Communication in the Software Vulnerability Reporting Process

Pro gradu thesis
Tiina Havana
Organizational communication & PR
Department of Communication
University of Jyväskylä
2003

JYVÄSKYLÄN YLIOPISTO

Tiedekunta **HUMANISTINEN**	Laitos VIESTINTÄTIETEIDEN
Tekijä Tiina Havana	
Työn nimi Communication in the Software Vulnerability Reporting Process	
Oppiaine Yhteisöviestintä	Työn laji Pro gradu
Aika April 2003	Sivumäärä 110

Tiivistelmä – Abstract

Our society has become more and more dependent on information technology and, thus, also on computer security. Reporting software vulnerabilities to vendors is central to software quality development. This study aimed to analyze how software vulnerability reporting is organized, and to compare the differences of opinions between reporters and receivers of the reports, i.e. the two main participant groups in the reporting process. The communication process in a software vulnerability reporting network was described. Knowledge production, mediation, and application in the network were analyzed. Publicity, crisis, and risk management as well as professional ethics, trust, and corporate social responsibility in the network were discussed. The study was based on a quantitative survey that was completed during summer 2002. So called snowball sampling was used to reach potential respondents. Altogether 157 valid answers were received, of which 60 were from receivers and 97 from reporters. The analysis of the results was conducted with the help of factor analyses, χ^2-tests, and Mann-Whitney U-tests.

In the study it was concluded that communication in the software vulnerability reporting process seems quite often to be one-way, although two-way symmetrical communication could in many cases make the knowledge application easier. This may have a negative effect on the publicity management of the communication participants and complicate the communication process. The communication network was described to be informative. The inter-organizational learning process was described. It was discerned that especially procedural knowledge, i.e., know-how and know-who, in the reporting process seems to need development. It was also detected that the combination of information with existing knowledge assets is essential in the receiving organizations. A lack of codification seems to be typical to the communication process, which may, among other things, have an effect on the development of trust between the communication participants. Also the opinions about the publicity and extent of the disclosures were determined in the study. Overall, both the receivers and reporters opposed immediate and full disclosure. The receivers opposed full disclosure more than the reporters in its every form. The two groups agreed on publishing some part of the information after a pre-defined time.

Asiasanat
Tietoturva, viestintäverkosto, viestintäprosessi, tiedonhallinta, tiedonsiirto, oppiva organisaatio;
Computer security, communication network, communication process, knowledge management, knowledge transfer, organizational learning

Säilytyspaikka
Jyväskylän yliopisto / Tourulan kirjasto

Muita tietoja

Acknowledgements

This study was conceived of and planned at the Oulu University Secure Programming Group (OUSPG). I want to thank all my colleagues at OUSPG for their valuable assistance, help and guidance during the research process. Especially I want to thank the group leader, professor Juha Röning, Marko Laakso, and Ari Takanen for their support. I also wish to thank my supervisors, professor Pertti Hurme and professor Elisa Juholin, at the University of Jyväskylä, for all their help, support and guidance during the study.

I also want to thank the Australian Computer Emergency Response Team (AusCERT) for all their assistance, and especially Kathryn Kerr for her valuable comments on my questionnaire. Furthermore, I want to thank the CERT Coordination Center (CERT/CC) for their assistance.

Finally, I want to thank my parents for their support and encouragement during my studies.

In Oulu, Finland, 31st March 2003,

Tiina Havana

Contents

1 Introduction

Computer security is a current and complex field of research. It concerns many people and companies. Due to growth in the usage of information technology, our society has become more and more dependent on computer security. Although attention in the research field of secure computing has recently focused mostly on pure technical aspects, for example Laakso, Takanen & Röning (1999) described the vulnerability handling process, which is an issue beyond pure technical research. However, the communication related to the disclosure of the vulnerabilities has not, to the author's knowledge, been studied before. The challenges in the communication process have been discussed widely for example on different mailing lists during the past few years. The communication process is essential, because if it fails the ultimate aim of protecting the actors of the information society may remain unattainable.

The purpose of the study is to describe the communication process related to software security vulnerability reporting, to find out how the information about software vulnerabilities is distributed in the communication network, and to analyze the differences in conception about the vulnerability process between groups that take part in reporting. Finally, the study seeks to define whether the communication process is working properly or not, and if not, why. The study is based on a quantitative survey that was completed during summer 2002.

The study seeks to interpret the communication network related to the security vulnerability reporting process. The focus is on how information about software vulnerabilities is received and processed and how that information is managed after reception. Interesting views in this particular communication process are how people communicate in crisis situations and how professional ethics affect the communication process.

2 Theoretical background of the research

To the author's knowledge, the software vulnerability reporting process has not been investigated from the perspective of communication sciences before. In this chapter previous research about software vulnerabilities is reviewed, the central concepts related to the software vulnerability reporting process are defined and the theoretical background of the research is presented. From the communication theory point of view the most important concepts related to the issue are communication networks, knowledge management, learning organization, ethics and trust in a relationship.

2.1 Software vulnerabilities – definition, life-cycle and previous research

Creating complex information and communication systems is a demanding task. At the moment different software products typically contain a large number of different flaws or bugs. Reasons for the emergence of these flaws include human errors, carelessness and ignorance in the design, implementation and management states of the software development process (Arbaugh, Fitchen & McHugh 2000, 52).

Some of these flaws lead to software security vulnerabilities. According to the NSA Glossary of Terms Used in Security and Intrusion Detection a vulnerability is a hardware, firmware, or software flaw that leaves an automated information system open for potential exploitation. Thus, it is a weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited to gain unauthorized access to information or disrupt critical processing. (Stocksdale 1998.) Arbaugh et al. (2000, 53) defines the vulnerability life-cycle as the whole process from the finding of a vulnerability to its repair.

One part of the vulnerability life-cycle is the reporting process and disclosure. The bug reporting process refers to the communication process during which

the knowledge of a vulnerability is transmitted to persons or organizations that are responsible for fixing the vulnerability or distributing the knowledge about the vulnerability further to other relevant parties, such as software vendors. Software vulnerabilities are disclosed in many ways, e.g. public disclosures, security advisories and security bulletins from vendors. Reporting channels for vulnerabilities are for example, full disclosure mailing lists, various distribution lists, and sometimes even mainstream media. New vulnerabilities are found by vendors, private persons (customers of the vendors or other interested parties), and independent organizations. Vulnerabilities are found during security reviews, quality assurance and normal system operation, and sometimes in more thorough penetration testing. (Laakso et al. 1999, 2.)

The whole vulnerability handling process is presented in Figure 1. This is a simplification of the model developed by Laakso et al. (1999, 7) and describes the ideal case of how the handling process should happen. The three main actors, the originator (i.e. the reporter of the vulnerability), the coordinator, and the repairer (i.e. the receiver of the report, e.g. the vendor) exchange information and handle it inside their own organizations. The whole process leads to the disclosure of the vulnerability after it has first been handled in cooperation with all three parties.

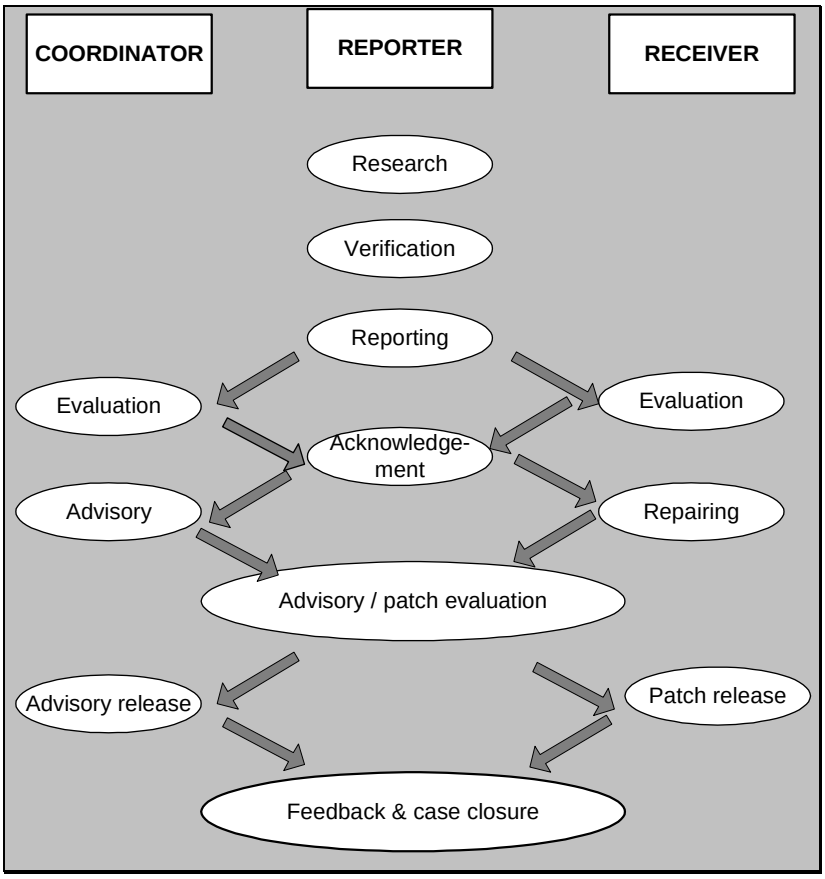


FIGURE 1: A model of the vulnerability life-cycle (Laakso et al. 1999, 7)

Many difficulties may occur in the vulnerability reporting process. Recent discussions on mailing lists and other forums for security professionals have shown that there is no consensus between groups that take part in the reporting process about the ethically correct disclosure policy[1]. All vendors do not have the expertise to handle vulnerability reports. Even the existing reporting policies differ from each other significantly. Failures in the reporting process could pose a remarkable risk for the information security of individuals and organizations.

The main actors that take part in the reporting process are the vendor, who is the receiver of the report, the discoverer of the vulnerability, i.e. the reporter,

[1] Several examples of these discussions can be found for example from the Vulnerability disclosure publications and discussion tracking list that is maintained by OUSPG and is available at http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/.

and in some cases a coordinating entity. The role of the coordinator is to supervise the work related to vulnerabilities by assisting other participators and gathering knowledge in one place. The coordinator forms a communication link between the reporter and the vendor. The coordinator can give certifications about vulnerabilities, provide contacts and influence the vulnerability life-cycle and evaluation. (Laakso et al. 1999, 4.) On the international level one of the most famous coordinators is the Computer Emergency Response Team/ Coordination Center (CERT-CC) at the University of Carnagie-Mellon in Pittsburgh, USA. AusCERT is the national Computer Emergency Response Team for Australia and New Zealand and a leading CERT in the Asia/Pacific region. The Finnish counterpart of these organizations is the Finnish Communications Regulatory Authority (Viestintävirasto).

There are three different possibilities for disclosure: 1) full disclosure, 2) partial disclosure, and 3) no disclosure. The publicity for the disclosure may be a) wide public, b) limited public (for example one organization) or c) totally limited public (for example an internal testing team in an organization). The source of a vulnerability report may be a white-hat hacker[2], a security professional, a vendor, a coordinator or an internal group in a company. These disclosure types are presented in Table 1, in which the typical sources of the vulnerability information are presented inside the table and are classified into different categories from the basis of the level of publicity and the extent of the disclosure. The numbers after the typical sources refer to the following disclosure policies.

[2] According to the NSA Glossary of Terms Used in Security and Intrusion Detection a hacker is a person who enjoys exploring the details of computers or programming systems and how to stretch their capabilities or a malicious or inquisitive meddler who tries to discover information by poking around (Stocksdale 1998). From these definitions the first refers to a white-hat hacker, and the second to a black-hat hacker.

TABLE 1: Disclosure types

Level of the publicity	*Widely public*	*Limited publicity*	*Private*
Extent of the disclosure			
full	White-hat hackers (1)	Professionals (3)	Internal testing teams (4)
partial	Vendors (2), Coordinators (2)		Internal bulletins inside the organizations (5)
no			Non-public bulletin inside the internal testing team (6)

Thus, one way to categorize the different disclosure policies could be as follows:

1) full, widely public disclosure
2) partial, widely public disclosure
3) full disclosure, limited publicity
4) full, private disclosure
5) partial, private disclosure
6) no disclosure, totally limited publicity

Publishing a full report to as wide a public as possible has been justified by saying that system security administrators are able to decide what actions need to be taken if they are aware of all aspects of the issue. It has also been suggested that publicity is a way to force the vendors to make patches as soon as possible. (Gordon & Ford 2000, 6.)

According to those who support partial and public disclosure or full disclosure with limited publicity, full and public disclosures are more harmful than useful. They can be exploited by criminals. For example, according to Culp (2001), worms called Code Red, Sadmind, Ramen and Nimda that caused difficulties in many countries during the year 2001 were born with the help of the weapons that computer security professionals had given to criminals. Partial disclosure seems to solve the problems in the no disclosure policy without giving away the benefits of full disclosure. However, problems arise because patches are often not ready on the publication day. Even conveying which software system is vulnerable may expose it to attacks. (Gordon & Ford 2000, 6.)

2.2 Communication as a process in a network

Organizational communication is a phenomenon that is familiar to all people but that has been a subject of research for a relatively short time. The main models of communication theory are presented in this chapter. They form the basis for the conception of communication that is used as a base for the analysis of communication in the present study.

The first basic model of communication was developed by Shannon and Weaver, and presented in the Mathematical Theory of Communication (1949). In this model a source formulates a message that is converted by a transmitter into a set of signals. These signals are sent through a channel to a receiver. The receiver converts the signals into a message. Any disturbance in the channel that may affect the signal is called noise. (Shannon & Weaver 1949, 33-34.) This view of communication can be called the linear process view.

The other basic way to describe communication was developed by semioticians. According to the semiotic-cultural school, communication is not the mechanical transfer of bits but a culturally determined interpretation. A message is not the central issue in communication but the interpretation of the message. (Fiske 1993, 62.) The semioticians are interested in analyzing the products of communication rather than the communication acts (Fiske 1993, 15).

In the present study communication is seen as a process in which a state of issues is interpreted and this interpretation is published (i.e. brought into others' knowledge) through interaction in a network. Communication networks in the software vulnerability process are handled in more detail in the next chapter. Thus, in the present study communication is analyzed from the process school point of view and the central issue is how the messages are transferred – the focus is on communication acts. Communication has traditionally been defined as interaction through which information is transmitted. For example, in the Collins Cobuild English Language Dictionary (1987) communication has

been defined as "the activity or process of giving information to other people or living things". The idea of communication as interaction in a network has been presented for example by Fiske (1993, 14) and Åberg (2000, 54). The two other categorizations that are used in the present study to describe the general characteristics of the software vulnerability reporting process and that can be seen as the starting point for the analysis are Juholin's (1999) categorization of organizational communication paradigms and the models of one-way and two-way communication presented by Dozier, Grunig and Grunig (1995).

The present study handles organizational communication, i.e. communication between and inside organizations. Juholin (1999, 57-59) has formed a categorization of paradigms that influence organizational communication. She differentiates three paradigms of organizational communication. The functional paradigm dominates in an organization that sees communication as a management tool and resource. This paradigm is dominant in traditional and hierarchical organizations. According to the functional paradigm, communication is organized and systematic. The dissipative paradigm is the opposite of the functional paradigm. Dissipative communication is dynamic, non-linear and creative. The dissipative paradigm is based on the chaos theory of communication. Dissipative communication may be effective, but predicting the nature and outcome of it is difficult. Juholin (1999, 57) calls the third paradigm the dialogic paradigm of communication. A characteristic of an organization, in which the dialogic paradigm dominates, is that every member of the organization is active in communication and takes part in it both as a receiver and a sender of messages. Typical for these organizations is a strong communality and that members take responsibility of the organization. (Juholin 1999, 57-59.) The difference between the dissipative and functional paradigms of communication is interesting for the present study, because these basic differences might be possible to detect from the basis of the respondents' answers between the different parties that take part in the vulnerability process. The idea is interesting to test, but the conclusions must be made with care because the grouping is very rough and abstract. This preconception is evaluated in more detail in Chapter 5.

Dozier, Grunig & Grunig (1995, 13) have presented four models of communication. These were initially developed to describe public relations management, but can also be used to describe communication in general. The models can be divided into one-way and two-way models. The one-way communication models emphasize the flow of information from organization to the public. In these cases there are no channels of information from the public back into the organization. When using the two-way asymmetrical model, the organization gathers information about the public, which helps the communicators to develop messages that are most likely to persuade the public to behave as the organization wants. Two-way symmetrical communication seeks to manage conflict and promote mutual understanding with key public groups. According to Dozier et al. (1995, 13) in this model, communicators seek to negotiate solutions to conflicts between their organizations and those groups. The aim is to seek “win-win” solutions to conflicts with the public. In the software vulnerability reporting process this model of communication can be used to analyze whether the communication between reporters and receivers is one-way or two-way, and whether it is symmetric or asymmetric. This is handled in more detail in Chapter 5.

2.3 Communication networks in the software vulnerability process

Stohl (1995, 23) states: "Organizational communication is the collective interactive process of generating and interpreting messages. Networks of understandings are created through coordinated acts and relationships." These networks of organizational communication may be organizational or, as in the case of the vulnerability reporting process, interorganizational.

Communication networks consist of links. A network link represents a connection between two parties. However, the nature of this connection varies. All links are not equal, and they can be divided into different groups on the basis of whether or not a particular type of interactive exchange takes place

among participants in some predetermined social system. One possibility, according to Stohl (1995, 35), is to divide link types into four groups according to the type of resources received from the link:

1) affective network (to obtain expressive resources)
2) power network (instrumental resources)
3) informative network (cognitive resources)
4) goods and services network (objective resources)

This categorization is also suitable for analyzing a vulnerability reporting network, which will be done in more detail below.

Links can also be divided into different groups according to their location and role within larger network configurations. Kreps (1990, 223-224) identified six different organizational network roles that describe a link's position in a network. These are 1) isolates, that are not intensively connected to others in the organization, 2) opinion leaders who guide others' behavior and influence decisions but do not necessarily have formal authority, 3) gatekeepers, that control the message flow, 4) cosmopolites who connect the organization to its environment, 5) bridges, that connect a clique to which they belong with another clique, and 6) liaisons, that connect cliques in the system without belonging to them.

Networks in the vulnerability reporting process are formally prescribed communication structures that are explicitly defined. As Stohl (1995, 23) argues, positions in these networks are derived from the organization, expectations for role relations are part of a greater set of norms, and specific individuals are interchangeable in a given position. The interaction of people is determined by the characteristics of the organization, not by the people themselves. However, these networks evolve because the limits imposed by the formal structures only constrain individual action, they do not control it. (Stohl 1995, 23-25.)

Benson (1975, 229) defines interorganizational networks as a political economy. He claims that interorganizational communication networks are mechanisms by which organizations get and give away scarce resources and by doing that they create a system of power relations. Organizations can be seen as dependent on their positions in the network. Pfeffer (1981, 106) developed this idea further and formulated the resource dependency theory. This theory argues that organizations try to structure their resource links in a way that they maintain their independence but are still able to benefit from their links.

The communication links at the interorganizational level have both personal and nonpersonal qualities. Interorganizational networks represent powerful connections: they can either create strong monopolies or on the other hand help small organizations to get their voice heard. (Stohl 1995, 33-35.)

The structure of the communication network can be characterized according to its size, centrality, and density. The size of a vulnerability reporting network can vary remarkably. It depends on the nature of the vulnerability[3]. The centralization, extent to which individuals have access to one another, and the density, the ratio of actual links to possible links, are also important points of view. (Littlejohn 1996, 305.)

An important view on the software vulnerability reporting process is that the different entities that take part in the reporting process can be seen as each others' stakeholders. This needs to be taken into account when evaluating the functionality principles of the communication network. Stakeholders are various groups of people, who are interested in affecting the acts of an organization and have a clear motive and opportunity to do that. Primary stakeholders are those, whose relationship to the organization is functional or is

[3] For example in the famous SNMP-case that was reported to the vendors during summer 2001 and published in spring 2002, there were 251 organizations involved and in each organization approximately 2-4 persons took part in the communication process. In some cases there may be only two participants in the communication process.

based on a contract. To this group belongs for example employees, authorities and partners. Secondary stakeholders are groups who are interested in affecting the organization's actions, but do not have any concrete bond to the organization. For example non-governmental organizations and pressure groups are secondary stakeholders. According to the stakeholder theory the purpose of an organization is to find a way of acting which fulfills the expectations of various stakeholders. This is eventually thought to bring also financial benefit to the organization. (Lehtonen 2002, 15-16.)

2.4 Information transmission in a communication network

In the following chapters the information transmission procedures in a communication network are considered. First, the ways of information production in the network are explained. After that, the focus will be placed on the various ways of information reception and processing.

2.4.1 Knowledge creation

The simplest model of the knowledge creation process is the linear model represented by Hargreaves (2000, 39). This model states simply that knowledge is first produced, then mediated, and finally applied. A closer look reveals that there are actually seven different stages in this process: production, validation, collation, dissemination, adaptation, implementation and institutionalization of the information. In practice these stages do not proceed sequentially. There is feedback from one stage to another. This suggests that the model should actually be interactive. The knowledge creation process is therefore an iterative process between knowledge production, mediation, and application. (Hargreaves 2000, 41.)

According to Greene and Geddes (1993, 26-49) individuals have two kinds of knowledge: content knowledge and procedural knowledge. This means that

people have both intellectual knowledge about things as well as know-how to do things. As Littlejohn (1996, 114) states, procedural knowledge consists of an awareness of the consequences of various actions in different situations. In different situations people use different procedural records. When these procedural records are summed together they form the overall procedural knowledge of an individual. Preorganized sets of behavior are called unitized assemblies. These routines help people to act efficiently in various situations. (Littlejohn 1996, 114.)

In the case of the vulnerability reporting process one preconception is that the procedural knowledge of the reporters may be weak. They do not know how the reporting should be done. On the other hand the content knowledge of the messages' receivers might at least in some cases be even weaker. They may have problems in understanding the reports. A major problem in the process is that different reporters and vendors are not unanimous about correct procedures, which may lead to problems in understanding the meaning of the reporting procedure.

On the other hand, if a subject has a lot of experience in reporting or receiving a report, she or he also most probably has more procedural knowledge. In organizations where there is a reporting or handling policy the receiver of the report or the reporter has probably more content knowledge and finds the reporting process for this reason easier.

Another theory of message production is constructivism. According to constructivism people interpret and act by following conceptual categories in mind. These constructs are organized into interpretive schemes. They are learned in social interaction with other people. An individual produces a message with the help of these schemas. (Littlejohn 1996, 116.)

