Understanding and Specifying Information Security Needs to Support the Delivery of High Quality Security Services

Xiaomeng Su[1], Damiano Bolzoni[2], and Pascal van Eck[1]

[1] University of Twente, Information Systems Group, Enschede, The Netherlands
x.su@ewi.utwente.nl p.a.t.vaneck@ewi.utwente.nl
[2] University of Twente, Distributed and Embedded System Group, Enschede, The Netherlands
damiano.bolzoni@utwente.nl

Abstract. In this paper we present an approach for specifying and prioritizing information security requirements in organizations. It is important to prioritize security requirements since hundred per cent security is not achievable and the limited resources available should be directed to satisfy the most important ones. We propose to explicitly link security requirements with the organization's business vision, i.e. to provide business rationale for security requirements. The rationale is then used as a basis for comparing the importance of different security requirements. Furthermore we discuss how to integrate the aforementioned solution concepts into a service level management process for security services, which is an important step in IT Governance. We validate our approach by way of a focus group session.

1 Introduction

Information security - the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain - has long been recognized as a critical issue. Two current trends indicate that its importance is growing. First, the integration of computers into more and more aspects of modern life continues. Second, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what has been observed to date.

The increasing concerns of customers, particularly in online commerce, plus the impact of legislations on information security have compelled companies to put more resources in information security. It is clear that senior managers in many organizations are now expressing a much greater interest in information security [8]. Understanding and specifying what kind of security an organization need is however a difficult task. Many underlying goals (why and what security is needed) remain tacit within organizations and requirements end up being articulated as specifications of the security control baseline (how security will be

achieved) without a clear rationale. The problem becomes more urgent when more and more organizations are involved in collaboration and commerce. Being able to articulate security goals and requirements consistently, based on an accurate view of existing security capabilities, and using shared understandings, becomes much more important. Networked business will be difficult to conduct if the organizations involved cannot agree on why security is necessary; the scope it should cover and what each organization expects it to achieve.

The complexity of undertaking an enterprise-wide view of security management can be illustrated in the challenges facing chief security officers (CSOs). Often CSOs are tasked with 'securing' the organization, but it may not be clear what that means. As a result, the CSO is often left to answer very important organizational questions without specific guidance: (i) What needs to be secured? Why, and with which priority? (ii) How to ensure that people agree on the above issue? (iii) How can the CSO be sure that the organization has been 'secured'? What will be used to measure success?

The aim of this paper is to develop techniques and instruments to help stakeholders articulate the connection between security requirements and business drivers in a systematic way. This connection is needed to provide the rationale to prioritize security requirements. E.g., for a production company, the availability of its production control system is of vital importance, whereas for a financial service provider, it is important to protect the integrity of its financial transactions. The reason of making explicit the business rationale behind security requirement is twofold. Firstly, it forces the stakeholders to turn their intuition into explicit judgments - judgments that are based on business goals and whose underlying assumptions are discussed openly. Secondly, since hundred per cent security is not achievable and the limited resources available should be directed to satisfy the most important ones, we need a way to prioritize security requirements. The business rationale serves as the underlying criterion for evaluating how important each security requirement is.

The structure of this paper is as follows. In Section 2, we present our conceptual model for linking security requirements to the business vision that motivates them, and we show how this model can be used to prioritize security requirements. Section 3 discusses an application of this model in service level management for security services. Our model has been validated by way of a focus group discussion, which we discuss in Section 4. We present related research in Section 5, and conclude the paper in Section 6.

2 Formulating and Understanding Security Goals and Requirements

A security requirement specification tells what should be secured and why. It identifies the organization; needs with respect to security. Consider, for example, the differences between the needs of a university and that of a cryptographic organization. The university fosters scholarship and open research: papers, discoveries, and work are available to the general public as well as to other aca-

demics. The cryptographic organization, on the other hand, prizes secrecy. The university will need to protect the integrity and confidentiality of the data, such as grades, on its systems. It might also want to ensure that the system is available via the Internet so that students, faculty, and other researchers have access to information. The cryptographic organization, though, will emphasize confidentiality of all its work.

