Enterprise Architecture-Based Risk and Security Modelling and Analysis

Henk Jonkers(✉) and Dick A.C. Quartel

BiZZdesign, P.O. Box 321, 7500 AN Enschede, The Netherlands
{h.jonkers,d.quartel}@bizzdesign.com

Abstract. The growing complexity of organizations and the increasing number of sophisticated cyber attacks asks for a systematic and integral approach to Enterprise Risk and Security Management (ERSM). As enterprise architecture offers the necessary integral perspective, including the business and IT aspects as well as the business motivation, it seems natural to integrate risk and security aspects in the enterprise architecture. In this paper we show how the ArchiMate standard for enterprise architecture modelling can be used to support risk and security modelling and analysis throughout the ERSM cycle, covering both risk assessment and security deployment.

Keywords: Enterprise architecture · Archimate · Risk and security modelling · Risk analysis

1 Introduction

Until quite recently, IT security was the exclusive domain of security specialists. However, due to the fact that the complexity of (networked) organizations and their IT infrastructure is growing, and cyber attacks are getting more sophisticated, traditional approaches to cyber security no longer suffice. In the last couple of years, organizations have started to realize that IT-related risks cannot be seen in isolation, and should be considered as an integral part of Enterprise Risk and Security Management (ERSM). ERSM includes methods and techniques used by organizations to manage all types of risks related to the achievements of their objectives.

It is only natural to place ERSM in the context of Enterprise Architecture (EA), which provides a holistic view on the structure and design of the organization. Therefore, it is not surprising that EA methods such as TOGAF [6] include chapters on risk and security (although the integration of these topics in the overall approach is still open for improvement), and a security framework such as SABSA [5] shows a remarkable similarity to the Zachman framework for EA. And as a corollary, it also makes perfect sense to use the ArchiMate language [8], the standard from The Open Group for enterprise architecture modelling, to model risk and security aspects as an integral part of the architecture.

In this paper, we introduce this risk and security "overlay" of the ArchiMate language (Sect. 2), and link these concepts to the phases of a typical ERSM

© Springer International Publishing AG 2016
B. Kordy et al. (Eds.): GraMSec 2016, LNCS 9987, pp. 94–101, 2016.
DOI: 10.1007/978-3-319-46263-9_6

process (Sect. 3). Subsequently, we show how the resulting models can be used as input for qualitative risk analysis, inspired by the Open FAIR Body of Knowledge [7] (Sect. 4). Using this analysis, the impact of different control measures to mitigate the identified risks can also be assessed. We illustrate this approach with a small example in Sect. 5. Finally, in Sect. 6, we draw some conclusions and give some pointers to other possible applications of enterprise architecture-based risk and security models.

2 Modelling Risk and Security in the ArchiMate Language

The ArchiMate language [8] is the leading open standard for enterprise architecture modelling, aimed at creating integrated models of the organization structure and business processes, supporting software applications and technology, and underlying technical infrastructure, as well as the business motivation and implementation and migration aspects. Although the ArchiMate language does not natively support risk and security modelling, guidelines for using specializations of ArchiMate concepts for this purpose have been published in a white paper from The Open Group [1].

To identify the relevant concepts in the ERSM field, several leading standards and frameworks for risk and security have been studied, including the ISO/IEC 27001 standard on information security management, the Open FAIR Body of Knowledge [7], and the SABSA framework [5], as well as scientific frameworks such as ISSRM [2]. The concepts found in these standards and frameworks show a lot of overlap, and it appears that most of the concepts used in these standards and frameworks can easily be mapped to existing ArchiMate concepts, as summarized in Fig. 1 (the original ArchiMate concepts are shown in brackets). Since ERSM is concerned with risks related to the achievement of business objectives,