Nonaka and Takeuchi (1995, 56-90) have developed a theory of organizational knowledge creation. This theory is based on knowledge conversion, which means the interaction between tacit and explicit knowledge. This conversion

happens in four stages, which are socialization, externalization, combination, and internalization. The theory has been named according to these stages, thus it is called the SECI theory.

In the socialization phase the knowledge is tacit and is transmitted in a tacit form. In this phase the members of the communication process share their experiences and may for example transmit know-how (Nonaka & Takeuchi 1995, 62-64). In the externalization phase the tacit knowledge is articulated in an explicit form. This requires that the organization members create concepts, metaphors, analogies, hypotheses or models (Nonaka & Takeuchi 1995, 64). In the third phase explicit knowledge is combined with existing explicit knowledge. The concepts are systematized into a knowledge system (Nonaka & Takeuchi 1995, 67). Finally the explicit knowledge is embodied into tacit knowledge (Nonaka & Takeuchi 1995, 69).

2.4.2 The effect of beliefs, values, attitudes and concentration on information reception and processing

One of the problems in the vulnerability reporting process is that receivers involved may have a negative attitude towards reporting software vulnerabilities. They do not necessarily see any value in supporting the development of the reporting process. The reports may not be taken seriously. For this reason it is important to have a closer look at the information reception and processing theories that consider attitudes and attitude change.

The information-integration theory explains how people accumulate and organize information about some person, object, situation, or idea to form attitudes toward a concept. The theory states that all information has the potential of affecting one's attitudes. However, the degree to which it does so depends on two variables: valence and weight assigned to the information. Valence is the degree to which the information is viewed as supporting one's beliefs or not. If the information supports one’s beliefs, the new information is

seen as positive. Otherwise it is seen to be negative. The weight assigned to the information is the importance of the information to the receiver. (Littlejohn 1996, 138.)

Attitudes differ from beliefs in that they are evaluative. Attitudes are learned as part of one's concept formation. They may change as new learning occurs throughout life. Behavior results in part from intentions, a complex outcome of attitudes. (Littlejohn 1996, 139.) Consistency theories claim that people are more comfortable with consistency than inconsistency. Therefore consistency can be seen as the primary principle that organizes cognitive processing. Attitude change can result from information that disrupts this balance. (Littlejohn 1996, 141.)

Rokeach (1968) has formed a theory of behavior based on beliefs, attitudes and values. Beliefs are the various statements people make about the world. Beliefs can be organized hierarchically. The most important of them form the core of the belief system. More insignificant beliefs lie at the periphery of the system. Core beliefs are difficult to change and change in them has a great impact on the whole system. (Rokeach 1968, 3.) Various beliefs toward an issue form an attitude. Rokeach (1968, 112) defines an attitude as follows: “An attitude is a relatively enduring organization of beliefs around an object or situation predisposing one to respond in some preferential manner”. Attitudes are even more difficult to change. Related to the vulnerability reporting process the interesting part of the theory is that Rokeach states that there are two kinds of attitudes: those toward an object and those toward a situation. These must always be considered together. For example, a person may consider that vulnerabilities should always be handled with care, but he might still support full disclosure because of the context in which the vulnerabilities are handled, i.e., the situation.

One of the most popular information processing theories today is the elaboration likelihood theory. It was developed by Petty and Cacioppo in 1986. According to this theory the likelihood of elaboration, or the likelihood of

critical interpretation of the content of the message, depends on the way a person processes the information. Critical thinking occurs if the person processes the information while concentrated. This means that they use the central route of their cognition when processing information. If the receiver is not concentrated, they process the information in the peripheral route. Factors that influence the degree of elaboration are for example motivation, ability to elaborate and the receiver's predisposition. (Kitchen 1999, 177.)

This phenomenon may have an effect on the vulnerability reporting process because the receiver may not be concentrated when they receive the message. When reading dozens of emails daily, a receiver may not fully understand the meaning of a vulnerability report. This is especially the case if they have no previous experience in the field.

2.5 Knowledge management and organizational learning

In this chapter the basic theories of knowledge management and organizational learning are presented. The aim is to give definitions of the concepts related to knowledge management and organizational learning that are used later in the analysis of the vulnerability reporting process. Proper knowledge management is a requirement for organizational learning and makes learning possible. Managing information and learning from it are essential in successful vulnerability handling.

2.5.1 Knowledge management

Knowledge can be classified as 1) facts or information (know-what), 2) principles that explain (know-why), 3) competence and skills (know-how), and 4) knowledge of the source of the information (know-who) (Lundvall 2000, 14). The central question in the bug reporting process as well as in many other

situations in the world today is whether knowledge should be private or public and should some of these knowledge types be more public than others.

Lundvall (2000, 15) states that technology makes it easier to disseminate some knowledge, but human networks remain crucial in accessing information. He also notes that in disseminating theoretical knowledge an electronic publication does not create instant understanding. For this reason companies and academia should interact efficiently. On the other hand this may also make knowledge less public. However, knowledge is rarely available freely to all, but nor can it be kept fully private, even when companies try to do so. (Lundvall 2000, 16-17.)

Lundvall (2000, 18-19) also notes that the transferability of knowledge depends in particular on the extent to which it is tacit. Knowledge is more easily shared if it is codified. On the other hand, the impact of codification depends on whether codes are made explicit and hence widely usable.

Data, information, knowledge, and wisdom are the basic concepts of knowledge management theories. According to Harryson (2000, 21) data is the raw material of a communication process. When receiving a message, people analyze this data. From the basis of this process they are able to form information. Information is the content of a message. It is the medium from which people create knowledge. In a learning process information becomes integrated into strategy through experience. Harryson (2000, 21) states also that new knowledge is created through interaction between existing bodies of knowledge. The usage of this knowledge to generate a genuine stock of insight means wisdom. (Harryson 2000, 21.)

2.5.2 Organizational learning

Argyris and Schön (1978, 18-26) describe organizational learning as taking place in two phases. According to them there can be single-loop learning, which means that the aim is to trace and fix an error within the scope of existing rules

and norms. Double-loop learning happens when these existing rules are opened to question.

One of the aims of the software vulnerability reporting process is to improve the quality of software systems. This can be achieved if the developers learn to make software that is originally secure. This is possible if the existing norms of the software development process are re-estimated, thus double-loop learning is achieved.

Nonaka and Takeuchi (1995, 45) criticize the existing organizational learning theories by saying that they lack the view that knowledge development creates learning, that they still use individual learning as their basis, and that they fail to conceive the idea of knowledge creation. They have tried to solve these problems with the SECI-theory presented above.

On the other hand organizational learning is primarily about individuals learning within their organizations. Theories on individual learning, communication and persuasion all are meaningful in discussions of organizational learning. Organizational learning also requires that conflicting forces are tolerated. (Weick & Ashford, 2000, 727.)

2.6 Managing publicity, risks, and crises

Ikävalko (1996) carried out research on publicity management and the mechanisms that affect the media relationships of an organization. She developed a model of the qualities that have an effect on how an organization can handle publicity. She argues that the size and social value of an organization has significant influence on how much interest the media has in the organization. Large and influential organizations are more interesting than small ones. To be victorious in the "publicity game" requires that the organization has an articulated, proactive publicity strategy, that the organization knows how publicity works, that the organization has trustworthy

PR-personnel, and that the organization has direct contacts to media. Thus, it is essential that the organization aims at managing its publicity, not only at benefiting from it. (Ikävalko 1996, 190.)

According to Lehtonen (2002, 6) an organization has to integrate three tasks to be successful in publicity management. It has to take care of its relationships to those stakeholders of which it is dependent on, it has to show to its environment that it takes responsibility for its actions, and it has to follow the changes of its stakeholders' values and expectations, as well as public discussions. Effective publicity management reduces the risk of a publicity crisis. To publicity management belongs reputation management, stakeholder strategy, and corporate social responsibility. If a company has paid attention to these views there is potential for the early notification of possible risks. Publicity management also requires effective issues management, which refers to following public discussions and stakeholders' values and expectations. Together these reduce the risk of a crisis situation. A company which takes care of its public relations has better chances to handle a possible crisis situation. For example, if a company has good relationships with the media it has better chances to get its own point of view heard if necessary. (Lehtonen 2002, 38.)

Lehtonen (1999, 67) has listed things to be done in order to avoid crises. First, the organization has to recognize and list all possible risks, problem situations, and weak links that could affect it. Second, the organization should imagine what would happen if some of the previous would come true. Third, the organization has to develop operational models of how to act in each of the previous situations. Fourth, the organization needs to list those parties that would be affected by the situation. Fifth, the organization needs a communication plan. And finally, the organization should test that everything works if needed.

At the moment vulnerability disclosure is often a crisis for the vendor. It is a sudden and unexpected notification about weaknesses in products. Fitzpatrick and Rubin (1995, 22-23) describe four possible ways to react to a crisis situation.

They based their division on a comparison of the candid public relation strategy and a strategy that they called the legal strategy. The four possible ways according to them are 1) traditional public relations strategy, 2) traditional legal strategy, 3) mixed strategy, and 4) diversionary strategy. In their research of how organizations respond to public charges of sexual harassment they concluded that the traditional legal strategy is the most common. Because of the potential risk of liability charges in software vulnerability issues, this grouping of possible ways to react to vulnerability reports might be effective. This is analyzed further in Chapter 5.

By the traditional public relations strategy Fitzpatrick and Rubin meant the way how traditional public relations advise the companies to react. These include stating the company policy on the issue, investigating the allegations, being candid, voluntarily admitting that the problem exists, if true, and finally announcing and implementing corrective measures as quickly as possible. However, because there is a possibility that any admission of guilt could be used against the organization in a lawsuit, a traditional legal strategy may be used. This includes saying nothing or as little as possible, releasing information as quietly as possible, citing privacy laws, company policies or sensitivity, denying guilt, acting indignant that such charges could have been made, and shifting the blame. In this case the organization understands the meaning of the publicity but thinks that it is a threat to the company's functions. The company may also deny fault while at the same time expressing remorse that a problem has occurred, which was called the mixed strategy. A diversionary strategy means a procedure, in which media and public attention were attempted to be diverted away from the accusations, the media was told that the organization is outraged at the situation, while taking little or no substantive action, and/or the problem was claimed to be solved. The organization tries to manipulate the public’s opinions. (Fitzpatrick & Rubin 1995, 22-23.)

2.7 Professional ethics, trust, and corporate social responsibility

In the software vulnerability reporting process professional ethics are of great value. Only if the professionals work in an ethical way is there a possibility that the participants in the process can trust each other. These two concepts are handled in this chapter.

To the semantics of the term professionalism belongs the requirement of moral justification of everything that is done. Professionals possess and exercise legitimate authority when they actually promote general benefit. Since the professional aims at the client's good, the individual client should be the focus of all work done. However, the professional may not be totally client-centered. The client is an individual part of a community. The community legitimates the work a professional does. The basis of the professional work is trust, which is critical because the professional-client relationship is usually voluntary. (Koehn 1994, 174-175.)

A moral commitment affects the acquisition of technical proficiency (Koehn 1994, 178). This means that a professional should always do things morally right. The moral commitment of the vendor is to develop secure software, and if the software is insecure, to correct the mistake. This is an old truth, but it also has an effect on the disclosure policy. The morally right procedure demands that a vendor makes information about the vulnerability available to the persons who may be impacted by the vulnerability. Only this way can the relationship between the vendor and the end user of the software remain trustworthy. Otherwise it may be possible that the end users loose their confidence in software systems in general, which may affect the whole development of the society.

Software vulnerabilities are a risk to any software vendor company because they can harm the public image of the company. Reporters are in a position to

influence the future of many companies. For this reason trust is an important factor in the communication between the two parties.

Doney, Cannon and Mullen (1998) define trust as a willingness to rely on another party and to take action in circumstances where such action may make one vulnerable. They notify that their definition incorporates the notion of risk as a precondition of trust, and it includes both the belief and behavioral components of trust. Mühlfelder, Klein, Simon & Luczak (1999, 350) state that there are at least four aspects in the term trust: the reduction of complexity, the existence of uncertainty, the orientation towards the future and the presence of risk. Both of these definitions describe well the aspects that affect the development of trust between the groups that take part in the software vulnerability reporting process.

Corporate social responsibility is an important concept in the context of organizational communication. The concept of corporate social responsibility has been developed for decades. Carroll (1979, 503-504) presented a three-dimensional conceptual model of corporate performance. He stated that corporate social performance requires that a firm's social responsibilities like legal, ethical, economic and discretionary responsibilities, are assessed, the social issues involved, like consumerism, the environment, product safety, occupational safety etc., are identified, and a response philosophy is chosen. This response could be proactive, accommodative, defensive or reactive. In software technology, handling the possible errors in software in a responsible way is one indication about social responsibility. It is also a sign of high professional ethics and tells that a corporation can be trusted.

2.8 Summary of the theoretical background of the research

In Chapter 2 the various theoretical aspects related to software vulnerability reporting were presented. It was noticed, that a great number of different views are relevant when analyzing the vulnerability reporting process. First, the

software vulnerability scene was presented. It was concluded that the vulnerability reporting process can be analyzed from the process school of communication point of view. Vulnerability reporting is communication inside a communication network. The communication is affected by the beliefs and attitudes of the participants. During the communication process new knowledge about the vulnerabilities is produced, mediated, and finally applied. Vulnerability reports may cause a crisis situation to the vendor, for which reason publicity, crisis, and risk management issues need to be taken into consideration. Finally, the ethical issues were discussed, which form an important framework for future development of the vulnerability scene.

3 Research methods

3.1 Research questions

The purpose of the study is to describe the software vulnerability reporting process. The receivers, reporters and coordinators of the process were asked in a survey how they do the reporting or receiving in practice. The survey covered issues such as which channels are used to transfer information, how the right contact persons are found, and who is informed about the vulnerability. The other main purpose is to describe the opinions of the respondents about the vulnerability reporting process. This information is essential in an evaluation of the functionality of the process.

This work aims also to analyze what kind of knowledge relates to the vulnerability reporting process, how this knowledge is transmitted in the communication network, and how public this knowledge should be. The issue of codification is essential as well. The principles and instructions for the vulnerability reporting process is an attempt towards a more codified way to handle the reporting process.

The research questions of this study are:

1) How is communication of the vulnerabilities organized in practice?
2) What kind of views people participating in the software vulnerability reporting process have about different aspects of it?
3) What differences are there in the way reporters and receivers of the reports see the reporting process?

People participating in the process include both the reporters and receivers of the vulnerability reports. The coordinators' answers are handled together with the reporters' answers, because their role in practice is very similar to the

reporter's role. The focus is on the respondents' opinions about how things should be handled.

3.2 Investigating attitudes, beliefs and values with surveys

Survey methods are used to gather information about a population's beliefs, attitudes, and behaviors for the purpose of describing both the characteristics of the respondents and the population they were chosen to represent (Frey, Botan & Kreps 2000, 198). It can be asked, why bother to investigate the attitudes, beliefs or values of people. Everyone is entitled to any opinion. Investigating what people think about issues is of value simply because these opinions are assumed to influence behavior. (Black 1999, 215.) A survey is a quantitative research method. Hence, what individuals do in different situations is of little interest. Predicting individual behavior is unlikely to be very successful. Research about attitudes, opinions, and beliefs with a quantitative research method can help to understand tendencies. The main problem to solve is how attitudes, opinions and beliefs tend to influence decisions and actions in groups of people who have some characteristics in common. (Black 1999, 216.) All these three aspects, beliefs, attitudes, and behaviors of all participants influence the vulnerability reporting process.

A survey is based on information gathered with a questionnaire, which is a self-report measure. The respondents are asked to tell, what they think their attitudes, opinions and beliefs about an issue are. The focus is not on behavior, but on how people think they would behave in a certain situation. Thus, questionnaires can measure the subjects' perceptions of a concept, not the concept itself. Finding out people's own ideas of their beliefs, attitudes and behaviors of the related parties forms the core purpose of the questionnaire. (Black 1999, 36-37.)

The data that is gathered with the questionnaire is analyzed with the help of statistical methods. The most important methods are those meant for describing

data through summary statistics, and those meant for analyzing relationships between variables. Through summary statistics it is possible to evaluate the central tendency and dispersion of data. The variables can be related to each other in one of the following three ways: they can be unrelated, linear, or nonlinear. These relationships can be measured further by using correlations and factor analysis. (Frey et al. 2000, 293; 357-377.)

3.3 The research methods of the present study

To answer the research questions of the present study, a quantitative survey-research was used. Two questionnaires, one for the reporters and one for the receivers of the reports (Appendices 3 and 4), were developed with the help of a qualitative group discussion with the professionals at the OUSPG. At the end the results of the survey were analyzed with quantitative methods.

In the present study so called snowball sampling was used to reach the potential respondents. For this reason the respondents in the survey form a purposive sample of the population. Snowball sampling is a technique in which subjects with desired traits propose further potential respondents to be contacted. Snowball sampling is an effective sampling method in cases where no lists of population members are available. (Black 1999, 125.) The survey was conducted through the Internet. It is the most efficient and inexpensive way to gather the answers from people that are geographically far from Finland. The survey was advertised to the two CERTs, AusCERT and CERT/CC, and on three mailing lists that reach many professionals in the field. In the advertisement the receivers were asked either to fill in the questionnaire if they belong to the population in question or to send the advertisement to their contacts that are dealing with these issues and for that reason belong to the population in question.

Because the research subject is very new, the questions for the questionnaire were formed in a group discussion. The participants are experts in the field of

computer security. They are working at the OUSPG and thus have experience in the reporting process. In this way also the validity of the questions were evaluated. The questions in the questionnaire were grouped into four parts. In the first questionnaire (Appendix 3), which was for reporters, the first part included questions about the background of the respondents. The background information about the reporters is presented in Appendix 1. In the second part the questions handled general issues related to the actual reporting process. In the third part the respondents were asked in more detail about the concrete reporting handling process and their opinions about it. The last section concentrated on specialties in the communication process. The second questionnaire (Appendix 4), was for receivers of the reports. In this version the same things asked from the reporters were asked, but from the receiver point of view. There were more questions for receivers than for reporters because more things were seen as relevant from the receiving point of view in the whole communication process. Background information about the receivers is presented in Appendix 2.

Altogether 164 responses were received from the survey. 102 of them were from reporters, 62 answers were from receivers of the report. After the invalid answers, i.e. obviously incomplete forms, were removed, there were 60 receivers' answers and 97 reporters' answers left. Thus, altogether there were 157 valid answers.

The analysis of the results was conducted with the help of factor analyses, χ^2-tests, and Mann-Whitney U-tests. These are handled in more detail below.

3.4. Statistical analysis

3.4.1 Factor analysis

The idea of factor analysis is to reduce the amount of variables, form new variables, and to find latent structures among groups of variables. New

variables are usually a kind of generalizations. The values that the factor analysis gives for the new variables can be understood as correlations between the original and the new variables. (Valkonen 1976, 110.)

Factor analysis is used to analyze the correlations between variables that can not be observed directly. In the present study, explorative factor analysis was used. Explorative factor analysis is a method to describe interdependencies between variables and to make generalizations by reducing the number of these variables or factors. New so called sum variables are formed. These link at least two variables that have been measured in the same way together. The reduction of variables is conducted by analyzing the correlations between the original variables. These correlations, i.e. factor loadings, are the main result of the analysis and show how much the variable has to do with the new factor. (Karma & Komulainen 2002, 40-41.)

After the loadings have been calculated there is a possibility to rotate the original factor co-ordinate. With the rotation the best factor matrix is sought, and the interpretation is made easier, but the original results of the factor analysis are not changed. One criterion for the best solution is a simple structure. In the present study a varimax rotation was used to simplify the structure. It maximizes the variances of the loadings' squares (Karma & Komulainen 2002, 45). A pure varimax rotation has traditionally been widely used especially in educational and behavioral studies. This has also disadvantages, because it would be advisable to compare results received from other rotations to the results of the varimax rotation as well. Selecting the rotation method also has an effect on how well the interpretation can be done. (Nummenmaa, Konttinen, Kuusinen & Leskinen 1997, 247.) In the present study the varimax rotation proved to be useful. The interpretation of the results became easier. Other rotation methods were attempted as well, but the results did not bring any new information compared to the results from the varimax rotation. For this reason the results of the factor analyses are presented with the tables that contain the results of the analyses after varimax rotations.

To ascertain that the preconditions for factor analysis are fulfilled the Kaisser-Meyer-Olkin Measure of Sampling and Bartlett's test of sphericity were done. The KMO measures the sampling adequacy, which should be greater than 0.5 for a satisfactory factor analysis to proceed. Bartlett's test of sphericity is significant if its associated probability is less than 0.05. This means that the correlation matrix is not an identity matrix.

3.4.2 χ^2-test and Mann-Whitney U-test

χ^2-tests can be used to compare two independent groups where the variable consists of a collection of at least nominal categories (Black 1999, 576). In the present work χ^2-tests were used to compare the answers given to questions that produced nominal data. The assumptions that underlie the test are to be taken into account before the test can be done. The respondents must form two separate groups. One respondent may belong only to one group, which is the case as the receivers and reporters are compared. The data should be categorical. There should exist sufficient categories to contend with all responses, which may require a category of no response. The sample size affects the calculations. The smaller the sample size the less the test can make conclusions about the sample. Small categories may be at most 20% of the whole data. (Black 1999, 577-578.)

The χ^2-test is based on absolute and theoretical frequencies. Test results are always presented and can only be interpreted together with a cross-tabulation. The χ^2-test estimates the difference between the independent groups by calculating the difference between absolute and theoretical (expected) frequencies. The greater the difference between the groups, the greater the dependence between the variables. For example if the difference between boys and girls in mathematic skills is big, it can be expected that these two things – gender and mathematic skills are dependent from each other. (Valli 2001, 72-76.)

Because a great deal of the data is ordinal, also Mann-Whitney U-tests were used to compare the two independent groups. The Mann-Whitney U-test is a proper statistical test to analyze ordinal data such as data about opinions of the respondents on the Likert scale. The Mann-Whitney U-test is based on sorting the data according to the ordinal numbers given to each response. The original values are forgotten and the ordinal numbers are compared to each other. (Valli 2001, 78.)

The results of the tests are so called p-values, i.e. probability values. The tests tell, what is the probability of making a wrong conclusion if the hypothesis behind the test is rejected. The rejection is made with the risk that the p-value tells. The highest risk that can be taken is 5%. So, if the p-value is between 0.01 and 0.05, the risk is small enough that some conclusions can be made. The result is called statistically nearly significant. The result is called significant, if the p-value is greater than 0.001 but smaller than 0.01. The result is statistically very significant, if the p-value is less than 0.001. (Nummenmaa et al. 1997, 43.)

