LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Security culture survey

case: ICT Company X

Saukonoja, Mariel

2017 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Security culture survey Case: ICT Company X

Mariel Saukonoja
Security Management
Bachelor’s Thesis
January, 2017

Laurea University of Applied Sciences
Leppävaara
Security Management

Abstract

Mariel Saukonoja

Security culture survey Case: ICT Company X

Year	2017	Pages	36

This thesis was implemented as a case study in a co-operation with a company operating in ICT industry. The corporation is called ICT Company X in this thesis. Thesis project was executed during the Autumn 2016. Name of the corporation will not be published in this thesis due to company's request.

Corporates are outsourcing their processes increasingly. Also the use of external employees is increasing.

The main objective of this thesis was to increase knowledge of the security culture in ICT Company X. The goal was to research if there is a difference in the security culture between the own employees and external employees.

The thesis was implemented in three parts. A qualitative literature reviews on the basis of organizational culture, human behavior, security culture and security risks in outsourcing was made on the first phase. The primary data for the thesis was collected with a quantitative survey. The survey was sent to 2974 people. The third phase of the thesis was analyzing the collected data. SPSS statistic tool was used in analyzing the result.

679 ICT Company X's and 97 External employee's answers was analyzed after excluding invalid results from the group. The results were represented in percentages because of the difference on the sizes of the samples.

Main findings were that even though external employees feel that they receive enough security training and guidance their security competence is not on a same level with the ICT Company X's employees. Organization has one shared security culture despite the previous fact. Survey results brought up that the main challenges in the security culture are on the management level.

Keywords: Organizational culture, security culture, outsourcing, security

Laurea-ammattikorkeakoulu
Leppävaara
Turvallisuusala

Tiivistelmä

Mariel Saukonoja

Security culture survey Case: ICT Company X

Vuosi 2017 Sivumäärä 36

Tämä opinnäytetyö toteutettiin syksyn 2016 aikana tapaustutkimuksena yhteistyössä ICT Company X:n kanssa. ICT Company X:n nimi on muutettu ICT-alalla toimivan yrityksen toimialaavastaavaksi. Toimeksiantajan pyynnöstä nimeä ei julkaista opinnäytetyössä.

Yritykset ulkoistavat toimintojaan yhä laajemmin. Lisäksi ulkoistetun työvoiman käyttö organisaation prosesseissa on yleistynyt.

Tämän opinnäytetyön tarkoituksen oli laajentaa ymmärrystä turvallisuuskulttuurista ICT Company X:n toiminnoissa. Erityisesti tarkastelussa oli se, että onko turvallisuuskulttuurissa eroja oman työvoiman ja ulkoistetun työvoiman välillä.

Opinnäytetyö toteutettiin kolmessa osassa. Ensimmäisessä osassa toteutettiin kvalitatiivinen kirjallisuuskatsaus, jossa etsittiin kirjallisuudesta tietoa seuraavista aihealueista: Organisaatiokulttuuri, ihmisten käyttäytyminen, turvallisuuskulttuuri ja ulkoistamisen turvallisuusriskit. Toisessa vaiheessa opinnäytetyötä tehtiin kvantitatiivinen kyselytutkimus, joka lähetettiin ICT Company X:n toiminnoissa työskenteleville 2974:lle ihmiselle. Kolmannessa vaiheessa kyselytulokset analysoitiin ja raportoitiin SPSS tilastotyökalun avulla.

Kyselyyn vastasi 679 ICT Company X:n ja 97 ulkoistettua työntekijää, kun soveltumattomat vastaukset oli poistettu joukosta. Tulokset esitetään opinnäytetyössä prosenttiosuuksina, koska otoskoot ovat huomattavasti erikokoiset.

Keskeisimpiä löydöksiä opinnäytetyössä oli, että ulkoistettujen työntekijöiden kompetenssi turvallisuusasioissa oli matalampi, kuin ICT Company X:n työntekijöiden, vaikka ulkoistetut henkilöt kokivat saavansa riittävästä koulutusta ja ohjeistusta turvallisuusasioista. Huolimatta edellisestä organisaatiolla voidaan tutkimuksen perusteella katsoa olevan yhtenäinen turvallisuuskulttuuri. Suurimmat ongelmakohdat turvallisuuskulttuurissa löytyivät esimiestasolta.

Asiasanat: Organisaatiokulttuuri, turvallisuuskulttuuri, ulkoistaminen, turvallisuus

Table of content

1 Introduction

It is common nowdays that companies outsource their processes, or use external employees working in their business processes. External employees have access to organization's data, information and premises and are often treated as equal with organization's own employees. Outsourced employees can be working in various positions inside the organization.

From security point of view this causes questions. Organization's security culture should cover these external employees. Organization can demand security controls and background screenings for employees from partner organizations via contracts or other arrangements. But it is more difficult to have an influence on the individual employee, his/her attitude and behavior.

This thesis was implemented as a part of ICT Company X's security culture development project. In this thesis a research among company's employees and external employees was done to find out if there is variation in attitudes, thoughts and behavior through a window of security culture.

1.1 Terminology

Linder (2004) discusses in her book that outsourcing as a term is sometimes understood in various ways. It seems that there is a common understanding that outsourcing means purchasing services from a service provider outside of the company. Leaders disagree if outsourcing means that company's own employees need to transfer to work at the service providers or not. Linder concludes that outsourcing is purchasing an ongoing service from outside of the organization. By ongoing service is meant the services that company is providing itself or are usually provided by the company (Linder, 2004). In this thesis outsourced employees who are working for ICT Company X in its premises, processes and are using its data network are called external employees or ext-employees. Service providers, the parent companies are called external employers or ext- employers.

There are several scientific school of thoughts, which all have a different ankle in explaining organizational behavior. Psychology researches organizational behavior by aiming to understand the attributions of individuals. Sociology researches it through a window of roles and groups. Social anthropology researches organizational behavior through awareness of organizational culture (Wilson, 2000). In this thesis the scope is in organizational culture.

1.2 Case company

This thesis has been done in a co-operation with ICT Company X. Thesis is part of company's security culture development project. ICT Company X is a company that operates in the fields of Information and Communication Technology (ICT), online-services and telecoms. In Finland the company has approximately 4000 own employees. Besides own employees there are about 3000 external employees working in organization's processes.

Company's operations are divided into three sections; business units, production unit and support unit. There are external employees working in every unit and business process of the company. Majority of the external employees are working in Business units 1 and 2. ICT Company X is treating external employees as equal compared to its own employees. There are no separated working spaces in the premises for external employees and external employees have same fringe benefits than company's own employees, with only a few exceptions.

ICT Company X offers its employees an opportunity to remote working. Employees are able to work outside of the office buildings regardless their formal employer, position or tasks. Having a security culture is essential in remote working, because there are no measures to ensure that employees are following security principles and guidelines when they are not working inside the office buildings. In ICT industry it is crucial that trade secrets, organization's own and its customers' information are secured.

2 Methodology

This thesis project includes two different research methods. Security culture has been researched with qualitative method from secondary sources and the case study has been implemented with quantitative survey. Thesis includes data from primary and secondary sources. Primary sources are methods of collecting data that has not been collected before. Data is collected for the purposes of ongoing research. By secondary sources are meant data that has been collected before the ongoing research for another research or purpose. In this thesis the secondary data source is literature. (Krishnaswami, Satyaprasad 2010.)

Case study is a research method that is commonly used to understand a phenomenon in a smaller context; a case. Characteristic for a case study is that researcher do not set hypothesis beforehand, even though a literature review has been made. This is because unique body of a case environment where the research is implemented. Suitable theories that suits for the research case cannot know before analyzing the data from the research (Gillham, 2010).

2.1 Qualitative literature review

Secondary data can be used to verify research findings (Krishnaswami, Satyaprasad 2010.) In this thesis a data collection method for collecting secondary data is a literature review. Literature review is a qualitative data collection method. Qualitative methods are used in this research to create a knowledge base to understand organizational culture and human behavior in a context of security. Bill Gillham (2010) argues in his book that a researcher has to be able to justify research findings based on the available theory. He is not arguing that all the theories that have been written would be accurate or perfect, but a researcher should understand the theoretical frame of reference (Gillham, 2010).

Also Oliver Paul (2012) writes about importance of diligent literature review as a part of any research. He is comparing literature review to a contractor who is building a house with solid foundation. Without foundation there will be no good house. Literature review's only purpose is not to be information source for the researcher. It is also a justification for the reader to understand why the research topic is relevant and important (Paul, 2012).

Literature review has been implemented with a few limitations. At first suitable key words for searching was chosen. Keywords were used in English and Finnish to extend the number of results. With the keywords relevant literature was searched from Laurea Finna, Laurea Leppävaara Library and Helmet library databases. At the first phase literature that were searched were about organizational culture and human behavior in groups and organizations. Understanding the overall picture of organizational culture is essential for understanding security culture. In second phase literature which have been wrote about security culture were searched. Outsourcing in the scope of this thesis has been explained earlier in the terminology section. In the literature review the aim is to find literature and articles which defines security risks in outsourcing.

2.2 Quantitative survey

In this thesis a quantitative survey has been used as a data collection method for primary data. With the survey there are some issues that can have an influence on the reliability of the research. The survey questions have to be formatted in a way that they are easy to understand and they do not have double-meanings. If questions are misunderstood or a person who is answering is purposely unwilling to answer truthfully the reliability of the survey will decrease. Professional jargon or technical vocabulary is recommended to avoid if the sample is not professionals on the field of the research topic. It is recommended to test the form before sending it out to the public to find and correct the inaccuracies (Brewerton & al, 2001).

The purpose of the survey is to collect data that provides information about the security culture in ICT Company X among its own and external employees. There was one survey that was created with organization's own survey tool. The self-administered survey was sent to all employees in 11 largest offices via e-mail in Finland. The survey did reach approximately 2970 employees in Finland. The approximate answering rate for online self-administered surveys within organizations are 30%. Can be estimated that with this sample the amount of received answers would be about 900. (Saunders & al. 2009.)

The survey included demographic questions, such as age, gender, business unit and working period. The security culture part of the survey was divided into four levels: Organizational level, Team level, Management Level and individual level. Topic was divided into levels to be able to understand where and how in the organization the security culture has been built on. For example, do a person think that on the organizational level ICT Company X thinks that security is an important part of its business, but person's manager does not think that security is important. Secondary aim is to find development areas, since this thesis is implemented as a part of security culture development project. Answering in the survey is by using Likert scale.