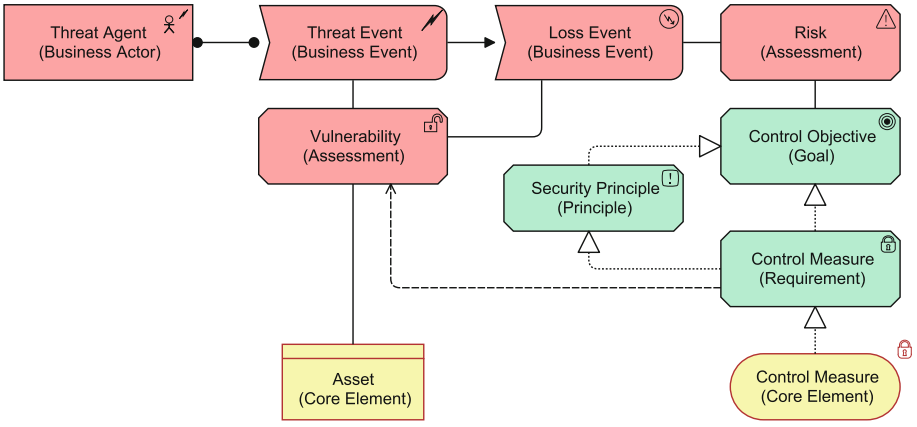

Fig. 1. Risk and security concepts as specializations of ArchiMate concepts

it is not surprising that many of these concepts are from the ArchiMate motivation extension, but also some of the elements from the core language (business, application and technical infrastructure layer) are used:

- Any core element represented in the architecture can be an *asset*, i.e., something of value susceptible to loss that the organization wants to protect. Assets may have *vulnerabilities*, which may make them the target of attack or accidental loss.
- A threat may result in *threat events*, targeting the vulnerabilities of assets, and may have an associated *threat agent*, i.e., an actor or component that (intentionally or unintentionally) causes the threat. Depending on the threat capability and vulnerability, the occurrence of a threat event may or may not lead to a *loss event*, i.e., an actual negative impact caused by the threat.
- *Risk* is a (qualitative or quantitative) assessment of probable loss, in terms of the loss event frequency and the probable loss magnitude.
- Based on the outcome of a risk assessment, we may decide to either accept the risk, or set *control objectives* (i.e., high-level security requirements) to mitigate the risk, leading to requirements for *control measures*. The selection of control measures may be guided by predefined *security principles*. These control measures are realized by any set of core elements, such as business process (e.g., a risk management process), application services (e.g., an authentication service) or nodes (e.g., a firewall).

In the following sections, we will show how these concept can be used for modelling and analysis in the different phases of the ERSM process.

3 The ERSM Process

Figure 2 sketches a typical iterative ERSM process, inspired on standards such as ISO 31000 [3]. The figure also links the concepts from the ArchiMate "risk overlay" to the phases of the process in which they are primarily used.

The left-hand side of this process (phases 1–4) are concerned with risk assessment. Based on monitoring, experience or inspection of the model, potential vulnerabilities of assets in the organization are identified. Combined with potential (internal or external) threats, these vulnerabilities may lead to loss events. An assessment of these loss events, consisting of an indication of their frequency (or likelihood) and the potential loss magnitude, results in an overview of risks.

The right-hand side of the process (phases 5–9) are about security deployment. The identified risks, together with existing security policies, are the input for the control objectives, i.e., the desired level of security. This may also involve a classification of assets, e.g., the required levels of confidentiality, integrity and availability (the "CIA triad") of different classes of information assets. Based on the control objectives, possibly guided by security principles that the organization has established, requirements for control measures (security controls) can be formulated. Ultimately, these control measures are designed and implemented

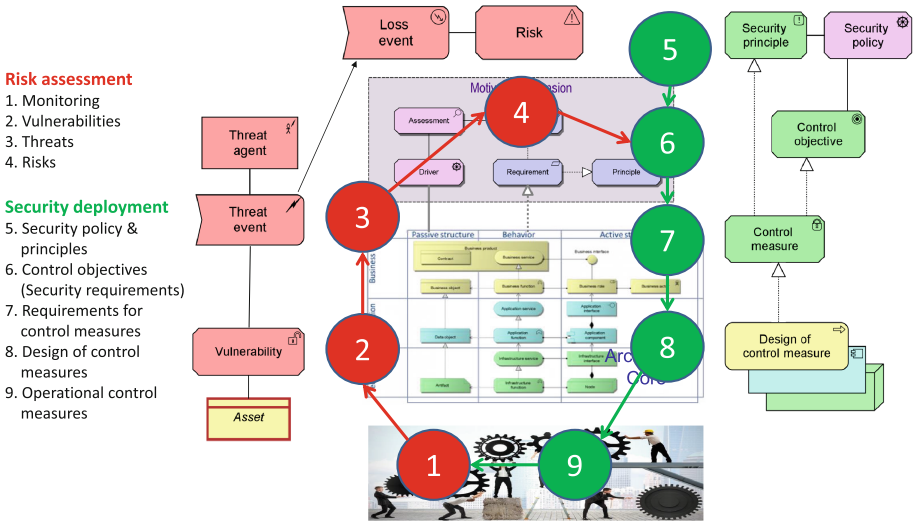

Fig. 2. The ERSM process

within the organization. This leads to a new baseline situation, which forms the starting point of a new iteration of the ERSM process.