3.4.3. Mean values and percentage values

In some cases simple mean values and percentage values were used for presenting the data. These numbers give a rough picture about the distribution of the data and can be useful in interpreting what issues need to be analyzed in more detail. Percentages were seen to be more useful than frequencies, because in this way the comparison between the two groups, the reporters and the receivers, became easier. Some of the data was not analyzed any further than the percentage distributions. This procedure was used in presenting the reporters' and the receivers' answers that can be seen in Chapters 4.1 and 4.2, before the comparison of the two groups and the analysis of the results. The mean values can be useful for analyzing data that is on a Likert scale. In other cases percentages were seen to be more reliable descriptions of the data.

4 Results

In this chapter the results of the survey are presented. The answers from reporters and receivers of the reports are first presented separately and then compared to each other.

4.1 Reporters

4.1.1 Description of the reporting process

In most cases the reporters gain information about vulnerabilities in the course of their own work. 84,7% of the reporters had discovered the vulnerabilities personally. 60,2% responded to have heard about a vulnerability from an internal testing group. Private announcements and external testing groups were more uncommon sources of vulnerability information. 21,4% of the reporters had gained the vulnerability information through a private announcement. 19,4% responded to have heard about a vulnerability from an external testing group. The source of the vulnerability information was asked as a checkbox-question, which means that there was a possibility to give more than one answer to this question. Altogether there were 198 answers. The percentages above are formed separately and represent the percentages of the total amount of respondents (98) who have responded to have received vulnerability information from the source in question. The same procedure was used for other checkbox-questions as well.

The communication channels, through which the reporters send the vulnerability information, are presented in Figure 2. The values of the figure are percentages. Thus, they represent the proportion of the respondents that answered that they use the particular communication channel. Communication channels were charted with a check-box question, for which reason there were altogether 194 answers given to this question. It can be seen that the most common channel is email, both in an encrypted and unencrypted form.

Altogether these two forms of email represent 54,1% of all the answers given to this question. Also WWW-based bug reporting forms are nowadays quite popular channels for distributing vulnerability information.

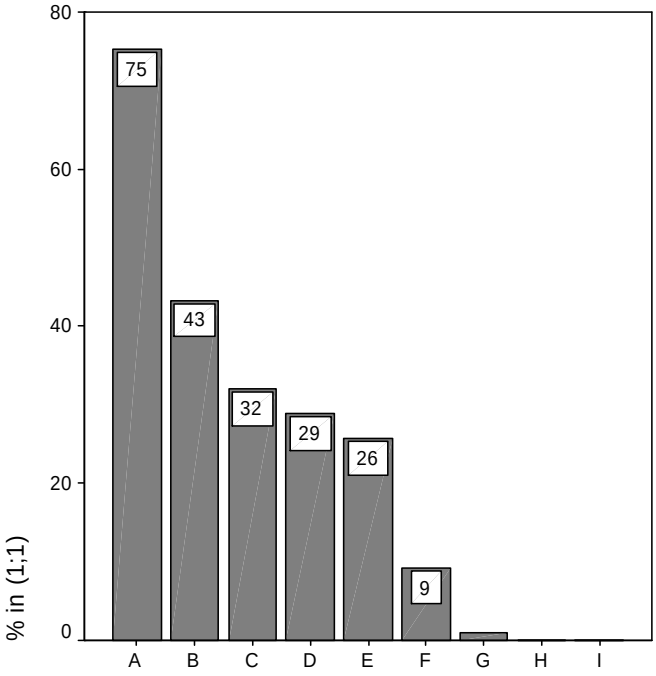


FIGURE 2: Reporters' communication channels (percentages)

The respondents were asked, who or what defines in their organization how the reporting should be done. 32,0% of the respondents reported that they have some kind of a reporting policy. As expected, standardized policies are not very common. A great deal of the reporters, 33,0% of the respondents, do the reporting in a way that they think is the most appropriate to the current situation. 27,8% of the reporters answered that the way how the reporting is done depends on their own situation. This is studied in more detail below when the differences between reporters and receivers are handled.

However, the reporters whose organizations had a reporting policy were also asked whether they were satisfied with it. 69,9% of the respondents answered to the question, which means that the respondents have probably understood the question in a different way than the question above, or that the order of the questions has influenced the results. Most likely the respondents have understood it as whether they were satisfied with the way the reporting is done in general in their organization. So, at least some of the respondents have thought that doing reporting depending on the situation can be thought as a reporting policy as well. 87% of the respondents that answered to the question were satisfied with their reporting policy and 13% thought that it should be modified.

Finding contact persons was somewhat problematic to the majority of the respondents. 20,6% answered that they rarely find the right contact persons without problems. 42,3% of the reporters find the right contact persons without problems frequently. 37,1% answered that they find the right contact persons without problems always or mostly.

The most popular way to find the right contact persons was to seek information about them from WWW or other sources. 44,3% of the reporters answered that they used this procedure. 21,6% of the respondents communicate about these issues only inside their own working group or organization, for which reason they know the persons they talk to personally. Surprisingly few, only 8,2% of the respondents use an independent third party, like a national CERT. 12,4% of the respondents answered that they have regular communication with the people they talk to about these issues, but that they do not know them personally.

The most popular communication partners in issues related to software vulnerabilities before the disclosure were colleagues. 77,6% of the reporters communicate about the issues at least with their colleagues. Only 3,1% of the reporters responded that they do not report the vulnerability to the vendor before publishing their findings to a wide audience. 18,4% responded that they

report their findings to an independent third party like a national CERT. 28,6% told, that they talk about these issues with their spouse and/or some friends. 38,8% communicate with representatives of the vendor company, 39,9% reported specifically that they communicate with security experts of the vendor company. 24,5% communicate at least in some cases with other professionals of the vendor company, who have been asked to pass the information to the security professionals (such as a support organization). 12,2% of the reporters told that they sometimes communicate with people who are not experts in software vulnerability issues. 17,3% of the respondents claimed that at least in some cases they do not tell about their findings to anyone.

50,0% of the reporters' organizations have a recognized or advertised point of contact for issues related to software vulnerability reports. 44,8% do not have one, and 5,2% of the respondents did not have knowledge about this issue. By 46,9% of the organizations the receiver of the report is specifically requested to send an acknowledgement that she or he has received the report. In 42,7% of the organizations this was not done, and 10,4% of the respondents were not able to give an answer to this question.

32,9% of the reporters responded that their organization has rarely been contacted by the receiver of the bug report after reporting. 26,5% have been contacted frequently. 8,5% of the reporters have never been contacted by the receiver of the report after reporting. 31,9% of the reporters told that they have been contacted by the receiver always or mostly after the reporting.

According to the reporters, most organizations keep a record of the name and version number of the operating systems and applications that they have found to be vulnerable, and about the patches and/or work-arounds that have been implemented to address these vulnerabilities. This was the case according to 76% of the respondents. These records were not kept in 18,8% of the organizations. 5,2% of the respondents were not able to answer this question.

4.1.2 The reporters' opinions about the vulnerability handling process

According to the reporters the vulnerability handling process is not well arranged in most of the organizations. Even 72,4% of the respondents either disagreed or strongly disagreed when they were asked whether the vulnerability handling process is well arranged. 11,2% of the respondents did not have an opinion about the issue, and only 8,2% of the respondents agreed or strongly agreed with the statement.

Figure 3 presents the opinions of the reporters about the right vulnerability information handling process. The values in the figure are mean values that were calculated from the basis of the Likert scale. Thus, the range is 1-5 (strongly disagree, disagree, neutral view, agree, strongly agree).

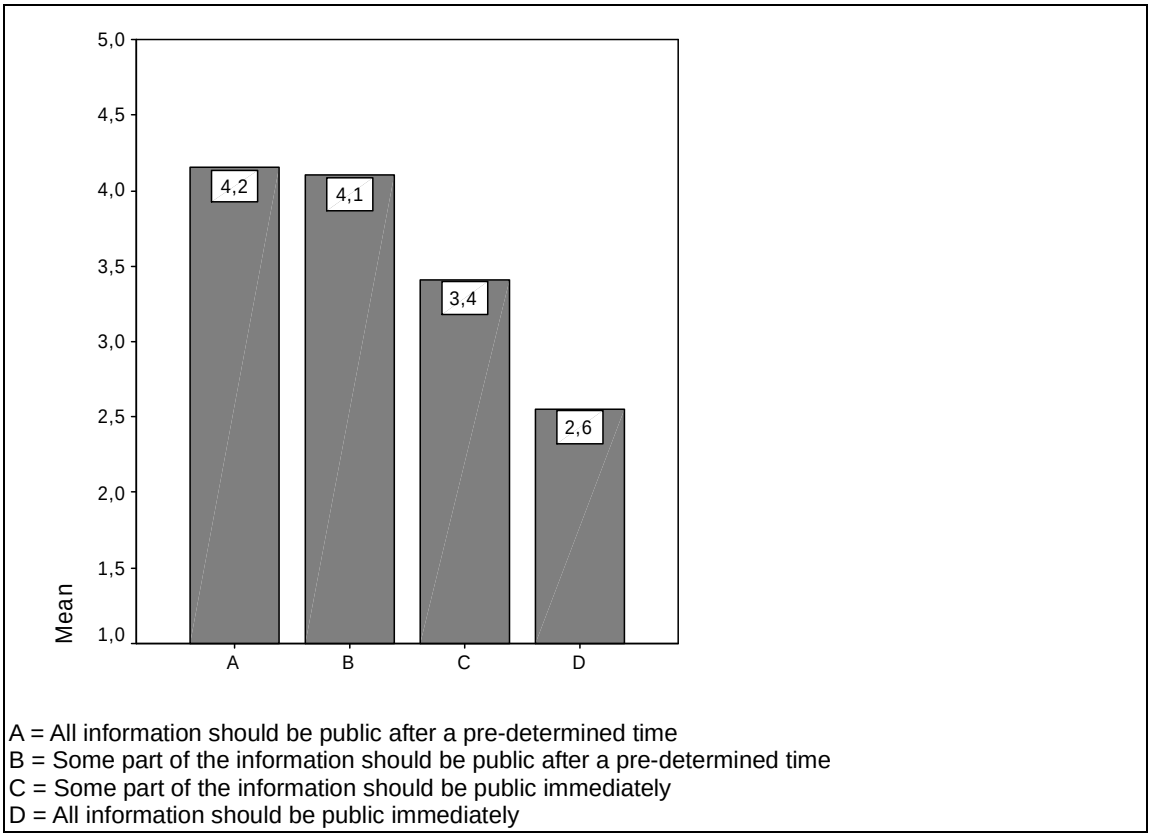


FIGURE 3: : Reporters' opinions about the right software vulnerability information handling process (Likert scale, mean values).

The most supported proposition is that all information related to software vulnerabilities should be public at some point. The mean value for proposition A (All information should be public after a pre-determined time) in Figure 3 is 4,2, which is relatively high. Most of the reporters also accepted the claim that some part of the information should be public after a pre-determined time. This is proposition B, and the mean value on the Likert scale for it is 4,1, which is nearly as high as for proposition A. 80,4% of the respondents either agreed or strongly agreed with the claim. Proposition C (Some part of the information should be public immediately) was clearly less supported. The mean value on the Likert scale is 3,4, which is still above a "neutral view". 52,5% of the respondents agreed or strongly agreed with the proposition. Clearly fewer of the reporters thought that all information should be published immediately when a vulnerability is found. The mean value on the Likert scale is below a "neutral view".

The results to these questions were also analyzed with the χ^2-test. It was found, that those people who thought that all information should be public immediately also thought that some part of the information should be public immediately, and that those who agreed that all information should be public after a predefined time also agreed that some part of the information should be public after a predefined time. Those who had agreed that all information should be public immediately did not agree that all information should be public after a predefined time and those who answered that some part of the information should be public immediately did not agree that some part of the information should be public after a predefined time.

The reporters and the receivers of the report were both asked about their opinion about the minimum level of response to the reporter of a software vulnerability. 40,4% of the reporters answered that the priorisation of the report in their vulnerability handling process should be informed. Quite many, 32,9%, also thought that a simple acknowledgement that the report has been received would be enough. Only 2,1% of the respondents thought that communication

would slow down the repairing process unnecessarily or that no response from the vendor is necessary. 22,3% of the reporters responded that the actual repairer, not just the receiver of the report, should contact the reporter, which is the most intensive form of communication in this case.

The reporters and receivers were also asked, which values guide their decisions about security vulnerability information the most. These results are presented in Figure 4. The values and beliefs of the reporters were asked from the reporters with a check-box question. The percentages in Figure 4 represent the proportion of choices given to each value compared to the total amount of respondents who answered to this question.

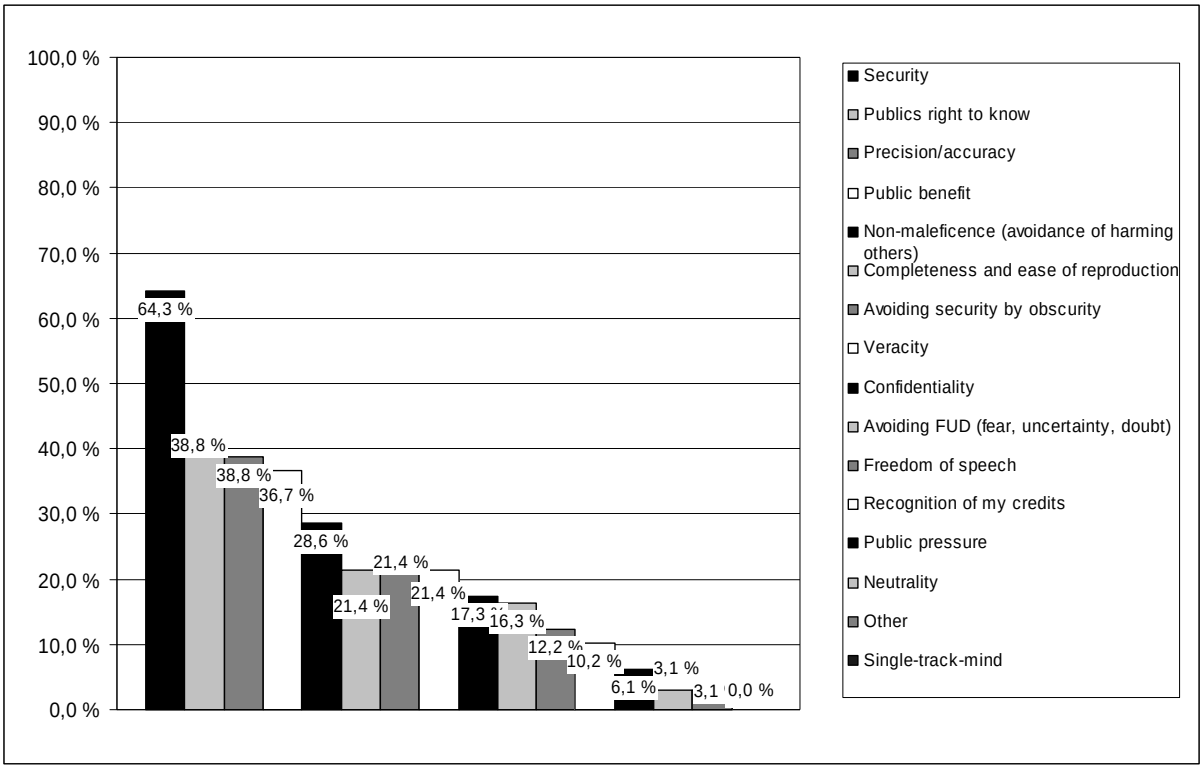
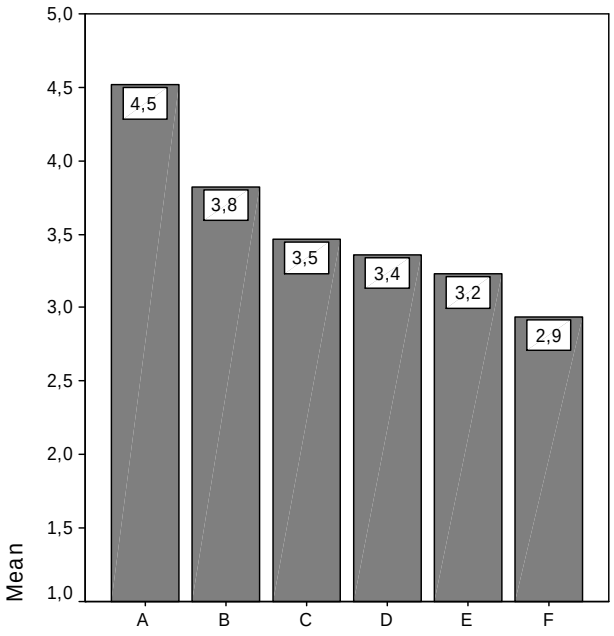


FIGURE 4: Values/beliefs of the reporters (percentages of the choices of each respondent per value)

Above all, the reporters seem to value security, but the public's right to know, precision/accuracy, and public benefit can also be distinguished from other choices. Also non-maleficence was seen to be important.

Figure 5 gathers the mean values calculated from the values on the Likert scale given to the propositions that sought to analyze the knowledge activities of organizations. The conclusion is, that electrical communication forms like intranet, email, electronic bulleting boards etc. form the basis of communication in the field. The mean values on the Likert scale that can be seen in Figure 5, were all above 3 ("neutral view"), which means that the attitudes toward these modern communication forms are positive. Traditional communication forms like internal magazines or bulletins seem to have little meaning compared to more modern ones. The mean value on the Likert scale for this proposition was below a "neutral view", which indicates a negative attitude towards these traditional communication forms. These answers are compared to the answers of the receivers and analyzed further below.



A = It is highly important that communication about vulnerabilities inside the team is open and trustworthy
B = Intranet and bug database are efficient means for knowledge sharing about vulnerabilities
C = Planned meetings about each vulnerability are very important for knowledge sharing
D = Cross-functional project teams are important
E = Electronic bulleting boards or chat channels are an efficient way to communicate about vulnerabilities
F = Internal magazines, newsletters or bulletins distribute knowledge about vulnerabilities efficiently

FIGURE 5: Knowledge activities (Likert scale, mean values)

According to the results, most reporters find that reporting is not easy. The reporters were asked to evaluate the statement "In my opinion, doing the

reporting is easy" on a Likert scale (strongly disagree-strongly agree). Even 74,4% of them either have no opinion about the issue or disagree. Only 3 of the 97 reporters answered that they agree strongly. The mean value on the scale of 1 to 5 is 2,4, which also indicates that the reporters do not find reporting easy.

4.1.3. The reporters' opinions about the communication network

Seven questions in the questionnaire were formed to analyze the respondents' opinions about the communication network. These included questions 25-30 and questions 32.1 and 32.2 in the questionnaire for reporters (Appendix 3). The analysis was completed with the help of factor analysis of the responses to questions 25-28, 30, 32.1 and 32.2. Question 29 was excluded from the factor analysis because it has different options for the answers and thus could not be included. First, a KMO and Bartlett's test of sphericity was completed to make sure that factor analysis was possible to be done with this material. The score of the Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0,528, which means that the test can be done. Also the Bartlett's test value was acceptable.

The results were rotated with varimax/Kaiser normalization. The values of the analysis after the rotation can be seen in Table 2. Rotation makes the interpretation of the results easier, but does not affect on the correlations of the original factor analysis. Significant correlations are written in bold text in the table.

TABLE 2: Results of the first factor analysis

Rotated Component Matrix			
	1	2	3
All information should be found and handled only inside the two organizations	**0,887**	0,189	-0,000
Only selected persons outside the organizations should be informed when an error is found	**0,883**	-0,010	0,172
In my opinion, the reporter should get the chance to evaluate the advisory	0,111	**0,735**	0,242
It would be easier and more useful if the communication between the reporters and the receivers would be direct	0,046	**0,704**	-0,181
In my opinion, the reporter, the coordinator, and the receiver should have regular discussions after the report	0,048	**0,645**	0,185
Our organization is dependent on its contacts to other organizations that handle these issues	0,001	0,011	**0,894**
An independent third party like a national CERT is a useful help in the communication proc	0,160	0,160	**0,685**

The first two variables correlate strongly with component 1. Component 2 correlates with the next three variables and component 3 with the last two variables. Hence according to the reporters' answers, these seven variables can be reduced to three new components, which could be called 1) restricted information transmission in the network, 2) open information transmission in the network and 3) the amount of network dependence/trust.

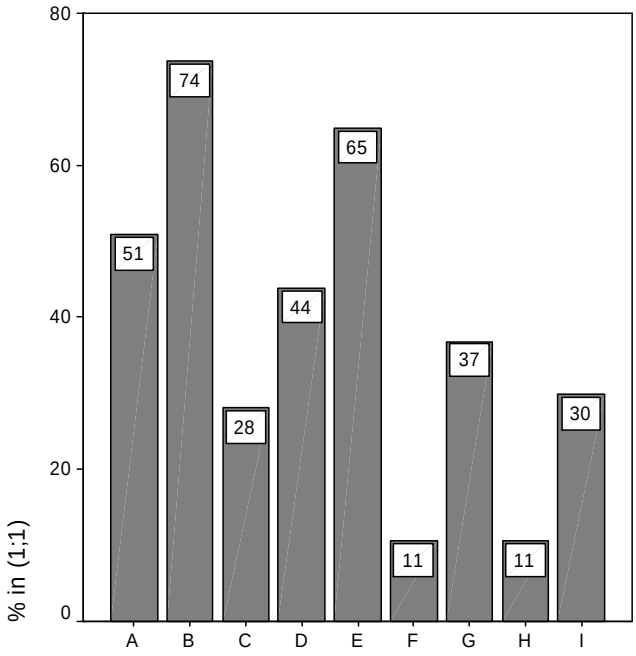
4.1.4 The reporters' relationship with publicity

The respondents were also asked to evaluate their organization's relationship to publicity. The conclusion was that according to the majority of reporters their relationship to publicity is relatively open. 34,8% of the reporters thought that media is an important and equal discussion partner to their organizations. 39,1% responded that their organization sees publicity to be important, but thinks that it must be kept in their own hands. They inform the media actively. 20,6% of the reporters answered that their organization takes publicity seriously and thinks that it usually harms their organization. If possible, they try to avoid publicity. According to 5,4% of the reporters publicity does nothing but harm. They try to influence the media as effectively as possible.

4.2 Receivers

4.2.1 Description of the receiving process

The channels, through which the receivers of the reports get the information about the vulnerabilities that have been discovered in software developed or used by their organization, are presented in Figure 6. The most common channels are public mailing lists and email, which were also the most common channels for the reporters. The values are percentages, as was the case in the previous chapter as well. This makes it easier to compare the two respondent groups. The order of the channels is similar to those in the previous chapter, which also simplifies the comparison of the two groups.