Security culture survey was sent to 2974 people who are working in 11 largest offices in Finland. Survey was sent via e-mail. ICT Company X has approximately 4000 own employees and about 3000 external employees in Finland. Survey reached 1325 (32,3%) company’s own and 1649 (54,9%) external employees. The survey form is available as an appendix in the end of the thesis report. (Appendix 1)

3 Literature review

Literature review has been done to find theoretical framework and to understand organizational culture and security culture. Following themes were searched from articles and literature:

- ✓ Organizational culture
- ✓ Human behavior in groups and organizations
- ✓ Security culture
- ✓ Security risks in outsourcing

3.1 Organizational culture

Culture as word has grounds in a Latin word *cultura*, which means planting. In a context of organizational culture, the word is understood as planting spirit. German researchers Kroeber and Kluckhohn argue that the word culture has grounds in German and it means sophistication. To the organizational research the term organizational culture became in the 1980s. At the 1980s Japan became highly competitive and USA understood that behind Japan's success there were something else than high-technology or economic structure. Culture researchers became interested in culture's effects on competitive advantage (Puusa & al 2014).

Organizational culture as phenomena is diverse. Researchers have not found a common understating and explanation of organizational culture. Some theories explain culture as a common way of action inside the organization. Clifford Gerez argues that culture is shared *web of signification* where people inside the organization has a common understanding. In business management and leadership theories it is often seen as a measure that has an influence on the organization. In anthropology organization is the culture (Puusa & al 2014).

Even though researchers do not share comprehension of how organizational culture can be defined there is one shared view. Corporate culture can be seen as corporate's character. Every organization has a culture that steers human behavior inside the organization. Culture can be detected from visible statements or positions in the organization, signs and symbols or cryptic messages. Some organizations are called cultureless organizations, if their organizational culture is hidden. Cultureless does not mean that there is no culture in the organization. It means that the organization may have not recognized the value of the culture (Flamholtz & Randle 2011).

3.1.1 Organizational culture through Schein's theory

Edgar Schein is a well-known researcher of organizational culture. In his book (2004) he highlights that changing behavior inside the organization is difficult, even impossible without understanding the existing cultural atmosphere. Culture is the hidden strength that drives behavior in groups and organizations. Culture behind the behavior is intangible and often challenging to observe. There is significant difference in organizational cultures even in companies that are operating on the same field of business (Schein 2004).

Business management and leadership studies often claims that there are two different types of organizational culture; good and bad. With this dividends effects of the organizational culture can be categorized. "Good" cultures are increasing company's performance and productivity, while "bad" cultures are decreasing them. Schein challenges these studies by arguing that it depends on the environment what kind of cultures are influencing positively to organization's operations (Schein 2004).

Schein lists four issues that consists in culture. Those are structural stability, depth, breadth and patterning of integration. Structural stability in organizational culture is a reason why changing culture is difficult. Culture exists even several members of the group would depart. Culture is intangible, but deep. Depth of the culture strengthens the stability. Culture steers behavior in the group, in every task and process. Patterning or integration in this context means that organization is trying to achieve a mode where working environment is in order (Schein 2004).

3.2 Human behavior in groups and organizations

Organizational behavior is studying human behavior in organizations. Common topic to research in a scope of organizational behavior is the communication and interaction between people and foretelling the behavior. To be able to succeed at the management level a person should have a skill to predict behavior of subordinates. Since organizations' have different types of cultural qualities it is important to understand the cultural environment to fit own behavior into existing model. Vanderveer and Menefee (2006) are writing in their book about an example company where an interviewer made a mistake in a highly formal company by not using person's title and last name when having a conversation. The interviewer did not succeed in the research because of the lack of answers (Vandeveer & Menefee 2006).

In today's business world companies have found competitive power from teams. Companies are using teams to ensure that everyone's knowledge and capability is in use to build companies performance. Organizational behavior studies discuss teams as groups. There are two types of groups in organizations; formal groups and informal groups. People are joining the group activity because of security, status, power, goal achievement and culture (Vandeveer & Menefee 2006).

Formal groups can be defined by the organizational structure, for example by business units. Formal groups are divided into two subclasses based on their jobs. Command groups are structured by the vertical hierarchy in the organization. Command groups are divided based on the fact who is responsible to whom. Tasks groups are teams that are working to achieve same goal, for example a project together. Informal groups form inside the organization without structured limitations set by the organizational hierarchy. People are grouping together based on social measures. Informal groups are also divided into two subclasses. Interest groups consist people who are interested in similar things, like lifestyle. In friendship groups there are people who share common characteristic qualities (Vandeveer & Menefee 2006).

3.3 Security culture

Corporations have always several subcultures. Security culture can be seen as one of subcultures in any organization. Earlier in this thesis organizational culture and behavior have been briefly introduced. Security culture can be seen similar than other cultural forms. Security culture is about shared values and beliefs inside the organization (D'Arcy & Greene, 2014).

Security culture is often seen as a development area inside any organization. Security culture as a term has different explanations, which vary among people and organizations. Security culture usually appears in two forms, negative and positive.
With a negative atmosphere in security culture means that awareness is in form of paranoia and suspicious. In negative atmosphere there usually are discipline and punishments whenever slipping from guidelines. In positive atmosphere can be discussed about trust and empowerment. People are encouraged by rewards when behavior is on a desired level from security's point of view. There is a risk of building a culture of shame, instead of building security culture, if used measures are negative. With positive tone and encouragement managers' ability to build desired security culture is more likely. Security culture covers the whole organization, but sometimes it is determined by the actions of security manager, or whoever is the manager when incidents occur (lacey, 2010).

Incidents and security breaches are often caused by humans. A security breach can appear because of a mistake or other misbehaving made in purpose or by accident. David Lacey argues that major security breaches can be prevented by humans. In his article about organizational security culture he highlights that no technical prevention or detection systems are not a blind-wall. Security culture is needed to prevent those accidents or purposely made abuses. Policies, processes and technology needs to be implemented in people's awareness, attitudes and behavior (Lacey, 2010).

Can be argued that security culture forms in any organizations in three phases. First is the commitment of top management. Organization's management is sending a message to the employees that security issues are important to the company. Researchers point out that security attitude, beliefs and values are adapted to the organization from management. Second foundation for security culture is security communication. Security communication should be proactive instead of reactive. In ideal situation security communication clarifies individual's roles and responsibilities in security related issues. Third is tracking employees. Employees have an understanding that the company is taking security seriously, policies and guidelines are not only words, but the compliance is monitored (D'Arcy & Greene, 2014).

3.3.1 Security compliance in the scope of security culture

Among the years there have been numerous amount of security breaches, personal and identification data, for example. It has been clearly understood that major development in security awareness and behavior is needed. Organizations needs to have more effective security culture to be able to prevent security breaches. In large amount of cases organizations fail when aiming to increase security awareness and encourage security behavior among employees. This phenomenon is a result of security managers' inability to adapt basic principles of phycology and communication into security awareness campaigns. Security awareness is developed ad hoc when incidents occur instead of as an ongoing process. (Lacey, 2010).

Security compliance among the employees is reached when employees are following the security policies, procedures and instructions. Researches demonstrates that people often violates the guidelines even though they are familiar with them. Violations may occur for example because of the will to increase own productivity. Security guidelines can be seen as a roadblock. Security compliance correlates straight to job satisfaction and organizational support(D'Arcy & Greene, 2014).

3.4 Security risks in outsourcing

Companies are increasingly outsourcing processes or using outsourced employees to have an access on new knowledge or to focus on essential business processes. Security concerns have occurred because of lack of knowledge how outsourcing effects on security, or does it? In idealistic situation there is one security culture that covers the whole organization; processes, employees and external employees. Often two types of outsourcing are introduced: domestic outsourcing and offshore outsourcing. Offshore outsourcing means that the work is done abroad by using organizations data and systems. (Nassimbeni & al, 2012)

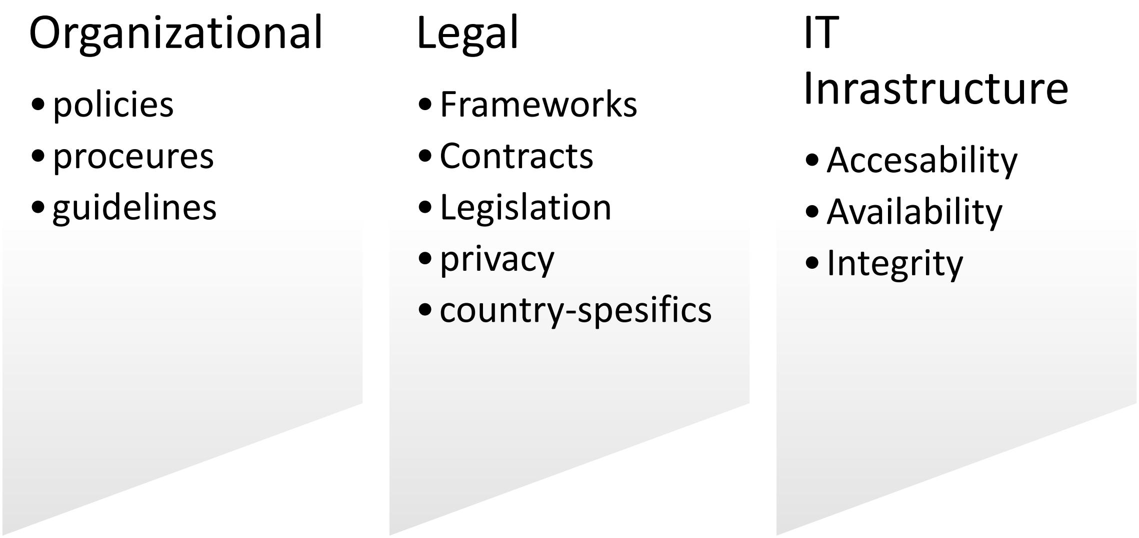
Kettunen and Reiman (2004) researched outsourcing's influence on security through a window of accidents at work in nuclear industry. They did not find significant increase in the number of accidents before and after companies started using external employees working in their processes. Their conclusion is that outsourcing does not necessary increase security risk(s) if the process is managed properly (Kettunen & Reiman, 2004).

Another point of view is that it is obvious that security risks increase when outsourcing business processes. Nassimbeni & al (2012) introduce an example model how to evaluate risks in outsourcing. The model consists three parts, which are organizational, legal and technical.

Organizational part covers policies and procedures, legal part cover legislation and technical the IT infrastructure (Nassimbeni & al, 2012).

Similar risk assessment tool is introduced in another scientific article by Colwill and Gray (2007). Risk assessment tool is meant to be used when assessing risks in outsourcing project (domestic or offshore). Model is more detailed and consists parts of international frameworks and contract demands besides legislation. The model does not include IT infrastructure in scope like the previous model (Colwill & Gray, 2007).

Risk management model apadtation for assessing risks in outsourcing based on the articles of Nassimbeni & al (2012 and Colwill & Gray (2007).



Picture 1 Adapted risk assessment model for outsourcing (Colwill & Gray, 2007 and Nassimbeni & al, 2012).