When an organization wants to secure its system, it must first determine what requirements to meet. Given that organizations normally have limited resources to protect its assets, it is equally important to determine which requirements are more important and thus should be prioritized. To achieve this, we propose to use a conceptual framework where security requirements are linked to the unique business drivers of the organization in question. Figure 1 portrays the conceptual framework. The business vision consists of high level business goals the organization has. Critical Impact Factors (CIFs) identify what will be the business impacts if security requirements are violated. Valuable assets and their security requirements are inventories of security requirements. Valuable assets and their security requirements have an effect on the CIFs and the CIFs in turn impact the accomplishment of the organization's business vision. In other words, we can use an organization's business vision to prioritize the CIFs, which can be used to further prioritize the security requirements. To achieve that, three subsequent steps need to be taken. Firstly an organization's CIFs and business vision need to be defined. Secondly, we need to enumerate valuable assets and their security requirements. Thirdly, security requirements shall be linked with CIFs and business vision. We will discuss them in detail.

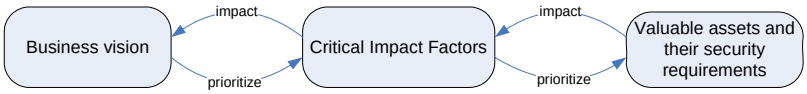

Fig. 1. Linking security requirements with business vision via CIF.

2.1 The business vision

Each organization has its own unique business vision that defines the very principles of how the business wants to achieve its goals. This vision, moreover, often changes over time to reflect changing circumstances. Notwithstanding this diversity, scholars in business administration have identified certain "patterns" in the business vision of leading firms. In this paper, we use the well-known *value disciplines* identified by Treacy and Wiersema [23, 24] as a framework for understanding the business vision.

Treacy and Wiersema argue that there are three generic ways a business can differentiate itself from the competition, which they call *operational excellence*,

customer intimacy, and *product leadership*. Each of these three value disciplines aims at creating distinguishing value for customers, but each does so in a different way.

- A company striving for *operational excellence* focuses on offering its products with the least amount of hassle possible and/or at the lowest cost to its customers.
- A *customer intimacy* company aims at delivering exactly what its customers want by investigating the needs of a narrow market and then customizing its offerings to this market.
- Finally, a *product leader* aims at delivering radically innovative products that create an unbridgeable gap with the competition.

Each of the three value disciplines leads to a radically different operating model for the company: the culture, processes, management systems and IT systems of the company. For instance, while operational excellence calls for highly standardized business processes, the customer intimacy discipline requires just the opposite: to meet customer requirements, business processes should be as flexible as possible. Security requirements should be likewise aligned with the requirements imposed upon culture, processes and management systems by the value discipline chosen.

2.2 Identifying the critical impact factors

When security incidents happen, they may lead to damage to organizations. Critical impact factors are the indicators of what kind of damage the security incidents incur to the organization. They can include those within the control of the organization (e.g. loss of productivity), as well as that the organization may not be able to fully control (e.g., legal liability, and reputation damage). We do not provide any explicit guidance for developing organization's CIFs in this paper. However, experienced executives and security officers generally identify some CIFs because they are part of their management domain. Other sources for identifying CIFs could include industry-specific CIFs or reviews of peer CIFs if available (for instance, The Information Security Forum archives a category of business impact [10]). Figure 2 illustrate an example list of critical impact factors.

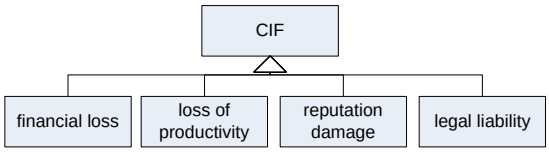

Fig. 2. An example of Critical Impact Factors.

2.3 Selecting valuable assets and security requirements

The business vision can be used to guide the selection of valuable assets. Surely, the assets that are critical for accomplishing the business vision are the valuable ones for the organizations. For example, a financial service company that focuses on customer intimacy will consider its customer relationship management (CRM) systems as extremely valuable, while a financial service company that focuses at product leadership will likely value its systems for developing new financial products even higher.

Information security is about defining encompassing systems and procedures designed to ensure the confidentiality, integrity and availability[3] of an organization's critical information and technical assets [2]. Information assets are the data and information, in either physical or electronic form, that is critical to the organization. Technical assets are those assets that support the storage, transmission, and processing of data and information and therefore are important to transforming data and information to be used by the organization. People can be an asset to the organization as well for similar reason – they can be a primary way of storing, transporting, or processing data.

So, IT security is about safeguard certain desired properties. The core of computer and information security is widely regarded as the preservation of three factors: confidentiality (ensuring that information is accessible only to those authorized to access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that only authorized users have access to information and associated assets when required) [7].