A = Email, encrypted
B = Email, unencrypted
C = Bug reporting WWW-form
D = Other personal communication
E = Public mailing lists
F = Other
G = Public discussion forums on WWW/IRC/News groups
H = Media
I = Telephone

FIGURE 6: Communication channels for receiving vulnerability information (frequencies)

Interesting view points are for example that receivers use more unencrypted email than reporters, that public mailing lists and public discussion forums are a remarkably more significant source of information for the receivers, and that bug reporting forms on the WWW do not have such a strong significance for them as for the reporters.

Even when the reporters told that they send vulnerability information mostly through other channels than CERTs, they were the most common source of information according to the receivers of the reports. 28,6% of the answers that were given to the question about the organization that provides information about software vulnerabilities to the receivers were that this organization is an independent third party like a national CERT. 22% of the respondents told that they get the information directly from an external reporter. In 22,8% of the cases the information comes from product support, and in 20,5% from internal research. 5,8% of the responses were that the source of the information is other than the ones mentioned.

The receivers were also asked whether their organization has a policy or instruction for situations where the organization gets a vulnerability report. Nearly half (47,5%) of the respondents answered that their organization has some kind of a reporting policy. The most common type was an internal reporting policy (25,4%), but public reporting policies were quite common as well (18,6%). In 3,4% of the organizations there was a non-written reporting policy in use. 33,9% of the receivers responded that according to their opinion there is no need for a standardized reporting policy, but the reporting procedure varies from situation to situation. 11,9% of the respondents answered that the reporter is responsible for deciding how the reporting is done.

82,5% of the receivers communicate about the reported vulnerabilities with their colleagues. More than half (57,9%) have also talked about these issues with the responsible project manager. 29,8% of the respondents told, that at least in some cases the vulnerability has already been public when they have heard about it. 12,3% of the respondents have talked about the vulnerabilities with

their spouse and/or some friends. Only 8,8% of the receivers have kept the report totally secret at least in some cases.

Next, the answers given to the questions that were formed to analyze the receiving procedure are presented. 43,9% of the respondents answered that in general they use some hours to process a vulnerability report, when the repairing process is not included. However, quite many (35,1%) responded to be able to process a vulnerability report within some minutes. 19,3% use days for the processing, and one of the respondents (1,8%) answered that their organization needs weeks for the processing. 33,3% of the receivers responded that after receiving a vulnerability report they always contact the reporter. 14,0% contact the reporter in most of the cases. 29,8% rarely contact the reporter, and 12,3% do that frequently. 10,5% of the receivers answered that they never contact the reporter after having received a vulnerability report. The last time the receivers had got a vulnerability report, 41,1% of the respondents had provided a non-automatic response to the reporter within hours of reception. 35,7% of the respondents had needed some days for the response, and 1,8% (1 respondent) had needed weeks to do that. 21,4% of the receivers had not provided any feedback at all.

The respondents were also asked, how do vulnerability reports affect their day-to-day tasks. 21,6% of the respondents answered that receiving a vulnerability report means an extensive amount of communication inside their organization until the matter is resolved. 20,6% agreed, that when receiving a vulnerability report the daily tasks are not interrupted because the organization has planned how to react to such situations beforehand. The rest of the respondents did not answer to this question. 33,3% of the respondents answered that they organize time for the repairing process by prioritizing the reports and handling them in priority order. A great deal of the respondents (30,0%) told that they organize time for the repairing process by interrupting other work and concentrating on the repairing process. In 15% of the receiving organizations there had been a specific schedule formed within which the reports were supposed to be handled, and this was used in the repairing process. 13,3% of the respondents

answered that they simply put the reports aside and wait for a suitable time for handling them.

65,5% of the receivers responded that their organization has a recognized or predefined point of contact for issues related to vulnerability reports. 29,3% of the organizations did not have one. 5,2% of the respondents did not have information about the issue.

35,7% of the receivers responded that only 0-10% of the all reports their organization had received during the last 12 months were valid. 16,1% answered that 10-20% of the reports were valid and 8,9% estimated that 20-50% of the reports were valid. 19,6% of the receivers thought that 50-70% of the reports were valid and as many (19,6%) answered that 70-100% of the reports were valid.

The majority of receiving organizations keep a record of the vulnerabilities and their patches. 71,9% of the receivers answered that this is the case in their organization. 21,1% responded that their organization does not keep such records, and 7% of the respondents did not know this. The respondents were also asked to evaluate, how often they think this information is used in their organization. 45,8% answered that this information is used frequently or very often. 6,3% answered that the information was never used, and 22,9% responded that the information is used rarely. In 25% of the organizations the information is used from time to time.

55% of the receivers told, that in their organization the information about a discovered bug is passed to the software developers of their organization in order to prevent similar bugs in the future and that the reports are also actually taken into consideration in the software development process. 15% of the respondents answered that the information is passed on to the software developers, but the reports do not have an essential part in the software development process. In 15% of the organizations the information was not

forwarded to the software developers, and 15% of the respondents did not have knowledge about the issue.

To analyze the development of routines and learning in the receiving organizations, a comparison of the answers concerning the respondents' working experience and the time they have used to handle a vulnerability was made. With an χ^2-test of the two answer groups it was proven that the more experienced the receivers are the less time they used for handling the vulnerability reports. The p-value of the comparison was .001, which means that the result is statistically significant. The cross-tabulation of the two questions is presented in Table 13. From the cross-tabulation it can be noticed that the time used to process a vulnerability report is more often short if the respondent has worked in the organization many years.

TABLE 13: The cross-tabulation to analyze receivers' learning (experience compared to the time used per vulnerability report by the receivers)

How much time do you use to process a vulnerability report, not including the repairing process?						
		Minutes	Hours	Days	Weeks	Total
Working years at the organization	0-2	4	4	4		12
	2-5	8	11	4		23
	5-10	3	7	3		13
	10-20	4	2			6
	20+	1			1	2
Total		20	24	11	1	56

4.2.2 The receivers' opinions about the vulnerability handling process

The receivers of the reports were asked about their general opinion on the importance of bug reports. The vast majority, 70,1%, thought that there probably are security bugs in their products, and they are important to be repaired for which reason bug reports are of great importance. 19,2% answered

that there probably are some security related bugs in their software that are important to be identified. 5,2% of the receivers answered that there are hardly any security related bugs in their products, for which reason bug reports are of marginal importance. 5,2% responded that there are security related bugs in their products, but it is not very important to get them fixed, for which reason bug reports are of marginal importance.

As with reporters, also receivers of the reports agreed that the right way of doing the reporting is publishing some part of the information after a predetermined time. This can be seen from Figure 7. It presents the mean values of the responses on a Likert scale given to the questions that were formed to analyze the suitable level of publicity.

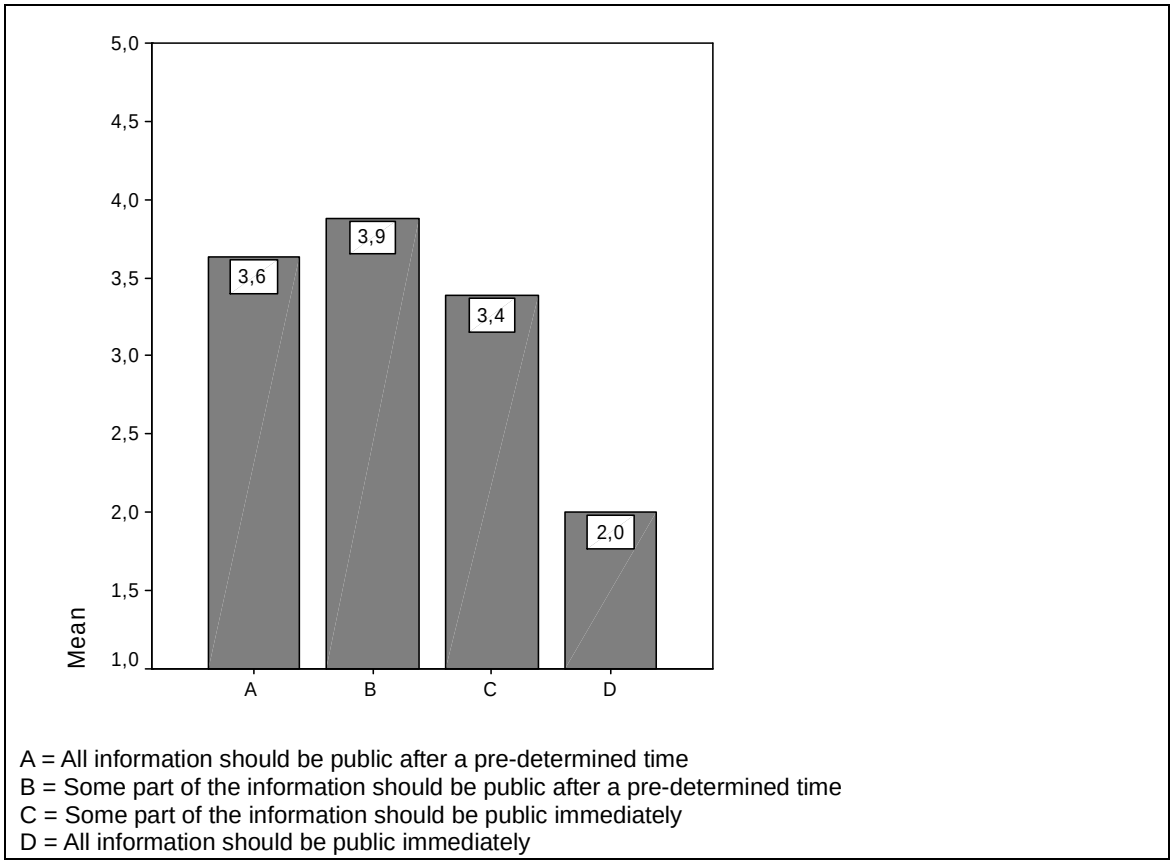


FIGURE 7: The suitable level of publicity according to the receivers (Likert scale, mean values)

When compared to the reporters, whose opinions about the propositions were presented in Figure 3, the receivers are very critical towards publishing all the

information. The mean value on the Likert scale of the reporters' answers for proposition A (All information should be public after a pre-determined time) is 4,2, but is only 3,6 for receivers. The receivers support the most publishing only some part of the information after a pre-defined time. The mean value on the Likert scale for this proposition is 3,9, which indicates relatively high support for the proposition. Receivers also seem to be more sceptic towards publishing all information about the found vulnerabilities immediately than reporters. The mean value of the receivers' answers on the Likert scale is 2,0, and for the reporters' answers 2,6. This is analyzed in more detail below.

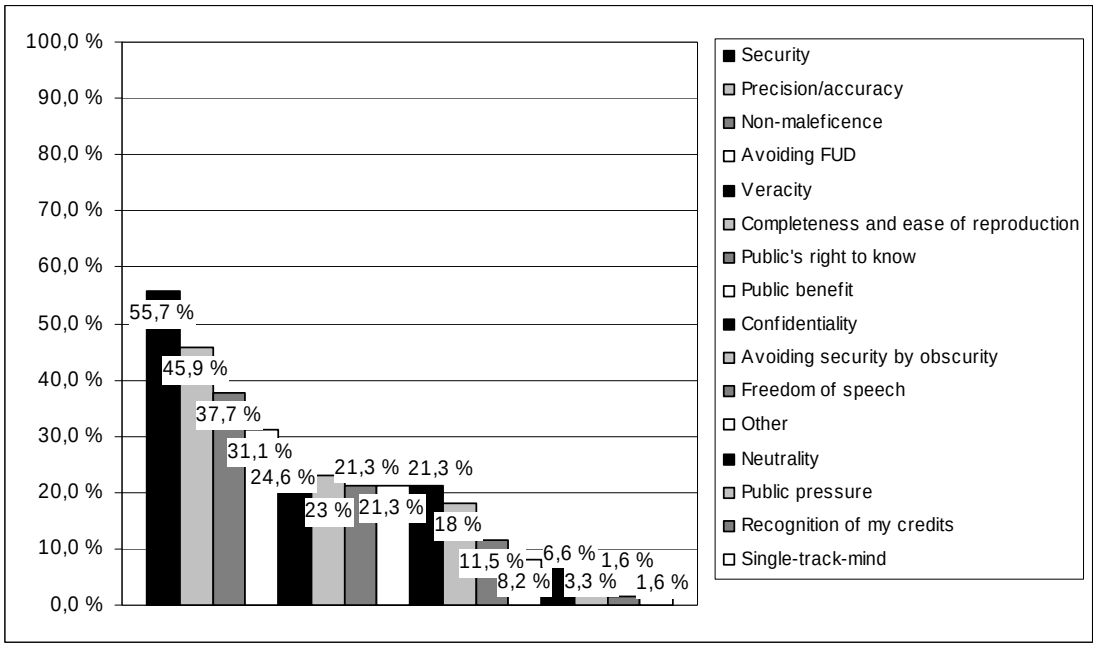
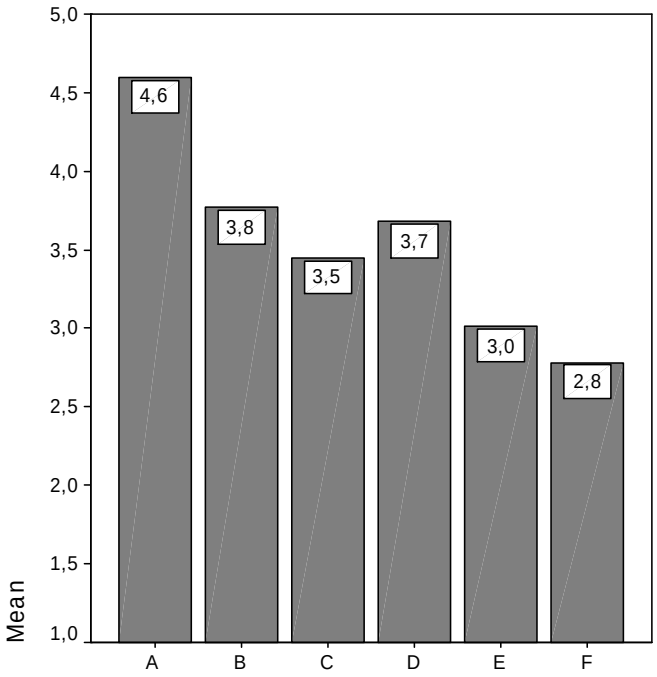


FIGURE 8: Values and beliefs related to the vulnerability handling process according to the receivers (percentages of the choices compared to the amount of the respondents)

Also the receivers of the reports were asked which values or beliefs guide their decisions related to vulnerabilities the most. The percentages of the choices of the receivers can be seen in Figure 8. The responses of the receivers were more evenly distributed than the responses of the reporters. However, as with reporters, also receivers value security the most. Precision and accuracy are also important to many, as it was to reporters as well. Public benefit and the public's right to know seem to be more typically important to reporters than to receivers

of reports. Avoiding fear, uncertainty, and doubt and non-maleficence seem however to be very important to the receivers.

Figure 9 gathers the mean values calculated from values on the Likert scale given by the receivers to propositions that sought to analyze knowledge activities of the organizations. Receivers seem to give more value to meetings and team work than the reporters and their opinion about electronic bulletin boards or chat channels is more skeptic than the opinion of the reporters. The mean value on the Likert scale of the answers related to traditional communication forms like internal magazines remains below a "neutral view" (3), as was the case with reporters as well. The possible differences between the two groups are handled in more detail below.



A = It is highly important that communication about vulnerabilities inside the team is open and trustworthy
B = Intranet and bug databases are efficient means for knowledge sharing about vulnerabilities
C = Planned meetings about each vulnerability are very important for knowledge sharing
D = Cross-functional project teams are important
E = Electronic bulleting boards or chat channels are an efficient way to communicate about vulnerabilities
F = Internal magazines, newsletters or bulletins distribute knowledge about vulnerabilities efficiently

FIGURE 9: Knowledge activities (Likert scale, mean values)

The reporters and the receivers of the report were both asked for their opinion about the minimum level of response to the reporter of a software vulnerability. 33,3% of the receivers agreed with the reporters that the priorisation of the report in their vulnerability handling process should be informed. 12,3% of the receivers thought that communication with the reporter is not necessary or slows down the actual repairing process unnecessarily. 28% responded that a simple acknowledgement about the reception of the report is enough. 26,3% responded that also the repairer of the flaw, not just the receiver of the report, should contact the reporter.

The majority (57,4%) of the receivers of the reports responded that their organization consults with the reporter about the importance of the vulnerability before determining what mitigation steps, if any, should be taken. A little less than half of the respondents (43,9%) answered that their organization does not do that. 10,5% of the receivers did not have knowledge about the issue.

The majority (55,7%) of the receivers of the reports agreed that according to them the vulnerability handling process has been well arranged in their organization. 44,3% of them either did not have an opinion or disagreed with the claim.

4.2.3 The receivers' opinions about the communication network

The communication network and CERT's role according to the receivers of the reports were analyzed in the same way as the opinions of the reporters. The questions 27-29, 34-35, 37.1 and 37.2 in the questionnaire for receivers (Appendix 4) handled the receivers' opinions about the communication network. The analysis was completed with the help of factor analysis of the responses to these questions. First, a KMO and Bartlett's test of sphericity were completed to make sure that factor analysis was possible to be done with this material. The score of the Kaiser-Meyer-Olkin Measure of Sampling Adequacy

was 0,524, which means that the test can be done. Also the Bartlett's test value was acceptable.

The results were rotated with varimax/Kaiser normalization. The values of the analysis after the rotation can be seen in Table 3. The first two variables correlate with component 1. The next three variables correlate strongly with component 2. The last two variables correlate with component 3.

TABLE 3: Results of the second factor analysis

Rotated Component Matrix			
	1	2	3
All information should be found and handled only inside the two organizations (reporter/receiver)	**,869**	-9,976E-02	-3,815E-03
Only selected persons outside the organizations should be informed when an error is found	**,835**	-8,457E-02	,112
In my opinion, the reporter should get the chance to evaluate the advisory issued by vendors and independent CERTs?	-5,587E-02	**,911**	-5,033E-03
In my opinion, the reporter, the coordinator, and the receiver of the report should have regular discussions about the vulnerability after it has been reported?	-,196	**,895**	-,180
It would be easier and more useful to communicate directly with the reporter than with an external party	-4,946E-02	**,114**	-,698
An independent third party like a national CERT is a useful help in the communication process	,379	,101	**,684**
Our organization is dependent on its contacts to other organizations	-,249	2,939E-03	**,622**

Hence it can be noted that these seven variables can be reduced to three new components, which are the same as in the first factor analysis with the reporters' responses. These were called 1) restricted information transmission in the network, 2) open information transmission in the network, and 3) the amount of network dependence/trust.

4.2.4 The receivers' relationship with publicity

Receivers of the reports seemed to be somewhat more critical towards publicity than the reporters. Only 22,6% of them responded that to their organization media is an important and equal discussion partner. 54,7% saw publicity

important but think that it must be kept in their own hands. They inform the media actively. 20,7% thought that publicity usually harms their organization, and that if possible it should be avoided. 1,8% thought that publicity does nothing but harm, and that they must try to influence the media as effectively as possible.

The receivers were also asked, whether their organization has a formulated, proactive publicity strategy for the case of a publicity crisis concerning vulnerabilities. 56,7% of the respondents answered that their organization does not have one. 26,7% of the organizations have this kind of publicity strategy, and 16,7% of the respondents did not have information about the issue.

60% of the receivers' organizations does not have PR-personnel that is familiar with vulnerability issues and has direct contacts to the media. 31,7% of the organizations have one, according to the respondents. 8,3% of the respondents did not have information about the issue.

4.3 Comparison of the reporters' and receivers' answers

In this chapter similarities and differences in opinions and reporting procedures related to the vulnerability reporting process between the reporters and receivers are presented. The comparison was completed with χ^2-tests and Mann-Whitney U-tests. The choice between these two was made according to the nature of the data. χ^2-tests were used for nominal data and Mann-Whitney U-tests for at least ordinal data and for the analysis of the results of the factor analyses.

4.3.1 The reporting process

The most common communication channel in issues related to vulnerability reporting is email. To investigate how many percent of the respondents use

email in some form (encrypted or unencrypted), the answers given to these options were summed together. It was noticed that 62,2,% of the reporters use either encrypted or unencrypted email for vulnerability reporting. 26,5% of the reporters use both forms of email. Also for the receivers of the vulnerability reports email is the most common communication channel. 43,3% of them get vulnerability reports in one of the email types, and 38,3% receive vulnerability reports in both forms of email

Also the answers that told that the respondents use totally public communication channels were summed together. These include public mailing lists and discussion forums. It was noticed that 74,5% of the reporters do not use totally public reporting channels. 24,5% of them use either public mailing lists or public discussion forums on the WWW at least occasionally. 1% uses both totally public reporting forums. 35% of the receivers do not get vulnerability information through these public communication channels. 30% of them get vulnerability information through one of these channels and 35% through both of them.

The experience of the organizations and the respondents in the reporting process were compared with χ^2-tests. The conclusion was that the receivers who answered to the survey, and also their organizations, were more experienced than the reporters or their organization. The cross-tabulation of the comparison of the respondents' personal experience is presented in Table 4. According to the χ^2-tests the difference between both the experience of the organizations and the experiences of the respondents were statistically very significant. The p-values for both were .000.

TABLE 4: The personal experience of the respondents in the vulnerability process, the number of times the respondents have received/reported a vulnerability, cross-tabulation and the results of the χ^2-test

	Never	1	2-4	5-9	10-49	50-99	100 or more	Total
Receivers	5	4	9	6	8	1	27	60
Reporters	5	7	28	19	26	4	8	97
	10	11	37	25	34	5	35	157

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	32,038	6	,000

4 cells (28,6%) have an expected count less than 5. The minimum expected count is 1,91.

It is more common for receivers of the reports to have a recognized or advertised point of contact for vulnerability issues than it is for reporters. Approximately two thirds of the receiving organizations and half of the reporting organizations answered to have one. The difference was statistically nearly significant. The p-value received from the χ^2-test was .032.

Figure 10 presents the percentages that were calculated from the reporters' and receivers' answers about the sources and communication partners that they use in the reporting process. Thus, the vulnerability information flows and directions of these can be seen.

