INFORMATION SECURITY FUNDAMENTALS

Graphical Conceptualisations for Understanding

Per Oscarson

Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden

Abstract: This paper deals with some fundamental concepts within the area of information security, both their definitions and their relationships. The included concepts are information asset, confidentiality, integrity, availability, threat, incident, damage, security mechanism, vulnerability and risk. The concepts and their relations are modeled graphically in order to increase the understanding of conceptual fundamentals within the area of information security.

Key words: Information security, security concepts, information asset, threat, incident, damage, security mechanism, risk

1. INTRODUCTION

As a university lecturer and researcher in the topic of information security, I have identified a lack of material that supplies conceptual fundamentals as a whole. Authors often stipulate definitions without any discussion regarding their semantic meaning, and I claim that the relationships between these concepts seldom are explicit discussed or defined. An increased understanding of relationships between concepts may lead to an increased understanding of the concepts themselves, and inversely. Hence, I argue that these two types of understanding may contribute to a conceptual understanding as a whole. The aim of this paper is to increase the understanding of information security fundamentals. This is done by graphical representations of the concepts mentioned above and their relationships.

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

This paper is based on a licentiate thesis (Oscarson, 2001) that was built upon theoretical as well as empirical studies. However, the conceptual work has been continued during the year 2002, and the fundamental concepts and their relationships have therefore been further developed. One important part of this work is interaction with students; the graphs have been used when tutoring students' final theses in bachelor and master programs. The experiences of that work are good, even if no systematic empirical research has been done. During the spring 2003, the graphical conceptualisations are used in a basic distance course in information security. An evaluation of the usefulness of the graphs in that course is currently under design.

2. INFORMATION ASSETS

The foundation for security is assets that need to be protected (see e.g. Gollman, 1999). Assets may be people, things created by people or parts of nature. In the area of information security, the assets are often labelled as information assets, and enclose not only the information itself but also resources that are in use to facilitate the management of information (e.g. Björck, 2001; ISO/IEC 17799, 2001), as depicted in Figure 1.

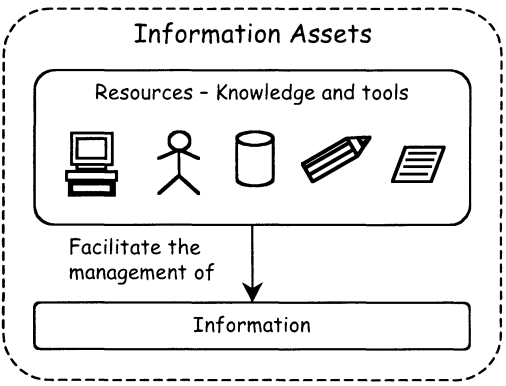

Figure 1. Information assets consist of information as well as resources to facilitate the management of information

I claim that it is the information that is the primary asset, and IT and other resources are tools to facilitate information management. Resources have hence an instrumental value in relation to the information (of course, information may be highly integrated with resources that manage the information, e.g. in a database). The term information security expresses therefore a more holistic view than IT-security, which manifests a more

technical view since technical resources are focused (Oscarson, 2001). As it will be seen in Figure 2, I define IT as *digital* tools for managing information. A more exhaustive definition of IT is (translated from Oscarson, 2001, p 56):

> Information technology (IT) is a concept that refers to digital technology, i.e. hard- and software for creating, collecting, processing, storing, transmitting, presenting and duplicating information. The information may be in the shape of e.g. sound, text, image or video, and IT mean hence a merging of the traditional areas of computers, telecom and media.

IT artefacts in the shape of e.g. personal computers, networks, operative systems and applications constitute thus one of several types of supporting resources for manage information. It is not only IT artefacts to be counted as resources when managing information. Information may be managed manually, which make humans an important resource. People are also indirectly an important resource because that is always people that handle tools that manage information. Tools that help humans to manage information may be electronic or non-electronic. Moreover, electronic tools may be divided into digital and analogue tools. Figure 2 shows a simple classification of information-managing resources.

