

# MEASUREMENT OF INFORMATION SECURITY IN PROCESSES AND PRODUCTS

Reijo Savola<sup>1</sup>, Juhani Anttila<sup>2</sup>, Anni Sademies<sup>1</sup>, Jorma Kajava<sup>3</sup> and Jarkko Holappa<sup>1</sup>

<sup>1</sup>VTT Technical Research Centre of Finland, Oulu, Finland; <sup>2</sup>Quality Integration, Helsinki, Finland; <sup>3</sup>University of Oulu, Oulu, Finland

**Abstract:** In order to better understand the information security performance in products, processes, technical systems or organizations as a whole, and to plan, control, and improve it, security engineers, system developers and business managers must be able to get early feedback information from the achieved security situation. Systematic security metrics provides the means for managing security-related measurements comprehensively. We reflect on the use of information security metrics by presenting the results of an interview study carried out in Finnish industrial companies and State institutions. Furthermore, we discuss the application of security measurements from the business process and technical points of view. The role of technical security metrics is analyzed using mobile ad hoc networks as a case example.

**Key words:** security metrics; information security process; performance; security measurement; mobile ad hoc networks

## 1. INTRODUCTION

In today's information technology world, there is a growing need for information security (IS) solutions: information systems are more and more vulnerable because of the increased complexity. At the same time, information security demands increase due to emerging applications such as e-commerce and ubiquitous computing.

Despite advances in the field, the state-of-the-art solutions still lack clear and widely accepted mechanisms to manage information security in products and in organizations producing them. A major problem is that it is not easy

to see the actual performance of the security achieved. In many cases, information security specialists in industry only get feedback from the market. There are no established practices for measuring information security performance for organizations' management purposes.

It is a widely accepted principle that an activity cannot be managed rationally if it cannot be measured. Information security metrics are needed to offer a means of assessing the security performance for business managers, information security specialists and system developers. Information security management has little value without measurements of the business processes and products produced.

The wide majority of the available security metrics approaches have been developed for evaluating the maturity of security engineering processes. Of these, the maturity model most widely used with some security metrics is the Systems Security Engineering Capability Maturity Model SSE-CMM ISO/IEC Standard 21827 (2002). Another well-known model, Trusted Computer Security Evaluation Criteria TCSEC, "The Orange Book" (1985), expresses the security engineering process using classes and divisions as evaluation levels. In the field of software engineering, practical measurement processes have already been standardized – for example – in ISO/IEC 15939 Software Engineering – Software Measurement Process (2002). The security metrics group in SSE-CMM model development is working towards standardization of the measurement processes within the scope of information security management.

According to Henning (2001), a security metrics model consists of three components: the *object* being measured, the *security objectives* (i.e. the "measuring rod" the object is being measured against, and the *method* of measurement. Jonsson (2003) sorts the methods of security measurement into the following topics:

- **Risk analysis** is an estimation of the probability of specific threats, and vulnerabilities, and their consequences and costs – it can be thought of as a trade-off to the corresponding costs for protection;
- **Certification** is the classification of the system in classes based on the design characteristics and security mechanisms;
- **Intrusion detection process** is a statistical measurement of a system based on the effort it takes to make an intrusion.

The main contribution of this work is an investigation of information security measurement practices in industrial and State institutions. Furthermore, the needs and possibilities of security metrics-based activities are studied from the process-thinking and technical points of view. The rest of the paper is organized in the following way: Section 2 discusses the needs for security metrics by analyzing the results of a recent interview study carried out in some Finnish industrial companies and State organizations.

Section 3 discusses information security and its measurements within business processes; Section 4 discusses technical information security metrics using mobile ad hoc networks as an illustrative example; and, finally, we present conclusions and discussion about future work.

## **2. SECURITY METRICS USED BY INDUSTRY – AN INTERVIEW STUDY**

In order to resolve how different industrial companies and organizations define and use information security metrics, it is valuable to conduct surveys and interviews. Security metrics is an area that has not been studied very much. One reason for this can be that the information can reveal vulnerabilities in the organizations; thus it is desirable to keep such information hidden.