In the next two sections we will outline how ArchiMate models can be used in the risk assessment and in the security deployment phases, respectively.

4 Qualitative Risk Analysis

Using the language customization mechanisms as described in the ArchiMate standard [8], risk-related attributes can be assigned to the concepts introduced above. The Factor Analysis of Information Risk (FAIR) taxonomy [7], adopted by The Open Group, provides a good starting point for this. If sufficiently accurate estimates of the input values are available, quantitative risk analysis provides the most reliable basis for risk-based decision making. However, in practice, these estimates are often difficult to obtain. Therefore, FAIR proposes a risk assessment based on qualitative (ordinal) measures, e.g., threat capability ranging from 'very low' to 'very high', and risk ranging from 'low' to 'critical'. Figure 3 shows how these values can be linked to elements in an ArchiMate model, how they are related, and how they can be visualized in 'heat maps':

A. The level of *vulnerability* (Vuln) depends on the *threat capability* (TCap) and the *control strength* (CS). Applying control measures with a high control strength reduces the vulnerability level. In case of multiple threats or multiple control measures, we assume that the maximum threat capability and maximum control strength determine the outcome, although more advanced ways to combine them are also conceivable.

B. The *loss event frequency* (LEF) depends on both the *threat event frequency* (TEF) and the level of *vulnerability*. A higher vulnerability increases the probability that a threat event will trigger a loss event.
C. The level of *risk* is determined by the *loss event frequency* and the *probable loss magnitude* (PLM).

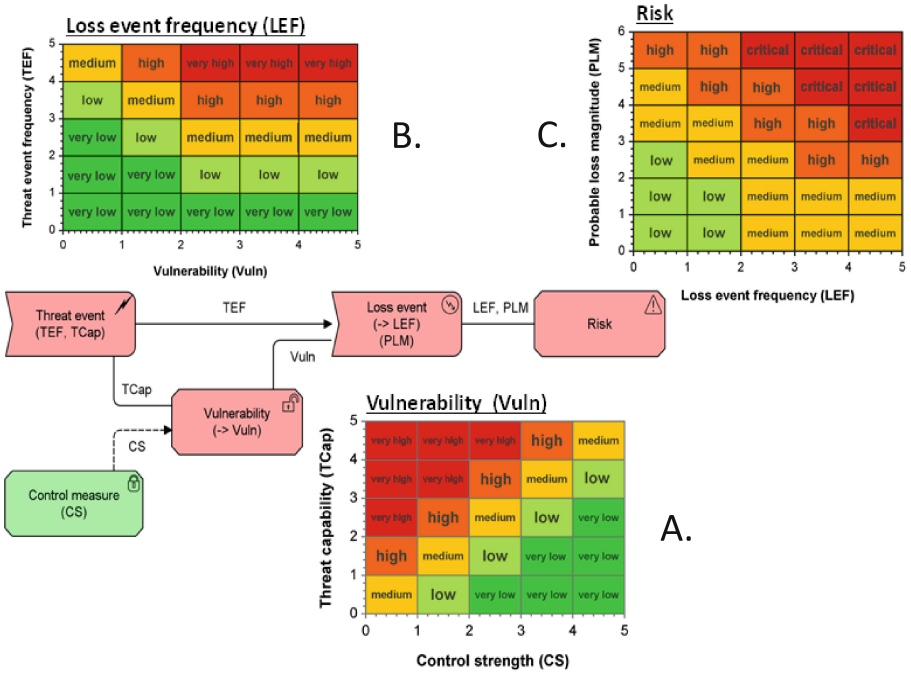

Fig. 3. Summary of qualitative risk analysis

5 Example

The example in Fig. 4 shows a simple application of a vulnerability and risk assessment. The "traffic lights" show the ordinal values of the risk attributes as defined in the FAIR Body of Knowledge and summarized in Sect. 4.