Non-electronic tools may be for example pens, papers, staplers and notice boards while analogue tools are for example over-head devices, paper-shredders and telephones (which also can be digital). Security mechanisms (safeguards) may also be counted as resources for managing information. Security mechanisms may belong to all of the categories illustrated in Figure 2 (more about security mechanisms in section 4).

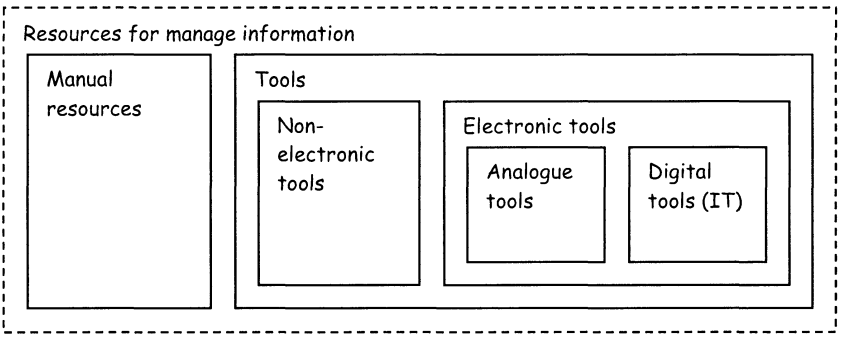

Figure 2. A classification of resources for information management

Information as an asset in organizations is a wide domain of knowledge, and is not only about information (represented by data) stored in IT-based information systems. A great amount of an organization's information is non-formalized and is not digitalized or even on print. Information that seems to be unimportant for one organization may be important to other actors, e.g. competitors. Some information, e.g. negative publicity, may arise at the same moment when an incident occurs. For example, the information that an information system has been hacked may become very sensitive information at the same moment the incident occurs. Moreover, information as an asset is not only about information that exists in an organization – it is also important that an organization can obtain relevant and reliable information when necessary.

2.1 Confidentially, Integrity and Availability

Security concerning IT and information is normally defined by three aspects, or goals; confidentiality, integrity and availability (see e.g. Gollman, 1999; Harris, 2002; Jonsson, 1995). The concepts can be seen as the *objectives* with security regarding IT and information and are often referred to as the 'CIA triad' (Harris, 2002). Definitions of the CIA triad may differ depending on what kind of assets that are focused, e.g. a specific computer/IT system, information system or information assets as defined above. Regarding information assets, the three concepts can be defined as follows:

- Confidentiality: Prevention of unauthorized disclosure or use of information assets
- Integrity: Prevention of unauthorized modification of information assets
- Availability: Ensuring of authorized access of information assets when required

The definitions are influenced by Gollman (1999) and Harris (2002), but are revised in the following way: Gollman and Harris use 'information' and/or 'systems' for the three concepts, while I claim that all three concepts should concern both information and resources for managing information, i.e. information assets. The objective is that both information and resources will stay confidential, unmodified and available. For example, weaknesses in confidentiality may be caused both by disclosure of sensitive information *and* by unauthorized use of a computer system. Integrity can be seen as a quality characteristic of information assets, while confidentiality and availability are characteristics of the relations between information assets and an authorized user (availability) and an unauthorized user (confidentiality), as depicted in Figure 3.

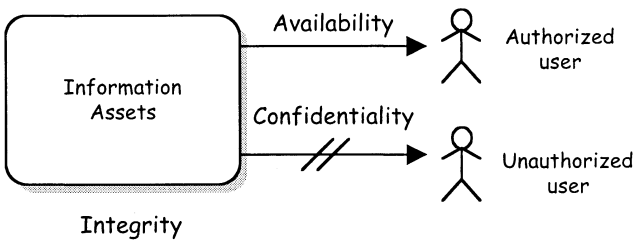

Figure 3. A graphical description of the CIA triad – Confidentiality, Integrity and Availability (influenced by Jonsson, 1995; Olovsson, 1992)

For simplifying reasons, the CIA triad will henceforth in the paper be treated as characteristics of information assets, even if correct definitions in two cases are characteristics between information assets and users (which may be authorized or unauthorized).

