



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

Xiaomeng Su, Damiano Bolzoni and Pascal van Eck

University of Twente, the Netherlands

Introduction

● Context

- Companies are putting resources in information security
 - ⌘ The growth of E-Commerce
 - ⌘ The impact of legislations on information security
 - ⌘ Business risks and security requirements of the business network
- Senior managers in many organizations are now expressing a much greater interest in information security

Introduction

● Issue

- 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
- Requirements end up being articulated as specifications of the security control baseline (how security will be achieved) without a clear rationale.

Introduction

● Motivation

- Illustrated by challenges facing chief security officers (CSO)
- Often CSOs are tasked with "securing" the organization, but may not be clear on what that means
- the CSO is often left to answers of 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?

Introduction

● Solution direction

- It is necessary to link the security requirements with the organization's unique business drivers
- Different organizations have different business drivers, which in turn determined their different requirements to security
- It is important to develop techniques and instruments to help stakeholders articulating the connection between security requirements and the business drivers in a systematic way

Formulating and Understanding Security Goals and Requirements

- A security requirement specification tells what should be secured and why?
- It is equally important to determine which requirements are more important and thus should be prioritized
- Use a conceptual framework where security requirements are linked to the unique business drivers of the organization

The conceptual framework

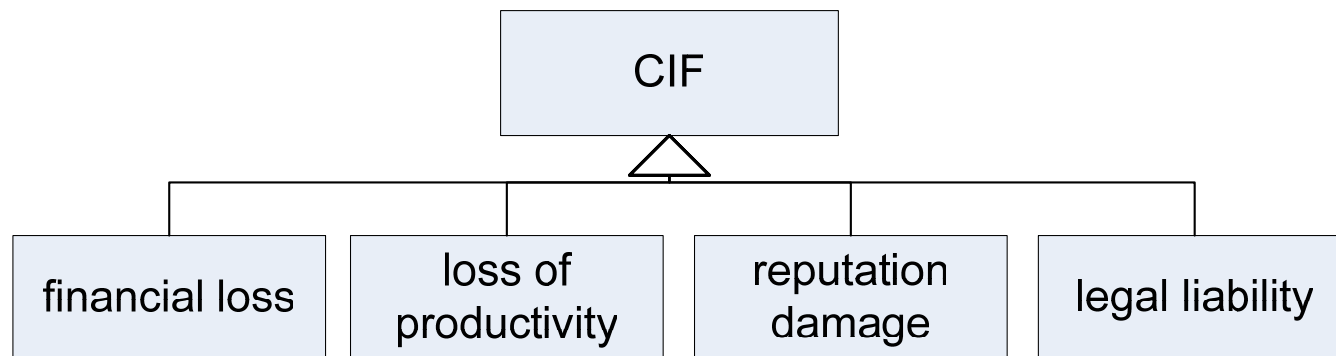


The business vision

- Each organization has its own unique business vision that defines the very principles of how the business wants to achieve its goals
- Value disciplines as a framework for understanding the business vision
 - Operational excellence
 - Customer intimacy
 - Product leadership
- Security requirements should be aligned with the requirements imposed by the value disciplines chosen

