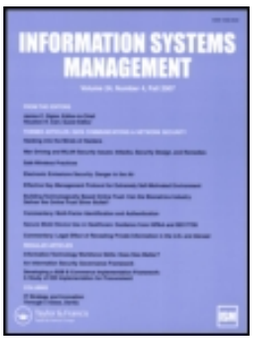

Information Systems Management

ISSN: 1058-0530 (Print) 1934-8703 (Online) Journal homepage: http://www.tandfonline.com/loi/uism20

Information Security Risks in Enabling e-Government: The Impact of IT Vendors

Peter Berghmans & Karel Van Roy

To cite this article: Peter Berghmans & Karel Van Roy (2011) Information Security Risks in Enabling e-Government: The Impact of IT Vendors, Information Systems Management, 28:4, 284-293, DOI: 10.1080/10580530.2010.514212

To link to this article: http://dx.doi.org/10.1080/10580530.2010.514212

Published online: 13 Oct 2011.

Information Systems Management, 28:284–293, 2011

ISSN: 1058-0530 print / 1934-8703 online
DOI: 10.1080/10580530.2010.514212

Taylor & Francis
Taylor & Francis Group

Information Security Risks in Enabling e-Government: The Impact of IT Vendors

Peter Berghmans and Karel Van Roy
Lessius Mechelen University College, Mechelen, Belgium

The purpose of this article is to identify information systems security risks in local governments resulting from the cooperation with IT vendors. We focus on government-to-government projects where the confidentiality, integrity, and availability of information is a key concern. In our risk identification process, we take a systems thinking approach, taking into account actual and perceived risks. We identified 13 causes of risk in three risk areas and analyzed them using outsourcing literature.

Keywords information systems security; outsourcing; systems thinking; value-focused thinking; e-Government

Information Systems Management 2011.28:284-293.

INTRODUCTION

In this article we discuss the information systems security (IS security) risks local governments face in their e-government activities. More specifically, we focus on risks resulting from the participation of information technology (IT) vendors in government-to-government projects. This activity will be referred to as outsourcing. We define e-Government outsourcing as contracting out the development, implementation, and maintenance of e-Government tools to third party suppliers (Cordella, & Willcocks, 2009). We study the IS security risks of IT outsourcing in e-Government activities of local governments in 70 local governments in the Western European region.

Among other activities, the local governments in this study assist their citizens by granting them specific minimum services for social security (the granting of subsidies for the handicapped, guaranteed family allowance, minimum income, and income guarantee for the elderly) after checking their subsistent resources. For this purpose, the federal government of public welfare in the West European region in study provides a reference repository (RR). This initiative provides the local government information on the social security status of each citizen. Here is where the role of the IT vendor comes into play. In the area of study, four IT vendors are certified to develop software for accessing the RR. The local governments use their services to get and maintain access to RR and to integrate the information in other applications.

When outsourcing IT services, the local government in the area of study stays responsible for the confidentiality, integrity, and availability (CIA) of the data they process. The federal government of public welfare expresses this responsibility by means of a security policy for local governments. The federal government can conduct audits to check compliancy. If the local government is not compliant with the federal security policy, access to RR can be denied. Despite their high impact on the CIA of the data processed, no such policy exists for the IT vendors. Hence, it is difficult for both the local government and the federal government to control the IS security behavior of the vendors. This triggered the federal government to conduct a risk analysis concerning the impact of IT vendors on the IS security of local governments. We were asked to accomplish this task. Our research reveals 13 causes for IS security risks (Table 1), which can be used by the federal government to develop an IS security policy for IT vendors. To better understand the consequences of our findings, we studied relevant outsourcing literature. The 13 causes of risks and their consequences are presented in Section 4 of this paper.

To conduct a risk analysis, we do not rely on strictly regulated methods, evangelized by consultants and business schools alike. We also take into account the perceived risks of stakeholders. In Section 3, we will explain our risk identification methodology more in detail.

It is important to note that the risks resulting from the outsourcing of e-Government in local governments are diverse. Hence, we further define the scope of our research in the next section.

THE SCOPE OF IS SECURITY RISKS IN OUTSOURCING E-GOVERNMENT

E-Government has emerged as a popular catch phrase. In literature, the scope of activities that are studied in this area is broad. The e-Government activities of local governments can be subdivided into the government-to-government, government-to-citizen, government-to-business (Brown, & Brudney, 2001), government-to-civil society organizations and

Address correspondence to Peter Berghmans, Lessius Mechelen University College, Zandpoortvest, 13, Mechelen, 2800 Belgium. E-mail: peter.berghmans@khm.be

TABLE 1
Risks resulting from the cooperation with IT vendors in e-Government projects