2.2 Threats against Information Assets

Information assets may be exposed for threats. There are a number of definitions of threat in the field of computers, IT and information. Here are a few examples:

'...an indication that an undesirable event may occur' (Parker, 1981),

'...any potential danger to information or systems' (Harris, 2002),

'...circumstances that have the potential to cause loss or harm' (Pfleeger, 1996).

If the objective of information security is to reach and maintain the CIA triad of information assets at a required level, threat is something that potentially can impair the CIA triad in the future. Parker (1981) mentions 'undesirable events' above (which I label as incident, see next section below), which I interpret as if confidentiality, integrity or availability will be impaired. That means that a threat consists of a potential action or occurrence that may affect the information asset's CIA triad negatively. Actions and occurrences do not happen by themselves, there must be causes lying behind. Harris (2002) calls such underlying causes for threat agents, and it may be actors (humans or organizations), by human made artefacts or natural phenomena (cf. e.g. Pfleeger, 1996). In my definition of threat I hence include both actions/occurrences and underlying causes:

> Threats are potential undesirable actions or occurrences, that performs or causes by actors, by human created artifacts or natural phenomena and which are supposed to impair the CIA triad of current information assets.

Using the definitions discussed so far, we can define the relations between threat agent, threat, the CIA triad and information asset as well (see Figure 4).

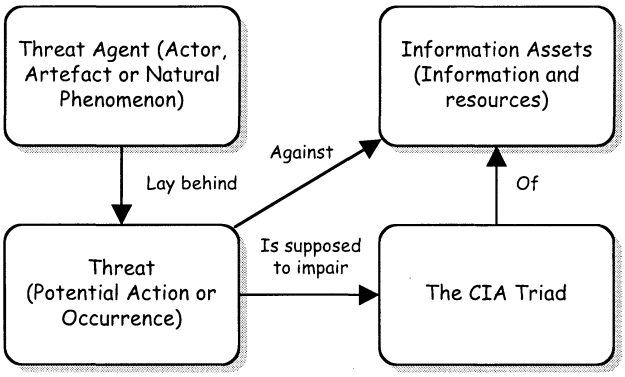

Figure 4. The relations between threat agent, threat, the CIA triad and information assets

Human threat agents may be intentional or accidental (see e.g. Harris, 2002). Terrorism, information warfare, sabotages and intrusions are examples of intentional threats, while carelessness, mistakes and ignorance are unintentional threats. Non-human threats, i.e. artefacts and natural phenomena, may be floods, fires, earthquakes and thunderstorms. Artefacts may function in undesirable ways, and since humans create artefacts, threats often have a combination of underlying threat agents. That is, humans may construct, implement, configure or handle artefacts in inappropriate or destructive ways, for example people who creates destructive IT-artefacts as viruses and worms.

Physical threats are threats that appear in a physical manner, like floods, thefts and fires. Non-physical threats, or logical threats, are often connected to software as viruses, computer intrusion and user's software mistakes. Such threats will mostly affect non-physical assets, but may affect physical assets as well.

Sometimes there are reasons to expect that actors, artefacts or natural phenomena that are not yet existing, or not for the moment performing actions or causing occurrences may do so in the future. They can be apprehended as potential threats.

3. INCIDENTS AND DAMAGES

While a threat is an assumption that an undesirable event may occur in a future, the term *incident* refers to the actual occurrence of such event. In other words, a threat may be realized as one or several incidents. A threat may still exist after a realization, since underlying causes still may have capabilities to realize the threat several times. The probability for realization will however often decrease since people often increase the protection against realized threats. Like threats, an occurred incident may be unknown. Such incidents may be discovered after a while or remain unknown. Incidents that are realized by unknown threats are unexpected incidents.

Incidents may lead to consequences. If a consequence affects the CIA triad of information assets uncontrolled and negatively, it is labelled as *damage*. There may be incidents that not impair the CIA triad, for example a virus that infects an information system without causing any damage. The infection is still an undesired event that probably happens out of the control of the system managers.