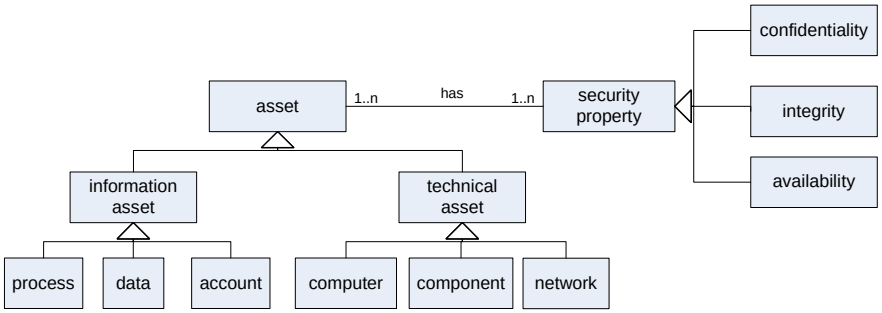

Fig. 3. A simple ontology of asset and security property.

Figure 3 depicts a simple ontology of asset and the security properties that are in the scope. Such an ontology can be used as a starting point to structure

[3] Some authorities treat communication security issues such as non-repudiation and privacy-related issues such as anonymity as additional aspects of security.

assets and their security properties. It is a minimum set and can be extended. For instance, some will include privacy issues like anonymity as a security property too[4]. Using such an ontology, the assets and their security properties can be structured accordingly. Figure 4 gives an example of a valuable information asset-medical record, and its desired security properties - confidentiality, integrity and availability.

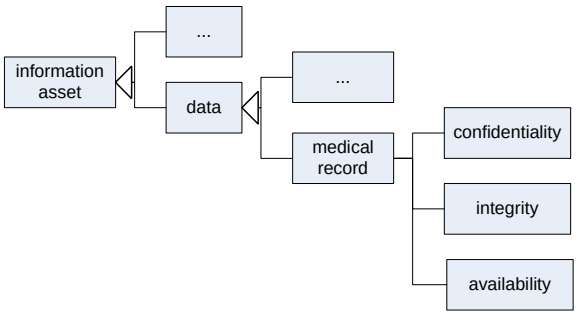

Fig. 4. An example of assets and their security properties.

2.4 Prioritizing security requirements

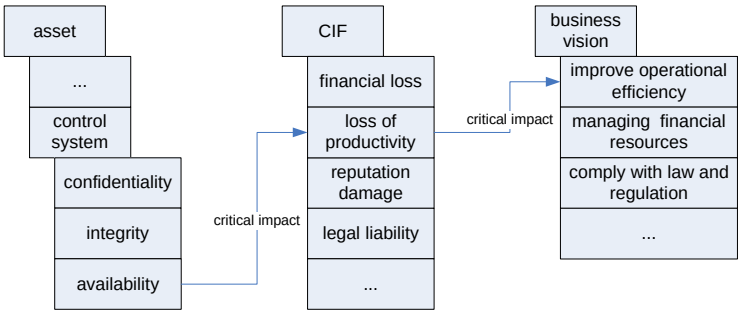

Fig. 5. An example of linking asset security requirement with business vision via CIFs.

To further elaborate the relations between security requirements and the business vision, the connection between them can be established via the linkage of CIFs. Figure 5 provides an example of such linkage for a production company.

[4] Firesmith provides a list of security properties in his work [6].

In this example, the organization is stating that any compromise to "availability" of the "control system" has "critical impact" to "loss of productivity", which in turn has "critical impact" to the organization's vision "improve operational efficiency". The impact severity can be categorized according to the organization's needs. An example categorization can be *critical impact*, *marginal impact*, and *negligible impact*. In this way, each security requirements can be connected to its CIFs and the CIFs further to business vision.

Using the impact diagram like figure 5, it is possible to categorize and prioritize the different security requirements. Requirements that have "critical impact" on CIFs, that in turn have "critical impact" on business vision, should be considered of most importance. These requirements shall be satisfied first if the resources (time, money, manpower etc.) are limited. In this example, it means that, for the production company, it is more important to mitigate threats to the control system's availability than for instance, threats to the control system's confidentiality. It is possible that one requirement may be linked to more than one CIFs. When that happens the overall significance of that security requirement can be determined in a number of ways. For example, one can choose the maximum impact level, e.g. if control system's availability not only has "critical impact" on loss of productivity but also has "marginal impact" on reputation damage, the overall impact should be "critical impact". Alternatively, one can choose the average impact level. The organization shall decide which combination methods best reflects its situation.