Cause ID	Cause description	Possible consequences
RISK AREA 1: Vendor (in)dependence		
1.1	Difficult or impossible to combine e-Government solutions of different suppliers	– Asset specificity – Vendor lock-in
1.2	Replacing a current RR solution is nearly impossible	– Asset specificity – Vendor lock-in
1.3	Unclear relationship between customer and provider	– Responsibilities are not well defined – IT governance is difficult to achieve
1.4	Absence of contracts and SLA's	– No agreement/ knowledge on mitigation controls taken by IT vendor – No agreement on task allocation leads to a lack of mitigation controls
1.5	Loss of organizational and technical competency	– Bad practices and loss of control over information environment (assessment of risks is hampered)
RISK AREA 2: Poor product quality		
2.1	The e-Government tool doesn't meet business requirements	– New and undiscovered risks – Lack of proper security configuration management (leads to unsafe configuration settings) – Security requirements of the product conflicts with internal policies
2.2	Lack of (communication about) software testing, updates and maintenance	– Unpredictable software downtime – Undiscovered software flaws – Requested software-features disappear
2.3	e-Government tools may require unsafe configuration of underlying technology	– Mitigation controls of underlying technology may not be applicable.
2.4	Software in- and output is not standardized	– Data may not be exported to other applications – Asset specificity – Vendor lock-in
2.5	Absence of key performance indicators in software	– Risk identification is difficult – Measurement of security management is hampered
RISK AREA 3: Poor quality of services		
3.1	Lack of communication between customer and vendor of the safe installation, configuration and maintenance of the e-Government tool	– Misunderstanding of the configuration of security settings – No clear installation and configuration guidelines in cases of emergency.
3.2	IT department loses control over vendor access to data	– Unrestricted access to data hampers CIA of information
3.3	Problem resolution, communication about software errors and feature requests are inefficient or non-existent	– The end user is not aware of software errors and can not anticipate – Future discovered errors by end users will not be communicated (user disillusionment)

the citizen-to-citizen category (Yildiz, 2007). In this article, we will focus on the IS security risks resulting from outsourcing the development, deployment, and maintenance of government-to-government tools, such as RR applications. In addition, our study includes the specific IS security risks that are the result of the integration of the tool in the back office of the local government. This integration is driven by cost reduction, efficiency, innovation, and centralized control (United Nations, 2008) and is common in our research field.

Information Systems Management 2011.28:284-293.

Developing, implementing, and the maintenance of these e-Government tools are complicated tasks. Hence, outsourcing the implementation of government-to-government applications is a common activity (Currie, 1996; Buck–Lew, 1992). However, outsourcing is subject to risks. Many researchers studied the risks of IT outsourcing in general. In their literature review, Lacity, Khan, and Willcocks (2009) revealed that 34 out of 191 articles discussed IT outsourcing risks. The identified risks in this literature review can be subdivided by taking into account the outsourcing stages. Dibbern, Goles, Hirschheim, and Jayatilaka (2004) identified five stages of outsourcing, based on Simon's (1960) decision model. Those stages are: *why* and *what* to outsource, *which* choice to make, *how* to outsource, and the *outcome* of the outsourcing activity. In each stage, outsourcing literature discusses risks and unwanted events. The *why* (or should one outsource) stage addresses the advantages and disadvantages of outsourcing. For example, the transfer of risks to a supplier may be one of the key drivers of this decision (Baskerville, 2005). When considering *what* to outsource, the scope of the outsourcing activity is considered. When outsourcing IS/IT security services (Karyda, Mitrou, & Quirchmayr, 2006) for example, the privacy aspect may be an obstacle. The *which* stage refers to the decision process of setting up the outsourcing deal. An example, covering a risk in this stage, is the longitudinal case research at Logistics Information Systems Agency (LISA) (Willcocks, Lacity, & Kern, 1999). In this study, the difficulties in constructing deals in the face of rapid business/technical change are discussed. In "The Risks of Outsourcing IT" (1996), Earl discusses the risks of the *how* stage when he mentions vendor selection: the risk of selecting a vendor that uses outdated technology skills for example, may affect the quality of the outsourcing activity.

The outsourcing activity in local government is already in place. Hence, we are mainly interested in the IS security risks of the *outcomes* of the outsourcing activity. A good example of a study of these risks is that of Aubert, Party, and Rivard (2005). In this research, industrial organizational literature is reviewed, resulting in eight undesirable outcomes of IT outsourcing. In addition, we also focus on aspects of the *how* stage. Following Dibberns' definition, the *how* stage includes the process of building and structuring the relationship between vendor and customer (i.e., the local government) and the management of the resulting relationship. This management is an ongoing process that affects IS security after the set-up of the outsourcing activity.

In literature on the IS security risks of outsourcing government-to-government tools, IS security is often neglected. Fink (1994) presents a security framework for IS outsourcing and Blackley and Leach (1996) present security considerations in outsourcing IT services. Sherwood (1997) discusses IS security in outsourcing contracts and Gaonjur and Bokhoree (2006) study the insider threats in IT outsourcing from a technical perspective. Khalfan (2004) in his study of IS security considerations in IT outsourcing in both the public and private sector in Kuwait, identifies data confidentiality as the highest ranked risk factor in both organization types. Although all the aforementioned studies identify relevant IS security risks, they are not really underpinned with empirical data and their theoretical basis is limited.

We take into account that the success of IT outsourcing (and hence the impact of IS security risks) is closely related to organizational characteristics (Moon, Jung, Chung, & Choe, 2007). It is important to address the differences (Bozeman & Bretschneider, 1986). This implies that literature based on research in private organizations may not be indiscriminately applicable in governmental organizations.