In early 2004, we conducted eight interviews in different types of major industrial companies and State institutions in Finland, and analyzed the results using the interpretative analysis method (Sademies, 2004; Sademies and Savola, 2004). The interviews encompassed seven interview themes and a total of 20 questions. The interview themes were:

1. Background
2. Security Objectives
3. Information Security Metrics
4. Metrics Implementation
5. Basis for the Metrics
6. Risk and Quality Management
7. Need for Metrics, Background and Development

### **2.1 Background**

The interviewees mainly represented administrative personnel and product managers. Work experience and specialization areas were separating factors, but a common feature was that they were all somehow responsible for the organization's security. The interviewees were selected from organizations that have a history of co-operation with the research group, enabling a high level of trust in their answers.

### **2.2 Security Objectives**

Defining security objectives is fundamental in security management as the objectives form the basis for the selection of the security requirements

that are set in the security specifications. It is also an indication of how well security phenomena – i.e. the threats and security – are understood in the operation of the whole organization or technical system. According to the interviews, there are many types of security objectives with different points of view and qualities, even in one organization, but certain statements can describe the functioning of the whole organization. The most important security objectives for State institutions include:

- building and maintenance of customer trust,
- ensuring critical process functioning and backup of the main activities,
- ensuring congruence between the main tasks and the legislation, and
- backing up the change and keeping the policy optimized so that it is not too strict and thus adds to the user's ease of use.

Typical industrial organizations' security objectives are:

- to integrate information security work into business processes,
- to back up the business strategy, and
- to ensure product security.

According to the interviews, some reasons for using metrics are the need to raise the level of information security awareness and education, and to reduce the risk factors of human behavior and ensure availability, integrity and confidentiality.

## **2.3 Information Security Metrics**

According to our interviews, information security metrics is usually understood as evaluation (auditing, vulnerability analysis, penetration testing) or as observation of system performance, mainly presented by technical means such as logs and firewalls. Also, it can mean measuring how the employees perform their work tasks.

We asked the interviewees what security objectives cause the need for security metrics in their organizations. The objectives are as diverse as the organizations, from raising personnel awareness about security matters to enabling business activities.

## **2.4 Metrics Implementation**

A significant problem in metrics implementation is *the absence of relationship with processes*. There are a variety of different measurement technologies or methods applied, but they cannot be considered as useful as if they were applied in connection to with business processes.

The most hindering factors seem to be the lack of readiness or ignorance on the part of the top-level management to commit to information security issues, as well as an absence of documentation caused by unclear or

inappropriate responsibilities. IS measurements should start from the organization's strategic planning. Metrics implementation strongly depends on the kind of decisions the responsible people in the organization are able to make about the information security resources and investments. Another problem, in addition to the lack of management information security awareness, is that some managers that do not understand the significance of information security force the IS managers to take all the responsibility. This leads to a situation where top-level management does not commit to the decisions and there is a lack of strategic leadership concerning information security.

Technical metrics are used in all organizations and their implementation is more advanced than any other metrics. The technical means used are mainly PC and network monitoring, incident counting, auditing and risk management. The majority of the organizations use reactive rather than proactive methods.

## **2.5 Basis for Metrics**

The need for security metrics is brought up in standards. Standards are used as guidance and applied according to an organization's own needs. The most common standards are the ISO/IEC 17799 (2001) or BS 7799 Code of Practice (BS 7799, 2002), VAHTI – Information Security Management Guidelines by the Finnish Government Information Security Management Board (Ministry of Finance of Finland, 2004). In addition, there is general related legislation.

## **2.6 Risk and Quality Management**

Risk analysis is one type of security metrics application. In the interviewed organizations, risk assessment is mainly applied so that it is adjusted to the organization's own processes and purposes. The risks associated with the metrics themselves are, however, usually not well handled.

A progressive information security management is considered to be one domain of quality management. Some organizations explicitly recognize information security as a quality factor in itself, and aim to make the information security management a part of their process management.

Information security as a quality factor refers particularly to product quality in business because it is based on the customer requirements. In State institutions information security in the quality context mainly represents issues concerning personnel behavior and responsibilities. Audits are considered a practical methodology for assessing quality management.