3.5 Summary and conclusions of the literature review

Human behavior is built in groups and organizations in formal and informal ways. Formal groups in behavior are often related to corporate hierarchy and other structural factors. Informal group are usually formed by people who share values, hobbies or other ways of thinking. These informal and formal groups are steering behavior in organizations. Management should be aware of different groups and be familiar with the basics of phycology and communication to be able to influence the behavior.

Organizational culture is built in thoughts, values and beliefs of the organization. Every organization has a culture despite the fact that some organizations are not aware of the existing culture. Organizational culture has slightly been seen as significant factor in competitive advantage.

Security culture can be seen as a subculture of any organization. Security culture can be described as shared values and beliefs in organization. Security culture is often difficult to observe which is what makes it difficult to influence on the organizational culture. Major security breaches are often caused by humans; researchers argue that these breaches may have been able to prevent if companies would have had effective security culture.

Literature and articles describes security risks in outsourcing from the perspective of IT-security and compliance. In the limitations of this thesis work there were no articles found which would have had included security culture in the risk tool. Security culture has been proved to be an essential part of corporate’s security measures.

4 Survey results and analyze

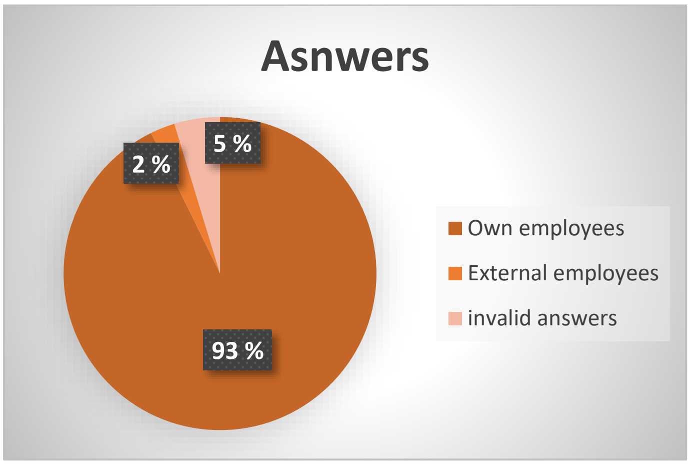
Security culture survey was sent to 2974 people who are working in 11 largest offices in Finland. Survey was sent via e-mail. ICT Company X has approximately 4000 own employees and about 3000 external employees in Finland. Survey reached 1325 (32,3%) company's own and 1649 (54,9%) external employees. Survey was open in the survey tool for ten (10) days. by the deadline 730 answers was received.

The e-mail contained a cover letter and a link to the survey. Due to technical reasons the survey tool asked for an e-mail address before accessing survey. In ten minutes several e-mails with feedback was received and the unfortunate feature was removed. I was happy to observe that I received this feedback in such a short notice. While some of the employees contacted me, as the survey owner some people made an information security deflection alert about phishing, through the official route.

I received three separated e-mails from ICT Company X’s employees after they had answered to the survey. These employees wanted to inform me as the owner of the survey that they felt that security culture as a such is important topic to discuss. They also shared more detailed observations they have made in a scope of security.

4.1 Survey results first attempt

Because of the scope was to do a comparison between ICT Company X's own and external employees 35 results were excluded from the results due to missing employer information. After exclusion remains 695 answers, 674 of the people who answered to the survey were ICT Company X's employees and 21 answers came from external employees. Picture 2 demonstrates the answers according to the amount of received answers. Answer rates according to the sample are: ICT Company X's employees 51% and external employees 1,3%.



Picture 2: Survey answers

At this point the comparison cannot be made, the results would not be valid. It would be irrational to start draw conclusions about the reasons why external employees did not answer to the security culture survey without doing interviews and finding out. Since the ICT Company X's employees answering percentage is higher than was expected there are no need to send the survey again to the whole sample. Survey was opened again for four days for external employees with a notification e-mail. ICT Company X's security manager contacted management in business units were majority of the external employees work. Managers of the external employees will advise their subordinates to answer to the survey and arrange time to do so. This measure was due to exclude a reason that external employees do not feel that they are in the scope of this survey.

4.2 Survey results final

After re-opening the survey for external employees 679 answers from employees of ICT Company X and 97 answers from external employees was received. Answering percentage of ICT Company X's employees was 51% and of external employees 5,9%. 41 answers were excluded because of missing employer information. Because of this large variation in the answer percentage, results will be analyzed and compared in percentages, not counts. In all illustrations there are side by side the results of ICT company X in blue and External employer in green.

The results are analyzed by using SPSS statistic tool. Only the key findings are introduced and analyzed in this thesis. All the answers illustrated are available as an appendix in the end of the thesis report. (Appendix 2) Being objective and nonpartisan has been important goal when analyzing the results (Vilkka, 2007).

4.2.1 Is the sample large enough?

Recommendation is to have at least 20-30 answers when the aim is to compare different groups. When the population is minor and researcher is using a statistic tool in analyzing the recommended amount of answers is about 100 (Vilkka, 2007). In this research both of these qualifications are fulfilled. The population is minor compared to for example research that are made on a national level. The sample is large enough. The reader of this thesis needs to take into account the difference in the samples when drawing own conclusions. There is larger margin of error in the results of external employees.

4.3 Background information questions

At first there was background information questions in the survey. These background information questions are in the survey to understand the sample. Reliability of the results can be analyzed based on the background questions by evaluating if the take is a miniature overview of the organization. If the distribution in the background questions is similar compared to the organization as a whole the results are most likely reliable from that point of view. Charts from the background information questions has been made from the main questions that demonstrates the age and business unit distributions.

when comparing the background information questions to the current knowledge about the realistic distribution in ICT Company X's processes can be argued that the sample in this thesis is a realistic overview of the corporation. Results for all the background information questions are available as an appendix. (Appendix 2)

4.3.1 Age distripution among employer

The following chart demonstrates the variance in age between ICT Company X's and External employer's employees. From the chart can be observed that the personnel from external employer who answered the survey are younger than personnel who answered from ICT Company X. The largest age group from ICT Company X were age at 36-50 years (45,40%)

when the largest age group from external employer was age at 26-35 years. The distribution is likely pretty realistic overview of people working in ICT Company X's processes.

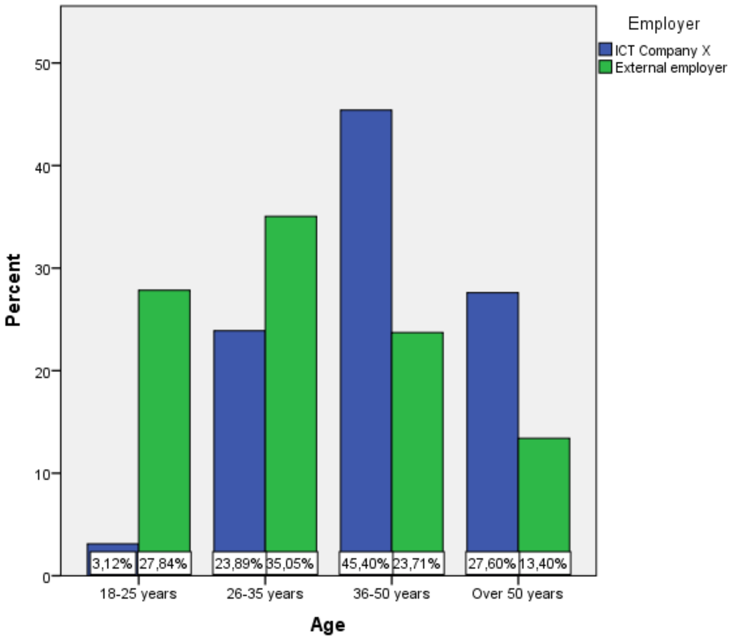


Chart 1 Age distribution N 770 (674 ICT Company X and 96 External employer)

4.3.2 Unit distribution among employers

In the chart below there is an illustration how people who answered to the survey are divided into units. Business units 1 and 2 are the largest units in the corporation. In business unit 1 is working the majority of external employees. In this survey approximately 51% of the ext.-employees are working in the business unit one

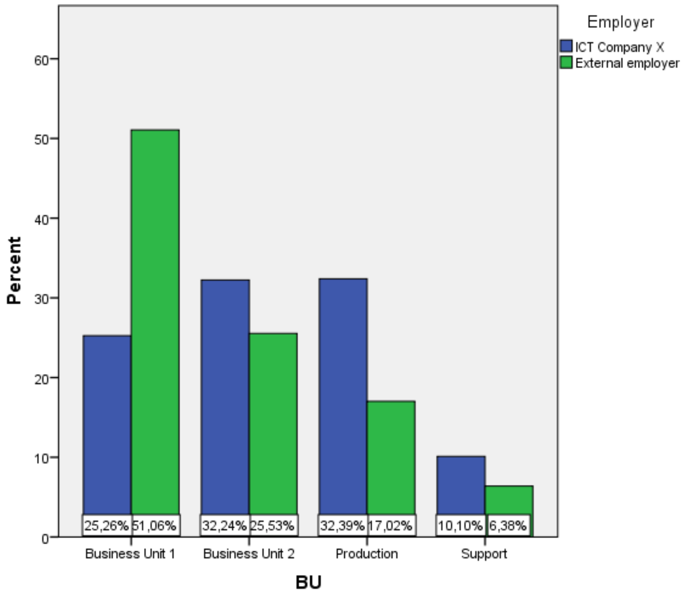


Chart 2 Distribution to units N 772 (679 ICT Company X and 93 External employer)

4.4 Questions with theme on a corporate level

The survey was divided into parts. This part included questions which meaning was to receive information about the security culture on a corporate level. For answering there was Likert scale. In this thesis report the results which gives added value to the topic will be more deeply analyzed and illustrated. Results for all the questions are available in appendix 2.

People are feeling safe working in ICT Company X and its processes, regardless the formal employer. There is only a minor gap between the ICT Company X's and External employer 's answers in these questions. Employees feel that they have received enough training and they are able to do their daily work by following the security guidelines of ICT Company X. Generally, people who answered to the survey thinks that security is important in ICT Company X.

When the survey was sent for the first time some of the ICT Company X's employees reported about security deviation, because the survey asked answer's e-mail address. In the survey 19,59% of external employees and 13,25% of the ICT Company X's employees stated that they do not agree that they knew how to report a security deviation.

4.4.1 ICT Company X’s security risks

Corporate level questions included a questions about security risks that ICT Company X is facing in its field of business. The question was formatted on a way that they were only small amount of risks. Only 13,33% of ICT Company X’s employees and 7,22% of external employees strongly disagree with the claim. From the chart also can be seen that 40,2% of external employees strongly agree or agree that there are only minor risks. The corresponding percentage in ICT Company X is 25,04%, which is also a large amount.