Outsourcing in the public sector is subject to specific risks, such as the possible loss of control over the technology and the current project status (Vilvovsky, 2008). Cordella and Willcocks (2009) call for a more disciplined approach to outsourcing in the public sector. The role of government to protect its citizens from risks, such as data security (i.e., confidentiality) is an additional concern. Our research is in accordance with these findings. It motivated us to first identify specific risks empirically in local governments before analyzing them.

THE IDENTIFICATION OF IS SECURITY RISKS WHEN COOPERATING WITH THIRD PARTY VENDORS

We used methodology triangulation to identify IS security risks in outsourcing government-to-government activities. We conducted in-depth interviews to identify the consumer-side (i.e., local government) perception of IS security risks. We combined these interviews with field research in which we identified IS security risks in the local governments using more traditional risk identification methods based on industry standards. These interviews and field research will be referred to as Research Activity (RA 1). On the side of the provider, we used a questionnaire to identify IS security risks in outsourcing (RA 2). The identified risks are put into a framework to reveal cause–effect relationships (RA 3). The validity of our results is tested by expert-verification (RA 4).

The Consumers' Side: IS Security Audits in Local Governments to Identify Latent and Manifest Risks when Cooperating with IT Vendors (RA 1)

In the first Research Activity, we identified risks on the consumer side (the local government). The goal of risk identification in general is to surface major risks before they harm the organization. By conducting a risk assessment, the risks will be prioritized against criteria relevant for the organization. As we already stated in our introduction, we do not solely relay on the mainstream risk frameworks and best practices (such as checklists of controls). By using strictly regulated methods to conduct a risk analysis, the focus on risk remains incomplete and narrow (Baskerville, 1993 and Dhillon & Backhouse, 2001). We adhere to the constructivist triangulation approach, seeing risk

Information Systems Management 2011.28:284-293.

as a social artifact, produced by social groups or institutions, and determined by structural forces in society (Oscarson, 2007). This worldview assumes risks to be mediated through social experience and interaction (Renn, 1998).

We implement the constructivists view into our research by studying the actual perceived and objective technical and organizational risks of the local government concerning the participation of the vendor in e-government projects. By "perceived" we mean the subjective and inter-subjective (epistemological) judgments of risks of employees in local governments (Oscarson, 2007). These risks are the result of interpretation of the real world, stakeholders' values, beliefs, etc. By objective risks we refer to the institutional facts, the objective knowledge about the risks (referred to as epistemic objective by Searle, 1995). Examples of this level of interpretation are industry norms and standards. When combining actual, perceived, technical, and organizational risks, we come up with four perspectives of risk identification. How we bring these four perspectives into practice will now be explained.

In the first perspective, we take into account risks resulting from technical implementations of soft- and hardware. Aspects such as firewalls, safe programming, documentation of code, security updates of underlying operating systems, etc. may be considered when analyzing the consumer-side risks. Indeed, the information quality (in terms of CIA) will be influenced by the presence or absence of all these risks mitigation techniques. To analyze this level of risks, we used a technical audit.

The importance of risks resulting from the technical implementation of e-government tools may not be underestimated. However, they are not exhaustive. As organizations become more and more dependent on information systems (Carr, 2003), the evolution from a narrow technical view on information systems toward an integrated view of organizational and technical concepts (Baskerville, 2005) will be necessary. As a result, IS security risks resulting from organizational concepts should be considered when conducting a risk analysis. For this level of analysis, we used objective measures such as ISO 27002:2005 (ISO, 2005) to identify these risks. This is the second perspective.

Both technical and organizational risk identification methods (the first two perspectives we explained) identify objective risks. To analyze the perceived risks on both technological and organizational level (third and fourth perspective), we use in-depth interviews based on the technique of Value Focused Thinking (VFT). This method identifies values, beliefs, expectations, and assumptions of stakeholders. The values are often subconscious. By using VFT, these values can be uncovered (Keeney, 1992, p. 24). The use of VFT in IS security literature is not new: Dhillon and Torkzadeh (2006) already used VFT in the area of IS security to identify IS security objectives.

We interviewed 56 respondents in 12 local governments using VFT. The respondents were both members of the board of managers and staff (e.g., the security officer and the manager of the IT, who are not always a member of the board). The data gathering process of the perceived risks started with the definition and description of IS security, in order to achieve a common understanding between different stakeholders. Next, we defined the scope of our interview: to make explicit their values in optimizing IS security in their organization and in the cooperation with IT suppliers in e-government projects. We put emphasis on the fact that these values are not necessarily technical in the first place. After defining IS security and the scope of our interview, we asked the interviewees to construct a wish list in which they express their values and goals regarding this topic. This list was used during the interview to trigger questions and to stimulate the identification process. Keeney describes the use of a wish list as a device that can help in the identification process (Keeney, 1992, p. 57). During the interview, we applied five other techniques to identify hidden values of the stakeholder. These are the use of goals, alternatives, consequences, problems, and shortcomings and the use of different perspectives of stakeholders. We recorded each interview and transcribed it verbatim. The identified risks were then analyzed to identify the IS security objectives of the stakeholders. These objectives revealed the perceived technical and organizational risks.