The reason why we use CIFs to link critical assets and their security requirements with business vision is twofold. The business vision typically resides at the strategic level. When the business vision is outlined, the stakeholders do not normally have a security focus in mind. The Critical Impact Factors on the other hand, reflect the business implication when security is compromised. It is of course possible to directly connect assets' security requirements to the business vision. But then the shift of focus from purely technical level security concerns to strategical level business concerns seems abrupt. The introduction of CIFs makes the shift smooth and the line of reasoning easier to follow.

Once the requirements are categorized and prioritized, other techniques, like attacks trees or misuse cases can be used to explore all possible threats and attack paths that would lead to the violation of security properties. In this example, it is to find out how the control system's availability can be compromised. Our approach is complementary to this line of work, in the sense that we provide a business-grounded rationale for why certain security requirements are important while others are not.

2.5 Discussion

A common way used in practice to get a very high-level specification and prioritization of security requirements is categorizing every IT asset or project on two dimensions [22]: risk level (low, medium, high), and security concern (confidentiality, integrity, availability). Compared to our approach, this very simple framework has several disadvantages: the security concerns are fixed, and there

is no explicit representation of the rationale behind placing an asset or project at a certain level. There is no reference to the business vision whatsoever.

3 Integrating the Solution Concepts into Service Level Management Cycle

The solution concepts presented in the previous section are of practical usage only when they can be integrated into processes and activities conducted in an organization. In this section, we discuss how our solution concepts can be integrated in service level agreements (SLAs) in the context of IT governance.

Due to recent legislation such as the Sarbanes-Oxley Act of 2002, IT Governance plays an important role in large organizations. IT Governance aims to improve the quality of IT services by introducing (or improving) controls and practices, stressing the definition of roles and duties among IT personnel and management. SLAs are considered one of the fundamental ways to define (and control) expected quality for a certain supplied service and are widely used not only between third parties (where a real contract exists) but also between units within the same company. In the latter case, this enforces responsibility (since both units together define what should be provided and in which way) and helps in avoiding unpleasant situations where it is difficult to define what went wrong (and who is responsible for that). Thus, SLAs perform an important function in managing the quality of IT services.

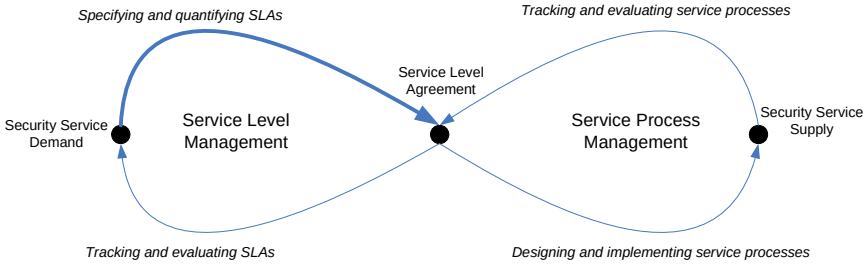

Fig. 6. Security sevice level management lemniscate adapted from [17].

Figure 6 shows an abstract process model taken from [17], which describes the process of managing and maintaining service level agreements. In Figure 6, it has been adapted to the security domain. The left part of the lemniscate concerns the specification of security services (upper arrow) and the evaluation and monitoring of the performance of the service provider (lower arrow). The right part concerns the evaluation and monitoring of security service processes (upper arrow) and the design and organization of those processes.

The SLA plays a pivotal role in this scheme. For example, a business unit in a bank uses several software systems to run its processes. If the business units

wants to make sure that the systems are secured properly, it is important that the IT department (service provider) and the business unit (the customer) make explicit what services the customer will receive. In this case, for example, the business unit's billing processes are in operation 24 hours a day, so the availability of the processes need to be guaranteed 24 hours a day. However, in order to decide this, the service provider and customer together need to investigate the needs of the customer. This process results in a SLA which states what the customer can expect, but also what obligations the customer has. To the service provider, the SLA forms the basis for implementing the service processes. Niessink argues that in order to improve IT services, all four phases of the Service Level Management lemniscate need to be taken into account [17]. The IT Infrastructure Library (ITIL) gives detailed guidelines for many of the processes that play a role in the delivery of IT services [12]. However, there are a number of aspects of IT service delivery that are not adequately covered by ITIL. One of them is that there is no structured guidelines to translate IT service needs into SLAs (the upper left arrow). It is this phase (specifying and quantifying SLAs) that our approach is designed to address.