A vulnerability scan of the transmission of payment data from a web shop to an online payment provider has shown that the encryption level of transmitted payment records is low (e.g., due to an outdated version of the used encryption protocol). This is classified as a vulnerability level 'high'. Also, the transmission channel using the public internet is insecure, which is classified as a vulnerability of level 'medium'. These two vulnerabilities enable a man-in-the-middle attack,

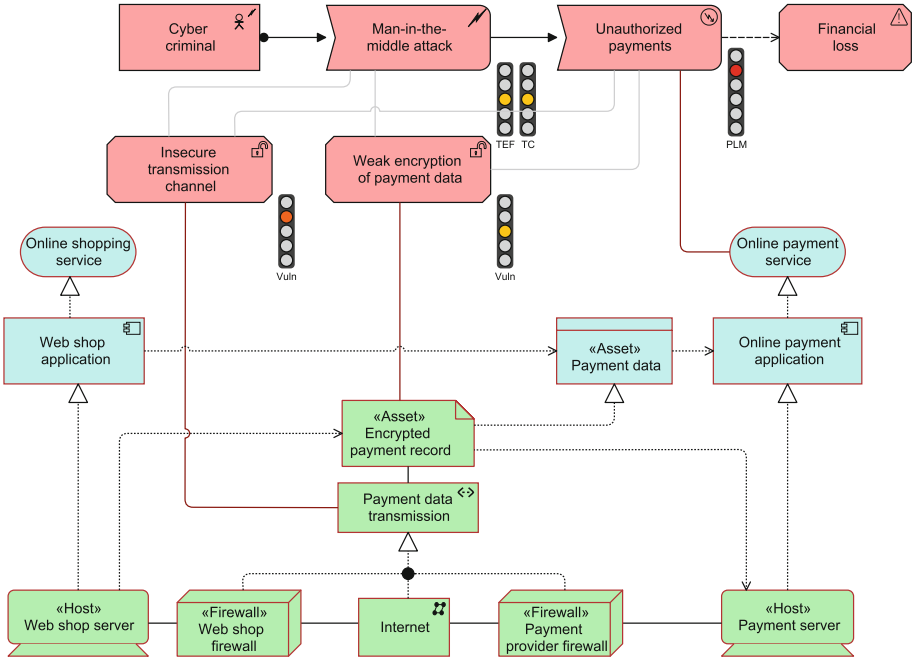

Fig. 4. Risk analysis example

in which a cyber criminal may modify the data to make unauthorized payments, e.g., by changing the bank account number of the receiver. Assuming a cyber criminal with medium skills (medium threat capability) and a medium threat event frequency (e.g., on average one attempted attack per week), according to the loss event frequency matrix shown in Fig. 3, the expected loss event frequency is also medium. Finally, assuming a high probable loss magnitude (potentially, a large sum of money may be lost), the resulting level of risk is high.

It is decided that this risk is unacceptable. Therefore, a control objective is defined to prevent unauthorized access to payment data, together with a security profile specifying the required security parameters for payment data: confidentiality and integrity must be high (it should not be possible for unauthorized persons to view or modify the data), and the required level of availability is medium (payment data does not have to be available 24/7). This is illustrated in Fig. 5. This profile can be translated to specific requirements for control measures. For example, as a preventive control measure that helps to achieve the required levels of confidentiality and integrity, a stronger encryption protocol is needed (which can be realized by, e.g., 256-bit encryption instead of 128-bit encryption), and a secure transmission channel is needed (which can be realized by using a VPN solution). By modifying the parameters, it can be shown what the effect of the different control strengths is on the residual risk. Further reduction of this risk may also require other measures, e.g., measures to limit