Survey and Interview with the Four Providers of the e-Government Tool for Accessing RR (RA 2)

In addition to the identification of the consumer-side risks (RA 1), we identified (objective) risks mitigation techniques implemented by the IT supplier. The federal government asked us to build a questionnaire regarding the compliance of the IT vendor practices with known industrial standards. We used ISO 27002:2005 (ISO, 2005) and OWASP guidelines for good programming (OWASP, 2009) for this purpose. The following topics were questioned regarding the organizational level: the occurrence of aspects of IS security in underpinning contracts, the use of procedures when IS security incidents are detected (procedures to detect, succeed, and report both to internal instances and to the local government responsible for the data) and the use of procedures to prevent the occurrence of IS security incidents. On the technical level, we asked the respondents to answer questions about the system requirements of their products and the responsibility of both the supplier and the local government to achieve these requirements, the precaution measures to secure the information processed (in terms of CIA), escrow arrangements, accessibility of the information by different groups of users, and accessibility of the application by the IT vendor for maintenance.

The federal government asked the four vendors to answer the questions. All vendors completed the questionnaire. We also organized a meeting with the respondents to validate heir answers and to align them with findings of our technical risk identification activity on consumer side. The objective risks identified in RA 1 were adjusted accordingly.

Information Systems Management 2011.28:284-293.

Bringing it All Together: Using Systems Thinking to Reveal Cause–Effect Relationships (RA3)

In the final step of our risk identification, we combine the risks we identified into a systems thinking exercise (Berghmans, Van Den Eede, & Van de Walle, 2008). 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). We use the framework depicted in Figure 1 for this purpose. This framework consists of the four perspectives we described above. All risks we identified are placed in the corresponding quadrants. Doing so, we reveal cause effect relationships.

An illustrative case, such as the following, explains the use of this framework. A city council outsourced the development, deployment, and maintenance of the e-government tool for accessing the RR to their preferred IT supplier. The main drivers for outsourcing are the complexity of e-governance tools, cost reduction, and the compatibility with other tools, delivered by the IT vendor. The local IT department, however, is still responsible for in-house programming of other applications, such as employee administration.

A contract was signed between the IT vendor and the local government years ago. However, no security considerations were incorporated in this contract. While analyzing the software infrastructure, researchers found the e-government tool and the tool for employee administration installed on the same server. Both tools use the same database infrastructure. No inbound internet connections are allowed to the server. When analyzing the security of both applications, the researchers identified the RR tool containing six accounts without passwords, one of them gaining access on administration level. This account was easily found due to the fact all possible users are enlisted in the "username" field of the application. When confronting the IT staff with this finding, they argued that the information processed by the tool remains internal, so no real risks exist. After a more thorough analysis however, the researchers revealed that the credentials of the weak administrator account could also be used to grant administrator access to the database infrastructure. Hence, private data of employees, which are also stored in the database, is accessible for internal users.

This case shows that a combination of different risks results in a serious risk concerning the CIA of critical data. Moreover, by placing the risks in the framework, cause–effect relationships become clear.

The management of the local government trusted the supplier, as there is an historical relationship. This trust is considered to be more important than any contractual statement about information security. As a consequence (see arrow A in Figure 1) of this perception of organizational risks (Quadrant (Q) I in Figure 1) security issues were not introduced in the underpinning contract with the service supplier (Q III). The trust of the management in the services of the provider, amplifies

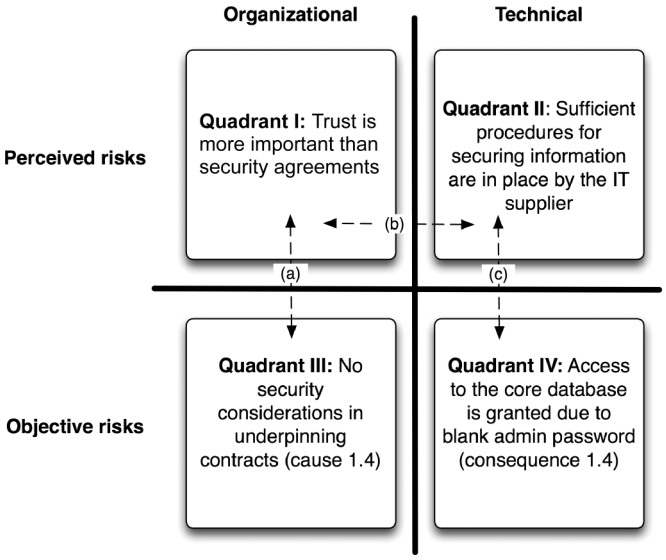

FIG. 1. Framework for identifying risks. This framework is used in RA 1–3.

the perception of the IT department that the information security procedures of the IT supplier are sufficient (Q II, arrow B). Hence, there is no awareness about the lack of password policies used by the IT vendor. However the IT department insists that administrator accounts should be protected by passwords, the lack of authentication is not perceived as a high risk (Q II). Our research has proved this perception to be wrong (arrow C): using the blank administrator password, one can also gain access to the core database (Q IV).