The service level management lemniscate is an abstract model that needs to be refined for the particular case at hand. Figure 7 shows our proposed refinement, in which the upper-left arrow of Figure 6 has been refined into seven process steps that can be categorized according to the model presented in Figure 1 (horizontal dimension). The vertical dimension depicts the distinction between the IT demand side of an organization (*Business*, i.e. those organizational units where IT is used but not provided) and the IT supply side (*IT*, i.e. those organizational units that provide IT services). The figure shows that in our vision, the need for security services originate at the demand side, in the sense that it is ultimately the demand side that is harmed by breaches resulting from lack of security. It is also the demand side that is responsible for determining the business vision and critical impact factors (but often, the IT supply side provides help in carrying out these steps). The IT side then takes over, and the whole process results in SLAs that formalize the relation between the demand side and supply side.

The steps for specifying and quantifying SLAs for security services illustrated in Figure 7 are as follows: 1) The business unit starts to define its business vision by the help of identifying its value discipline. If the business vision already exist as a result of earlier activities, this step can be omitted. 2) Critical Impact Factors are identified based on a combination of industry specific CIFs , reviews of peer CIFs and the organization's own security officer's input. 3) The valuable business assets are listed and prioritized using the CIF impact analysis. This step is performed by the business unit and IT security unit together. 4) For the prioritized business assets, IT security unit identifies the IT assets that are needed to support the business assets and further identifies the desired security properties for the IT assets. 5) SLAs are prepared by IT and proposed to the business unit. 6) Due to budget concerns and maybe other causes, business may decide to accept a higher risk for certain assets in return for a lower service