Figure 5 shows the relationships between threat agent, threat, information asset, the CIA triad, incident and damage (the definitions of threat and assets have been removed from the illustration to make the graph more simple).

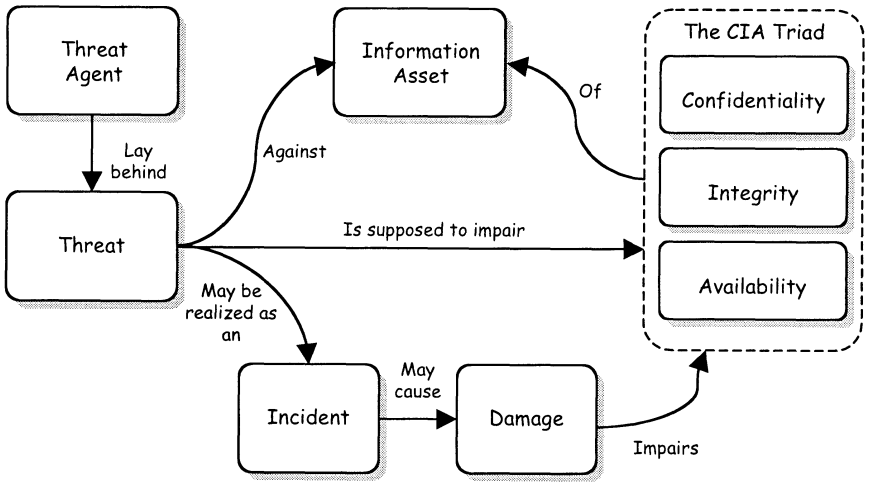

Figure 5. The concepts incident and damage are added to the growing graph

A definition of damage may be extracted from the objectives of information security:

Damages are uncontrolled impairs of the CIA triad of information assets.

Practically, there may be many kinds of damages. Information can be changed in an uncontrolled and undesirable way, information may disappear or be read by unauthorized persons and information and IT artefacts may be unavailable for authorized persons.

4. SECURITY MECHANISMS

Security mechanisms are something that will improve the CIA triad of information assets, i.e. increase the information security (Oscarson, 2001). The terms protections, countermeasures, controls and safeguards may be used as synonyms to security mechanisms. Security mechanisms can be categorized in several ways. Bases for categorizations may be for example their relation to the CIA triad (Jonsson, 1995; Oscarson, 2001) or what they consists of – e.g. hardware, software and policies – (e.g. Pfleeger, 1996). One way is to categorize them based on their functionality in relation to the time of an incident; security mechanisms can be preventing, averting or recovering (SIG Security, 1999). Preventing security mechanisms are highly directed to the threat; to affect threat agents in purpose to reduce the danger of a threat, or the probability that a threat will be realized to incidents. Examples of preventing security mechanisms are security awareness and laws. Averting security mechanisms intend to obstruct incidents, e.g. in the shape of firewalls or encryption programs. Recovering (or restoring) security mechanisms recover already damaged information assets. An example of a security mechanism is anti-virus software that repairs infected files.

In accordance to the four objects threat, incident, damage and the CIA triad, there is one link missing in the chain. There are security mechanisms that reduce damages, as for example fire extinguisher, that either avert incidents nor recover an already damaged information asset; such security mechanisms are *damage reducing*. Summing up, a categorization of security based on time of an incident consists of four categories: preventing, averting, damage reducing and recovering security mechanisms (see Figure 6).