## **2.7 Needs for Metrics, Background and Development**

The interviews demonstrated that a need for the security metrics is that they naturally make it easier to analyze fault situations, and this requires systematic data collection and analysis. The metrics are found most useful when predicting or trying to understand future situations – i.e. when using metrics proactively. Often, there is too much information, making it difficult to find the *relevant data*. Data classification and rationalization is important in order to obtain better results, but it also helps to justify the need for effective information security methods. There is also a need for experience from history data collection and analysis, otherwise the situation usually remains purely reactive.

Security policies are sometimes difficult to keep up to date, and the situation very much depends on the personnel's information security skills and management's commitment. The documentation and structure of the security policies are not seen to be as significant as adjusting them to the organization's working culture.

The metrics are useful, not only for getting feedback on the information security level in the organization and products but also for proving it to the partners.

A standard objectively defining the information security performance would be useful. However, it is recognized that such a standard may be impossible to define so as to be applicable to every application field or case.

The most significant and challenging aspects in information security and measurement of information security are, without a doubt, the human factors. There is a need for education and maintenance of continuous awareness. The tool for that is developing the information security process with relevant policies and procedures.

Information security strategy can be difficult to define, and there are many factors that can rapidly cause changes in its direction. The situation will get more complicated as the technical systems become more complex, the threats more diverse and the attackers more skillful. It would be beneficial if the organization could adjust to changing situations by detecting its current state and studying its history, thus making predictions for the future.

Security requirements come from customers and legislation. This increases the value of the skill of being able to resolve customer needs as accurately as possible as well as being on top of legislation and market changes.

Fig. 1 describes some needs for IS metrics that were emphasized by the target organizations. The interviewees thought that those types of metrics would be relevant for the organizations to improve their functioning and

security management. The metrics classification is according to Henning (2001), with certain modifications.

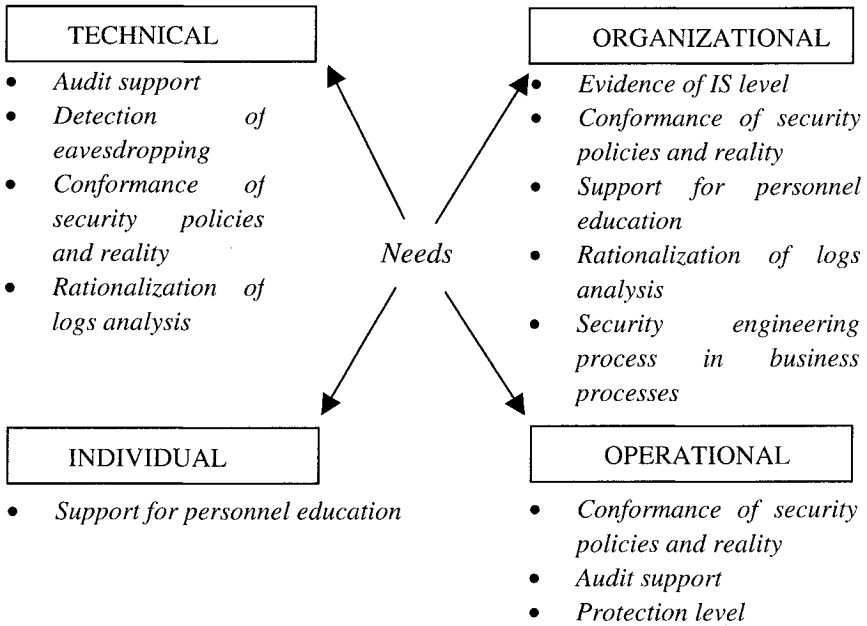


Figure 1. Some needs that are connected to security metrics according to the interviews

### 3. INTEGRATION OF INFORMATION SECURITY MANAGEMENT INTO BUSINESS MANAGEMENT SYSTEMS – A PROCESS VIEW OF SECURITY METRICS

The implementation of information security and its performance measurement forms an integral part of all business activities, and management activities in particular, both on the strategic and operational management level. Thus we may speak of integrated information security management.

As our interview study shows, security metrics are most efficient when they are used within business processes. In industrial companies and other organizations, business processes are just for carrying out the actual everyday business. The performance measurement process should be integrated into these natural organizational disciplines.