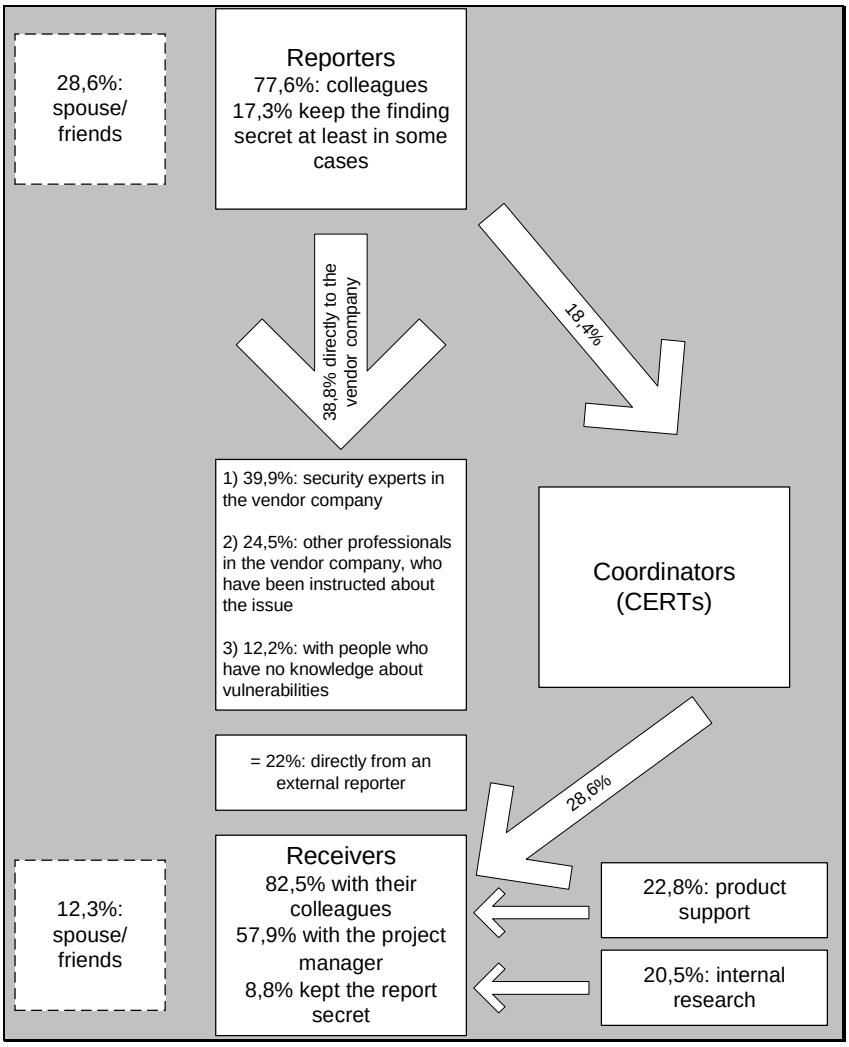


FIGURE 10: The vulnerability information flows and their directions

The majority of both the receivers and reporters communicate about vulnerabilities inside their own working group. 38,8% of the reporters send information about vulnerabilities directly to the vendor company. 39,9% of these reporters answered that they talk directly with security experts in the vendor company. 24,5% of the reporters who send information directly to the vendor company are in contact with other professionals of the vendor company who have been instructed about the issue but are not security experts. 12,2% of the reporters who send information directly to the vendor company communicate with people who have no previous knowledge about vulnerabilities. 22% of the receivers answered that they at least in some cases receive information about the vulnerabilities directly from the reporter. The

most common source of vulnerability information for the receivers were coordinators.

The difference between the answers to the question whether the respondents talked about the vulnerabilities with their spouse and/or some friends were compared with an χ^2-test. It was noticed that the reporters talk about these issues more often with their spouse and/or some friends and the result was statistically significant. The p-value of the test was .002. These results can be seen from Table 5.

TABLE 5: Cross-tabulation and the χ^2-test of the results to the question whether or not the respondents talk about vulnerabilities with their spouse and/or some friends

	No	Yes	
receivers	52	8	60
reporters	62	35	97
	114	43	157

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9,647	1	,002
N of Valid Cases	157		

The answers given to the question "Who/what defines how the reporting should be done?" were compared with the χ^2-test. According to the results the receivers have a more standardized procedure. The p-value of the test was .002. They have more often at least an internal reporting policy than the reporters do. The reporters do not have a standardized policy as often, and even if they have it is a non-written or internal one and thus is not available to people who are not members of the organization in question. The cross-tabulation of the results is presented in Table 6.

TABLE 6: The comparison of the usage of different reporting policies in the organizations (cross-tabulation)

	We have a public reporting policy	We have an internal reporting policy	We have a non-written reporting policy	There is no standard way - depends on the situation	It is up to the reporter to determine the best way	Other	Total
receivers	10	15	2	20	7	4	58
reporters	6	10	15	32	27	7	97
Total	16	25	17	52	34	11	155

There was also a statistically significant difference between the receivers' and reporters' conception about how often receivers contact reporters after having received a vulnerability report. The receivers think that they contact the reporters more often than the reporters think that they are contacted. The result was achieved by comparing the two questions with an χ^2-test. The p-value received from the test was .002.

4.3.2 Comparison of the opinions about the reporting process

Receivers' and reporters' opinions about the extent of the disclosure were analyzed with Mann-Whitney U-tests. A statistically significant difference between the two groups in how they see publishing all the information about the vulnerabilities was detected. According to the reporters all information related to software vulnerabilities should be public at least after a predefined time. The reporters also think more often than receivers that all information should be public immediately, even though they also were pretty skeptic towards this issue. The receivers disagreed with both of these statements. The test statistics for the questions related to the extent of the disclosure can be seen in Table 7. The p-values that were calculated with the Mann-Whitney U-test can be seen from the last row of the table (Asymp. Sig). It can be seen that the p-values for both questions that concern publishing all known information indicate statistical significance.

TABLE 7: Test statistics, Mann-Whitney U-test, Questions related to the extent of the disclosure

	Some part of the information should be public after a pre-determined time	All information should be public after a pre-determined time	Some part of the information should be public immediately	All information should be public immediately
Mann-Whitney U	2453,500	2191,000	2886,500	2229,500
Wilcoxon W	4283,500	4021,000	7639,500	4059,500
Z	-1,760	-2,801	-,087	-2,553
Asymp. Sig. (2-tailed)	,078	,005	,930	,011

Grouping Variable: receivers/reporters

Otherwise the two groups were in agreement with each other about the right procedure. Thus, both the receivers and the reporters thought that some part of the information could at least in some cases be published after a pre-determined time. The reporters regarded the issue more positively than the receivers as in the case when it was asked about publishing all the information after a pre-determined time, but the difference between the opinions was not statistically significant. Both the receivers and the reporters had a pretty neutral view towards the statement that some part of the information should be public immediately. This refers to agreement about the necessity of publishing some part of the information at least in some cases.

The receivers and reporters agreed with each other that the minimum level of response to the reporter is that the receiver informs the reporter about the priorisation of the report inside the receiver organization. Many of both the receivers and reporters also thought that a simple acknowledgement that the report has been received would be enough.

The answers given to the question in which the respondents were asked to name the three values or beliefs that guide one's decisions about security vulnerability information were analyzed with an χ^2-test. A statistically significant difference in how the two groups see public benefit and the public's right to know was discovered. The p-value for the first was .002 and for the

second .004. These two things were named to belong to the three most important values by the reporters more often than by the receivers of the reports. The views of valuing recognition of the respondents' own credits also differ between the two groups. The p-value for the question was 0.039, which indicates that the difference is statistically nearly significant. The reporters value recognition of their own credits more that the receivers, even though this was not specifically common for them either. 10 of the 97 reporters said that this thing belongs to the three most important values to them, but only one receiver agreed with the statement. Avoiding fear, uncertainty and doubt was more important to the receivers than the reporters. The p-value for the comparison of the results was 0.03. In other cases the two groups were in agreement with each other about which things are important. To these belong above all security, precision and accuracy, and non-maleficence.

Opinions about knowledge activities were analyzed with a Mann-Whitney U-test. It was noticed, that the views about intranet and bug databases as well as about cross-functional project teams of the two groups differ from each other. The reporters see more often that intranet and bug databases are important in knowledge distribution, but the receivers value cross-functional project teams more often. Both groups think that internal magazines, newsletters or bulletins are not a specifically good way to distribute knowledge about the vulnerabilities. The results of the Mann-Whitney U-test are represented in Table 8. The p-values can be seen from the last row of Table 8.

TABLE 8: Test statistics, Mann-Whitney U-test, Knowledge activities

	Planned meetings about each vulnerability are very important for knowledge sharing (q49)	Intranet and bug database are efficient means for knowledge sharing about vulnerabilities	Electronic bulletin boards or chat channels are an efficient way to communicate about vulnerabilities	Cross-functional project teams are an important aid in communication	Internal magazines, newsletters or bulletins of our organization distribute knowledge about vulnerabilities efficiently
Mann-Whitney U	2723,000	2393,000	2494,000	2299,500	2670,500
Wilcoxon W	7476,000	4223,000	4324,000	7052,500	4500,500
Z	-,704	-1,997	-1,553	-2,406	-,900
Asymp. Sig. (2-tailed)	,482	,046	,121	,016	,368

Grouping Variable: receivers/reporters

4.3.3 Comparison of the opinions about the communication network

The factor analysis was completed once more with all the answers together, i.e., both the receivers' and the reporters' answers were analyzed at the same time. The results of this third factor analysis are presented in Table 9.

TABLE 9: The third factor analysis, reporters' and receivers' answers analyzed together

Rotated Component Matrix	**Component**		
	1	2	3
All information should be found and handled only inside the two organizations (reporter/receiver)	**,882**	4,276E-02	-5,123E-02
Only selected persons outside the organizations should be informed when an error is found	**,862**	,118	-8,646E-02
In my opinion, the reporter should get the chance to evaluate the advisory issued by vendors and independent CERTs?	-2,759E-02	**,859**	-7,150E-02
In my opinion, the reporter, the coordinator, and the receiver of the report should have regular discussions about the vulnerability after it has been reported?	-,106	**,843**	-5,903E-02
It would be easier and more useful to communicate directly with the reporter than with an external party	7,089E-02	2,805E-02	-,728
An independent third party like a national CERT is a useful help in the communication process	,112	3,000E-02	**,767**
Our organization is dependent on its contacts to other organizations	9,943E-02	-,105	**,657**

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 4 iterations.

It can be noticed that this time the statement "It would be easier and more useful to communicate directly with the reporter than with an external party" does not correlate with any of the other claims. It however correlates negatively with the statements that were called to form the new factor number 3 (the amount of network dependence/trust). This is also contentually reasonable, because this statement can be seen as the opposite to dependence and trust in the network. The other two new factors remain the same. Thus, the new factors called 1) restricted information transmission in the network, 2) open information transmission in the network, and 3) the amount of network dependence/trust in the network can be compared to each other when the statement mentioned above has been removed from the analysis.

The comparison of the answers of the two groups, the receivers and the reporters, to these new factors was completed with a Mann-Whitney U-test. The results of the test can be seen in Table 10.

TABLE 10: Mann-Whitney U-test of the values of the new factors

	factor1	factor2	factor3
Mann-Whitney U	9775,000	10285,500	8538,000
Wilcoxon W	28690,000	17545,500	27453,000
Z	-2,452	-1,813	-4,096
Asymp. Sig. (2-tailed)	,014	,070	,000

Grouping Variable: receivers/ reporters

The most significant difference between the two groups is in the third factor, i.e. in how the respondents' see trust and dependence on the communication network. The p-value of this result indicates that the result is statistically very significant. Also the answers that were given to questions which form the first factor differ from each other. The result is statistically almost significant.

To compare the new factors information about the basic statistics for both groups is still needed. This information is presented in Table 11, from which the group values of the each factor can be seen.

TABLE 11: Statistics of the three factors

	Factor 1, receivers, restricted information transmission	Factor 2, receivers, open information transmission	Factor 3, receivers, network dependence/ trust	Factor 1, reporters, restricted information transmission	Factor 2, reporters, open information transmission	Factor 3, reporters, network dependence/ trust
N	120	120	120	194	194	194
Mean	3,53	2,93	3,81	2,58	3,72	3,21
Median	4,00	3,00	4,00	2,00	4,00	3,00
Mode	3	4	4	2	4	3
Std. Deviation	,934	1,193	,990	1,224	1,015	1,178

4.3.4 The two groups' relationship with publicity

Finally, the answers that the two groups gave to the last question in the questionnaire ("How, in your opinion does your organization view publicity related to software vulnerabilities?") were analyzed with an χ^2-test. It was noticed that the receivers' and the reporters' conceptions about their organizations' relationship with publicity do not differ from each other significantly. The p-value for the χ^2-test was .107. Both the receivers and the reporters of the reports see publicity to be important and think that the organization has to inform the media actively. In other words, the majority of the respondents does not see the media as an equal discussion partner, even though this view is quite popular too. Hostility towards publicity is not very common among the respondents. The cross-tabulation of the responses to this question can be seen in Table 12, from which it can be concluded that the frequencies of the answers are highest in both groups to the proposition "Publicity is important, we inform the media actively". The sum of the answers of the two groups to this proposition is 73, which is 46% of the total amount of answers. The answers given to the last proposition ("Media is an important and equal discussion partner") form 28% of the total answers. The two other propositions are less supported in the respondent groups.

TABLE 12: The opinions of the respondents about how their organization views publicity related to software vulnerabilities, cross-tabulation

	Publicity does nothing but harm, we must try to influence it	Publicity usually harms us, it should be avoided	Publicity is important, we inform the media actively	The media is an important and equal discussion partner	Total
receivers	1	11	35	13	60
reporters	5	22	38	32	97
Total	6	33	73	45	157

5 Discussion

In this chapter the issues presented in the theoretical background are related to the results. Also an evaluation about the study is presented and the reliability and validity of the research are discussed. Finally some topics for possible further research are presented.

5.1 The software vulnerability communication process, information transmission, and knowledge management

In this chapter the answer to the first research question, how the communication of the vulnerabilities is organized in practice, is sought. It is also discussed, how knowledge management is handled in both the reporters' and receivers' organizations.

5.1.1 The communication process and the communication network

In the present study communication was seen as an information interpretation and publication process through interaction in a network. The various characteristics of this specific network are presented in this chapter.

The most common communication channel in the software vulnerability reporting process is email. This was the case both for the reporters and receivers of the reports. Email usage tells about the nature of the communication network. Communication between the links in the network is electronically mediated. The answers given to questions that sought to analyze the respondents' knowledge activities also told about the preference of electronically mediated communication. This was especially typical to the reporters.

In Chapter 2.2 Juholin's categorization of paradigms that influence organizational communication was presented. The preconception was that there might be a difference between the receiving and reporting organizations' communication paradigms. This seems actually to be the case, but the interpretation must be evaluated with care. The theoretical concepts of communication paradigms form an interesting view on the issue, but the conclusions about the paradigms in the vulnerability scene would need more thorough data. However, when this is taken into account, some tentative conclusions can be made. The receivers of the reports seem to have more faith in the reporting network, and be more dependent on it than the reporters. They also typically support restricted information transmission, have more often a reporting policy and think more often that only some part of the information should be published. These things indicate a functional communication paradigm. According to the receivers of the reports the information transmission should be codified and organized. On the other hand, the reporters seem to value a more dissipative paradigm of communication. Reporting policies are not as common as for the receivers, and the reporters seem more often to do the reporting without prior planning. They also discuss about the issues with outsiders more often than the receivers. Communication seems to be more dynamic and creative than for the receivers. Dynamics and creativeness are typical characteristics of a dissipative communication paradigm. Meanwhile, the dialogic paradigm of communication does not have a big part in the reporting process. The respondents think that the participants should have regular discussions about vulnerabilities, but this is quite seldom the case in reality. Even getting some kind of response to the report may be hard. Communality is not a characteristic for the vulnerability reporting process.

As noted above, according to Dozier, Grunig & Grunig (1995, 13) a win-win relationship can be developed with symmetrical two-way communication. However, in software vulnerability communication the flow of information seems relatively often to be one-way. In the author's opinion communication in the software vulnerability reporting process requires the usage of two-way

symmetrical communication, because with two-way symmetrical communication organizational learning can be possible. The wide usage of one-way communication can be noticed for example from the fact that getting a response to a report may be difficult. Even if the receiver would give a response to the reporter, a dialog between the two parties is not necessarily the standard procedure.

The structure of the software vulnerability reporting network can be analyzed by considering its size, centrality and density. It was stated above that the size of the network may vary remarkably from case to case. However, it seems obvious that centrality, the extent to which individuals have access to one another, needs more development in the software vulnerability reporting process. Meanwhile, the density of the network, the ratio of actual links to possible links, seems to be acceptable. The people, who are possible to be reached, also are reached.

As stated above, Stohl (1995, 35) divides link types in a communication network into four groups according to the type of resources received from the link, which are the affective network, power network, informative network, and goods and services network. These link types were evaluated in the survey by asking the recipients the type of information that they get related to the software vulnerabilities and the source of that information. It was discovered that the reporters primarily find the information about vulnerabilities personally. They communicate about their findings first with their own colleagues (77,6% of the respondents) and report it to either an independent third party like a national CERT (18,4%) or directly to the vendor company. Hence, it can be noticed that the reporters form informative communication networks. They analyze the cases with their colleagues and obtain cognitive information through this communication. This cognitive information is distributed wider to the whole network. However, it can also be seen that the reporters offer instrumental resources to the receivers of the reports, and thus, they form a power network link.

Links can also be divided into different groups according to their location and role within larger network configurations. In the software vulnerability reporting process the various links can be divided into the six network roles presented by Kreps (1990, 223-224) as follows. The role of the coordination centers can be seen as one of the liaisons in the network. They connect cliques in the system without belonging to them. The reporters can be seen as a kinds of opinion leaders. They influence decisions and guide others' behavior, but do not have formal authority. Both the reporters and the coordination centers can also be seen as gatekeepers, that control the message flow. The receiver's role is more difficult to evaluate with the help of Kreps' classification. The best role in which they can be classified is cosmopolites who connect the organization to its environment.

As stated above, Benson (1975, 229) described communication in a network as a political economy, in which organizations get and give scarce resources and by doing that create systems of power relations. This theory was developed further by Pfeffer and Salancik, which leads to the resource dependency theory. In the software vulnerability reporting process the receivers of the reports see their dependence on the network to be deeper than the reporters. The information received from the reporters is seen as valuable and their trust in the communication network is relatively strong. The information that the reporters offer is important and thus the reporters form a powerful link in the communication process.

Often, the reporters can be seen as secondary stakeholders of the receivers in the present situation of the software vulnerability reporting process. They are interested in affecting the actions of the receiving organizations, but they do not have a concrete bond to them. Lehtonen (2002, 36) states that relationships to stakeholders can develop from a monolog, through dialog to participative co-operation. All these actions are alternatives for handling the stakeholder relationships. A participative stakeholder strategy is, however, not very common. Organizations may think that listening to their stakeholders is a signal

of weakness or it may think that co-operation could lead to juridical obligations. (Lehtonen 2002, 22.)

In the software vulnerability reporting process the reporters' and receivers' stakeholder relationship could be classified as being somewhere between a monolog and a dialog. This conclusion can be made on the basis of the survey, in which it was discovered that the participants rarely have regular communication with each other. However, in the factor analyses made about the participants' opinions of open information transmission in the network, it was noticed that both the receivers and the reporters agreed that communication between all the parties should be more intensive. The mean value of the answers given to questions that formed factor 2 was 3,65.

Takanen, Raasakka, Laakso & Röning (2003, 27) have listed all the potential stakeholders in the software vulnerability process. According to their analysis, to these belong for example non-affiliated evaluators, home users, customer organizations, retailers, vendors, free-software developers, service providers, different governmental actors, CERTs (or similar), NGOs, the media, insurance organizations etc. This is an indication about the complexity of the whole vulnerability scene. A total analysis of the whole scene including all these stakeholders would be an interesting topic for further analysis.

5.1.2 Software vulnerability knowledge management

In Chapter 2.4.1 it was concluded that the knowledge creation process is an iterative process between knowledge production, mediation and application. This is also the case in the vulnerability reporting process, in which the reporters produce knowledge about the vulnerabilities, and mediate it to the vendors, who apply the knowledge in the way they find most appropriate. All the parts of this iterative process are essential to the effective distribution of vulnerability information. In this chapter the knowledge management process is discussed.

As stated above, people have both procedural and content knowledge. These two types of knowledge help people to act in the right way in a specific context. Routines are developed, when a person learns the procedure that helps them to act correctly. It was stated that experience in vulnerability reporting will probably make the reporting easier. A comparison of the working years and the time used per vulnerability by the receivers can be seen as an indication about this issue. In the analysis it was noticed that there actually is a statistical interdependence between these two things. This also indicates that in the software vulnerability reporting process some routines are developed. This result must however be interpreted with care, because there were only 56 valid answers that could be used for this particular analysis.

In Chapter 2.5.1 the different knowledge types were classified into four groups: know-what, know-why, know-how and know-who. The first two of these are content knowledge, and the next two procedural knowledge. In the software vulnerability reporting process especially procedural knowledge, know-how and know-who, seems to need development. This can be seen for example from the fact that 62,3% of the reporters told that they find the right contact persons without problems at most frequently. Thus, the know-who -knowledge is not very good. In the survey only 8,2% of the reporters told that for finding the right contact persons they use an independent third party, like a national CERT. Actors, such as CERT, could provide the potential to be utilized more efficiently in the communication network.

An important thing to be taken into consideration is that knowledge is more easily shared if it is codified. Tacit knowledge is more difficult to distribute forward inside the organization. This has also been noticed in the organizations. Up to 76% of the reporting organizations and 71,9% of the receiving organizations keep a record of vulnerabilities and their patches. Policies can also be seen as a way of codifying information. This should be taken into account in the organizations that take part in the reporting process. At the

moment policies are more common in receiving organizations. Policies are also a way to improve procedural knowledge in the organization.

According to the SECI theory developed by Nonaka and Takeuchi (1995) organizational learning is based on a knowledge conversion that happens in four stages: socialization, externalization, combination and internalization. In the software vulnerability reporting process these stages can also be noticed, and in this case the learning process is described as interorganizational learning. The socialization stage is the stage in which knowledge is still tacit. This refers to the phase when the communication participants figure out what the issue is all about inside their own working group. The externalization phase is the stage during which the information is distributed to the vendor. The combination phase is the evaluation phase in the vendor company. The information is compared to the knowledge the vendor has about its products and its significance is evaluated. In the internalization phase the information is embodied in the tacit knowledge, which means in practice the distribution of the knowledge to the software developers in the vendor company.

The survey made it clear, that the combination stage inside the receiving organizations is essential. More than half of the respondents (51,8%) told that of all the reports their organization had received during the last 12 months less than 20% were valid. This underlines the essentiality of the receiving organizations learning process and knowledge management. On the other hand this fact rises the question of a more intensive dialog between the reporters and the receivers. There is an obvious need for a dialogical connection between the potential participants for the development of the communication process.