When interpreting the illustrative case, it becomes clear that CIA risk is propagated on the boundary of the quadrants representing the perception of technical and organizational risks (Q I and II). Unsafe programming and the absence of security considerations when deploying the software, cause the CIA risk. The effect is a possible harm of CIA in employee data. As a result, this illustrative case shows that cause–effect relationships are made clear by the use of the proposed framework.

The Use of an Expert Panel to Validate the Risks we Found in Previous Activities (RA 4)

To validate results, Emory & Cooper (1991) proposed the use of a panel, as an appropriate method. We decided to use a panel of experts. The criteria used for selecting the panelists was that each of the members should be experienced in the domain of IS security in local governments. We asked the federal government to organize a meeting with the president of the professional association for IT managers for local governments and the president of the association for security executives in the concerning area, an experienced auditor in the public domain, an employee of the most important supplier of IT services for governments, and the staff member responsible for information security in local governments from the federal government. The

Information Systems Management 2011.28:284-293.

IS security risks we identified were presented and comments were processed.

RESULTS AND DISCUSSION

In previous section, we explained how we identified the risks when cooperating with third party vendors in enabling e-government. In this section, we analyze these risks with the help of our framework depicted in Figure 1 and literature that deals with unwanted outcomes of IT outsourcing and outsourcing government-to-government projects. We catalogue the identified risks into three areas: vendor dependence, poor product quality, and poor quality of services. Each area is divided into causes of risks we identified while looking for cause–effect relationships between risks. Both the areas of risks and the correspondent causes are discussed below.

Risk Area 1: Vendor (In)dependence

Several risks are the result of the dependence of local governments on their e-government vendor. As stated in the introduction, only four companies provide an e-government solution for RR.

When identifying risks, it became clear that it was difficult or impossible to combine e-government solutions (cause 1.1) of different suppliers. Hence, the local governments are forced to buy their e-government solution for RR from the supplier of their other e-government products. Moreover, after studying the contracts between the IT vendor and the local government (if present, see cause 1.4), often the guarantee of the product is voided when products of other suppliers are installed on the same server.

In the area of vendor (in)dependence, our research activities identified that replacing a current RR solution by that of a different provider (cause 1.2) is nearly impossible. These and other e-government modules are deeply embedded in the e-government infrastructure of the local government.

Cause 1.1 and 1.2 lead to asset specificity (Williamson, 1985). This term refers to the degree to which an asset can be redeployed without scarifying its productive value if the contract is to be interrupted or prematurely terminated. Asset specialty, together with a small number of suppliers (four suppliers for more than 300 local governments in the concerned region), may result in high switching costs and vendor lock-in (Teece, 1986 and Aubert et al., 2005) which is a risk for IS security.

Vendor (in)dependence is further influenced by the historical relationship between the IT vendor and local government. In most of the cases, the IT vendor has been the exclusive IT partner for several decades. In the 1970s, each province of the concerned Western European region created an "IT center for governments". These centers became specialized in the development of products for e-government. Each center was constrained to operate within the province boarders. Hence, local governments had to cooperate with a (the) regional supplier, which restricted their choice when seeking for an e-government provider. The centers were partly private and partly public. In 2003, stimulated by European law, a new law gave the centers the possibility to operate outside their province and their statutes changed. However, this unique historical situation results in an unclear relationship between customer and provider (cause 1.3). As a result, responsibilities are not well defined. Hence, it is difficult to achieve IT governance. Indeed, as the role of the IT vendor in the organization is not defined, mechanisms to achieve IT governance (processes, structures, and relational mechanisms as described by De Haes &Van Grembergen, 2005) are not able to succeed. This negatively influences the overall quality of information processing, of which IS security is part of.

The unclear relationship is confirmed by another surprising cause we identified. In only a few cases did the governments in our study have contracts and a Service Level Agreement (SLA) and even when existent, no statements about the CIA of information were included. Moreover, escrow arrangements are not considered in underpinning contracts (if existent). This is surprising, because of the sensitive nature of the information that RR applications process. Hence, there is no clear knowledge of prevention measures that are taken by the IT vendors. For example, in a lot of local governments, the IT department had little or no control and knowledge about the security measures taken by the IT vendor when accessing the RR tool from remote sites (e.g., for maintenance). Another example is the observation that local government has little or no control over the security measures taken by the vendor to mitigate the risks of human errors of their employees. This may lead to inadequate measures: on one hand the local government has policies in place for safe information processing of their own employees, but has no control over the employees of the vendor. However the latter group may cause more harm because of the access rights they are granted. Of course, this has a negative impact on the CIA and is a true risk for the information security of the local government. In the questionnaire that was sent by the federal government to the IT vendor, we asked for more information about this issue (Berghmans, Lenaerts, & Van Roy, 2007). According to their answers, the historical relationship is the main reason for this situation. The IT vendors motivate the absence of contracts and SLA's by referring to "a good relationship between vendor and customer". Another important consequence of the absence of contracts and SLA's (cause 1.4) is the finding that there is little or no agreement on task allocation. For example, when the IT manager was asked who is responsible for the updates of the underlying operating system of the server that hosts the e-government application of RR, he/she referred in most of the cases to the IT vendor. According to the IT managers, this was obvious as the vendor of the e-government application installed the server and operating system. However, we repeatedly observed that the operating systems were not patched at all. When questioned about this issue, the vendors in our survey stated that this service is not part of their standard services, but

Information Systems Management 2011.28:284-293.

is offered as an additional service. This example shows that the absence of task allocation results in incomplete tasks, which is definitely an IS security risk.