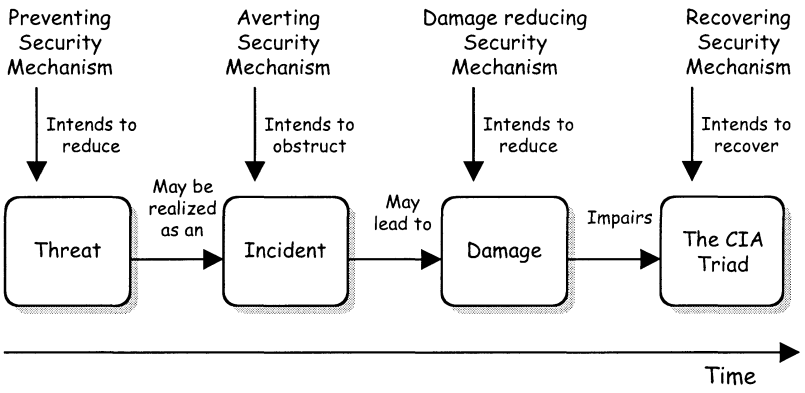

Figure 6. Four categories of security mechanisms based on their relation in time to incidents

Two other categories that closely fit in to this categorization are detective (e.g. Gollman, 1999; Olovsson, 1992) and reporting security mechanisms (Statskontoret, 1997). The reason why they do not can be used in this type of categorization is that they may be used in any time in relation to an incident; before, during or after the realization of a threat. Detecting security mechanisms may be used for discovering/reporting new kinds of threats, detecting/reporting intrusions or intrusion attempts, as well as detecting/reporting already damaged information assets. Detective security mechanisms are almost always also reporting; when some threat, incident or damage has been detected, it may also be reported. That means that preventing, averting or recovering security mechanisms may be detecting and/or reporting as well. Additionally, it is important to understand that specific security *products* may have several functionalities, i.e. preventing, averting, damage reducing, recovering, detecting and reporting.

The four categories of security mechanisms that are presented in this section can be connected to the growing conceptual graph and is shown in Figure 7; preventing security mechanisms may affect threat agents, averting security mechanisms may obstruct incidents, and damage reducing mechanisms may reduce damages. Finally, recovering security mechanisms may completely or partially restore impaired confidentiality, integrity or availability of information assets.

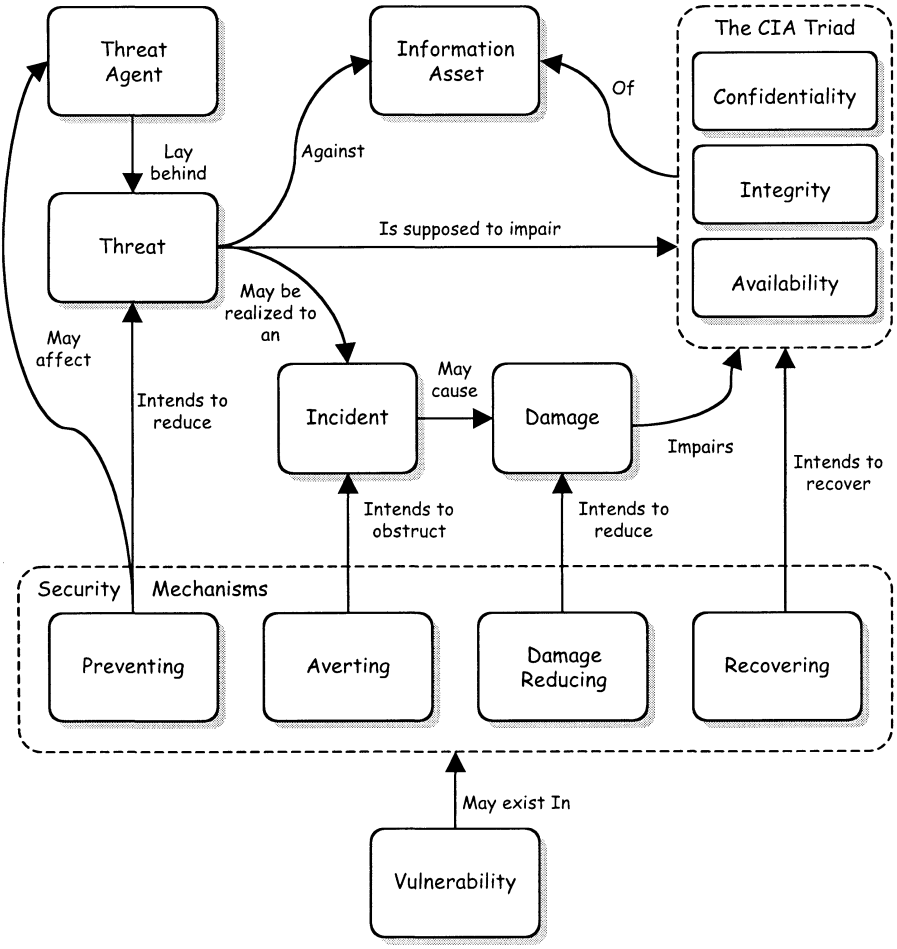

Figure 7. A graphical representation of fundamental concepts and their relationships