The internalization of the information was also evaluated in the survey. The conclusion was that little over half (55%) of the receivers pass the information about discovered bugs to their software developers in order to prevent similar vulnerabilities in the future. 15% of the respondents pass the information to their software developers, but this information does not have an essential part

in the software development process. Thus, in these organizations the information is not internalized in the organization to create new knowledge.

In Chapter 2.4.2 the theories about the effect of beliefs, values, attitudes and concentration on information reception and processing were presented. It was concluded that one preconception related to the vulnerability reporting process is that the receivers may have a negative attitude towards finding software vulnerabilities, and that they do not necessarily see any value in supporting the development of the security. These preconceptions could not be proven on the basis of the survey. To the question about the values and beliefs of the respondents a great deal of the receivers answered that security is to them the most important value. On the other hand they did not see public benefit and the public's right to know about the vulnerabilities to be very important. The receivers valued more precision and accuracy as well as non-maleficence. This indicates that the receivers are interested in security, but for other reasons than the reporters. The attitudes toward software vulnerabilities can be seen to be somewhat different. Presenting the idea in a pointed way, it could be argued that the receivers seek to fulfill the expectations that their stakeholders have towards their products, and the reporters seek to gain security that is the best possible for the benefit of the public. From the basis of these conclusions it could be argued that the weight assigned to vulnerability information is high in both groups, but the valence is different. Thus, according to the information-integration theory the two groups accumulate and organize information about vulnerabilities in a somewhat different way and see the information negative in different contexts. As stated above, the attitudes may change as new learning occurs. This may result from information that disrupts the balance that the information has with previous attitudes. For example, the vendors may learn that the customers demand better security, and change their attitudes. The belief system concerning the vulnerabilities could be analyzed in more detail in future research.

In Chapter 2.4.2 also the basic concepts of the ELM theory (elaboration likelihood model) were presented. It was concluded that the likelihood of

critical interpretation of the content of a message depends on the way a person processes the information. It was stated that this phenomenon may have an effect on the vulnerability process because the receiver may not always process the message fully concentrated. This issue can not be concluded to be watertight from the basis of this survey. It is however interesting to notice that 35,1% of the respondents answered to be able to process a vulnerability report within some minutes from reception. This time frame does not give the receiver a possibility for an in-depth analysis of the information. However, to answer this question, a qualitative analysis of the reception procedure would be needed.

5.2 The concepts of crisis, trust, professional ethics and publicity in the software vulnerability reporting process

In this chapter the differences and similarities in reporters' and receivers' opinions related to different aspects of vulnerability reporting are analyzed. Hence, the second and third research questions, what kind of views people participating in the software vulnerability reporting process have about different aspects of it, and what differences are there in the way reporters and receivers of the reports see the reporting process, are answered.

Especially the answers given to question about the values and beliefs that guide the participants' decisions about software vulnerabilities are interesting. Also the issues related to the extent of the disclosure are discussed further.

5.2.1 Crisis and risk management in the vulnerability reporting process

Both receivers and reporters told that the most important value to them that guides their decisions related to the vulnerability process is security. It must however be noticed that the term security can in this context refer to two things: to the security of communication and to the security of the products that are

evaluated. For this reason it is obvious that most of the respondents answered to value security. However, it was also discovered that trust in the communication network is seen to be essential. Trust and security go hand in hand in the communication process.

The participants in the software vulnerability reporting process can prepare for the vulnerability reporting process by developing a policy for the situation. Surprisingly few of the participants have a crisis or risk management plan, such as a reporting policy. In the survey it was detected that nearly half of the receiving organizations but only one third of the reporting organizations had some kind of a reporting policy.

Policies are more common in receiving organizations, but still more than half of them are not prepared for a vulnerability report. Lehtonen (2000, 12) states that if an organization is prepared for a crisis situation there is a bigger chance that the situations never goes so far. He (2000, 67) also notes that if an organization is prepared for any crisis situation, it is easier to act in a crisis situation that was not expected.

In crisis communication theory it is traditionally recommended that a notification about the issue should be given to all people who are concerned with the issue in a short time frame. This is advised to be done even if all the necessary information about future actions is not available. The related parties should be told what is known at the moment and the necessary details should be given as soon as they are known. (Wilcox 2000, 181-182.)

However, the bug reporting process is a somewhat exceptional case. At the point in which the vulnerability is found, the most essential thing is to get it repaired, and the situation has not yet escalated to a crisis. The escalation is possible if information about the vulnerability is made public too early. For this reason software security professionals often oppose a full and public report that is written immediately after the vulnerability has been found. The consensus is to first inform only the vendor, giving the vendor enough time to develop the

patch and then publish the patch. After that it is possible to publish a full report if that is wanted. (Deline 2000.) In this way only a small circle of people knows about the vulnerability before it has been repaired. Keeping the information secret during this time is crucial.

5.2.2. The effect of trust and professional ethics in the process

The receivers and reporters seem to have a different view about the ethically right way to view software vulnerability reporting. This is an interesting phenomenon, because it indicates that the two groups are not unanimous about professionalism in the field. The field is very new compared to many other professions, which may be one reason why the common rules for the right procedure have not yet been fully developed. There is a need for an international codification of the rules that could help the disclosure policies.

In Chapter 2.7 the concepts of professional ethics, trust, and corporate social responsibility were presented. It was concluded that professionals posses and exercise legitimate authority when they actually promote general benefit. In the survey it was observed that the reporters value general benefit (public benefit and the public's right to know) about the issues to be more important than the receivers of the reports. Thus, the reporters' attitudes toward general benefit are more positive. They see their work to be useful for the whole society. The receivers see the issue to be important first and foremost for their company, and the company's role is to promote general benefit – it is not primarily their personal task.

It was stated that trust and risk go hand in hand. The potentiality of a crisis situation affects on communication. At the moment trust between the two parties is developed separately in every reporting process, again and again. Trust is not something that fundamentally belongs to the nature of the relationships. The reason for this is at least partially the lack of codification in the communication process.

In the context of vulnerability reporting an indication of corporate social responsibility is that the receiving organization seeks to eliminate the vulnerability as soon and effectively as possible. This is an expression to the environment that the receivers take responsibility for their actions. This was evaluated in the survey by asking the receivers how they react to the vulnerability reports. The conclusion was that only 13,3% of the receivers put the reports aside to wait for a suitable time to handle them. The rest of the respondents handle them in the priority order, interrupt other work immediately when they receive a report and concentrate on the repairing process, or have formed a specific schedule within which the reports are supposed to be handled. Thus, from the corporate social responsibility point of view, it can be argued that vulnerability reports are at least attempted to be handled fast and effectively in most of the receiving organizations, and that corporate social responsibility is managed effectively. However, it must be taken into consideration that the answers may also indicate pure reputation management.

On the basis of the factor analysis it was concluded that the opinions of the two groups about network dependence and trust differ significantly from each other. The receivers trust more in the communication network. They see CERTs more useful than the reporters and see that their organization is dependent on its contacts to other organizations in the network.

The vulnerability life-cycle was defined as the process from the finding of a vulnerability to its repair (Arbaugh et al. 2000, 53) in Chapter 2.1. However, it can be argued that the vulnerability life-cycle starts from the introduction of the vulnerability and ends with the elimination of it. This is a fundamental difference from the liability point of view. If it is seen that the vulnerability life-cycle starts at finding the vulnerability, the finder can be claimed to be responsible for it. If, however, the vulnerability life-cycle is seen to start at the point in which the vulnerability is created, the vendor is responsible for it. The

liability issues also effect trust in the communication network. This could be analyzed further in the future.

5.2.3 Publicity management and attitudes toward publicity

Publicity management is especially important for receiving organizations, because the vulnerability disclosures may have a negative effect on the receivers' public image. For this reason the receivers were asked in the survey about their publicity management procedures in more detail than the reporters, who, on the contrary, may see disclosures as a way to create fame. In Chapter 2.6 it was stated that according to Ikävalko (1996, 190) to be victorious in the "publicity game" the organization needs an articulated, proactive publicity strategy and trustworthy PR-personnel with direct contacts to the media. In the survey less than one third of the respondents from receiving organizations answered that they have a proactive publicity strategy for a case of publicity crisis concerning vulnerabilities. Approximately one third of them also answered that their organization has PR-personnel who are familiar with vulnerability issues and have direct contacts to the media. This seems to indicate that one third of the receiving organizations have prepared for publicity management related to vulnerability reports.

According to Lehtonen (2002, 6) in order to be successful in publicity management an organization has to take care of its stakeholder relationships, to show to its environment that it takes responsibility for its actions, and to follow the changes of its stakeholders' values and expectations and the public discussions. In the vulnerability reporting process the receivers' most important stakeholders are reporters. The relationship to them could, in the author's opinion, be handled better. This conclusion can be made from the basis of the fact that according to the survey the communication between the two groups is not especially open or conversational. Only one third of the receivers answered that they always contact the reporter after receiving the report. Of course also the reporters could promote communication with the receivers more, thus also

they could handle their stakeholder relationship to receivers better. As stated in the previous chapter, fast repair of the found vulnerabilities is essential if the company wants to manage its corporate social responsibility. Corporate social responsibility can be seen as a part of publicity management. Thus, it is the other side of the issue handled in this chapter. In order to manage the public image of the reporters, the reporters should above all handle the reporting in an ethical way. This is discussed in more detail below, where the publicity level of the reports are handled. In the survey it was not asked how the respondents follow the changes of their stakeholders' values and expectations, and public discussions. For this reason the last point can not be commented on in this context.

In the survey it was discovered that both the receivers and the reporters see publicity in most cases to be primarily positive. Typically, the communication with publicity is not dialogical. Most of the organizations seek to inform the media actively. However, also seeing the media as an important and equal discussion partner is relatively common. This was concluded from the basis of the last question in the survey. In the question it was analyzed, which of the four possible ways to react to publicity in a crisis situation the respondents would most probably use, thus, what kind of attitudes the respondents have towards publicity. It was noticed that when related to Fitzpatrick's and Rubin's grouping, in the vulnerability scene the most common strategies are the mixed strategy and the traditional public relations strategy.

Also the opinions about publicity and the extent of the disclosures were determined in the study. Overall, both the receivers and the reporters opposed immediate and full disclosure. The receivers' and reporters' opinions about both immediate full disclosure and first partial and afterwards full disclosure differed from each other. The receivers opposed full disclosure more than the reporters in its every form. The two groups agreed on publishing some part of the information after a predefined time. Partial disclosure is seen to be the ethically correct way to handle vulnerabilities. Also the factor analyses gave similar results. According to the analyses the reporters value open information

transmission in the network more than the receivers, and on the other hand, the receivers value restricted information transmission in the network more than the reporters.

Thus, publicity management related to the vulnerability reporting process has many interesting specialties compared to typical publicity management of an organization. Keeping things secret at least to some point is seen to be the ethically right way to handle the disclosure, which is not the way that publicity management is usually recommended to be handled. In this context it seems, however, to be the most secure and effective way.

5.3 Evaluation of the study

The validity of a study means that measuring instruments measure fully and accurately the constructs that they are claiming to measure (Smith 1988, 48). Frey et al. (2000, 109) divide validity into two groups: internal and external validity. Internal validity means that the conclusions drawn from a study are accurate. External validity indicates that the findings can be generalized to the whole population. A third group has in some cases been added to these two: conceptual validity. Conceptual validity means that the measurement is an empirical element of the theoretical concept being studied (Anderson 1987, 119).

Measurement validity can also be divided into three groups: 1) content validity, 2) criterion validity, and 3) construct validity (Frey et al. 2000, 116; Smith 1988, 48). A questionnaire possesses content validity if it measures the attributes (content) of the concept being investigated. Content validity can be tested a) by making sure that the measurement instrument at least intuitively reflects the construct (face validity) or b) in a panel approach where qualified people describe the aspects of that variable or agree that an instrument taps the concept being measured. Criterion validity exists if a measurement technique is shown to relate to another instrument already known to be valid. Construct validity is

the extent to which scores on a measurement instrument are related in logical ways to other measures. (Frey et al. 2000, 116-117.)

Reliability means that a measuring instrument is consistent and stable. A measuring instrument is reliable if a research is repeated and the results are the same. (Smith 1988, 46). Nevertheless, also consistent and stable measurements may contain errors. These can be divided into random errors and measurement errors. Random error is chance error due to uncontrolled factors and is assumed to equal out over time. Measurement error originates from faulty measurement procedures and is therefore more directly under the researcher's control. (Frey et al. 2000, 112.)

Reliability can be measured in many ways. The three most popular techniques are 1) the test-retest method, 2) the alternative-forms method, and 3) internal consistency methods. (Smith 1988, 47.) The test-retest method administers the same measurement procedure to the same group of people at different times. The consistency of the results is measured with a coefficient of stability. The method is considered reliable if this coefficient of stability is greater than 0.70. The alternative procedure method involves having the same people complete another, equivalent instrument. The scores on the two instruments are compared statistically. The result, a coefficient of equivalence, is the basis for making claims about the reliability of the first instrument. Measuring the internal consistency of a method means evaluating the extent to which different people answer consistently. (Frey et al. 2000, 113.)

In the present study the content validity of the questionnaire was examined through a panel discussion with the experts at OUSPG. The reliability was measured using internal consistency methods. This was done with a relatively small amount of answers that were gathered before the final answers. The first answers received from the survey seemed to give reasonable results. The weaknesses of the questionnaire were noticed later during the analysis.

The weaknesses of the study are the content validity of the questionnaire and the possibility to generalize the results. The amount of the answers was relatively small. For this reason the generalization of the results must be done with care. In the course of the analysis the author noticed that the content validity of the questionnaire could have been better. Thus, there were things detected that would have helped the analysis but that were not asked in the questionnaire. But, these are to be analyzed better in future research. Topics for future research are presented in the following chapter.

5.4 Possible issues for future study

This research gives many possibilities for future studies. During the research it was noticed how many-sided communication in the software vulnerability reporting process actually is. Each of the diverse sides of communication give opportunities to look at the issue in more detail. Interesting viewpoints would be for example to conduct qualitative research by making a group/personal interview to get deeper understanding about the opinions of the participants of the reporting process. A comparison of existing company documents, for example existing reporting policies, would also give an interesting point of view to the issue. A wider perspective would be of great interest: how does the information or knowledge about computer security influence the behavior of computer users. Overall, while this research was based on a self-report measurement practice, the results must be related to the fact that they are people's opinions about the issue. An observation about the vulnerability reporting process could give many new points of view to the analysis.

The software vulnerability reporting process is a complicated and interesting phenomenon from the perspective of communication research. Because the research field is new and pioneering, the challenge for studying it is great.

References

Anderson , J. A. 1987. Communication Research. Issues and Methods. New York: McGraw-Hill.

Arbaugh, W. A., Fitchen, W. L. & McHugh, J. 2000. Windows of vulnerability. A Case Study Analysis. IEEE Computer. Vol. 33, No. 12. Available in www-form: http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf [Accessed 11th November 2002]

Argyris, C. & Schön, D. A. 1978. Organizational learning. A theory of action perspective. Reading, Massachusetts: Addison-Wesley.

Black, T. R. 1999. Doing Quantitative Research in the Social Sciences. An Integrated Approach to Research Design, Measurement and Statistics. London: Sage Publications Ltd.

Benson, J. K. 1975. The Interorganizational Network as a Political Economy. Administrative Science Quarterly 20/2: 229-249.

Culp, S. 2001. It's Time to End Information Anarchy. Microsoft Technet Newsletter. Available in www-form: http://www.microsoft.com/technet/columns/security/noarch.asp. [Accessed: 5th March 2003]

Deline, B. 2000. Full disclosure. SANS Institute - Information Security Reading Room. Available in www-form: http://www.sans.org/infosecFAQ/hackers/disclosure.htm. [Accessed: 11th November 2002]

Doney, P.M., Cannon, J.P. & Mullen, M.R. 1998. Understanding the influence of national culture on the development of trust. Academy of Management Review, 23/3: 601-620.

Dozier, D.M., Grunig, L. A. & Grunig, J. E. 1995. Manager's guide to excellence in public relations and communication management. New Jersey: Lawrence Erlbaum Associates Inc.

Fitzpatrick, K. R. & Rubin, M. S. 1995. Public relations vs. legal strategies in organizational crisis decisions. Public Relations Review 21/1: 21-34.

Frey, L.R., Botan, C. H. & Kreps, G.L. 2000. Investigating Communication. An Introduction to Research Methods. Needham Heights: A Pearson Education Company.

Greene, J. O. & Geddes, D. 1993. An Action Assembly Perspective on Social Skill. Communication Theory 3/1993: 26-49.

Gordon, S. & Ford, R. 2000. When the Worlds Collide. Information Sharing for the Security and Antivirus Communities. Brussels: EICAR 2000 Best Paper Proceedings, 1-20.

Hargreaves, D. 2000. The Production, Mediation and Use of Knowledge in Different Sectors. In: Knowledge Management in the Learning Society. 2000, 37-66. Paris: OECD (Organization for Economic Co-operation and Development).

Harryson, S. J. 2000. Managing Know-Who Based Companies. A Multinetworked Approach to Knowledge and Information Management. Cheltenham: Edward Elgar Publishing Limited.

Ikävalko, E. 1996. Ylivoimapeli mediassa. Julkisuusmekanismit ja julkisuuden hallinta. Helsinki: Inforviestintä Oy.

Juholin, E. 1999. Paradise lost or regained? The meanings and perceptions of organizational communication of 1990's in Finnish work organizations. Helsinki: Inforviestintä Oy.

Karma, K. & Komulainen, E. 2002. Käyttäytymistieteiden tilastomenetelmien jatkokurssi. Helsinki: Helsingin yliopisto. Available in www-form: http://www.edu.helsinki.fi/oppimateriaalit/ktj.htm [Accessed: 21th January 2002]

Koehn, D. 1994. The Ground of Professional Ethics. London: Routledge.

Kitchen, P. J. 1999. Marketing Communications. Principles and Practice. London: International Thomson Business Press.

Kreps, G.. L. 1990. Organizational Communication. Theory and Practice. London: Longman Group Ltd.

Laakso, M., Takanen, A. & Röning, J. 1999. The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases. In the proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response. Brisbane. 13th to 18th June 1999. Available in www-form: http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST1999-process/ [Accessed: 11th November 2002]

Lehtonen, J. 1999. Kriisiviestintä. Helsinki: Mainostajien liitto.

Lehtonen, J. 2002. Julkisuuden riskit. Helsinki: Mainostajien liitto.

Littlejohn, S. W. 1996. Theories of Human Communication. Belmont: Wadsworth Publishing Company.

Lundvall. B. Å. 2000. Understanding the Role of Education in the Learning Economy. The Contribution of Economics. In: Knowledge Management in the

Learning Society. 2000, 11-35. Paris: OECD (Organization for Economic Co-operation and Development).

Niiniluoto, I. 1992. Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi. Helsinki: Valtion painatuskeskus.

Nonaka, I. & Takeuchi, H. 1995. The Knowledge-Creating Company. How Japanese Create the Dynamics of Innovation. Oxford: Oxford University Press.

Nummenmaa, T., Konttinen, R., Kuusinen, J. & Leskinen, E. 1997. Tutkimusaineiston analyysi. Porvoo: WSOY Kirjapainoyksikkö.

Mühlfelder, M., Klein, U., Simon, S. & Luczak, H.1999. Teams without trust? Investigations in the influence of video-mediated communication in the origin of trust among cooperative persons. Behaviour & Information technology, 18, 349-360. London : Taylor & Francis.

Pfeffer, J. 1981. Power in Organizations. Cambridge, Massachusetts: Ballinger Publishing Company.

Rokeach, M. 1968. Beliefs, attitudes and values: a theory of organization and change. San Fransisco: Jossey-Bass.

Shannon, C. E. & Weawer, W. 1949. The Mathematical Theory of Communication. First paperbound edition, 1963. Urbana: The University Illinois Press.

Smith, M. J. 1988. Contemporary communication research methods. Belmont: Wadsworth.

Stocksdale, G. 1998. NSA Glossary of Terms Used in Security and Intrusion Detection. Available in www-form:

http://www.sans.org/newlook/resources/glossary.htm. [Accessed: 18th February 2003]

Stohl, C. 1995. Organizational Communication. Connectedness in Action. Thousand Oaks: SAGE Publications Inc.

Takanen, A., Raasakka, P., Laakso, M. & Röning, J. 2003. Agents of responsibility in software vulnerability processes. Accepted for publication in: Ethics and information technology, 5. Dordrecht: Kluwer academic publishers.

Valkonen, T. 1976. Haastattelu- ja kyselyaineiston analyysi sosiaalitutkimuksessa. Helsinki: Oy Gaudeamus Ab.

Valli, R. 2001. Johdatus tilastolliseen tutkimukseen. Jyväskylä: Gummerus Kirjapaino Oy.

Weick, K. E. & Ashford, J. 2001. Learning in Organizations. In: Jablin, F. M. & Putnam, L. L. (eds.) 2001. New Handbook of Organizational Communication. pp.704-731. Thousand Oaks: Sage Publications Inc.

Wilcox, D. L. 2000. Public relations. Strategies and tactics. New York: Addison-Wesley Educational Publishers Inc.

Åberg, L. 2000. Viestinnän johtaminen. Helsinki: Inforviestintä.