Note for this cause that local governments as well as IT vendors discussed the efficacy of escrow arrangements. Some interviewees identified the standardization of standard data in- and output as being a more effective mitigation control. According to this group of respondents, it is nearly impossible to maintain software after a failure of the IT vendor. Hence, as software requirements are changing fast, data migration to other software is perceived as being more important.

An important finding in the area of vendor (in)dependence is the loss of organizational and technical competence of the IT department regarding e-government tools (cause 1.5). The information architecture and information flow in local governments are complex. In our risk identification we repeatedly observed that the IT department was not able to execute some basic tasks, such as configuring access rights or checking the RR log files. According to Prahalad and Hamel, essential skills can be lost if outsourced activities are too close to the core business of the firm (1990). Such loss might threaten future organizational action (Aubert et al, 2005). Earl (1996) also discussed this item: "Much learning about the capability of IT is experimental. Organizations tend to learn to manage IT by doing". This paves the way for bad practices such as bad backup schemes and unsafe configurations in software.

Causes 1.3, 1.4, and 1.5 are catalyzing factors. Poor knowledge amplifies the lack of communication (and vice versa) between the IT department and the vendor. Moreover, these causes pave the way to the unclear participation of the IT vendor (see cause 1.3). Often a direct communication link exists between the different departments of the local government and the IT vendor, without the involvement of the IT department. Hence, the IT department loses control. This enhances the lack of IT governance: no fusion between IT and business can take place. It is clear that the loss of organizational and technical competency has a negative impact on IS security. A proper assessment of risks is hampered, as is the integration between the e-government tools and the technical environment offered by the IT department of the local government.

Risk Area 2: Poor Product Quality

Risk area 1 discussed the risks resulting from the dependence on IT vendors for e-government. The second area combines risks that are the result of (perceived) poor product quality.

We found that the e-government tool does not always meet the requirements of the business processes (cause 2.1) forcing the end user to seek for alternatives. We identified three consequences for this risk cause in our interviews. Firstly, users stated that they were better off without the access to RR. The main reasons according to those respondents are technical issues, like slow connections with the RR reference repository and a lack of user friendliness. As a result, end users are seeking for other ways to access or process the same data. These alternative ways to access data lead to new and undiscovered risks (Reason, 1990). Examples of "workarounds" we identified are accessing alternative, incomplete databases, or using other software tools to accomplish their tasks, like the use of MS Word documents. That results in new risks. In addition, as tasks are completed in a different way than expected, the identification of an incident is hampered. Hence, no mitigation controls for these risks are taken.

Another consequence of the conflict between software and business processes concerning information security is the lack of proper security configuration management. A good example is the finding that the control panel of the RR tool, used for (among other tasks) access control, does not meet the requirements of the local governments. Hence, the access rights cannot be configured adequately which may lead to improper access to information and improper control mechanisms.

A third consequence which relates to cause 2.1 is the finding that during our visits respondents reported that the security configuration of software conflicts with the IS security model of the local government. A good example of how this threatens information security is the way usernames and passwords are managed. In many cases the local government had at their disposal a code of conduct describing the aspect of minimal password length and the interval to renew passwords. When we consulted the e-government tools in use, we identified that those rules often could not be applied due to software restrictions (i.e., the incompatibility with industrial standards for central authentication and authorization management, such as the Lightweight Directory Access Protocol). Moreover, the mutual e-government tools are using conflicting security configurations (which are hard-coded in the software). This results in confusing regulations and discourages the end user in applying the code of conduct.

The lack of (communication about) software testing, updates, and maintenance (cause 2.2) is also an important cause of risks that influences the product quality. Most of the respondents of the local governments were not able to answer the question of how the RR software tool was tested and if, in case of updates, the effect on the software in production was considered. Respondents reported severe incidents due to the lack of testing new software or software updates. These incidents include a complete failure of the e-government environment the day after an unannounced software patch and loss of data caused by untested software updates. The respondents added that the IT vendors worked hard on this issue lately. But on the other hand, they still were not able to define the quality of the test procedures used by the vendors.

The lack of software testing is certainly influenced by the absence of a dummy data set for RR. Indeed, the social security of citizens may be complex, with many exceptions existing in the dataset in production. Making a copy of the real data set is not possible because of privacy regulations. Hence tests are

Information Systems Management 2011.28:284-293.

often conducted in the production environment, causing CIA risks concerning the dataset in production.

We also identified other risks resulting from updates and maintenance. Respondents of the local government reported that a requested change in the feature set of the RR application may be removed when software was updated. This is resulting from the lack of consistent update management and documentation of release candidates. However, respondents also reported that these risks are reducing lately.