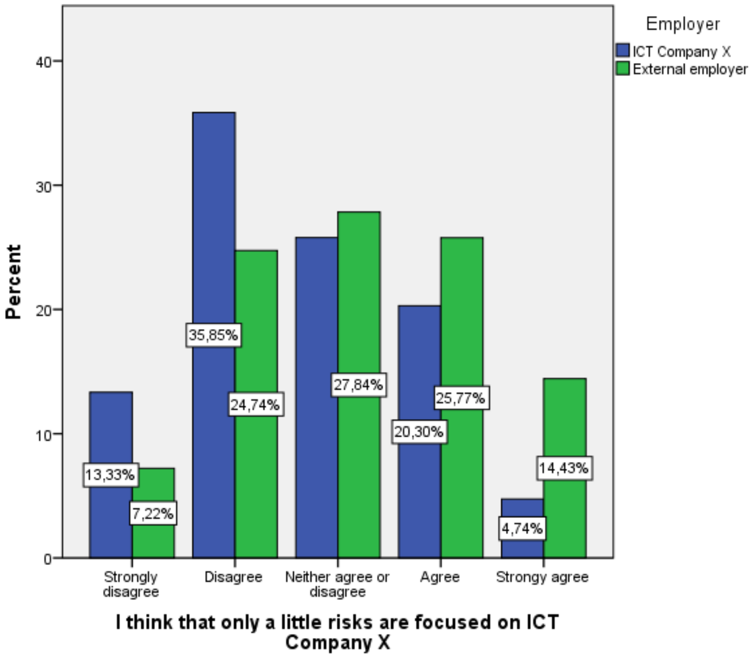


Chart 3 Security risks N 772 (675 ICT Company X and 97 External employer)

4.4.2 Security measures are exaggerate compared to risks

Because or regardless the people who answered to the survey have an opinion that there are only minor security risks they seem to think the security measures are fitted to the risks. 73,25% of ICT Company X's employees think that the security measures are accurate when comparing them to the risks. Corresponding percentage among external employees is 60,82%.

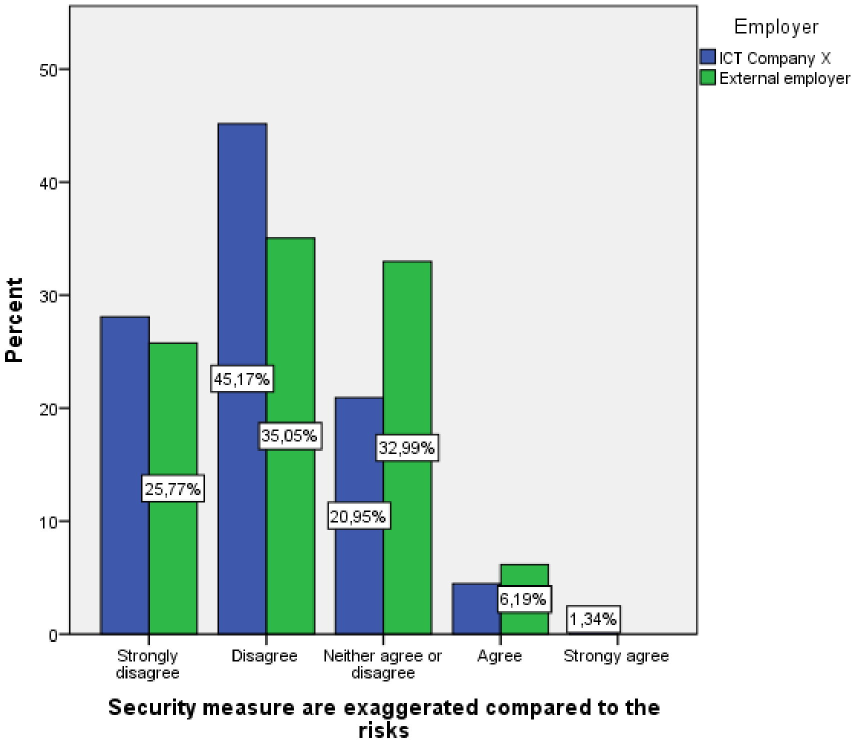


Chart 4 Security measures compared to risks N 770 (673 ICT Company X and 97 External employer)

4.4.3 Main findings on the corporate level

There were four main findings in the corporate level questions:

- Employees feel safe in general
- Employees feel that they have received enough training to work in daily basis following security guidelines
- Employees needs more training on reporting security deviations
- Employees do not have skills to understand risks on a corporate level

4.5 Questions with theme on a team level

Based on the survey answers the same theme continues, employees don't feel insecure working in teams in ICT Company X or in its processes. Atmosphere in teams seems to be also approving and positive, because only 3,19% of external employees and 4,17% ICT Company X's employees would prefer not to report a security deviation because of the achieved negative attention.

Even tough on a corporate level employees seem to neglect the security risks it seems that on a team level employees understand the key risks on their scope. 89,49% of ICT Company X’s employees and 85,26% of external employees confirm that they know the key risks of their work.

4.5.1 Security issues are brought up in teams

26,32% of the external employees strongly disagree or disagree that the security related issues are brought up in teams. Corresponding percentage in ICT Company X is 18,3%. Among ICT Company X’s employees 53,87% strongly agree or agree that security issues are discussed in teams. (External 48,43%).

When comparing the results sorted by business units it seems that business unit 1 and especially business unit 2 are the units where external employees do not feel that security related issues are brought up. In ICT Company X the amount of disagrees and strongly disagrees have been divided equally on a scale of units.

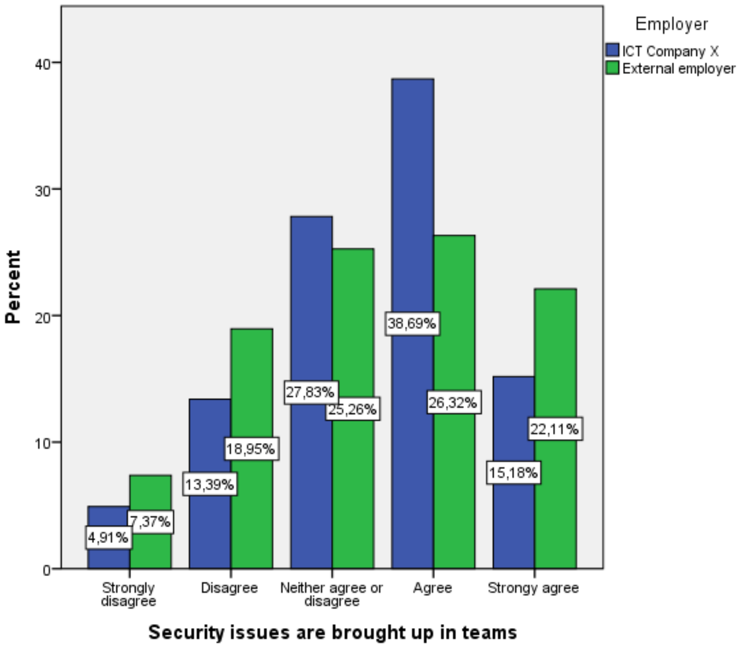


Chart 5 Security issues are brought up in teams N 767 (672 ICT Company X and 95 External employer)

4.5.2 Security is important to my team

Majority of the people who answered in both samples thinks that security is important from their team's perspective. Still 27,12%, almost a third of external employees do not agree with the claim. Corresponding percentage in the results of ICT Company X is 18,87%: To bring into focus the results a little, the answers was divided again to see the distribution between units.

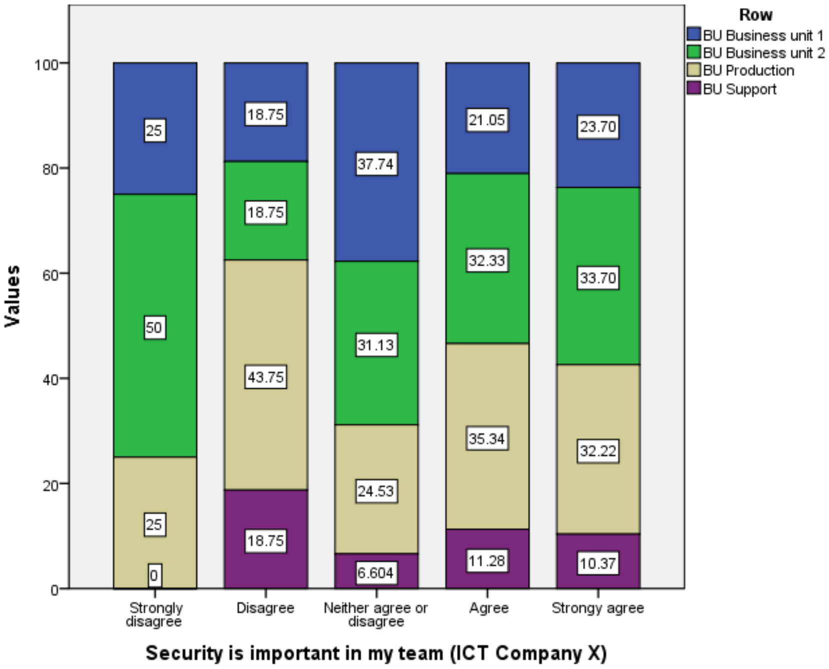


Chart 6 Security importance in teams / units. N 668

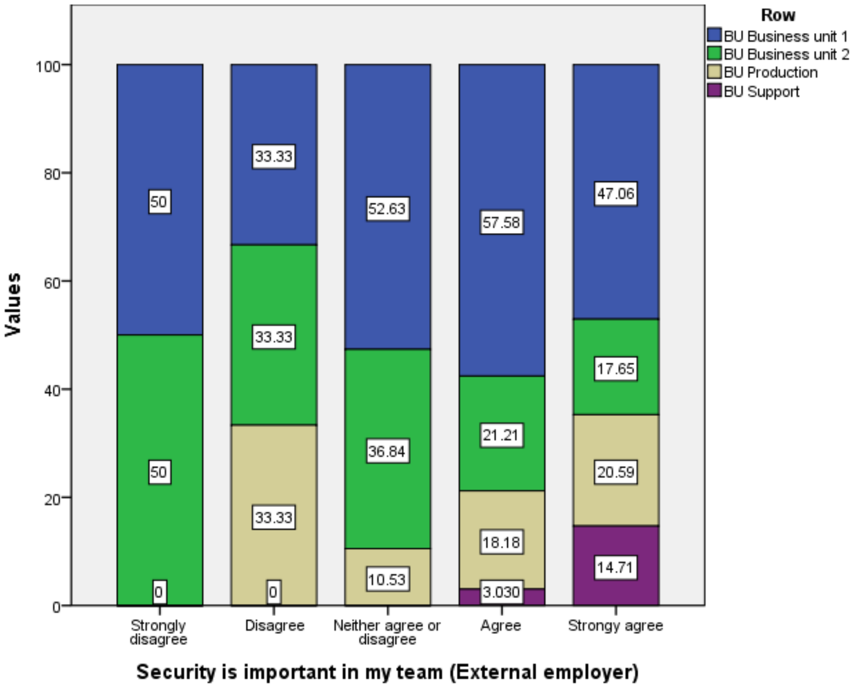


Chart 7 Security importance in teams / units. N 94

There is no clear distribution in ICT Company X's answers, when divided into teams. When observing results from external employees can be seen that people who strongly disagreed with the claim are working in the business units 1 and 2. People who disagreed are working also in production teams.