Appendix 1

The receivers' background information

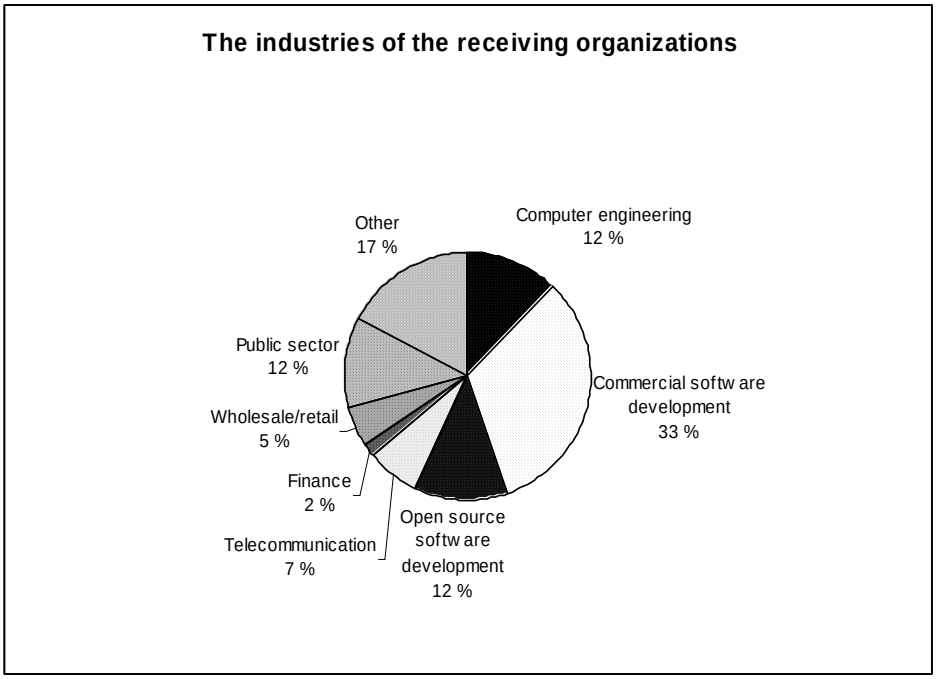


Figure 1

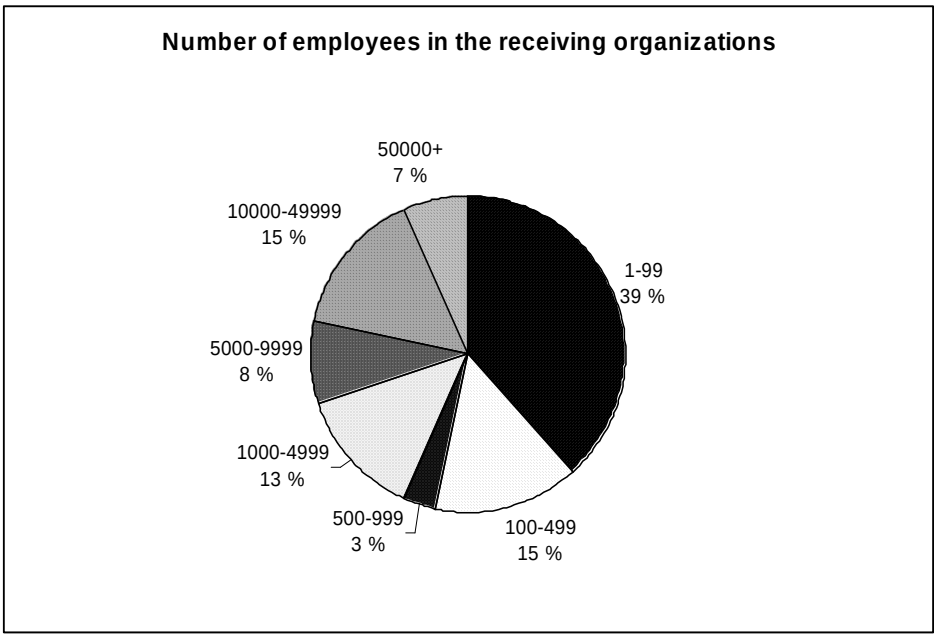


Figure 2

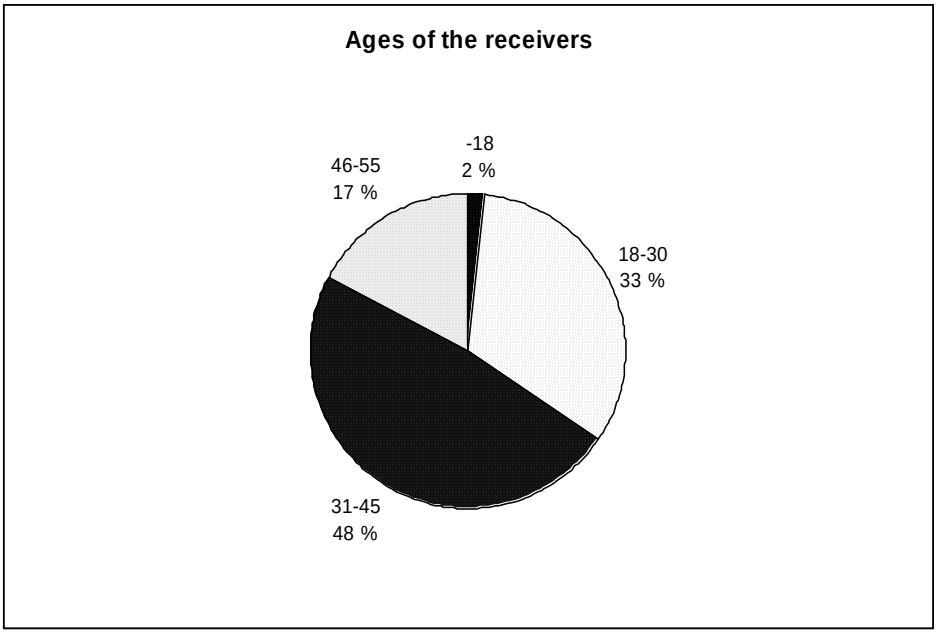


Figure 3

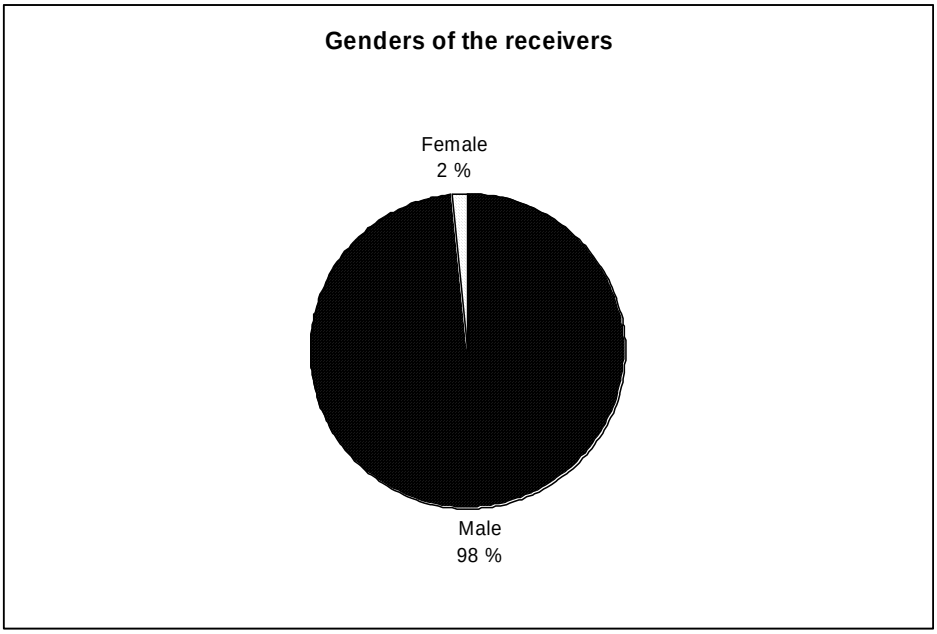


Figure 4

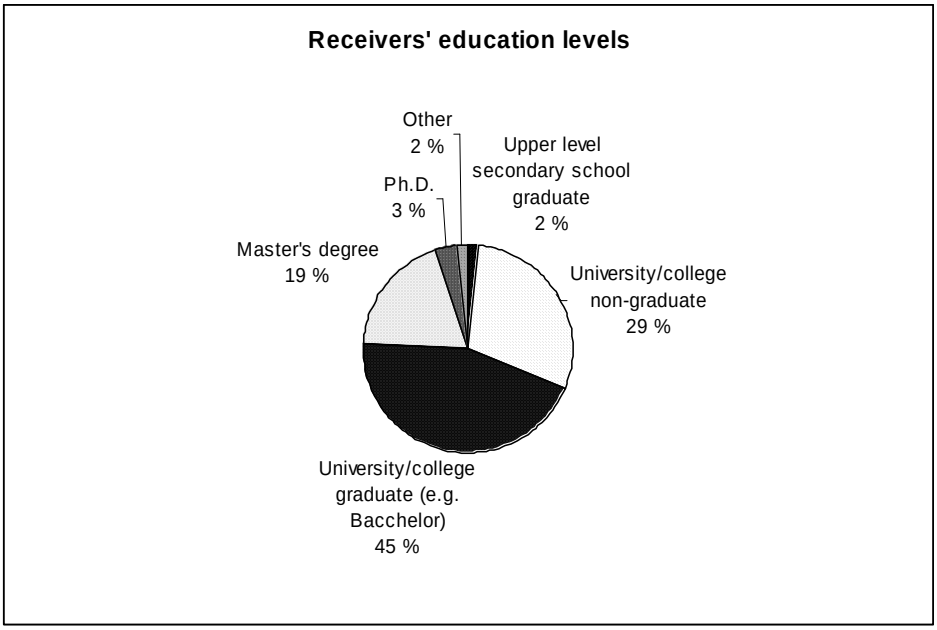


Figure 5

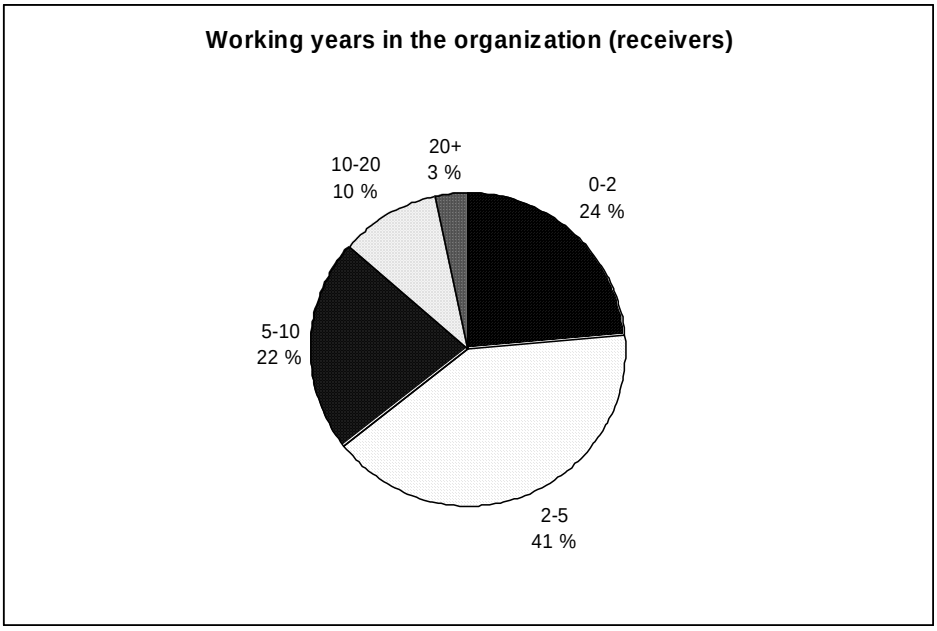


Figure 6

Appendix 2

The reporters' background information

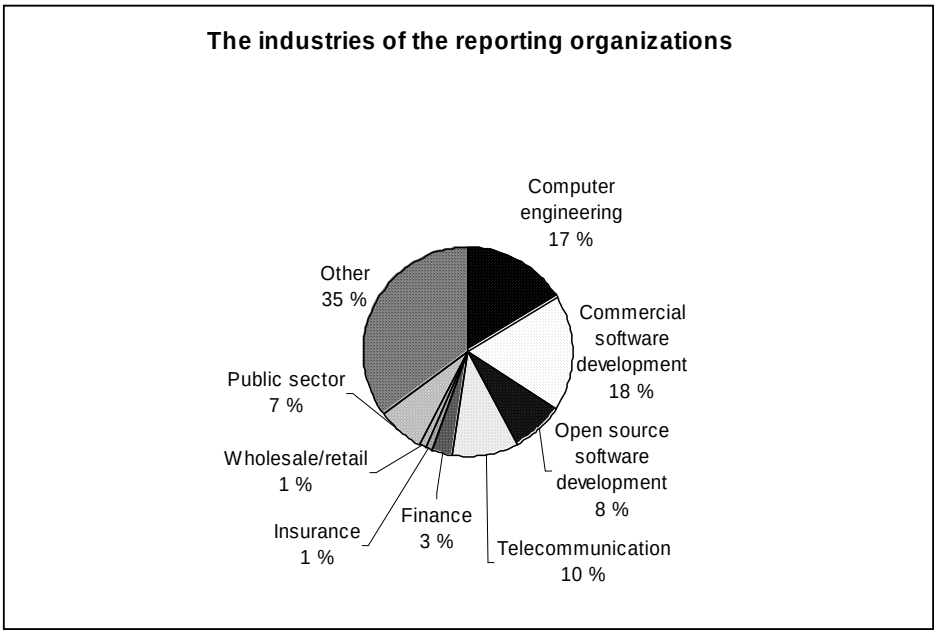


Figure 7

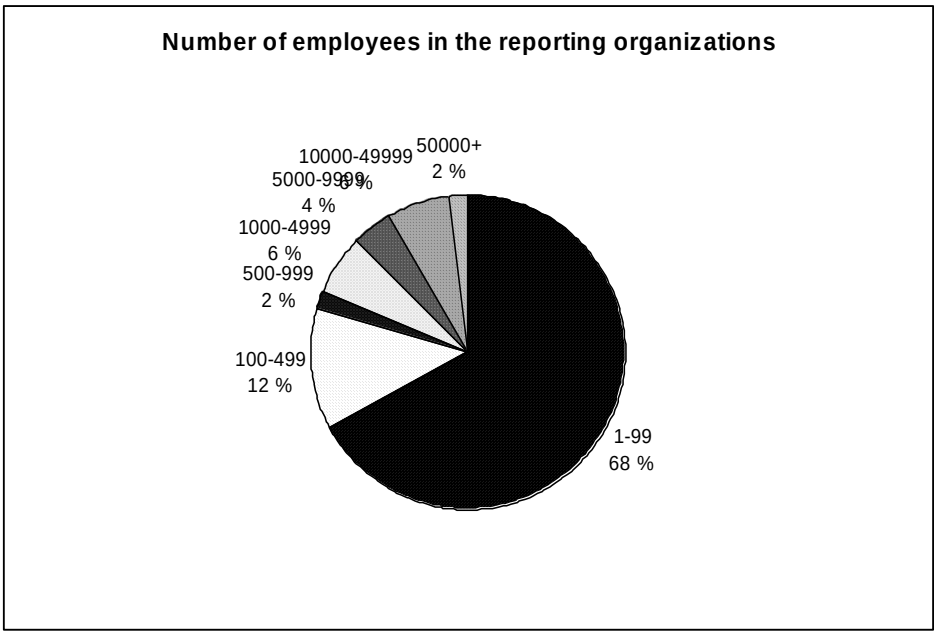


Figure 8

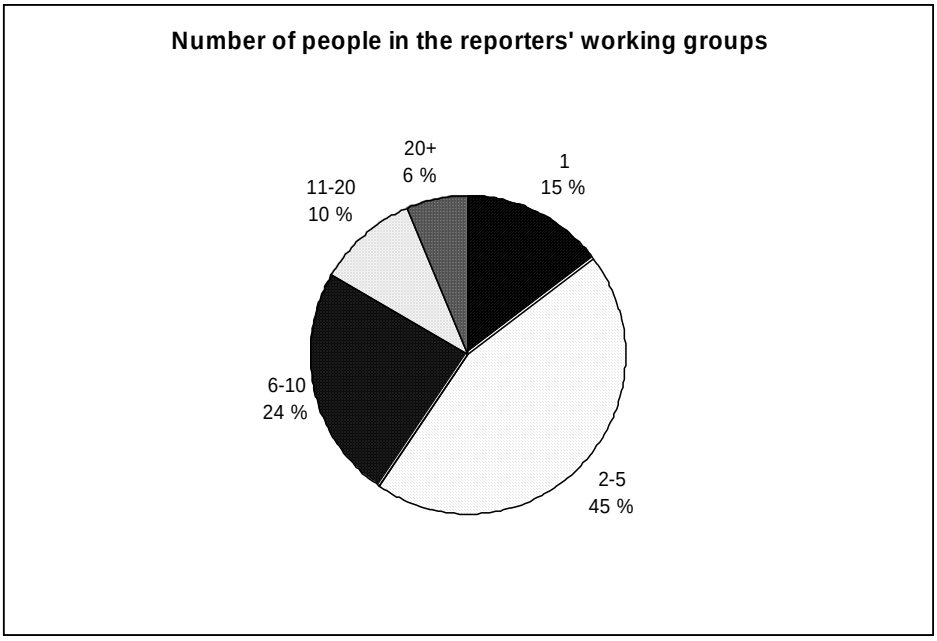


Figure 9

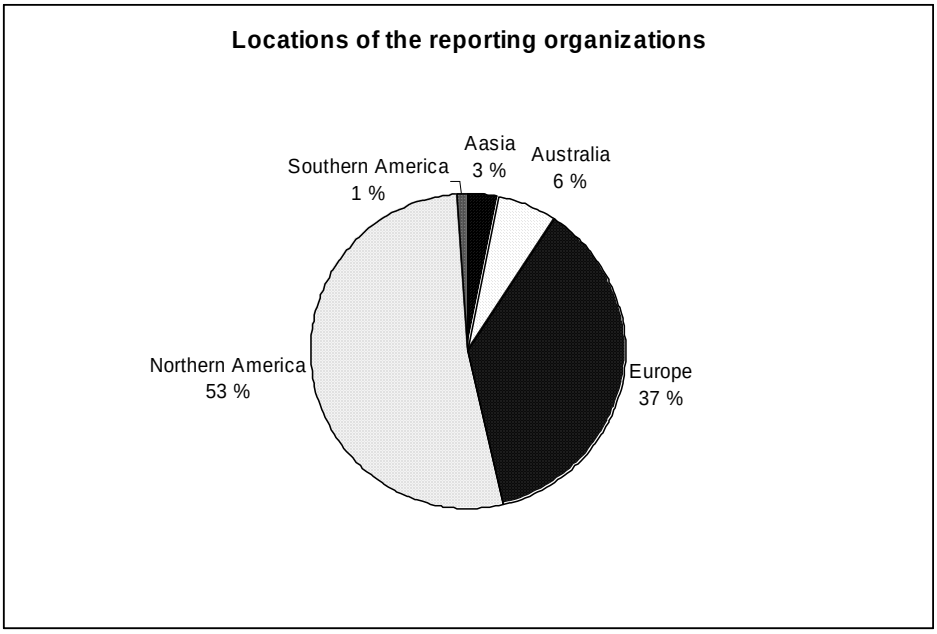


Figure 10

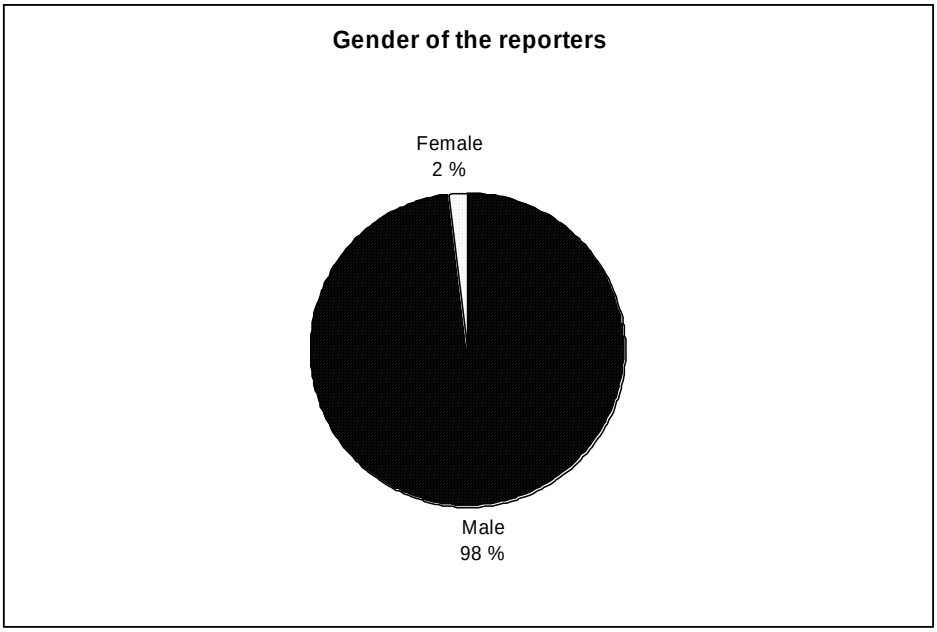


Figure 11

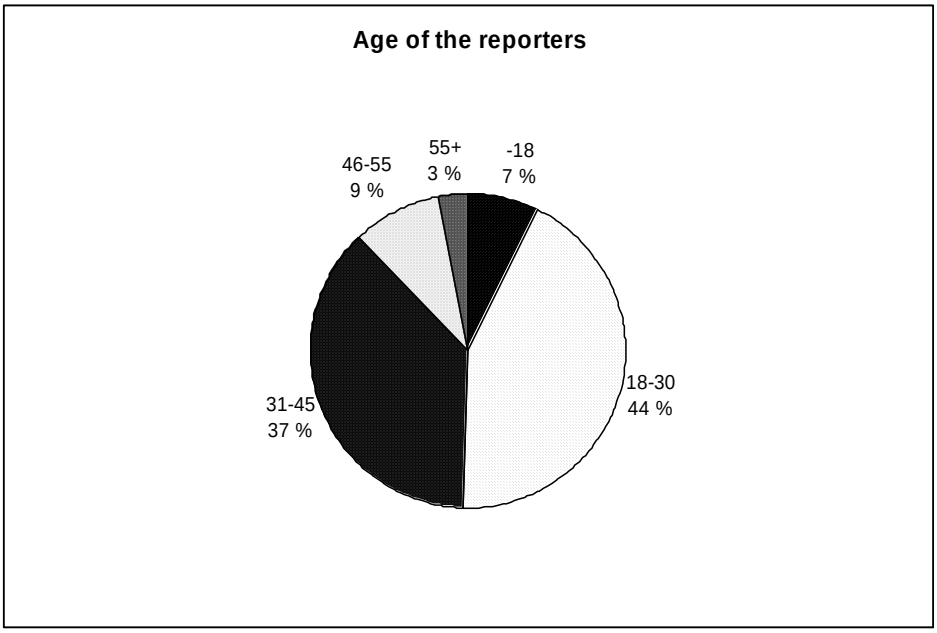


Figure 12

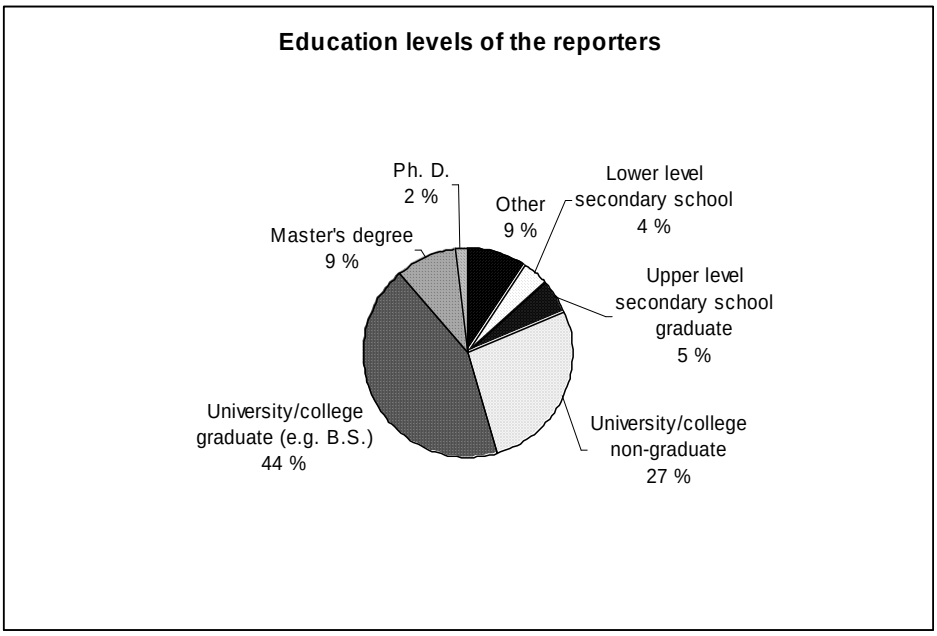


Figure 13

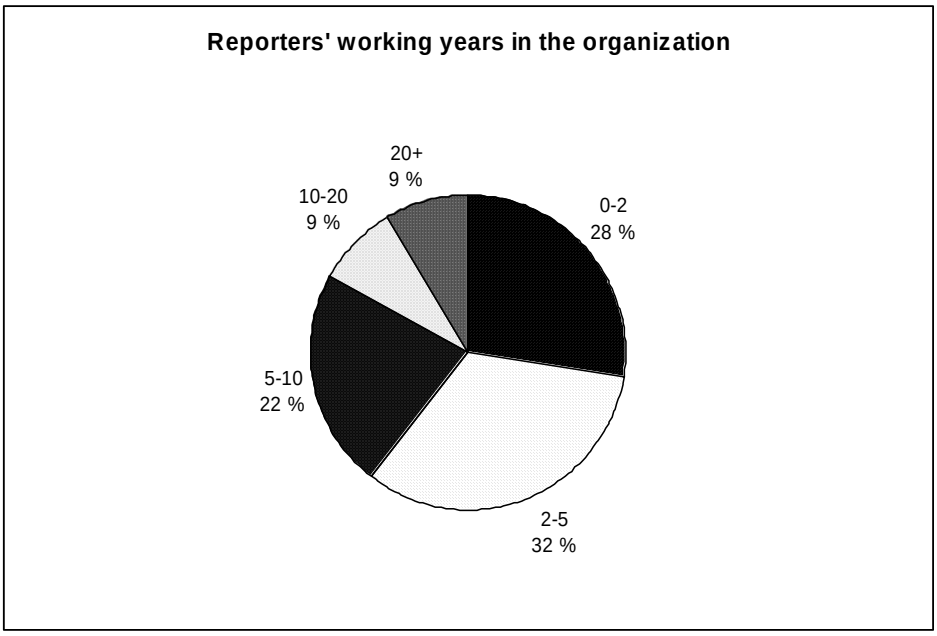


Figure 14

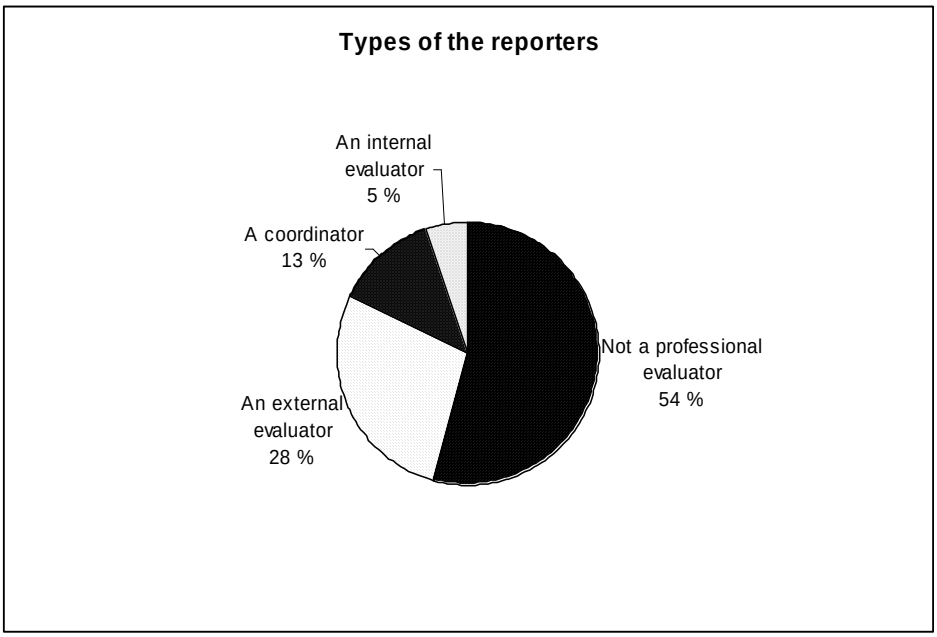

Types of the reporters
An internal evaluator 5 %
A coordinator 13 %
Not a professional evaluator 54 %
An external evaluator 28 %

Figure 15

Appendix 3

The questionnaire for the reporters

Software vulnerability reporting survey

Please note that to some questions you can give several answers. In these questions the options are marked with checkboxes. If you are supposed to give only one answer the answering choices are marked with radio buttons.

Background information

1. The industry of your organization
- Computer engineering
- Commercial software development
- Open source software development
- Telecommunication
- Finance
- Insurance
- Wholesale/retail
- Public sector
- Other, please specify:

2. Size and location of the organization

2.1 Number of employees
- 1-99
- 100-499
- 500-999
- 1000-4999
- 5000-9999
- 10 000-49 999
- 50 000+

2.2 Number of people working in your working group
- 1
- 2-5
- 6-10
- 11-20
- 20+

2.3 Location of your division/department
- Africa
- Asia
- Australia
- Europe
- Northern America
- Southern America

3. Sex
- Female
- Male

4. Age
- -18
- 18-30
- 31-45
- 46-55
- 55+

5. Highest level of education attained
- Lower secondary school
- Upper level secondary school graduate
- University/college non-graduate
- University/college graduate (e.g. Bachelor's degree)
- Master's degree
- Ph.D.
- Other, please specify:

6. Working years at the organization

0-2
2-5
5-10
10-20
20+

7. Position title

Reporting

8. My working group reports bugs with security implications, and we are
an internal evaluator of software security (belong to the developer company)
an external and independent evaluator of software security (have no binds with the vendor)
not a software security evaluator but have noticed vulnerabilities during the course of my regular work
a coordinator of software security reporting

9. How many times has your organization reported or participated in reporting a software vulnerability (total number)?
never
1
2-4
5-9
10-49
50-99
100 or more

10. How many times have you personally reported or participated in reporting a software vulnerability (total number)?
never
1
2-4
5-9
10-49
50-99
100 or more

11. How or where do you get the information about the vulnerabilities that you report or whose reporting you coordinate?
Discovered personally
Internal testing/research group
External testing/research group
Private announcement
Other, please specify:

12. Who/what defines, how the vulnerability reporting should be done?
Our organization has a public vulnerability reporting policy (e.g. on the web)
Our organization has an internal vulnerability reporting policy (e.g. limited distribution)
Our organization has a non-written vulnerability reporting policy (e.g. explained verbally)
There is no standard way for the reporting to occur, it varies depending on the situation
It is up to the reporter to determine the best way to proceed
Other, please specify:

13. If you have a reporting policy in written or non-written form, are you satisfied with it or do you think it should be modified?
Satisfied
Should be modified
If should be modified, please state in what way:

14. In my opinion, doing the reporting is easy (on the basis of the reporting policy or some other information)
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree
Comments:

15. Through which channel do you send the information?
Public mailing list
Public discussion forums on WWW/IRC/News groups
Telephone
Direct email (encrypted)
Direct email (not encrypted)

Other personal communication
Bug reporting form on WWW
Media
Other, please specify

16. How do you typically find the right contact persons?
I communicate about these issues only inside our working group/organization, which means that I know these people personally
I have regular communication with these people, but I do not know them personally
I use an independent third party who has contacts with the vendors (e.g. CERTs)
I have a regular mailing list for these issues
I search contact information from WWW or other sources
Other, please specify:

17. Do you usually find the right contact persons without problems?
Never
Rarely
Frequently
Mostly
Always

18. With whom do you communicate about the vulnerability before reporting it to the vendor (i.e. how wide is the disclosure before reporting)?
With no-one
With trusted colleagues in my own working group
With an independent third party like a national CERT
With the original reporter
I do not report to the vendor before publishing my findings to the wide audience
With my spouse and/or some friends
With representatives of the vendor company
With security experts at the vendor company
With other professionals who have been instructed to pass the information to the security professionals (such as the support organization)
With people who are not experts in software vulnerability issues (such as sales / marketing / development people)
Other, please specify:

19. Does your organization have a recognized or advertised point of contact for issues related to software vulnerability reports? (e.g. for sending them and for feedback to reports sent by you)
Yes
No
Don't know

20. Is the receiver of the report specifically requested to send an acknowledgement that s/he has received the report?
Yes
No
Don't know

21. If yes, how is this information used in your organization?

Handling the vulnerability report

22. From your experience, how often have you or your organization been contacted by the receiver of the bug report after the reporting?
Never
Rarely
Frequently
Mostly
Always

23. Does your organization keep a record of the name and version number of the operating systems and applications that you have found to be vulnerable, and where applicable, the patch and/or work-arounds that have been implemented to address these vulnerabilities?
Yes
No
Don't know

24. In my opinion, the minimum level of response to the reporter of a software vulnerability would be:
No response is necessary
If the flaw is to be repaired fast, is not necessary to slow that down by any communication with the reporter
The receiver of the report should inform the reporter about the priorisation of this particular reports in the vulnerability handling process

Simple acknowledgement that the vulnerability report has been received and is being processed
The repairer of the flaw (not just the receiver of the report) should contact the reporter

25. An independent third party like a national CERT is a useful help in the communication process.
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

26. It would be easier and more useful if the communication between the reporter and the receiver would be direct (no coordination).
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

27. Our organization is dependent on its contacts to other organizations that handle issues related to software vulnerabilities
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

28. In my opinion, the reporter, the coordinator, and the receiver of the report should have regular discussions (via email/telephone/face-to-face) about the vulnerability after it has been reported?
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

29. Have you done that?
Yes
No

30. In my opinion, the reporter should get the chance to evaluate the advisory issued by vendors and independent CERTs and verify that the security patches vendors release eliminate the particular vulnerabilities?
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

31. List the three most important values or beliefs that guide your decisions about security vulnerability information
Confidentiality
Veracity
Recognition of my credits
Security
Non-maleficence (avoidance of harming others)
Public's right to know
Freedom of speech
Avoiding FUD (fear, uncertainty, doubt)
Precision/accuracy
Completeness and ease of reproduction
Avoiding security by obscurity
Public benefit
Public pressure
Neutrality (i.e. only state the facts, no risk or impact assessment)
Single-track-mind (i.e. no other things included in the report, such as suggestions for co-operation etc.)
Other, please specify:

The communication process

32. How, in your opinion, should the information about a discovered software vulnerability be handled

32.1 All information should be found and handled only inside the two organizations (reporter/receiver)

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

32.2 Only selected persons outside the organizations should be informed when an error is found

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

32.3 Some part of the information should be public after a pre-determined time

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

32.4 All information should be public after a pre-determined time

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

32.5 Some part of the information should be public immediately

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

32.6 All information should be public immediately

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33. Please rate the following statements. The statements seek to analyze your attitudes of knowledge activities of your organization at the moment.

33.1 It is highly important that communication about vulnerabilities inside the team/group is open and trustworthy

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33.2 Planned meetings about each vulnerability are very important for knowledge sharing

Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33.3 Intranet and bug database are efficient means for knowledge sharing about vulnerabilities

Don't have an opinion
Strongly agree
Agree

Neutral view
Disagree
Strongly disagree

33.4 Electronic bulleting boards or chat channels are an efficient way to communicate about vulnerabilities
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33.5 Cross-functional project teams are an important aid in communication
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33.6 Internal magazines, newsletters or bulletins of our organization distribute knowledge about vulnerabilities efficiently
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

33.7 In my opinion, it is more important to communicate in a fashion that all are used to than invent new ways to communicate about vulnerabilities
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

34. In my opinion, the software vulnerability handling is well arranged in most of the organizations
Don't have an opinion
Strongly agree
Agree
Neutral view
Disagree
Strongly disagree

35. How, in your opinion does your organization view publicity related to software vulnerabilities?
Publicity does nothing but harm. We must try to influence media as effectively as possible.
Publicity must be taken seriously. It usually harms our organization. If possible, it should be avoided.
Publicity is important. It must however be kept in our own hands. We inform media actively.
Media is an important and equal discussion partner. We tell them what they want to know.

Thank you for your answers!

Appendix 4

The questionnaire for the receivers

Software vulnerability reporting survey

Please note that to some questions you can give several answers. In these questions the options are marked with checkboxes. If you are supposed to give only one answer the answering choices are marked with radio buttons.

Background information

1. The industry of your organization
Computer engineering
Commercial software development
Open source software development
Telecommunication
Finance
Insurance
Wholesale/retail
Public sector
Other, please specify:

2. Size and location of the organization

2.1 Number of employees
1-99
100-499
500-999
1000-4999
5000-9999
10 000-49 999
50 000+

2.2 Number of people working in your working group
1
2-5
6-10
11-20
20+

2.3 Location of your division/department
Africa
Asia
Australia
Europe
Northern America
Southern America

3. Sex