A cause of risk reflected in different findings, is the fact that e-government tools may require unsafe configuration of underlying technology (cause 2.3), like shared network drives and the compulsory use of administrator rights on workstations. In several cases, we identified that network drives must be anonymously shared between the users. These drives are not only used to store components of the software, but also sensitive data, processed by the application. In other cases, the use of administrator rights was mandatory, resulting in a severe risk for viruses and malware.

An important finding concerning product quality is that software in- and output is not standardized (cause 2.4), resulting in difficulties when applications are integrated or when the data has to be exported (i.e., when the local government wants to change provider). This is a major risk related to continuity: when the cooperation is interrupted or prematurely terminated, the local government may experience major problems in exporting data to other applications. Moreover lock-in situations are encouraged. This cause is closely related to cause 1.1 and 1.2, asset specificity.

The last cause in the area of poor product quality is the absence of good key performance indicators (cause 2.5). In the context of RR, for example, it should be useful that the management has (easy) access to information and the amount of executed requests in each period of time. This informs the management about the performance and workload of employees. Moreover, this gives an identification of the amount of information that was consulted. Suppose that the local government processes 10 cases of citizens each day, but on average, the social information of 12 citizens is requested by using RR, the management can detect abnormalities. This example shows that when proper key indicators are implemented, the security performance can be measured. This raises the quality of the software and the overall security management in the organization. Moreover, a better link between business and IT is realized.

Risk Area 3: Poor Quality of Services

The last area we categorized the IS security risks resulting from the cooperation between the local government and IT vendors, is the (perceived) poor quality of the service. The implementation and maintenance of e-government tools is a service-oriented task. The growing interest and development of these tools raises the complexity of the tasks. According to Aubert et al. (2005), task complexity leads to inferior performance, such as service debasement (Lacity & Hirschheim, 1993).

There is a clear cause–effect relationship between poor quality of services and the lack of communication between customer and vendor of the safe installation, configuration, and maintenance of the e-government tool (cause 3.1). In cause 2.3, we described the obligated use of administrator rights on desktops. We questioned the concerning vendor about this issue. The IT supplier declared that in the past, administrator rights were used during a short period of time (e.g., a short period of time after the release of Microsoft Windows XP service pack 2) to solve a programming issue. After updating the software, this issue was solved. However, the IT vendor recognized that communication was poor. Also in many local governments, the respondents reported the lack of information about the secure installation and maintenance of the software. These tasks were most often exclusively executed by the IT vendor. However, a good description of these activities could be helpful in case of emergency. Note that the absence of communication about test environments, as described in cause 2.2, also can be mentioned here.

Poor quality of services may also be the result of a lack of control. Of course, this cause is in close relationship with causes described in area 1, the vendor (in)dependence. Due to the absence of agreements on the quality of services and the loss of competences in the local government, the IT department loses control over vendor access to data (cause 3.2). Hence, the integrity and confidentiality of the data may be at risk. We detected that in many cases, the IT vendor had unrestricted access to the network and data of the consumer.

The last cause in this risk area is the finding that problem resolution, communication about software errors, and feature requests are inefficient or non-existent (cause 3.3). End users of the RR tool reported that software errors are often slowly solved by the IT vendor or not at all. Also, the vendor does not (or slowly) handle feature requests. When analyzing this, we identified both local government and vendor have a responsibility in this issue. On the one hand, the priorities of the local government must be clearly defined by the government itself. Moreover, communication about errors must be well organized (e.g., though a standard trouble-ticketing system). The vendor, on the other hand, has to communicate about the result of the problem treatment or feature request, even if they are unable to solve the error in a short period of time or feature requests cannot be handled. Note that the IT vendors are coping with these kinds of risks by organizing steering committees in which end users can participate.

CONCLUSION

To identify IS security risks resulting from the cooperation of IT vendors in the development and maintenance of government-to-government products, we have built a risk identification

Information Systems Management 2011.28:284-293.

framework. Four research activities have helped us to identify IS security. We conducted in-depth interviews to identify the consumer-side risks. On the side of the provider, we used a questionnaire to identify IS security risks in outsourcing, we used systems thinking to reveal cause–effect relationships between the risks and we validated our results by expert verification.

As we see risks as a social artifact, the identification of the perception of risks, in addition to risks identified using traditional risk identification methods, is important to achieve a better understanding. We used VFT to identify the risks, like the stakeholders perceived them.

We used systems thinking to better understand cause–effect relationships between the risks we identified. Applying this technique to all identified risks we revealed 13 causes of risks, categorized in three risk areas (Table 1): vendor dependence, poor product quality, and poor quality of services.

At the moment of writing, the federal government uses our results to develop policies for IT vendors regarding IS security risk control. Here, future research activities can define effective mitigation controls.

Information Systems Management 2011.28:284-293.

ACKNOWLEDGMENT

The authors would like to thank all participating local governments, IT vendors, and experts for their help during the risk identification activities. Special thanks to the SmartCitiesScran (Peter Cruickshank), Gerd Van Den Eede and the MeTTeg'09 Community for their reviews and comments.

AUTHOR BIOS

Peter Berghmans is a lecturer and researcher in IS security on the Mechelen University College. His main research focus is on Information Security in local governments and hospitals.