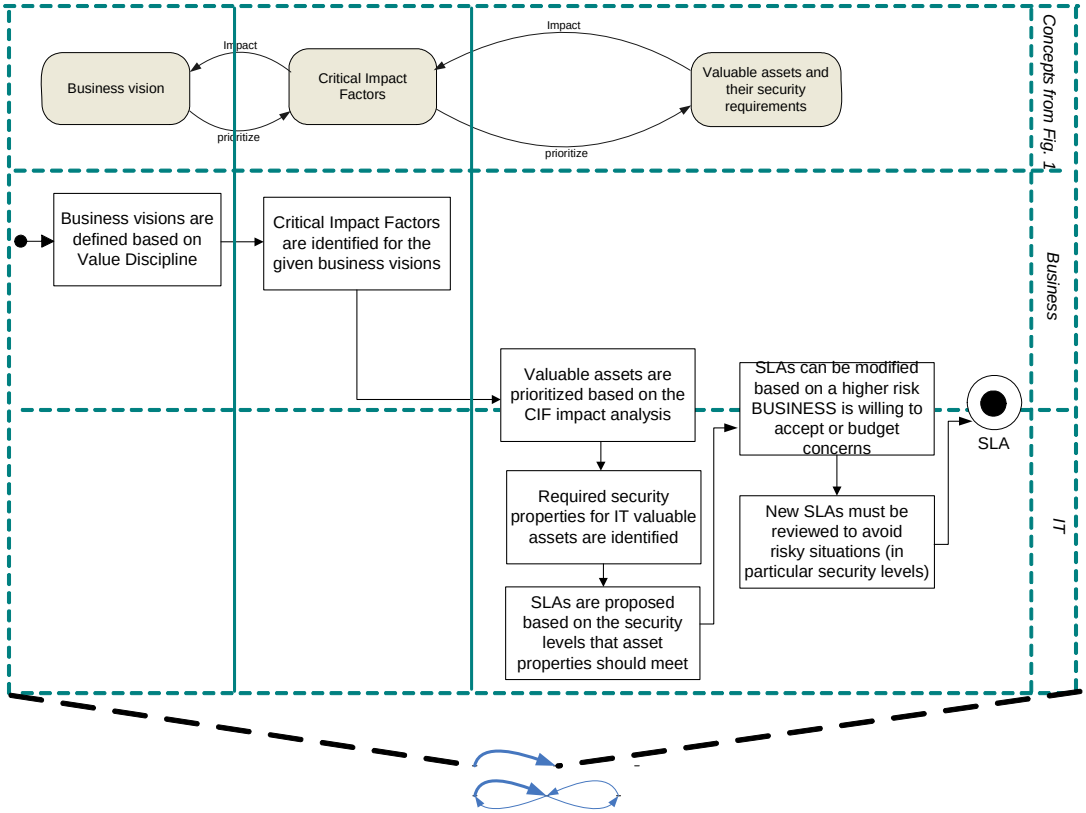

Fig. 7. Steps for structured translation of IT security needs into SLAs

price. 7) Finally, the new SLAs must be reviewed by IT to make sure that the higher risks in one business unit does not impose unacceptable high risks to other business units. This could happen because of the inter-dependence of processes across business units.

4 Validating the Approach Using a Focus Group Session

We have validated the approach with two aims in mind: i) we wanted to examine to what extent the approach addresses practical issues, and ii) we wanted to known whether our approach has the potential to improve current practice. We conducted a focus group session for the validation.

The use of focus groups has been gaining in popularity over the past few years. The effort to find a qualitative way to generate a rich understanding of a topic by having a group of people involved in a discussion, rather than by using a single quantitative method, such as a survey, is the reason of its increased

popularity [9]. A focus group session is commonly conducted with a group up to 12 professionals, so it has similarities with small samples research. Focus group sessions are useful to validate findings and gather recommendations that can derive changes from design or new hypothesis [5]. According to Hartman, five fundamental assumptions exist regarding focus groups: (i) people are valuable sources of information; (ii) people are capable of discussing themselves and articulating their thoughts, feelings, and behaviors; (iii) the moderator can help people retrieve information; (iv) the dynamics of the group can help generate valid and reliable data; and (v) group interviewing can be more effective than individual interviewing in particular research circumstances [9]. In our research circumstances, we find it an appropriate instrument to validate the usefulness and suitability of the framework.

In our focus group session we presented the framework to a group of 7 professionals. The professionals are drawn from the IT security unit of a leading Dutch bank (hereinafter referred to as Bank A). Their expertise range from technical level issues such as access control to business level issues such as business impact analysis. We explained our motivation of the work and why we decided to include the elements in the framework. After that, we received comments, suggestions and judgments from them and engaged in discussions. The results are listed next:

- Are the three concepts (business vision, CIFs and assets) present in Bank A practice? Yes. Bank A starts with business impact analysis, resulting in 3-level codes for every asset.
- The professionals agree that ISO17799 and COBIT do not provide guidelines for how to translate IT security needs into service level agreements.
- At Bank A, information is the main asset. Assets and CIFs are in the circle of influence of the IT supply organization. The business vision concept is in the scope of the IT demand organization. The IT demand organization is eventually responsible for choosing the right security level. This is then recorded in the SLAs. The IT supply organization is then responsible for actually reaching the security level agreed upon in the SLA.
- The IT department has service level agreements with the business units, and it is the business units that are responsible for coming up with the right security level. However, due to the intricate connections between the different units, IT department also need to aid in this process to make sure that business units choose the *right* level. Sometimes, the business units choose a low security level when considering its operation in isolation. But when examined in a bigger scope, it may put the company reputation in danger or may incur bigger risks to other dependent processes. In that case, IT department may advice the business units to choose a higher security level. Should disagreement happen in this situation, top level management shall be resorted to for final decision.
- There may be different business visions across different subdivisions of the IT demand side. At Bank A, the IT supply organization (itself using an operational excellence discipline) has to deal with all three disciplines on

the demand side, as this differs from business unit to business unit (e.g. Mortgages is a product leader).
- The merit of this approach is that it is similar to what Bank A does in practice, and the professionals do quickly recognize bits and pieces of the approach. The difference is that the approach makes the whole process explicit and structured. By doing so, it forms a good base for better understanding between the IT and business part and eventually for providing tool support for the process.

Our original intention with the focus group session was to evaluate the usefulness of our approach in practice. Based on what we gathered from the professionals (listed above), we can positively conclude that (i) the solution concepts we proposed are recognizable in practice, (ii) the embedding of the approach to the cycle of SLA management seems reasonable, (iii) the approach is useful in providing a structured way to understand and specify IT security needs and (iv) to connect security needs with service level agreements. In addition, the professionals pointed out a few more lines of possible extension to the framework, e.g. (i) dynamics: how to re-assess all assignments (of assets to CIFs and CIFs to the business vision) in a changing world? and (ii) how to deal with security awareness? The level of security awareness is a determining factor in how people assess security risks, priorities, etc. We shall look into the possibility of including the aforementioned aspects into the framework.