4.5.3 Main findings on a team level

There were four key findings on a team level

- Employees feel safe and they feel they are able to do their work securely
- Employees have ability to understand the key risks of their work
- There are a large number of teams were security related issues are not discussed
- There are large number of teams which do not understand the importance of security

4.6 Questions with a theme on the management level

The third part of the survey included questions on a management level. The idea was to research how employees feel that they superiors are interested in security. Usually managers are able to communicate about security risks with their subordinates. Superiors are skilled in giving guidance on security related issues and have ability to answer security related questions. 85,09% of the ICT Company X's employees agree or strongly agree that their superior thinks security is important. Corresponding percentage with external employees is 79,38%.

4.6.1 Superior brings up security related issues in one-on-one discussions

Only about one third (32,99%) agree or strongly agree that their superior discusses about security related issues in face-to-face meetings, for example in a goal setting palaver. Percentage is on the same level (34,67%) when observing ICT Company X's answers.

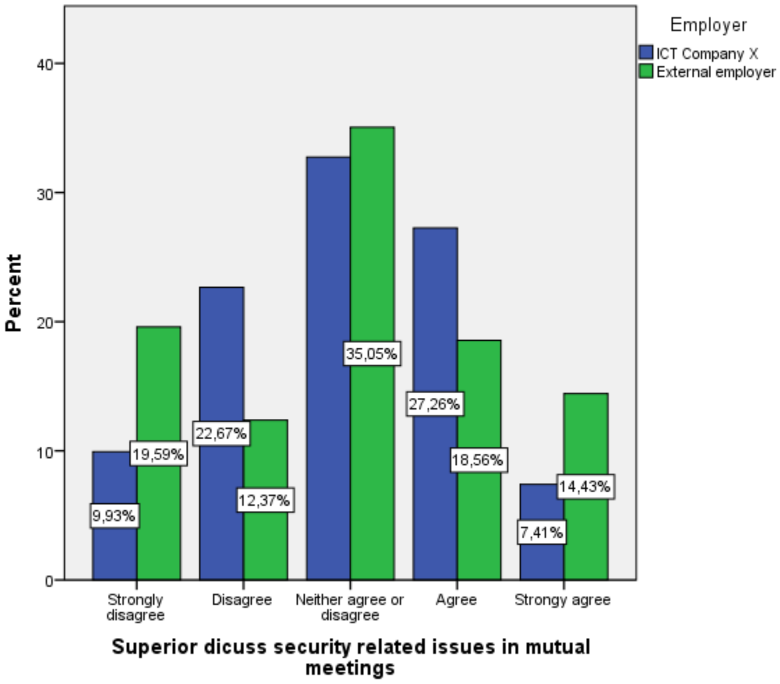


Chart 8 Superior discusses security issues. N 772. (675 ICT Company X and 97 External employer)

4.6.2 Superior encourages to observe and report security deviations

Following chart demonstrates that external employees receive more encouragement to observe and report security deviations than ICT Company X's employees. There is a conflict with the corporation level question, where 19,59% of external employees claimed that they do not know how to report a security deviation.

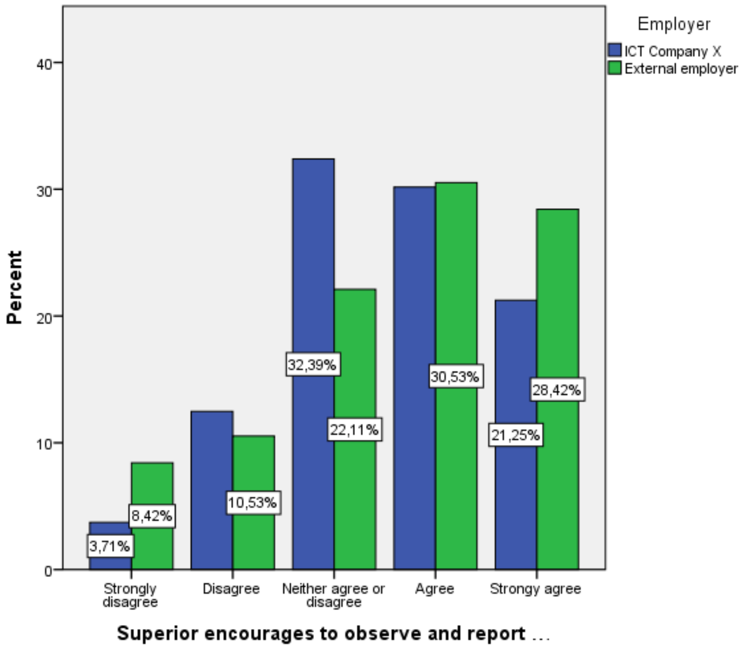


Chart 9 Superior encouragement N 768 (673 ICT

4.6.3 IT security as team's responsibility from superior's point of view

In ICT industry the importance of IT security cannot be highlighted enough. It is also important that IT- security is communicated as mutual responsibility. 70,92% of ICT Company X's employees feels that their superior think IT-security is also on their team's responsibility area. Corresponding percentage among External employer's is 61,85%. Almost 40% of External employeess think that from their superior's point of view IT-security is not seen as a part of their responsibilities.

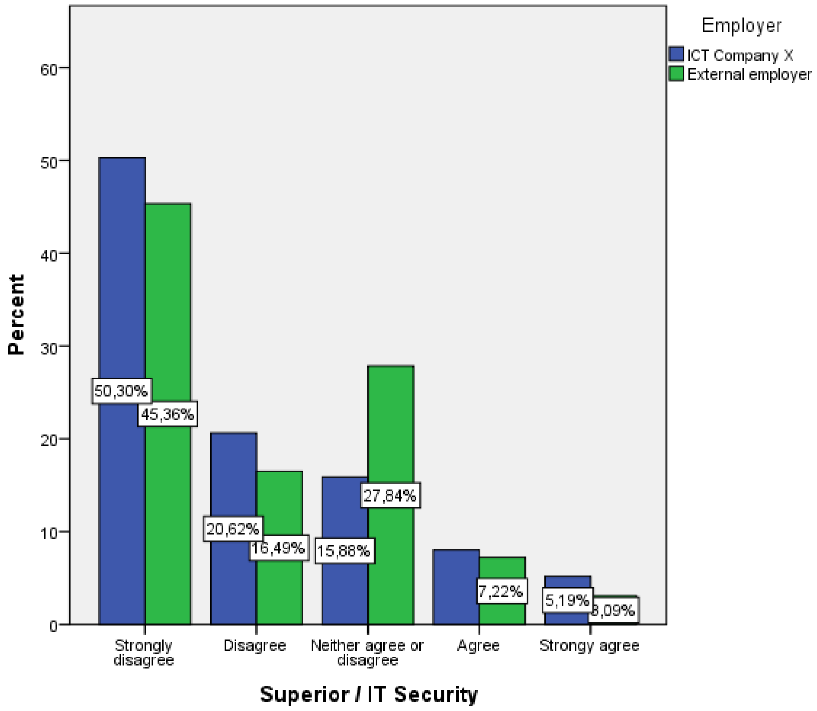


Chart 10 Superior's opinion about IT-security N 771 (674 ICT Company X and 97 External employer)

4.6.4 Main findings theme on a management level

There were three main findings on the management level questions:

- In general superiors have competence on security and they have ability to share it
- External employees may be misguided
- IT-security's importance is not understood in the organization

4.7 Questions with the theme on the individual level

In general, it seems that employees are interested in security and are at least sometimes reading security documentation to maintain their competence. There was no significant variation in results when comparing ICT Company X’s results to External employer’s results.

Positive observation was also that 98,37% of ICT Company X’s employees and 96,61% of external employees agree or strongly agree that security is everyone’s responsibility. This finding means that almost all of the people working in the premises or processes of ICT Company X thinks that they are personally responsible of security.

5,16% of ICT Company X’s employees could not state that they know how to act in an exceptional situation, for example in fire alarm. The corresponding percentage among external employees are 12,37%. 12,37% is a high percentage, every employee should have participated training or received guidance how to exit premises in case of fire alarm. The way of acting at the fire alarm should be also considered as conventional wisdom.

4.7.1 I follow security guidelines even at remote work

28,86 % of the external employees do not agree following security guidelines when they work outside of the office area. Corresponding percentage among ICT Company X’s employees is 7,15%. The variation among the answers is significantly large. Security guidelines should always be followed regardless the physical working environment.

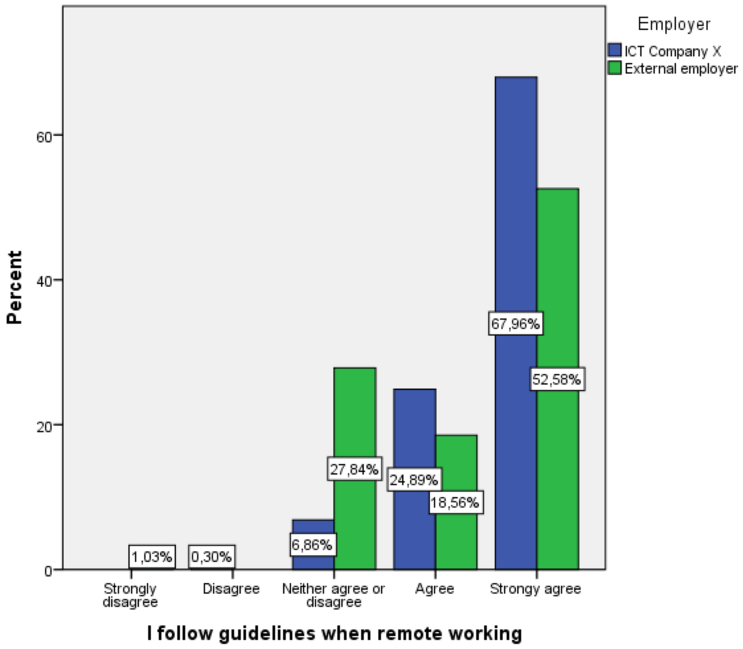


Chart 11 Following security guidelines at remote work N 768 (671 ICT Company X and 97 External employer)

4.7.2 I have observed at least one security deviation during the past half years

In survey there was a shared understanding that security is everyone's responsibility. Observing and reporting security deviation should be a part of taking the responsibility of security. Only 33,53% of ICT Company X's and 26,04% external employees have observed at least one security deviation during the past half years. 47,92% of external employees and 41,5% of ICT Company X's employees disagree with the claim.