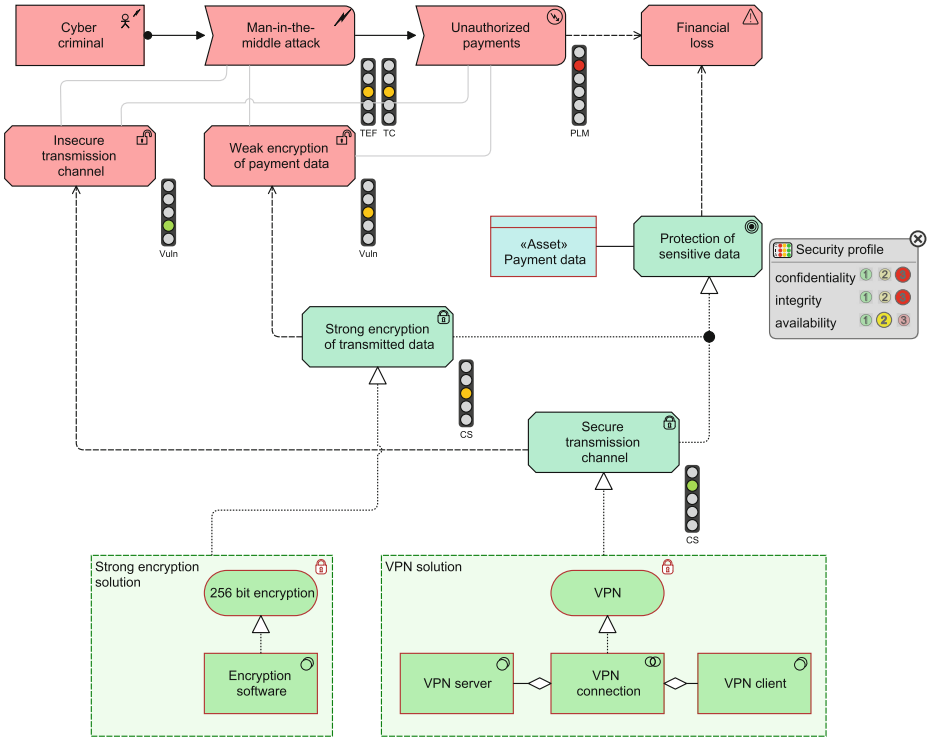

Fig. 5. Risk mitigation example

the probable loss magnitude (e.g., by limiting the maximum amount of money that can be transferred using this system).

6 Conclusions

Because of the increasing complexity of organizations and their IT infrastructure, and the growing capabilities of cyber attackers, traditional information security approaches no longer suffice: it becomes necessary to adopt an integrated approach to Enterprise Risk and Security Management (ERSM).

The ArchiMate modelling language provides the hooks to integrate risk and security aspects in the overall enterprise architecture. By linking risk-related properties to specializations of ArchiMate concepts, risk analysis can be automated with the help of a modeling tool. In this way, it becomes possible to analyze the impact of changes in these values throughout the organization, as well as the effect of potential control measures to mitigate the risks. For example, the business impact of risks caused by vulnerabilities in IT systems or infrastructure can be visualized in a way that optimally supports security decisions made by managers.

The modelling concepts and analysis technique described in this paper have been implemented as a prototype in BiZZdesign's modelling tool suite Enterprise Studio. The approach and tool have been applied in a real-life case study to set up an initial security architecture at a health insurance company. The focus of this case study was on the systematic identification of control objectives and requirements for control measures, and a gap analysis between the baseline and target security architectures. This aspect is underexposed in this paper, but the presented modelling concepts are also very suitable to support this. Another option that has been explored is the import of the results of an automated vulnerability scan (penetration test) of the IT infrastructure into an ArchiMate model, thus making it possible to visualize the found vulnerabilities and their impact throughout the rest of the enterprise architecture [4].

Acknowledgement. Part of the research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant agreement no. 318003 (TRESPASS). This publication reflects only the authors views and the Union is not liable for any use that may be made of the information contained herein.

References

1. Band, I., Engelsman, W., Feltus, C.S., González Paredes, S., Hietala, J., Jonkers, H., Massart, S.: Modeling enterprise risk management and security with the ArchiMate language. White Paper, The Open Group (2015)
2. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A systematic approach to define the domain of information system security risk management. In: Nurcan, S., et al. (eds.) Intentional Perspectives on Information Systems Engineering, pp. 289–306. Springer, Heidelberg (2010)
3. ISO, Itc, UNIDO: ISO 31000 Risk Management: A Practical Guide for SMEs (2015)
4. Jonkers, H., Seghers, B.: Visualizing the business impact of technical cyber risks. In: The Open Group Summit Amsterdam, and as an Open Group Webinar (2014)
5. Sherwood, J., Clark, A., Lynas, D.: Enterprise security architecture. White Paper, SABSA Institute (2009)
6. The Open Group: TOGAF® Version 9.1. Van Haren Publishing, Zaltbommel (2011)
7. The Open Group: Risk taxonomy (O-RT), version 2.0 (2013)
8. The Open Group: ArchiMate® 3.0 Specification. Van Haren Publishing, Zaltbommel (2016)