5 Related Research

There exist a number of security standards, among which COBIT (Control Objectives for Information and related Technology) [4] and BS7799 [3] are of particular relevance to our work. COBIT is an international de-facto standard for information control and IT risk management, addressing IT governance and control practices. It provides a reference business-oriented framework for management, users and control and security auditors. COBIT defines control objectives but does not provide guidelines on how to reach the objectives. BS7799 (originally published in 1995) is strictly focused on IT security and it is divided into two parts. The first part, *Code of Practice for Information Security Management*, became an official ISO standard, ISO 17799, in 2000. It contains general security guidelines including policies, practices, procedures, organizational structures and software functions. The second part, *Information Security Management - Specifications*, became an ISO standard, ISO 27001, in 2005. It contains technical requirements. ISO17799/27001 addresses a company's security from a best practice point of view, which does not provide any answer to why certain security mechanisms are in place for a particular organization. In [21], we argue that both COBIT and ISO17799 do not define guidelines on how to prioritize in a proper way the company assets and their security properties.

In the line of service management, the IT Infrastructure Library (ITIL) is a framework consisting of a set of management concepts and methods to maximize

the quality in delivering IT services. The IT service management section is split into *service delivery* and *service support*. As part of the service management implementation, the framework suggests to create a *vision statement* regarding the general service quality improving plan, which should align business and IT strategies. ITIL, however, does not provide any structured guidelines on how to translate IT service needs into service level agreement.

Our approach is also related to the work of security requirement modeling. Sindre and Opdahl [19] suggest to have negative use cases or scenarios in connection with security. Yu and Liu [26, 14] in their work shows actors and misactors having contradictory goals in an extension of i^* diagrams [16]. Links such as "break" or "hurt" can show how an attack prevents the legitimate users from reaching their goals, or how countermeasures can thwart an attacks. Van Lamsweerde addresses malicious obstacles (called anti-goals) set up by attackers to threaten security goals and threat trees are built systematically through anti-goal refinement [25]. This line of work focuses on how to model threat, including the threat actors and their attack paths. Our approach, on the other hand, focuses on providing business rationale for explaining why certain security requirements exist in the first place. We also address how to prioritize security requirements, which is a problem not addressed by the other approaches. We believe it is important to prioritize security requirements since not all can be satisfied, because in reality only limited resources are set aside for improving security in organizations. Our approach can be combined with the modeling work. First, the security requirements are ranked using our approach. Next, for the prioritized security requirements, misuse case or attack trees [18] can be use to model how attacks that will violate the security requirements could actually happen. A number of proposals have proposed enhancements to UML to cope with security constraints. [13] proposes an extension of UML where cryptographic and authentication features are explicitly modeled. Another proposal of enhancing UML is the SecureUML language [15] which, however, is geared towards access control. This line of work is fairly low level and is therefore suited to more operational analysis. A challenging line of research may involve the integration of the above methodologies, so that one can start from a high level rationale analysis of the security requirements with our approach and then continue down the line to investigate possible attack paths using negative use cases and finally to an operational specification using UML.

Finally, our work is also related to the work of security risk assessment. Traditionally, in risk assessment methodologies, e.g. OCTAVE [1] (Operationally Critical Threat, Asset and Vulnerability Evaluation), risk of each threat is determined by the impact of the threat once it happens and how likely it will happen [20]. For the impact, a severity level (e.g. high, low or medium) is assigned. What often happens is that the severity level is assigned based on the person's own experience without explicit rationale. Our approach can enhance this process because it provides an explicit tie to the organization's business drivers.

6 Conclusions

The ISO 17999 [11] standard on information security requires an organization to protect information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities. It is clear from this requirement that information security is ultimately about business security. In this paper, we have proposed a conceptual framework that makes the link between security requirements and the organization's business drivers explicit. The three main elements of our framework are business vision, CIFs and valuable assets and their security requirements. The connection between business goals and security requirements, once established, can be used to provide rationale for prioritizing security requirements.