4.1 Vulnerability

Vulnerability is absence of security mechanisms, or weaknesses in existing security mechanisms (see e.g. Harris, 2002; Ozier, 2000). Vulnerability may exist in all of the categories of security mechanisms that are mentioned in the previous section (see Figure 7), and may be known or unknown.

5. RISK

Risk is another fundamental concept in the area of security. However, the risk concept is difficult to range in the graph presented above, since risk is a concept that concerns assessed future conditions; some of the objects in the graph are changing when it comes to risk assessment, e.g. 'potential damage' instead of 'damage'. Moreover, the graph tends to be too complex if it includes a large number of concepts and relations. This section presents hence another conceptual graph concerning risk assessment.

Risk is someone's estimation concerning the occurrences of incidents and potential damages caused by incidents (e.g. Parker, 1981 and Ozier, 2000). Consequently, the concept of risk consists of two parts; the *probability* or the *expected frequency* of that an incident will occur and the *potential damages* an incident may cause. This can be expressed in the following equation:

$$R = L * P$$

R stands for risk, L is potential loss, and P is probability or expected frequency of loss (Parker, 1981). Even if an incident leads to a serious damage, there is no risk if the probability or expected frequency is zero, and reverse. This means that R = 0 require L = 0 and/or P = 0. In accordance to the discussion about damages above, the terms damages and loss are used synonymously. In the standard ISO/IEC 17799 (2001, p 8), risk (assessment) is defined in a similar way, i.e. it consists of the likelihood of an incident as well as the potential negative consequences.

The risk concept including probability, expected frequency and potential damage may be connected graphically to threat, incident, information asset and the CIA triad (see Figure 8). As shown in Figure 8, the risk concept is closely related to threats, incidents and the CIA triad of information assets. That means that risk assessment must deal with estimation of those phenomena. However, the risk concept is not connected to security mechanisms and vulnerabilities in this graph. As discussed previously in this paper, security mechanisms may intend to affect threat agents, reduce threats, obstruct incident, reduce damages or recover impairs of the CIA triad of information assets. This means that security mechanisms may decrease risks by decreasing the probability or the expected frequency of the occurrences of incidents, or by decreasing damages of occurred incidents. Vulnerabilities in security mechanisms will increase risks.