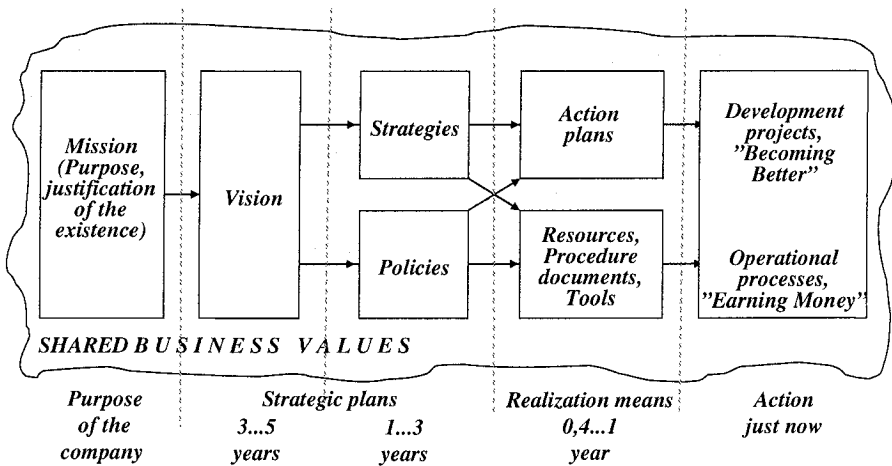


Figure 2. Elements of the business management system form the basis for integrating information security management. Each company must develop its own management practices incorporating the necessary skills for security solutions. Information security measurement and management should be embedded within this management system.

To achieve its aims, information security requires a professional approach and close co-operation between security experts and business executives. A company with superior information security knowledge has a great advantage over the competition, a lead that is difficult to close.

Neither technological solutions nor software-based security measures are sufficient as such. Even in principle, it is hardly likely that information security could be accomplished by means of separate information security systems; in fact, these might cause more harm than benefit. Business management systems (see Fig. 2) have no room for such systems; all business activities must be flavoured with professional information security measures.

According to the recognized international references (BS 7799, 2002; ISO/IEC 17799, 2000), information security comprises a variety of management-related issues, including:

- Security policy,
- Security organization,
- Asset classification and controls,
- Personal security,
- Physical and environmental security,
- Computer and network management,
- System access control,
- System development and maintenance,

- Business continuity planning,
- Compliance management,
- Data and information security, and
- Privacy protection.

Operationally, information security originates from process-related activities and information flows between these activities. Thus information security is affected directly in real time through process arrangements, tools and people which, in turn, are influenced by appropriate and systematic process management practices. As a consequence information security measurements should also be realized as a process management activity.

In today's world, E-Business is an existing reality and offers increasing opportunities to organizations in all sectors. It is important to realize that Internet-based E-Business is not merely a technological issue. The Internet provides a rapidly expanding worldwide communication infrastructure that covers all aspects of life. The net includes all people, organizations, cultures and communities, and it has already changed conditions for interaction as well as behaviors. E-Business is no longer concerned only with explicit data and information possessed by organizations but extends to *tacit knowledge*, which people rely on in communication. It follows that information security should also be adapted to these new business realities. And that is not the end of it – E-Business also creates new opportunities both for business management and operations and - consequently - for information security.

All these issues relate very strongly to the decisions and actions of the top management (the strategic viewpoint) and to the practices used in the management of business process (the operational viewpoint). In integrating information security practices and management, it is extremely important to understand information security issues within the context of business processes. This is because, in practice, information security is a cross-functional discipline, which requires close cooperation and multifarious expertise. Quality management has an established position in many organizations, along with an internationally recognized standardization basis. It has given rise to numerous practical principles and methodologies that are also useful in the field of information security (ISO 9000, 2000). Information security management is fully analogous to the management of many other areas of expertise important to a company. These include, for example:

- Finance,
- Quality,
- Business risks,
- Human resource development,
- Information management and communications,
- Occupational health and safety factors, and

- Environmental protection.

#### 4. A TECHNICAL VIEW OF SECURITY METRICS

In the following we investigate security metrics from a technical system's perspective. A number of technical information security solutions – like Intrusion Detection Systems (IDS), firewalls, anti-virus software – use security metrics internally and as a basis for their reports.

Technical security metrics can be used to describe the security performance of technical objects. This includes algorithms, specifications, architectures and alternative designs, products, and as-implemented systems at different stages of the system lifecycle.