The conceptual framework presented in this paper is only useful in practice when it is embedded in a concrete process for security management. In this paper, we have shown how this can be accomplished in the context of IT service level management. We have evaluated our approach by means of a focus group session at a large financial institution. Our experience with the focus group session tells us that giving people the appropriate tools to frame and structure their decision making process in relation to the underlying business goals and encouraging the right kind of dialog among stakeholders are beneficial to the delivery of high quality services. From what we have learned, several directions for further research become apparent. For example, our focus group indicated that creating security awareness is a very critical success factor. It is also our intention to extend our security management process to cover tracking and evaluating service level agreements.

Acknowledgments

We thank our focus group at Bank A for their valuable contribution. The second author is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

References

1. C. Alberts, A. Dorofee, J. Stevens, and C. Woody. Introduction to the OCTAVE approach. Technical report, Carnegie Mellon Software Engineering Institute, 2003. URL http://www.cert.org/octave/.
2. R. J. Anderson. *Security Engineering: a Guide to Building Dependable Distributed Systems*. John Wiley and Sons, 2001.
3. BS7799. BS 7799-3:2005 information security management systems. guidelines for information security risk management, 2005. URL http://www.bsi-global.com/Global/bs7799.xalter.
4. COBIT. CobiT: Control Objectives for Information and related Technology, 2006. URL http://www.isaca.org.

5. D. R. Cooper and P. S. Schindler. *Business Research Methods*. McGraw-Hill, 2003.
6. D. G. Firesmith. Common concepts underlying safety, security and survivability engineering. Technical report, CMU/SEI-2003-TN-03, 2003.
7. S. Furnell. *Computer Insecurity – risking the system*. Springer, 2005.
8. L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Rochardson. 2005 CSI/FBI computer crime and security survey. Technical report, Computer Security Institute, 2005.
9. J. Hartman. Using focus groups to conduct business communication research. *Journal of Business Communication*, 41:402–410, 2004.
10. ISF. The standard of good practice for information security. Technical report, Information Security Forum, 2005.
11. ISO17799. Code of practice for information security management, 2000.
12. ITIL: IT Infrastructure Library. URL http://www.itil.co.uk/.
13. J. Jürjens. Using UMLsec and goal-trees for secure systems development. In *Proceedings of the ACM Symposium of Applied Computing (SAC 2002)*. ACM Press, 2002.
14. L. Liu, E. Yu, and J. Mylopoulos. Analyzing security requirements as relationships among strategic actors. In *Proceedings of the 2nd Symposium on Requirement Engineering for Information Security (SREIS-02)*, 2002.
15. T. Lodderstedt, D. A. Basin, and J. Doser. Model driven security for process oriented systems. In *Proceedings of the 8th ACM Symposium on Access Control Models and Technologies*, 2003.
16. J. Mylopoulos, L. Chung, and E. Yu. From object-oriented to goal-oriented requirement analysis. *Communications of the ACM*, 42(1):31–37, January 1999.
17. F. Niessink. *Perspectives on Improving Software Maintenance*. PhD thesis, Division of Mathematics and Computer Sciences, Faculty of Sciences, Vrije Universiteit, Amsterdam, the Netherlands, March 2000.
18. B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.
19. G. Sindre and A. L. Opdahl. Eliciting security requirements with misuse cases. *Requirement Engineering*, 10(1):34–44, 2005.
20. G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical report, National Institute of Standards and Technology, 2002.
21. X. Su, D. Bolzoni, and P. A. T. van Eck. A business goal driven approach for understanding and specifying information security requirements. In *11th International Workshop on Exploring Modeling Methods in Systems Analysis and Design (EMMSAD2006), Luxembourg*, pages 465–472. Presses Universitaries de Namur, 2006.
22. M. Swanson. Security Self-Assessment Guide for Information Technology Systems. Technical report, NIST (National Institute of Standards and Technology), November 2001. Special Publication 800-26.
23. M. E. Treacy and F. D. Wiersema. Customer Intimacy and Other Value Disciplines. *Harvard Business Review*, 71(1):84–93, jan 1993.
24. M. E. Treacy and F. D. Wiersema. *The Discipline of Market Leaders: Choose Your Customers, Narrow Your Focus, Dominate Your Market*. Perseus Publishing, 1997.
25. A. v. Lamsweerde. Elaborating security requirements by construction of intentional anti-models. In *Proceedings of the 26th International Conference on Software Engineering (ICSE'04)*. IEEE Computer Society, 2004.
26. E. Yu and L. Liu. Modelling trust in i^* strategic actors framework. In *Proceedings of the third workshop on deception, fraud and trust in agent societies*, June 2000.