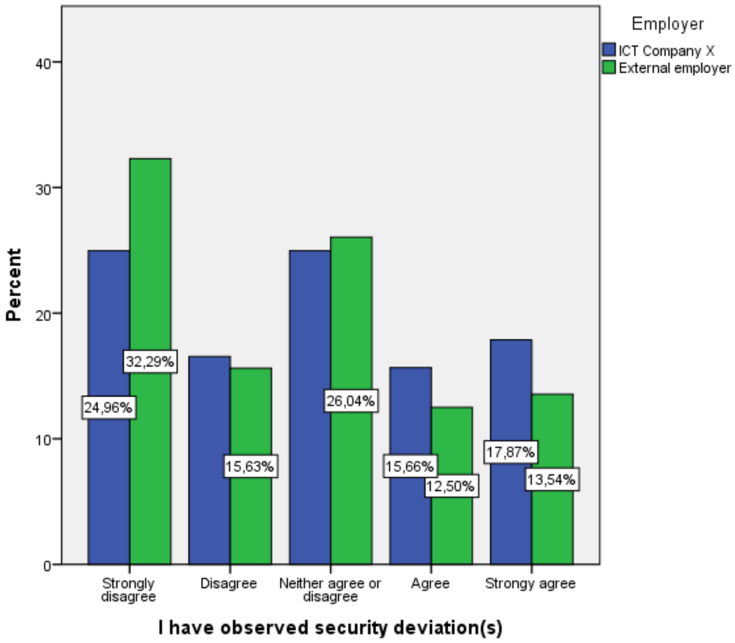


Chart 12 Observing deviations N 773 (677 ICT Company X and 96 External employer)

4.7.3 I report mistakes that have an influence on security, even if they were made by me

From the following chart can be observed that external employees report more likely mistakes that have influence on security, despite who did the mistake. It would be good to understand why ICT Company X's employees are more unwilling to report mistakes.

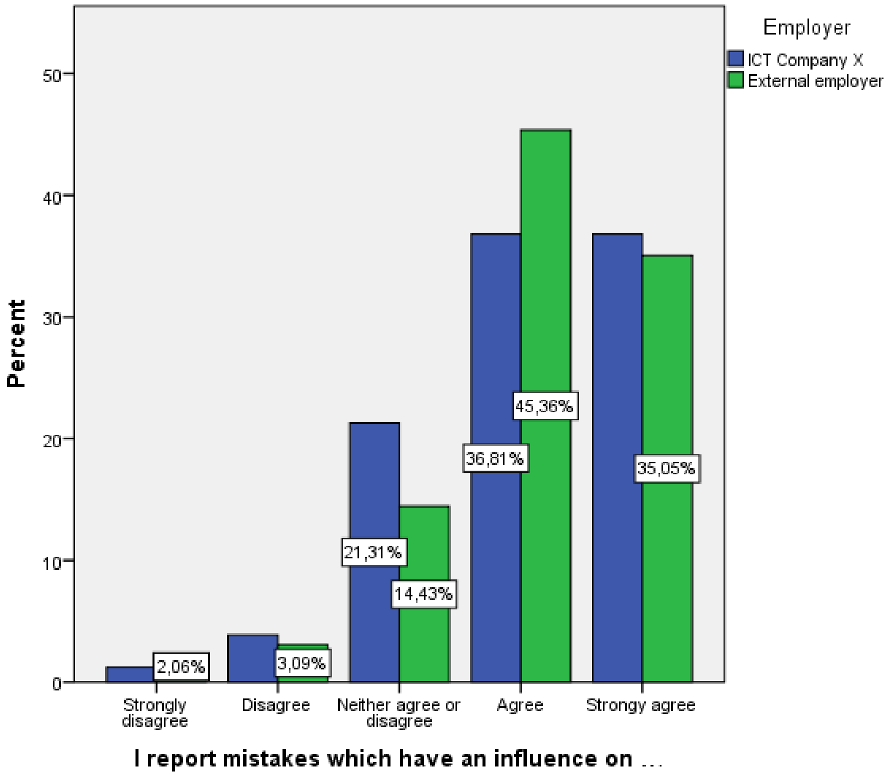


Chart 13 Reporting mistakes N 768 (671 ICT Company X and 97 External employer)

4.7.4 Main findings on the individual level

There were three main findings:

- Employees understand their responsibility in the field of security
- A large percentage of external employees needs more training on exceptional situations
- A large percentage of employees do not observe security deviations or report mistakes influencing security

4.8 Other questions

Survey included several multiple choice questions in which the choices were: agree, disagree and cannot say. Most of the questions included a claim which has its roots on ICT Company X's security policies, principles and instructions. Positive observation was that majority of the people who answered knew the correct answers for the questions.

External employees seem to have in some cases less knowledge of the correct way of action. For example, 18,55% of the external employees could not say, or disagreed with the claim that they should ensure that people entering with the same door opening are wearing company's ID cards. Corresponding percentage in ICT Company X's answers is 9,34%.

In this section there were questions about knowing where to ask more guidance in security, if security instructions are easily available and if they are clear and understandable. Majority of the personnel knows where or whom to contact in security related issues. External employees are able to find the security guidance more easily than the ICT Company X's employees, but ICT Company X's employees are able to understand the guidance better. 29,17% of the external employees did not find security instructions clear and understandable.

4.9 Open questions

There were three open questions in the survey. Goal of these questions was not to find out to problem in security culture, but to observe how do employees understand security, its challenges and development needs. In a scope of this thesis there is to research if there is variation in security culture among ICT Company X's and external employees its using to work in its premises and processes. Open formatted questions were "finish the sentence"- type of questions. Employees was supposed to answer these questions in a scope of their own tasks.

The first sentence started: "I think that security is". 45% of the ICT Company X employees (N 306) answered to the question. The main themes in the answers were:

I. Security is important
II. Shared responsibility
III. Securing information, also customers'
IV. Security is part of everyday processes
V. Security is about feeling safe at the workplace

8,24 % of external employees answered to this question (N 8). Answers followed the same theme. 7 people continued the sentence with one word: important and one answers was: shared responsibility.

The second sentence was asking the key problem in maintaining security. 41% of the ICT Company X's employees answered to this question (N 279). The main themes in the answers were:

I. People are irrespective
II. Constantly developing cyber criminality
III. Lack of knowledge and guidance
IV. Security is often seen as an obligation
V. Organization do not understand the risks

44% of the external employees answered to this question (N 43). Two themes were observable from the answers and they were again similar with ICT Company X's answers:

I. People are irrespective
II. Lack of knowledge and guidance

The third question was about development needs in the field of security. 36,5% of ICT Company X's employees answered to this question Following themes was found from the answers:

I. Security awareness of the risks should be increased
II. Security competence should be increased (training, guidance)
III. Security communications

(N 248).40% of the external employees answered to this question (N 39), no new findings.

5 Conclusion

Organizational researches introduce a possibility that an organization could have several cultures. In this case study the aim was to research if the informal and formal groups between ICT Company X's employees and external employees have created several security cultures in to the organization. Open formatted questions in the survey measured the differences in the groups. In this case study the answers about how people feel about the security when they have an opportunity to express their feelings there were no difference in the answers. There is a one way to think, one security culture in the organization among employees regardless the employer.

When comparing ICT Company X's employees and external employees there are several findings that can be observed from the survey. The first observation that external employee's answers to questions that they understand the risks, their superiors have ability to give guidance in security related issues and they have ability to work following the security principles of ICT Company X. In these questions the results were on a better level than ICT Company X's employees. Despite the previous, almost 20% of external employees do not know how to report a security deviation, 40,2% of the external employees agreed that there is only minor amount of risks in the ICT field of business and 47,92% disagreed with a claim of at least one observed security deviation during the past half years. Also in the survey answers external employees seem to have less knowledge of ICT Company X's security policies, principles and instructions.

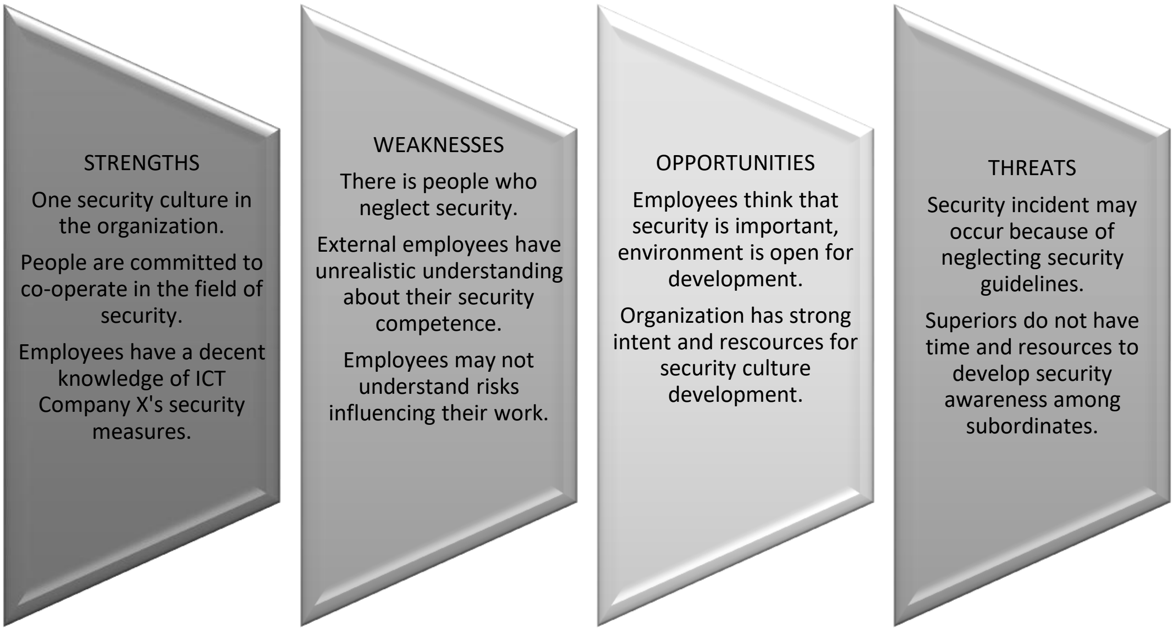
Based on the survey results can be concluded that both takes will need more security training to understand risks and their role in the field of security. More security training is needed also for the superiors of external employees. External employees feel that they receive information of security form their superiors, but the information is not in a correct form or it is not understood. Superiors in ICT Company X need encouragement to bring up security related issues and communicate with their subordinates about security.

In literature review one part was to find out if a change in security culture has been observed as a risk in outsourcing. From literature could not been found a risk assessment model for outsourcing which would have taken risk to security culture into account. Based on the results of this case study survey could be concluded that there is a risk in security culture when using external workforce. External employees should receive equal opportunity to adapt security guidelines than organization's own employees.