Female
Male

4. Age
-18
18-30
31-45
46-55
55+

5. Highest level of education attained
Lower secondary school
Upper level secondary school graduate
University/college non-graduate
University/college graduate (e.g. Bachelor's degree)
Master's degree
Ph.D.
Other, please specify:

6. Working years at the organization
0-2
2-5
5-10
10-20
20+

7. Position title

Receiving a report

8. How many times has your organization/working group received a software vulnerability report (total number)?
Never
1
2-4
5-9
10-49
50-99
100 or more

9. How many times have you personally received a software vulnerability report (total number)?
Never
1
2-4
5-9
10-49
50-99
100 or more

10. Who/what defines, how the software vulnerability reporting should be done?
Our organization has a public vulnerability reporting policy (e.g. on the web)
Our organization has an internal vulnerability reporting policy (e.g. limited distribution)
Our organization has a non-written vulnerability reporting policy (e.g. explained verbally)
There is no standard way for the reporting, it is done depending on the situation
It is up to the reporter to determine the best way to proceed
Other, please specify:

11. Through which channel(s) do you usually get information about vulnerabilities that have been discovered in software developed by your organization?
Public mailing list
Public discussion forums on WWW/IRC/News groups
Telephone
Direct email (encrypted)
Direct email (not encrypted)
Other personal communication
Bug reporting form on WWW
Media
Other, please specify:

12. Who/what organization usually provides the information about a software vulnerability to you?
Internal research
An independent third party like a national CERT
Product support
I get the information directly from an external reporter
Other, please specify:

13. What, in your opinion, is the importance of software vulnerability bug reports?
There are hardly any security related bugs in our products, for which reason bug reports are of marginal importance
There probably are some security bugs in our products that are important to be identified by bug reports to get them fixed
There probably are security related bugs in our products, but it is not very important to get them repaired, for which reason bug reports are of marginal importance
There probably are security bugs in our products, and they are important to be repaired for which reason bug reports are of great importance

14. With whom do you discuss about the reported vulnerability during the following weeks after you have got the information about the vulnerability?
With no-one
With trusted colleagues in my own working group
With the responsible project manager
The disclosure was already public when I got information about it

With my spouse and/or some friends
Other, please specify:

15. Is the information about a fixed bug passed to the software developers of your organization in order to prevent similar bugs in the future?
Yes, and bug reports are taken into consideration in the software development process
Yes, but bug reports do not have an essential part in this process
No
Don't know
If yes, please describe the process.

16. Where did you first get the information about the latest multiple SNMP v1 vulnerabilities (http://www.cert.org/advisories/CA-2002-03.html) which was publicly announced globally on 12/13 February 2002?
CERT advisory (public announcement)
CERT's advise before the public announcement specifically targeted to your organization
Oulu University Secure Programming Group (OUSPG)
Media
I have not heard about this vulnerability
Affected vendor(s)
Other, please specify:

17. If you had received information about the multiple SNMP v1 vulnerabilities prior to the public announcement of these vulnerabilities on 12/13 February 2002, with whom did you discuss the information?
With no-one
With trusted colleagues in my own working group
With the responsible project manager
With my spouse and/or some friends
Other, please specify:

18. Does your company have a recognized or predefined point of contact for issues related to software vulnerability reports?
Yes
No
Don't know
If yes, please state what is the type of it and how have you informed about it:

19. If you have a vulnerability handling policy or guidelines (on how to handle the reports internally), are you satisfied with it or do you think it should be modified?
Satisfied
Should be modified
If should be modified, please state why and how:

20. Please estimate what is the proportion of valid software vulnerability reports to all reports your organization has received during the last 12 months (spam-email excluded).
0-10%
10-20%
20-50%
50-70%
70-100%

Handling the vulnerability report

21. How much time do you use, on average, to process a vulnerability report, not including the repairing process? (time from receiving to passing it forward)
Minutes
Hours
Days
Weeks

22. From your experience, how often have you or your organization contacted the reporter after the reporting?
Never
Rarely
Frequently
Mostly
Always

23. From the last time you or your organization received a software vulnerability report, how long did you or your organization take to provide a non-automatic response (feedback) to the reporter?
Hours
Days
Weeks
Months

Years
Did not provide any feedback at all

24. Does your organization keep a record of the name and version number of its operating systems and applications and the known vulnerabilities which affect these systems/applications, and where applicable, the patch and/or work-arounds that have been implemented to address these vulnerabilities?
Yes
No
Don't know

25. If yes, how often do you think that members of your organization use this information?
Never
Rarely
From time to time
Frequently
Very often

26. In my opinion, the minimum level of response to the reporter of a software vulnerability would be:
No response is necessary
If the flaw is to be repaired fast, is not necessary to slow that down by any communication with the reporter
The receiver of the report should inform the reporter about the priorisation of this particular report in the vulnerability handling process
Simple acknowledgement that the vulnerability report has been received and is being processed
The repairer of the flaw (not just the receiver of the report) should contact the reporter

27. An independent third party like a national CERT is a useful help in the communication process.
Don't have an opinion/ Strongly agree /Agree /Neutral view /Disagree /Strongly disagree

28. It would be easier and more useful to communicate directly with the reporter than with an external party.
Don't have an opinion /Strongly agree /Agree /Neutral view /Disagree /Strongly disagree

29. Our organization is dependent on its contacts to other organizations that handle issues related to software vulnerabilities
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

30. Does your organization consult with the reporter about the importance of the vulnerability before determining what mitigation steps, if any, should be taken?
Yes
No
Don't know

31. How do vulnerability reports affect your day-to-day tasks?
When receiving a vulnerability report the daily tasks are not interrupted because we have planned how to react to such situations beforehand
Receiving a vulnerability report means an extensive amount of communication inside of our organization until the matter is resolved
Other, please specify:

32. Have you got a policy/instruction or similar for situations where you get a vulnerability report?
We have a change management plan for situations like this so everyone knows what is expected from him/her
We get a vulnerability report that affects our systems so rarely that it is not necessary to have a plan for that kind of a situation. We evaluate necessary tasks case by case
The receiver decides the process and manages it as he sees best
Other, please specify:

33. How do you organize time for the repairing process?
We interrupt the work we are doing and concentrate on the issue at hand
Most of the security vulnerability reports are not critical to handle immediately, so we put reports aside and wait for a suitable time for handling it
Reports are prioritized and handled in priority order
Upon receipt of the report, we develop and test the patch in a test environment within a pre-determined period, before publishing it
Other, please specify:

34. In my opinion, the reporter, the coordinator, and the receiver of the report should have regular discussions (via email/telephone/face-to-face) about the vulnerability after it has been reported?
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

Have you done that?
Yes
No

35. In my opinion, the reporter should get the chance to evaluate the advisory issued by vendors and independent CERTs and verify that the security patches vendors release eliminate the particular vulnerabilities?
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree
Comments:

36. List the three most important values or beliefs that guide your decisions about security vulnerability information
Confidentiality
Veracity
Recognition of my credits
Security
Non-maleficence (avoidance of harming others)
Public's right to know
Freedom of speech
Avoiding FUD (fear, uncertainty, doubt)
Precision/accuracy
Completeness and ease of reproduction
Avoiding security by obscurity
Public benefit
Public pressure
Neutrality (i.e. only state the facts, no risk or impact assessment)
Single-track-mind (i.e. no other things included in the report, such as suggestions for co-operation etc.)
Other, please specify:

The communication process

37. How, in your opinion, should the information about a discovered bug be handled

37.1 All information should be found and handled only inside the two organizations (reporter/receiver)
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

37.2 Only selected persons outside the organizations should be informed when an error is found
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

37.3 Some part of the information should be public after a pre-determined time
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

37.4 All information should be public after a pre-determined time
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

37.5 Some part of the information should be public immediately
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

37.6 All information should be public immediately
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

38. Does your organization have a formulated, proactive publicity strategy for a case of publicity crisis concerning software vulnerabilities?
Yes
No
Don't know
Comments:

39. Does your organization have a PR-personnel, who is familiar with vulnerability issues, with direct contacts to media?
Yes
No
Don't know
Comments:

40.Please rate the following statements. The statements seek to analyze your attitudes of knowledge activities of your organization at the moment.

40.1 It is highly important that communication about vulnerabilities inside the team/group is open and trustworthy
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

40.2 Planned meetings about each vulnerability are very important for knowledge sharing
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

40.3 Intranet and bug database are efficient means for knowledge sharing about vulnerabilities
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

40.4 Electronic bulleting boards or chat channels are an efficient way to communicate about vulnerabilities
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

40.5Cross-functional project teams are an important aid in communication
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

40.6 Internal magazines, newsletters or bulletins of our organization distribute knowledge about vulnerabilities efficiently
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

41. In my opinion, it is more important to communicate in a fashion that all are used to, than invent new ways to communicate about vulnerabilities
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

42. In my opinion, the software vulnerability handling process has been well arranged in our organization
Don't have an opinion Strongly agree Agree Neutral view Disagree Strongly disagree

43. How, in your opinion does your organization view publicity related to software vulnerabilities?
Publicity does nothing but harm. We must try to influence media as effectively as possible.
Publicity must be taken seriously. It usually harms our organization. If possible, it should be avoided.
Publicity is important. It must however be kept in our own hands. We inform media actively.
Media is an important and equal discussion partner. We tell them what they want to know.

Thank you for your answers!