Using product-oriented technical security metrics, both *design vulnerabilities* and *implementation vulnerabilities* can be sought (Savola and Holappa, 2005). Design vulnerabilities can result from an insecure design, whereas implementation vulnerabilities are connected to poor implementation of a product. Thus the former term typically refers to lower technology maturity, see Fig. 3.

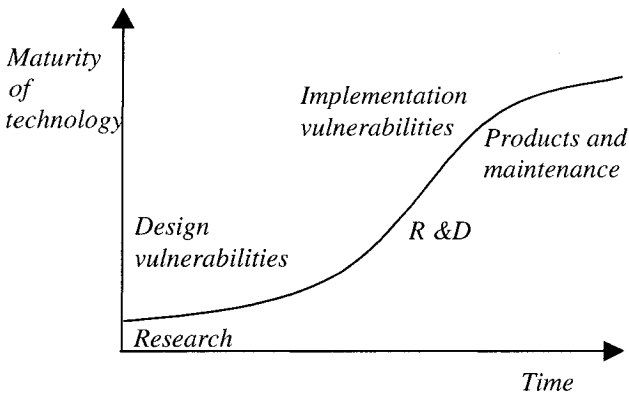


Figure 3. Design and implementation vulnerabilities

Traditionally, industrial-strength technical security metrics solutions mostly rely on the “*penetrate and patch*” or “*tiger team penetration*” approach. The technical systems are security tested by applying common security attacks and determining if such attacks are successful. If an attack results in an intrusion, an appropriate patch for the software is developed and applied to the system. Tiger teams often use dissimilar approaches, and their capabilities and experience vary a great deal. An essential problem is that the

manual process of tiger team penetration testing easily results in statistically non-reproducible data.

Technical security metrics can be applied in many ways, including:

- **Goal establishment:** to establish goals and measure how well the object achieves those goals;
- **Prediction:** to predict security performance before implementation or in an implemented system, to predict possible intrusion using an Intrusion Prevention System (IPS);
- **Comparison:** to compare the security performance of objects;
- **Monitoring:** to monitor or scan the security performance of an object (e.g. Intrusion Detection System IDS); and
- **Fault analysis:** in the case of fault injection methods, metrics enable analysis.

The metrics are found most useful when they can be used *proactively* – predicting or trying to understand future situations. Security metrics can be used both for quantitative and qualitative analysis methods. Furthermore, metrics are more useful when they are meaningful for most of the object's lifecycle:

- **During research and development,** security metrics help researchers to develop more secure solutions and to find design vulnerabilities. Global-level security metrics are the most valuable metrics since they give the strongest feedback on security component solutions. Research-oriented security metrics can be constructed using analytical models that take account of factors contributing to security and the cross-relationships of components. Research-oriented metrics can concentrate on the critical parts, especially the technical challenges (e.g. routing and trust management in mobile ad hoc networks).
- **During system implementation,** technical security metrics can be used to find design and implementation vulnerabilities as a part of security engineering. These are also based on analytical models. If metrics are part of a security engineering process, they are more valuable.
- **During the system (product) maintenance phase,** technical security metrics can be used for preservation of the achieved security level during possible updates, integration or modifications, and to find implementation vulnerabilities. From the point of view of the security engineering process, a technical system can be constantly in the system maintenance phase. In addition to preservation of the security level, this level can be improved using feedback obtained from the application of security metrics.

#### 4.1 Case: Security Metrics for Mobile Ad Hoc Networks

Mobile ad hoc networks – or MANETs – (IETF) have great potential for broad use in making ubiquitous computing possible and successful, enabling self-organization and dynamic operation. Applications vary from mobile entertainment to e-payments and all kinds of business services, often with high security demands. The ultimate goal of the security solutions for MANETs is to provide services for the desired security needs, mainly confidentiality, integrity, availability, authentication and non-repudiation, at the desired security level.