A positive finding was that both takes share similar ideas and values of security, when comparing the answers received in open formatted questions. Both groups understand that security in the ICT Company X is important and the responsibility is shared. Somehow the main difficulty seems to be to share the responsibility. Employees feel that some people neglect security issues and are not following the guidelines. Employees in both groups find it disturbing that people neglect security, security is seen as a state that can be achieved only in co-operation.

5.1 Conclusions in SWOT

SWOT analysis multifunctional tool for assessing strengths, weaknesses, opportunities and threats of an organizations. As a result of SWOT is often observed that strengths can be opportunities and weaknesses can turn into threats (Lindroos & Lohivesi, 2013).



STRENGTHS

One security culture in the organization.

People are committed to co-operate in the field of security.

Employees have a decent knowledge of ICT Company X's security measures.

WEAKNESSES

There is people who neglect security.

External employees have unrealistic understanding about their security competence.

Employees may not understand risks influencing their work.

OPPORTUNITIES

Employees think that security is important, environment is open for development.

Organization has strong intent and rescources for security culture development.

THREATS

Security incident may occur because of neglecting security guidelines.

Superiors do not have time and resources to develop security awareness among subordinates.

Picture 3 SWOT

5.2 Development ideas

It seems that in the case company the security culture itself is existing and based on the survey it has a good foundation. Organization as a whole has holistic understanding about security. Own employees and external employees share beliefs and values about security. They have common understanding about the meaning of security in ICT Company X and feel frustrated about the same issues in the field of security. The key difficulty on both groups is that they do not understand the risks that they are facing in their daily work. In the group of external employees, the security competence is on a lower level because of misleading information they are receiving from their superiors.

Based on the findings a development plan will be introduced for the case company. Results will be divided into groups based on the business units so the development ideas can be focused. Following topics is introduced in the development plan:

- Security communication
- Focused security training
- Key Performance Indicators (KPIs)

Starting point for the development is to ensure that key personnel from security’s point of view have enough competence on the field. It seems that superiors of external employees do not have enough competence to train and guide their subordinates in security-related issues. Security organization should also increase the level of security communication, to reach the people who purposely neglect security guidelines. The message in security communication could be opportunity-oriented instead of communicating about the risks and threats. KPIs should be considered, to be able to measure the development in the future.

5.2.1 Work evaluation

The thesis project did not achieve the timetable because of the unexpected reasons. The main reason why this project was delayed was partly due to the delayed survey. It should have been considered in the beginning of the thesis project that whenever there are co-operative parties their interest may not be on a same level that the thesis worker’s.

Likert scale that was used in the survey is giving a “neutral” option to the people who are answering to a survey. Could be discovered that a large amount of people would pick this neutral option. Analyzing the results was somehow difficult due to the fact that could not be sure of the meaning of the answer.

The survey results were pretty reliable; the take was a miniature copy of the ICT Company X’s employees. Because of the size difference in the takes there is larger margin of error in the results of external employees. The results were analyzed in percentages and not in counts because of the reliability.

A question of office location was excluded from the survey because of lack of anonymity. From some offices only a few people answered and if concluding the answers of gender, age, position the person could have able to point out.

Some issues which would be worth for researching in the future appeared during the process. One possible research topic could be to find out if the external employees feel that they are part of the customer company or do they feel as part of their formal employer. The second interesting finding was that the external employees needed more encouragement to answer to this survey. What are the reasons behind the fact?

References

Brewerton, P.& Millward, L. 2001. *Organizational research methods: a guide for students and reseaches*. London: Sage Publications Ltd.

Colwill, C. & Gray, A. 2007. Creating an effective security risk model for outsourcing decisions. Ipswich: British Telecommunications PLC. Accessed 24.11. 2016 http://search.proquest.com.nelli.laurea.fi/docview/215203371?accountid=12003

D'Arcy, J. & Greene, G. 2014. Security culture and the employment relationship as drivers of employees' security compliance. Bradford: Emerald Group Publishing. Accessed 23.11.2016. http://search.proquest.com.nelli.laurea.fi/central/docview/1634006771/fulltext/9F278A0BB4B441APQ/1?accountid=12003

Edgar, S. 2004. *Organizational culture and leadership*. San Francisco: Wiley 3rd Edition.

Flamholtz, E., & Randle, Y. 2011. *Corporate culture: the ultimate strategic asset*. California: Stanford Business Books.

Gillham, B. 2010. *Case study research methods*. London: Continuum.

Kettunen, J., & Reiman, T. 2004. Ulkoistaminen ja alihankkijoiden käyttö ydinvoimateollisuudesssa. *VTT Tiedotteita*. Accessed 24.11.2016. http://www.vtt.fi/inf/pdf/tiedotteet/2004/T2228.pdf

Krishnaswami, O. & Satyaprasad, B. 2010. *Business research methods*. Mumbai: Himalaya Publishing House.

Lacey, D. 2010. Understanding and transforming organizational security culture. Emerald Group Publishing Ltd. Accessed 16.11.2016. http://search.proquest.com.nelli.laurea.fi/central/docview/212340099/7349B4B31AD04BF2PQ/19?accountid=12003

Linder, J. 2004. *Outsourcing for radical change: A bold approach to enterprise tansformation*. New York: Amacom.

Lindroos, J.-E., & Lohivesi, K. 2013. *Onnistu strategiassa*. Helsinki: WSOYpro.

Nassimbeni, G., Sartor, M. & Dus, D. 2012. Security risks in service offshoring and outsourcing. Wembley: Emerald Group Publishing. Accessed 23.11.2016.

http://search.proquest.com.nelli.laurea.fi/docview/927128430?accountid=12003

Paul, O. 2012. *Succeeding tith your lliterature review: a handbook for students.* Berkshire: Mainhead.

Puusa, A., Reijonen, H., Juuti, P. & Laukkanen, T. 2014. *Akatemiasta markkinapaikalle johtaminen ja markkinointi aikamme kuvina.* Helsinki: Talentum.

Saunders, M., Lewis, P. & Thornhill, A. 2009 *Research methods for business students.* Harlow: Pearson education Limited.

Vandeveer, R. & Menefee, M. 2006. *human Behavior in organizations.* New Jersey: Pearson Education.

Vilkka, H. 2007. *Tutki ja mittaa: määrällisen tutkimuksen perusteet.* Jyväskylä: Tammi.

Wilson, E. 2000. *Organizational Behaviour Reassessed : The Impact of Gender.* London: SAGE Publications Ltd.

Pictures

Charts

Appendixes

Appendix 1: Survey form

Security culture survey form. Case: ICT Company X

1. Gender
2. Age

18-25 years	26-35 years	36-50 years	Over 50 years

3. Employer
4. Unit

Business Unit 1	Business Unit 2	Production	Support

5. Office location
6. Your position in ICT Company X or its processes

Employee	Officer	Managerial Officer	Director

7. Have you conducted security training in ICT Company X's online training portal?

Yes	No

8. If you answered yes; When did you conduct trainings?

Before employment	During the probation	During the first year of employment	Later than any of the previous

9. Rank the qualities of security trainings by giving stars from 1 to 5. (1 minimum, 5 maximum)
   - utility
   - practicality
   - factors

Answer following questions by choosing one of the following: 1. strongly disagree 2. disagree 3. neither agree or disagree 4. agree 5. strongly agree

Theme: Corporate level

10. I think that the work environment in ICT Company X is safe.
11. I have received enough training and guidance to security related issues in ICT Company X
12. I can work by following ICT Company X's security requirements.
13. I know how to report a security deviation.
14. I think that only a little security risks are focused on the business of ICT company X in its field.
15. I think that ICT Company X's security measures are exaggerated compared to security risks.
16. Security is important in ICT Company X.

Theme: Team level

17. My team brings up security related issues regularly.
18. I know the central security risks in a scope of my own tasks.
19. I do not feel insecure.
20. I prefer not to report security deviation I have noticed to not get reputation as a nitpicker.
21. My team thinks that security is important.

Theme: Management level

22. My superior brings up to the conversation security related issues in mutual meetings, for example in goal setting palaver.
23. My superior has ability to answer my security related questions.
24. My superior has ability to communicate security risks influencing our operations.
25. My superior encourages me to observe and report security deviations.
26. I have received enough guidance to do my tasks following security guidelines of ICT Company X.
27. My superior thinks that IT Security is not one of our team's responsibilities.
28. My superior thinks that security is important.

Theme: Individual level

29. I am interested in security at the workplace.
30. I maintain my security awareness by reading instructions, for example from internal website.
31. I follow ICT Company X's security guidelines also when I am not working in the company's premises.
32. I have observed at least one security deviation during the past half years.
33. I report the mistakes that have an influence on security, regardless if I did the mistake by myself.
34. I think that everyone working in premises and/or processes of ICT Company X are responsible for security.
35. I know how to act in exceptional situations, for example during a fire alarm.

Answer following questions by choosing one of the following: 1. Agree 2. disagree 3. I don't know

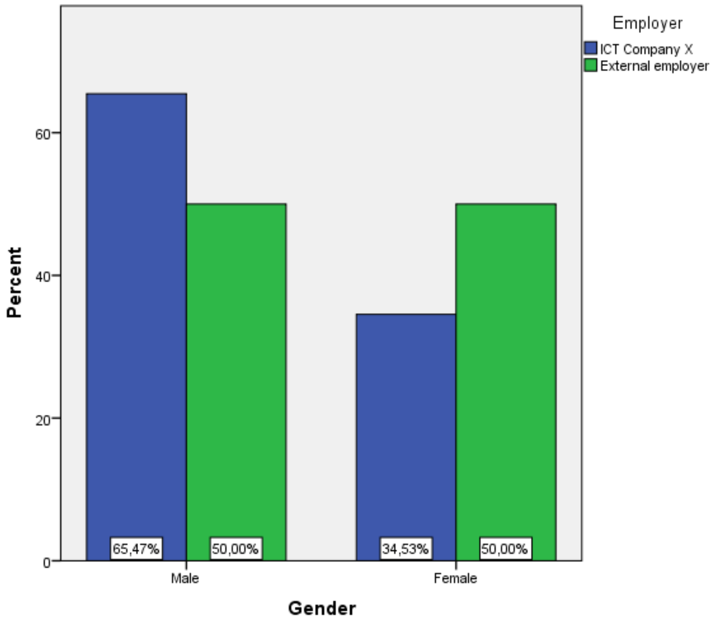
36. I ensure that people entering with the same opening of the door are wearing their ICT Company X ID cards, at the workplace.
37. Visitors are temporally allowed to be in the working area of ICT Company X without their host.
38. I do not have wear ICT Company X's ID card when I am visiting the premises during a weekend.
39. It is not allowed to storage laptop at car, even though the power has been switched off.
40. When I am working from distance I do not need to worry about the confidentially of the information, because there are less risks.
41. Reporting security deviation can cause nitpicker reputation.
42. I know from where/whom I can approach for guidance in security issues.
43. Security related instructions are easily available.
44. Security related instructions has been written clearly and they are understandable.