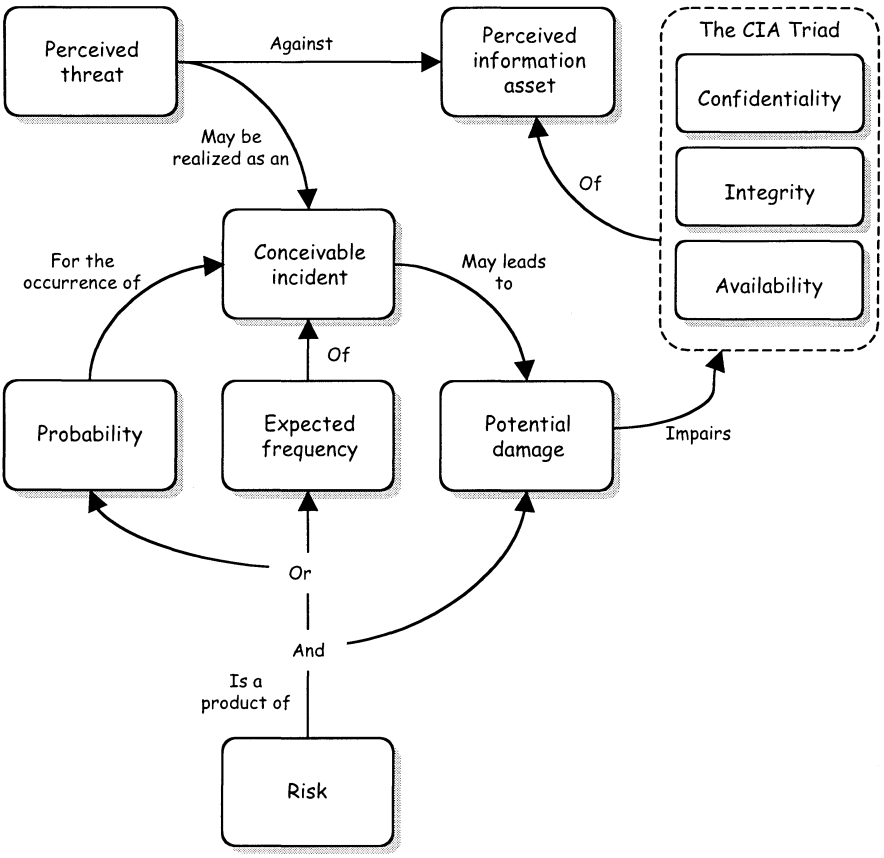

Figure 8. The risk concept in relation to threat, incident, the CIA triad and information assets

6. SUMMARY

This paper has introduced some graphical conceptualisations of fundamental concepts within the information security area. Conceptual modelling is based upon linguistic and philosophical perceptions and standpoints, and is hence heavily dependent on underlying perspectives. That means that linguistic definitions of concepts, or relations between concepts, never can be regarded as a "universal truth", but may represent a way to study a phenomenon or an area. With that in mind, the graphs may be useful in future research as well as for educational purposes. As mentioned in the introduction section, an empirical study in form of a course evaluation is planned. Such study may work as a further grounding, and/or a refining of the graphs presented in this paper.

Even if my own perspective is business oriented, I believe this conceptual work is quite generic in the sense that it may be valid even for more technical areas of security, and therefore may be useful in more technical oriented education. However, I believe that the business-oriented perspective has some impact on the result, especially the concept of information asset. In more technical oriented perspectives, assets often consist of data and system rather than information and resources for information management (cf. e.g. Jonsson, 1995). My intention is to continue this work in purpose to create a framework regarding actual and perceived information security. This work will among other things include modelling of concepts in different conditions of time and if they are referring to actual conditions or subjective perceptions. For this work, this paper may serve as one part of a conceptual base.

REFERENCES

Björck F (2001). Security Scandinavian Style – Interpreting the Practice of Managing Information Security in Organisations. Licentiate Thesis, Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, Stockholm

Gollman D (1999). Computer Security. Wiley

Harris S (2002). CISSP Certification Exam Guide. McGraw-Hill/Osbourne,

Jonsson E (1995). A Quantitative Approach to Computer Security from a Dependability Perspective. Doctoral Dissertation, Department of Computer Engineering, Chalmers University of Technology, Göteborg

Olovsson T (1992). A Structured Approach to Computer Security. Technical Report No 122, Department of Computer Engineering, Chalmers University of Technology, Göteborg

Oscarson P (2001). Informationssäkerhet i verksamheter. (Information Security in Organizations – in Swedish). Licentiate Thesis, Department of Computer and Information Science, Linköping University

Ozier W (2000) Risk Analysis and Assessment, in Information Security Handbook, Tipton H F & Krause M, Auerbach publications

Parker D B (1981). Computer Security Management, Prentice Hall

Pfleeger C P (1996). Security in Computing. Prentice-Hall,

SIG Security (1999). Säkerhetsarkitekturer (Security Architectures, in Swedish). SIG Security, Studentlitteratur

ISO/IEC 17799 (2001). Information Technology – Code of Practice for Information Security Management. International Organization for Standardization

Statskontoret (1997). Handbok i IT-säkerhet (IT Security Handbook, in Swedish), The Swedish Agency for Public Management