*Table 1. Some component security metric areas for mobile ad hoc networks*

Component metrics area	Sub-component metrics area
Trust and key management	Initial trust
	Operational trust
Routing	Routing information
Mobility	Identity information
	Packet forwarding information
Human factors	Usability
	Performance
	Security awareness of users
	Resistance to social engineering
	Freedom of application use
Cryptographic algorithms	Cryptographic strength
Wireless-ness	Listening
	Interference
	Scale of size
Scale	Scale of use
	Tamper resistance of hardware
Physical protection	Tamper resistance of software
	Location of node
	Functionality
Product quality	Reliability
	Usability
	Efficiency
	Maintainability
	Portability
Other factors	Privacy
	Legislation
	Commercial
	Cultural
	<i>Force majeure scenarios</i>

As an example, Table 1 lists some component security metrics areas (Savola and Holappa, 2005), a composition of which forms the basis for estimation of the overall security level in mobile ad hoc networks. The most

critical component metrics emphasize *trusted information distribution* in a mobile ad hoc network. Trusted information includes key, routing, mobile entity identity and packet forwarding information. Technical challenges, such as the trusted information distribution, dominate the overall security level in the first stages of the technical evolution of MANETS. As the technology matures, aspects such as product quality become more emphasized. Please note that the framework presented in Table 1 does not offer an unambiguous view of the overall security assessment of mobile ad hoc networks since we do not know *a priori* the compositional hierarchy of causalities in such a concept as security.

Suitable mechanisms for information gathering from different classes of component security metrics are needed. This is a challenging task and requires a rigorous analysis of the metrics to be used.

## 4.2 Network Monitoring

Technical security metrics can also be used as a basis for security performance monitoring or scanning. In future security solutions, it might be possible to monitor the *security performance profile* of a network. Different networks operating at different security levels can be interconnected using more rigorous security protocols than networks operating at the same security levels.

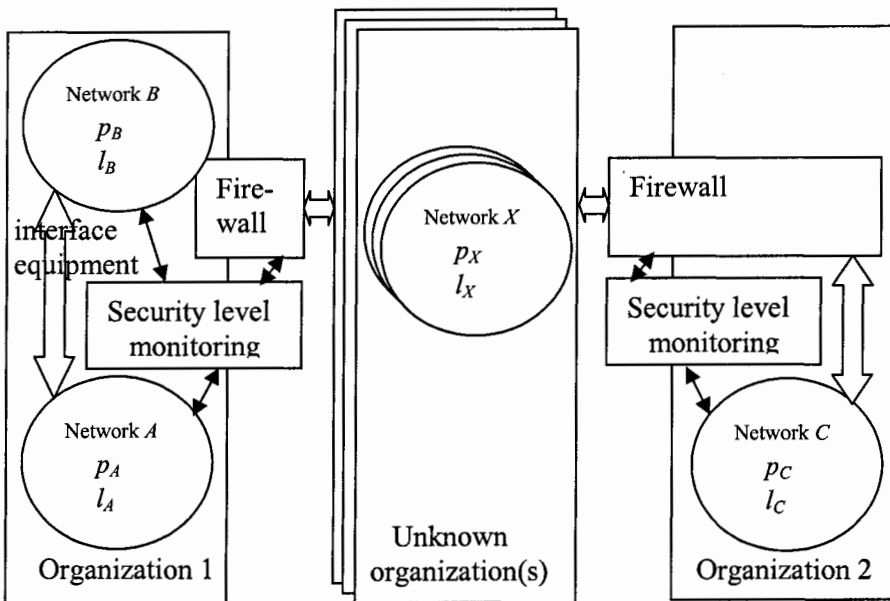


Figure 4. Security level monitoring used to support seamless interconnection of networks

Fig. 4 depicts an example of how security measurement could be arranged when connecting different networks together. Networks may have different security policies and different security levels, and they may be located in various organizations. While having different policies ( $p_A$  and  $p_B$ ) within organization  $O_1$ , the networks security policy must be a subset of both organizations' policies – i.e. all policies must comply with those defined at the organization level:

$$p_1 = (p_A, p_B) \quad (1)$$

The organization's network security level is determined by the network that has the lowest security level:

$$l_1 = l_A \wedge l_B \quad (2)$$

Administrative and organizational boundaries are usually protected with firewalls. This is to protect the organization's assets from threats that come from e.g. the public Internet without clearly defined security policies. A firewall is often combined with an intrusion detection function, which is one example of a technical security measurement tool.

