Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, ACM Computing Surveys, 25, 44, 375-414.
3. Baskerville, R. (2005) Best Practices in IT Risk Management, Cutter Benchmark Review, 5, 12, 5-12.
4. Berghmans, P., Van Roy, K. and Lenaerts, M. (2008) Menselijke factoren in de informatiebeveiliging van lokale besturen, Praktijkgids Lokale Besturen, In press.
5. Butler, B.S. and Gray P. (2006) Reliability, Mindfulness, and Information Systems, MIS Quarterly, 30, 2, 211-224.
6. Carr, N.G. (2003) IT Doesn't Matter, Harvard Business Review, 81, 5, 5-12.
7. Courtney, J.F. (1977) Security risk analysis in electronic data processing, Proceedings of the AFIPS Conference, 97-104
8. Dhillon, G. and Backhouse J. (2001) Current directions in IS security research: towards socio-organizational perspectives, Information Systems Journal, 11, 2, 127.
9. Dhillon, G. and Torkzadeh G. (2006) Value-focused assessment of information system security in organizations, Information Systems Journal, 16, 3, 293-314.
10. Forrester, J.W. (1961), Industrial Dynamics, MIT Press, Cambridge.
11. Gerber, M. and von Solms R. (2005) Management of risk in the information age, Computers & Security, 24, 1, 16-30.
12. Gonzalez, J. and Sawicka A. (2002) A Framework for Human Factors in Information Security, Proceedings of the 2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro, Brazil
13. Joint Technical Committee ISO/IEC JTC1 (2005) Information Technology - Security Techniques - Code of Practice for Information Security Management.
14. Keeney, R. (1992) Value-focused Thinking: A Path to Creative Decisionmaking, Harvard University Press, Cambridge, MA.
15. Oscarson, P. (2007) Actual and Perceived Information Systems Security. Doctoral dissertation, Linköping University (S), Department of Management and Engineering.
16. Perrow, C. (1999) Normal accidents, 2nd ed., Basic Books, Princeton, NJ.
17. Reason, J.T. (1997) Managing the Risks of Organizational Accidents, Ashgate, Burlington.
18. Renn,O. (1998) Three decades of risk research: accomplishments and new challenges, Journal of Risk Research, 1, 1, 49-71.
19. Rutkowski, A.-F., Van de Walle, B, van Groenendaal, W. and Pol, J. (2005) When Stakeholders Perceive Threats and Risks Differently, Journal of Homeland Security and Emergency Management, 2, 1,1-15.
20. Rutkowski, A.-F., Van de Walle, B. and G. Van Den Eede (2006) The effect of Group Support Systems on the Emergence of Unique Information in a Risk Management Process: a Field Study. Proceedings of the 39th Hawaii International Conference on System Sciences, Poipu, HI.
21. Siponen, M.T. (2000) A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8, 1, 31-41.
22. Slovic, P. (2000) The Perception of Risk, Earthscan Publications, London, Sterling, UK.
23. Sterman, J.D. (2000) Business Dynamics: Systems Thinking and Modeling for a Complex World, McGrawHill, Boston, MA.
24. Van Den Eede, G. and Van de Walle B. (2006) Four Perspectives - Three Dimensions. Risk Management as a Cognitive Object. Proceedings of the Third International Symposium on Systems & Human Science, Vienna (A).
25. Weick, K.E. (1995) Sensemaking in Organizations, Sage Publications, Thoasand Oaks, CA.

SmartCities

3 Document information

3.1 Author(s) and Institution(s)

Peter Berghmans is an industrial engineer (De Nayer Instituut). He is a professor in network technologies at the University College of Mechelen. Since September 2005 he works part time at Memori, on a PWO research project “ICT-security for local governments”. He maintains strong relations with several Flemish e-security companies, and he is also very familiar with the specific working environment of local governments.

Co-authors of this research brief are Gerd Van den Eede (University College of Brussels – Belgium) and Bartel A. Vandewalle (Tilburg University – The Netherlands)

This research brief is based on a conference presentation that was published in the “Proceedings of the 5th International ISCRAM Conference – Washington, DC, USA, May 2008”

3.2 Critical issues addressed

This paper takes a system theoretic perspective to the process of security risk identification in the context of city councils and construct a framework that helps to identify risks.

3.3 Document history

Date	:	2008.05
Version	:	1
Author	:	Berghmans et al.

The Interreg IVB North Sea Region Programme

Investing in the future by working together for a sustainable and competitive region

www.smartcities.info

www.epractice.eu/community/smartcities

The Smart Cities project is creating an innovation network between cities and academic partners to develop and deliver better e-services to citizens and businesses in the North Sea Region. Smart Cities is funded by the Interreg IVB North Sea Region Programme of the European Union.

Smart Cities is PARTLY funded by the Interreg IVB North Sea Region Programme of the European Union. The North Sea Region Programme 2007-2013 works with regional development projects around the North Sea. Promoting transnational cooperation, the Programme aims to make the region a better place to live, work and invest in.

9 781907 576034