Karel Van Roy is a former IT-director and former Managing director of the business department of the Mechelen University College. He now is a senior advisor and the coordinator institutional research.

REFERENCES

Aubert, B. A., Party, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *The DATABASE for Advances in Information Systems*, *36*(4), 8–29.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, *25*(44), 375–414.

Baskerville, R. (2005). Best practices in IT risk management. *Cutter Benchmark Review*, *5*(12), 5–12.

Berghmans, P., Lenaerts, M., & Van Roy, K. (2007). Menselijke factoren in de informatieveiligheid van lokale besturen. *Praktijkgids management lokale besturen*, Belgium: Kluwer.

Berghmans, P., Van Den Eede, G, & Van de Walle, B. (2008). A Systems Perspective on Security Risk Identification: Methodology and Illustrations from City Councils. *Proceedings of the 5 International ISCRAM Conference*, Washington, DC, USA, ISCRAM.

Blackley, J. A., & Leach, J. (1996). Security considerations in outsourcing IT services. *Information Security Technical Report*, *1*(3), 3–4.

Bozeman, B., & Bretschneider, S. (1986). Public management information systems: Theory and prescription (Special issue). *Public Administration Review*, *46*, 475–487.

Brown, M. M., & Brudney, J. L. (2001). Achieving advanced electronic government services: An examination of obstacles and implications from an international perspective, *The National Public Management Research Conference*, Bloomington, IN.

Buck–Lew, M. (1992). To outsource or not? *International Journal of Information Management*, *12*, 3–20.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*, *81*(5), 5–12.

Cordella, A., & Willcocks, L. (2009). Outsourcing, bureaucracy and public value: Reappraising the notion of the "contract state". *Government Information Quarterly*, *27*, 82–88.

Currie, W. (1996). Outsourcing in the private and public sectors: An unpredictable IT strategy. *European Journal of Information Systems*, *4*, 226–236.

De Haes, S., & Van Grembergen, W. (2005). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference*, Waikoloa, Big Island Hawaii, Jan 3–6, 2005.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293–314.

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004) Information systems outsourcing: A survey and analysis of the literature. *ACM SIGMIS Database*, *35*, 6–102.

Emory, C. W., & Cooper, D. R. (1991). *Business research methods*. Boston, MA: Irwin.

Earl, M. J. (1996). The risk of outsourcing IT. *Sloan Management Review*, *37*(3), 26–32.

Fink, D. (1994). A security framework for information systems outsourcing. *Information Management & Computer Security*, *2*, 3–8.

Gaonjur, P., & Bokhoree, C. (2006). Risk of insider threats in information technology outsourcing: Can deceptive techniques be applied? *Proceedings of Security and Management*, 522.

ISO, B. (2005). "IEC 27002:2005." Information technology. Security techniques. Code of practice for information security management. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=42103.

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, *14*, 402–415.

Keeney, R. (1992). *Value-focused thinking: A path to creative decision making*. Cambridge, MA: Harvard University Press.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. *International Journal of Information Management*, *24*, 29–42.

Lacity, M., & Hirschheim, R (1993). *Information Systems Outsourcing*. New York, NY: John Wiley & Sons.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *The Journal of Strategic Information Systems*, *18*, 130–146.

Moon, J., Jung, G., Chung, M., & Choe, Y. (2007). IT outsourcing for E-government: Lessons from IT outsourcing projects initiated by agricultural organizations of the Korean government. *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS 2007)*, Waikoloa, Big Island Hawaii, Jan 3–6, 2007.

Oscarson, P. (2007). Actual and Perceived Information Systems Security. [Doctoral dissertation] Linköping University, Department of Management and Engineering.

OWASP (2009). OWASP Top 10 Project. *OWASP*. Retrieved from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Prahalad, C., & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review*, *68*(3), 79–91.

Reason, J. (1990). *Human error*. Cambridge, UK: Cambridge University Press.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 49–71.

Searle, J. R. (1995). *The construction of social reality*, New York, NY: Penguin Books.

Sherwood, J. (1997). Managing security for outsourcing contracts. *Computers and Security*, *16*, 603–609.

Simon, H. A. (1960). *The new science of management decision*, New York, NY: Wiley.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

Teece, D. J. (1986). Firm boundaries, technological innovation and strategic management. In L. Thomas (Ed.), *The economics of Strategic Planning* (pp. 187–199), Lexington, MA: Lexington Books.

Vilvovsky, S. (2008). Differences between public and private IT outsourcing: Common themes in the literature, *Proceedings of the 2008 international conference on Digital government research*, Montreal, Canada, Digital Government Society of North America.

United Nations (2008). e-Government Survey 2008, *From e-Government to connected Governance*. Retrieved December 28^{t} 2009 from unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf.

Willcocks, L. P., Lacity, M. C., & Kern, T. (1999). Risk mitigation in IT outsourcing strategy revisited: Longitudinal case research at LISA. *Journal of Strategic Information Systems*, *8*, 285–314.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism*, New York, NY: The Free Press.

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, *24*, 646–665.

Information Systems Management 2011.28:284-293.