## 5. CONCLUSIONS

Information security demands are growing due to the higher interconnection of networks and systems between individuals and organizations. The security performance of products, processes, technical systems, or a whole organization, can be managed if it is possible to measure it in a purposeful way, offering fast feedback to the organization's management. If the research community is able to develop intelligent and feasible mechanisms for the measurement and information gathering, in effective co-operation with the organization's responsible leaders, we might even learn more about the nature of security. In today's information technology world there is a lot of knowledge that has to be combined in a suitable way to assess the overall security performance – i.e. “find the forest from the trees.” The current limited knowledge of the nature of security is hindering us from finding rigorous solutions to the aspects of overall security. Information security experts may also learn a lot from other areas of expertise, including general metrology science and quality management, as well as from the recognized measuring practices of business management.

The practice of measuring information security in Finnish industrial companies and in State institutions has not been well studied prior to this study. This study clearly demonstrates the unrefined state of the practical information security measurement practices in such organizations, the theoretical foundations of the issue, and the level of communication among experts and business people. The results of the interview study show that different organizations use different kinds of practices, and the measurements are not integrated with the business management disciplines. One reason for this is that the literature does not offer an unambiguous or consistent means of measuring information security performance. State-of-the-art approaches for security metrics do not include clear guidelines for their practical use in products, processes or organizations. Rigorous industrial-strength approaches for measuring information security components are certainly needed.

## 6. FUTURE WORK

Our intention is to develop an information security management and measurement methodology based on practices used in the field of quality management and measurement of products, processes and organizations. The quality management research community has gathered valuable knowledge and practical experience on approaches that, with suitable modifications, also have the potential to be applied in information security management.

In information security management, business processes and security policies and principles are used in combination with technological support. Together with business-integrated and process-based security metrics, technical security metrics are useful for overall measurement methodology.

Measurement of information security performance mainly serves an organization's internal business needs. Furthermore, collaborative organizations should be able to communicate with each other on the strengths and limitations of the information security management of their products and business processes.

## REFERENCES

- BS 7799-2., 2002, Information Security Management Systems – Specification with Guidance for Use. Part 2. British Standards Institution, London.
- Henning, R. (ed.), 2001, Workshop on Information Security Scoring and Ranking – Information System Security Attribute Quantification or Ordering (Commonly but Improperly Known as “Security Metrics”), Applied Computer Security Associates.
- ISO 9000. 2000, Quality Management Standards. International Standardization Organization, Geneva, Switzerland.
- ISO/IEC 15939. 2002, Software Engineering – Software Measurement Process, International Standardization Organization, Geneva, Switzerland.
- ISO/IEC 17799., 2001, Information Technology – Code of Practice for Information Security Management, International Standardization Organization, Geneva, Switzerland.
- ISO/IEC 21827., 2002, Information Technology – Systems Security Engineering -- Capability Maturity Model (SSE-CMM), International Standardization Organization, Geneva, Switzerland.
- Jonsson, E., 2003, Dependability and Security Modelling and Metrics, Lecture Slides, Chalmers University of Technology, Sweden.
- Internet Engineering Task Force (IETF) MANET Working Group;  
[www.ietf.org/html.charters/manet-charter.html](http://www.ietf.org/html.charters/manet-charter.html).

- Ministry of Finance of Finland, 2004, Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006 (The Finnish Government Information Security Development Programme 2004-2006). In Finnish, English summary available.
- Sademies, A., 2004, Process Approach to Information Security Metrics in Finnish Industry and State Institutions. VTT Publications 544, Technical Research Centre of Finland, Espoo.
- Sademies A. and Savola R., 2004, Measuring the Information Security Level – A Survey of Practice in Finland. In: 5<sup>th</sup> Annual International Systems Security Engineering Association (ISSEA) Conference, Arlington, Virginia, October 13-15. 10 p.
- Savola R. and Holappa J., 2005, Self-Measurement of the Information Security Level in a Monitoring System Based on Mobile Ad Hoc Networks. In: Proceedings of the 2005 IEEE Int. Workshop on Homeland Security, Contraband Detection and Personal Safety, Orlando, FL, 29-30 March, 8 p.
- Trusted Computer System Evaluation Criteria (TCSEC) “Orange Book”, 1985, U.S. Department of Defense Standard, DoD 5200.28-std.