A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements

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 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 link explicitly 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. A conceptual framework is presented, where the relationships between business vision, critical impact factors and valuable assets (together with their security requirements) are shown.

1 Introduction

The increasing concerns of clients, 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. 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 function if the organizations involved cannot agree: 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 (CSO).

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 organization questions without specific guidance: What needs to be secured? Why, and in what priority? How to ensure that people agree on the above issue? How will I know when the organization has been "secured"? What will be used to measure success?

We believe that to answer the above questions, it is necessary to link the security requirements with the organization's unique business drivers. 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, different organizations have different business drivers, which in turn determine their different requirements to security. 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 underlining criterion for evaluating how important each security requirement is. It is our intention in this paper to develop techniques and instruments to help stakeholders articulate the connection between security requirements and the business drivers in a systematic way. Further, we shall use the rationale to prioritize security requirements.

2 Formulating and Understanding Security Goals and Requirements

A security requirement specification tells what should be secured and why. It identifies the organizations' 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 academics. 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 [1, 2] 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 competitors, 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 (usually, 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 reputational 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. Figure 2 illustrate an example list of critical impact factors.

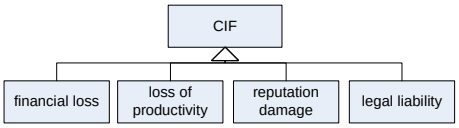

Fig. 2. An example of Critical Impact Factors.

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 [3]. Information assets are the data and information, in either physical or electronic from, 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

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

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) [4]. 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 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.

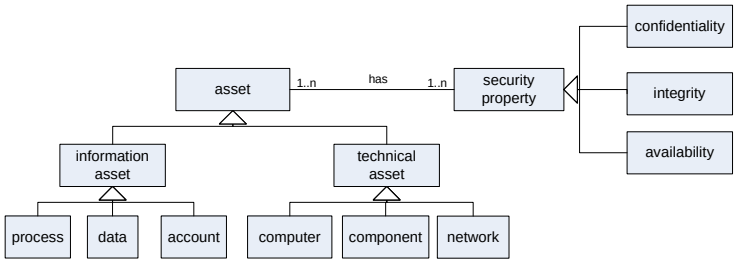

Fig. 3. A simple ontology of asset and security property.

2.4 Prioritizing security requirements

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 4 provides an example of such linkage for a production company. 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 4, 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

[4] Firesmith provides a list of security properties in his work [5].

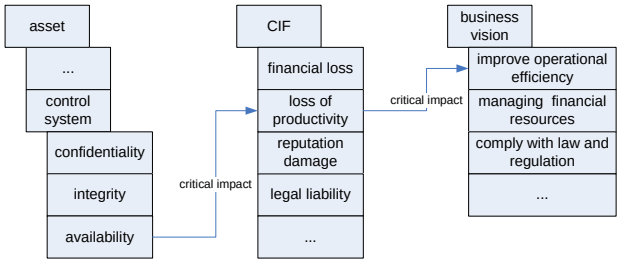

Fig. 4. An example of linking asset security requirement with business vision via CIFs.

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 [6]: 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. Apart from the advantages and disadvantages of the approaches, it is worthwhile to consider the context in which these approaches are used in practice. It is our intention to further study the context of specifying security requirements in practical situations, and see to what extend our approach addresses practical issues.

3 Related Research

There exist a number of security standards, among which COBIT (Control Objectives for Information and related Technology) [7] and BS7799 [8] are of particular relevance to our work. COBIT defines control objectives but does not provide guidelines on how to reach the objectives. BS7799 (later became ISO17799/27001) is strictly focused on IT security and 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. Both COBIT and ISO17799 however, do not define guidelines on how to prioritize in a proper way the company assets and their security properties.

Our approach is also related to the work of security requirement modeling [9–12].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 [13] can be use to model how attacks that will violate the security requirements could actually happen.

4 Conclusions

The ISO 17999 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 argued the necessity of making explicit the link between security requirements and the organization's business drivers. Furthermore we have proposed a conceptual framework to that aim. 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. A number of issues will be addressed further in the future. An in-depth case study with a dutch government agency will reveal to what extend our approach addresses practical issues. We need to define guidelines that help the creative process of coming up with a proper set of CIFs. Also in the face of contradicting business visions, proper guidelines should be given on how to combine the results.

Acknowledgments

We thank professor Roel Wieringa and dr. Raimundas Matulevicius for their valuable comments.

References

1. Treacy, M.E., Wiersema, F.D.: Customer Intimacy and Other Value Disciplines. Harvard Business Review **71**(1) (1993) 84–93
2. Treacy, M.E., Wiersema, F.D.: The Discipline of Market Leaders: Choose Your Customers, Narrow Your Focus, Dominate Your Market. Perseus Publishing (1997)
3. Anderson, R.J.: Security Engineering: a Guide to Building Dependable Distributed Systems. John Wiley and Sons (2001)
4. Furnell, S.: Computer Insecurity – risking the system. Springer (2005)
5. Firesmith, D.G.: Common concepts underlying safety, security and survivability engineering. Technical report, CMU/SEI-2003-TN-03 (2003)
6. Swanson, M.: Security Self-Assessment Guide for Information Technology Systems. Technical report, NIST (National Institute of Standards and Technology) (2001) Special Publication 800-26.
7. COBIT: CobiT: Control Objectives for Information and related Technology (2006) URL http://www.isaca.org.
8. 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.
9. Sindre, G., Opdahl, A.L.: Eliciting security requirements with misuse cases. Requirement Engineering **10**(1) (2005) 34–44
10. Yu, E., Liu, L.: Modelling trust in i^* strategic actors framework. In: Proceedings of the third workshop on deception, fraud and trust in agent societies. (2000)
11. Liu, L., Yu, E., Mylopoulos, J.: Analyzing security requirements as relationships among strategic actors. In: Proceedings of the 2nd Symposium on Requirement Engineering for Information Security (SREIS-02). (2002)
12. v. Lamsweerde, A.: 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)
13. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons (2000)