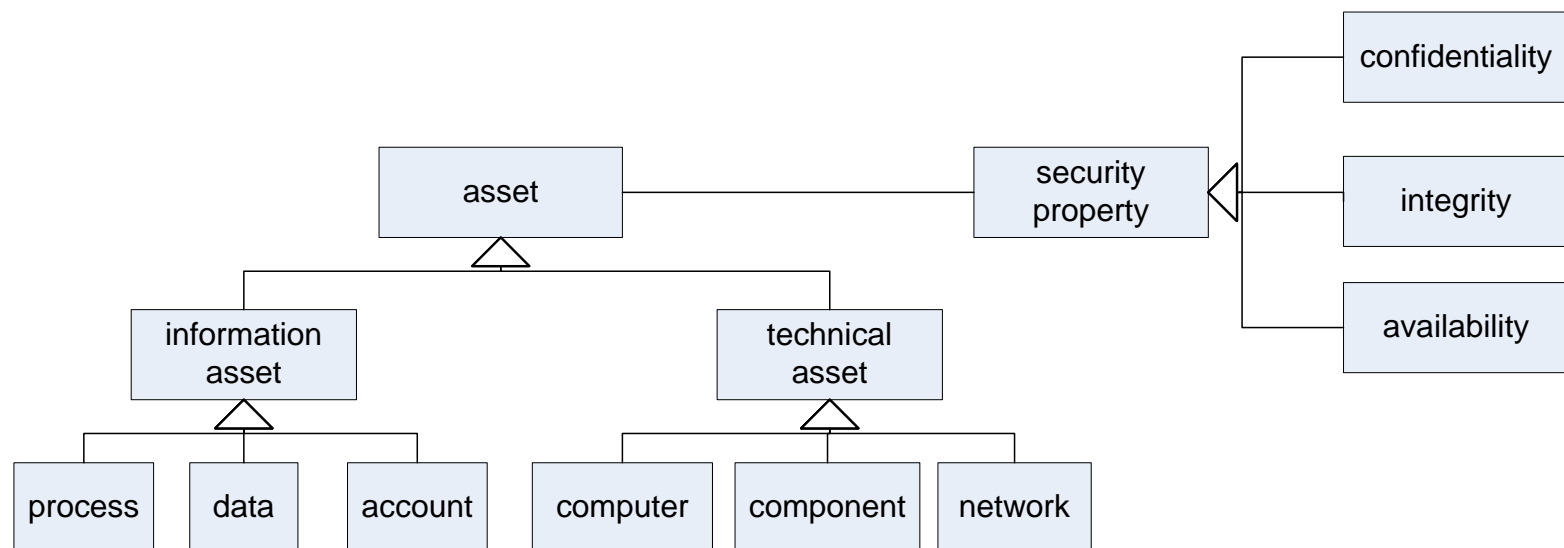
Identify critical impact factors

- Critical impact factors are the indicators about what kind of damage the security incidents incur to the organization.
- An example CIF list

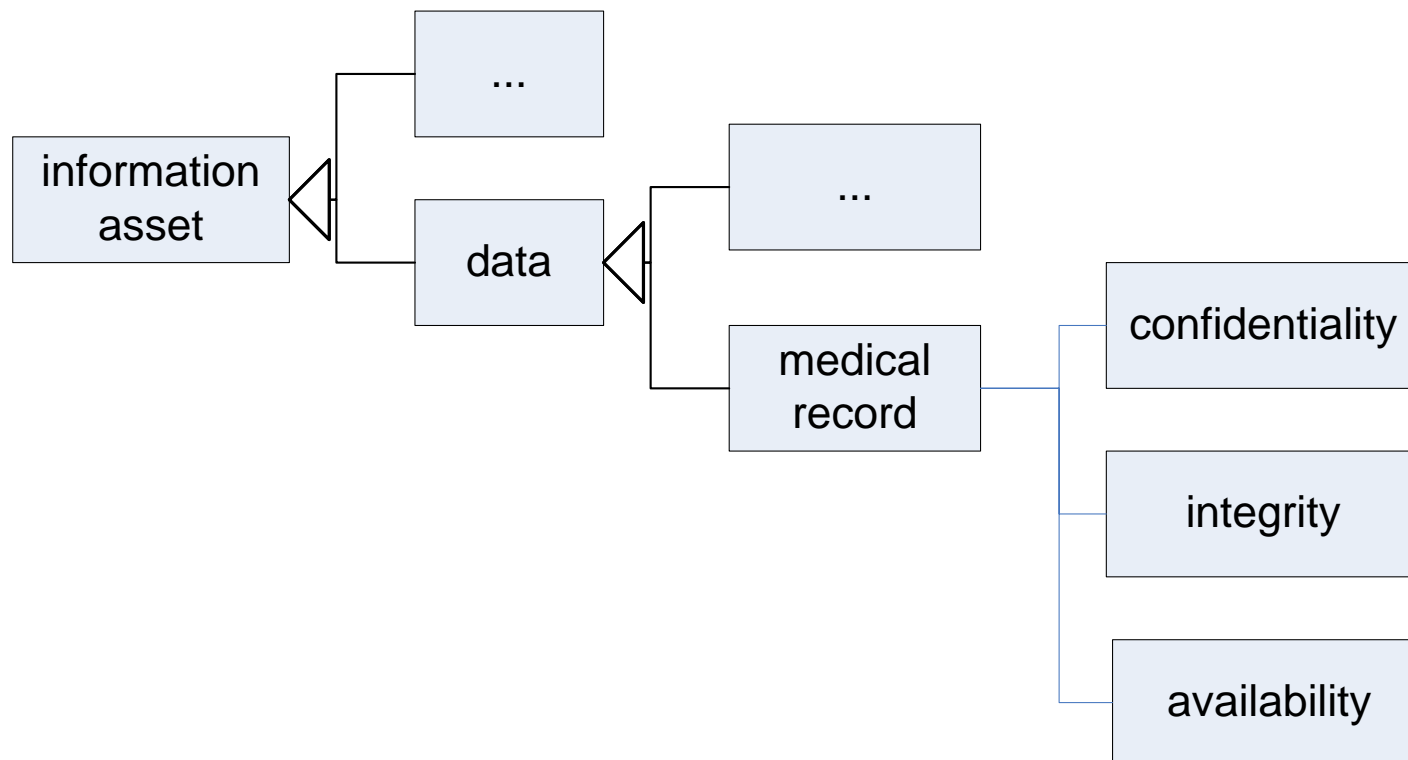


Selecting valuable assets and security requirements

- Assets
- Security properties
- A simple ontology

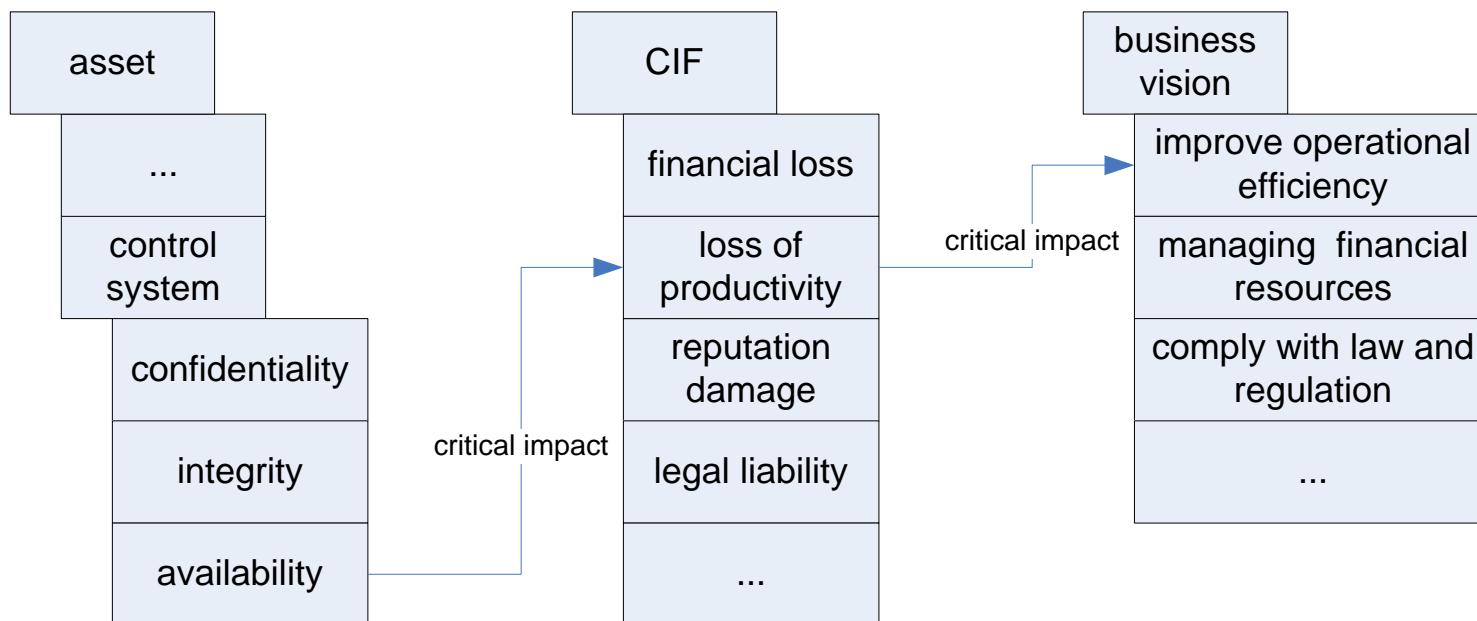


An example



Prioritizing security requirements

- Link asset security requirement with business vision via CIFs.
- Using the impact diagram, it is possible to categorize and prioritize the different security requirements.



Why we use CIFs to link critical assets and their security requirements with business goals?

- Business goals typically reside at strategic level
- The Critical Impact Factors on the other hand, reflect the business implication when security is compromised
- The introduction of CIFs makes the shift of focus smooth and the line of reasoning easier to follow



Related research

- Security standards
- i^* with security
- Misuse and abuse cases
- Attack trees
- Risk analysis methods

Conclusion

- Information security is about business security
- Make explicit the tie between security requirements and the organization's business drivers
- The connection once established can be used to provide rationale for prioritizing security requirements
- Using case studies to further develop and validate the framework



Thanks you for your attention

Comments...