Please finish following sentences. Try to have the scope in your own tasks.

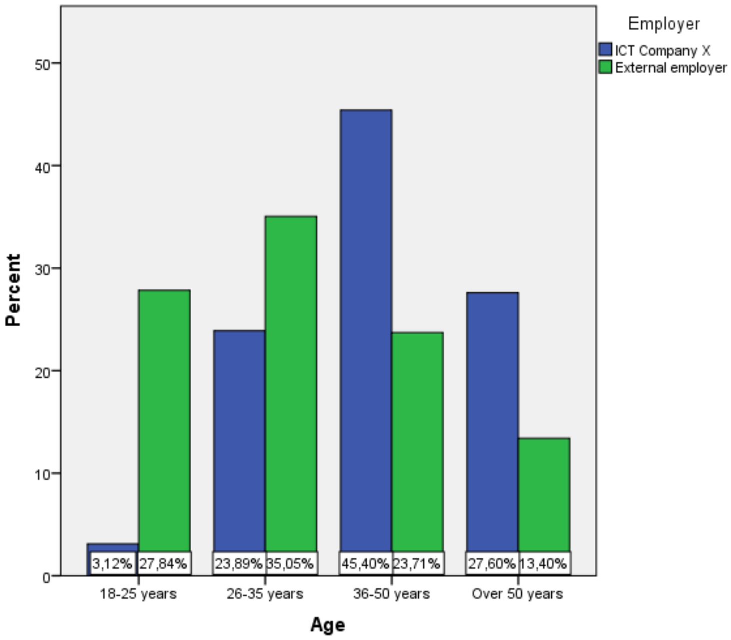
45. I think that security is ____
46. I think that the key problem maintaining security________________________________
47. In the field of security there should be development in________________________________

Appendix 2: Survey Results

Gender N 762 (666 ICT Company X and 96 External employer)



1. Age N 771 (674 ICT Company X and 97 External employer)



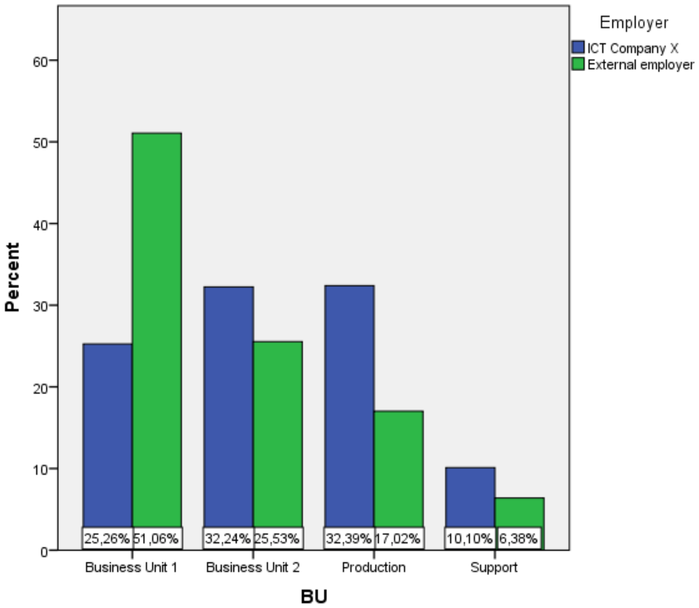
2. Employer N 817

   97 External employees

   679 ICT Company X employees

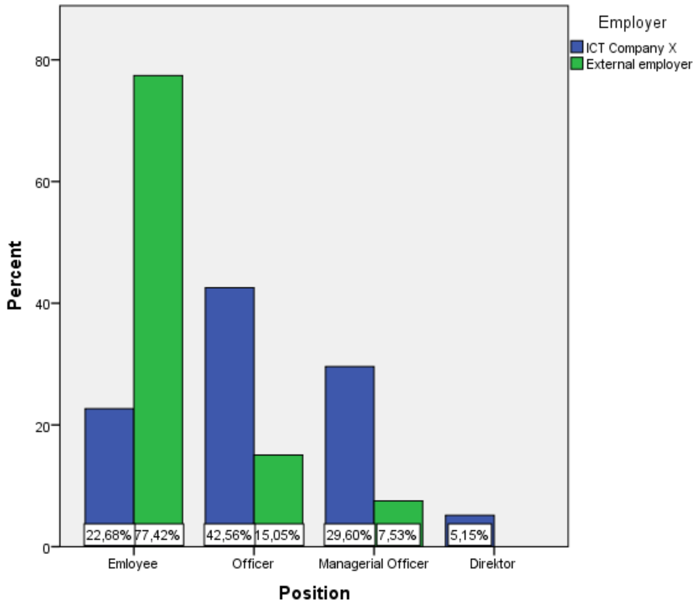
   41 No value, excluded from the thesis

3. Unit N 767 (673 ICT Company X and 94 External employer)

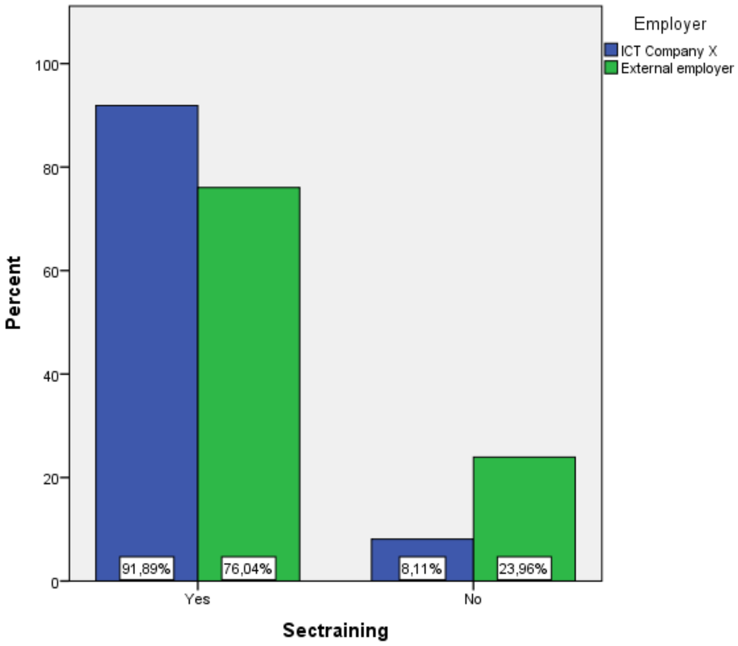


4. Office location – question excluded because of lack of anonymity.

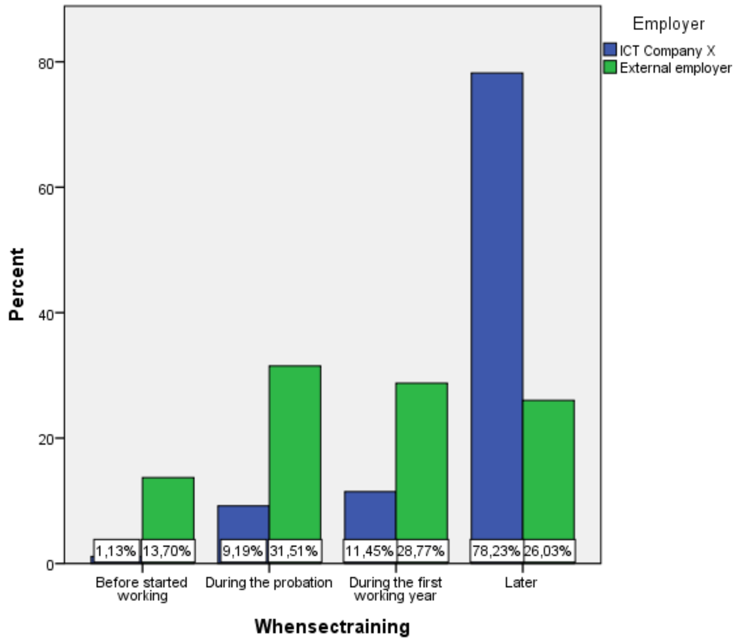
5. Your position in ICT Company X or its processes? N 772 (679 ICT Company X and 93 External employer)



6. Have you conducted security training in ICT Company X's online training portal? N 774 (678 ICT Company X and 96 External employer)



7. If you answered yes; When did you conduct trainings? N 693 (620 ICT Company X and 73 External employee)



8. Rank the qualities of security trainings by giving stars from 1 to 5. (1 minimum, 5 maximum) N 689 (617 ICT Company X and 72 External employer)

- Utility

  ICT Company X: Average 3,5 / Median 4 / SD 1,4

  External employer: Average 3,5 / Median 4 / SD 1,4

- practicality

  ICT Company X: Average 3,5 / Median 4 / SD 1,4

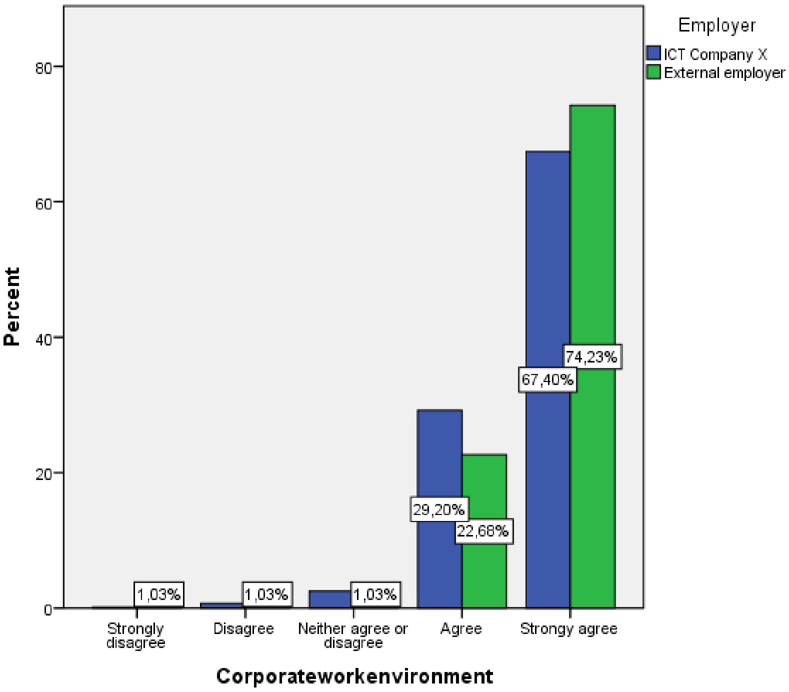
  Externa employer: Average 3,4 /Median 4 / SD 1,4

- facts

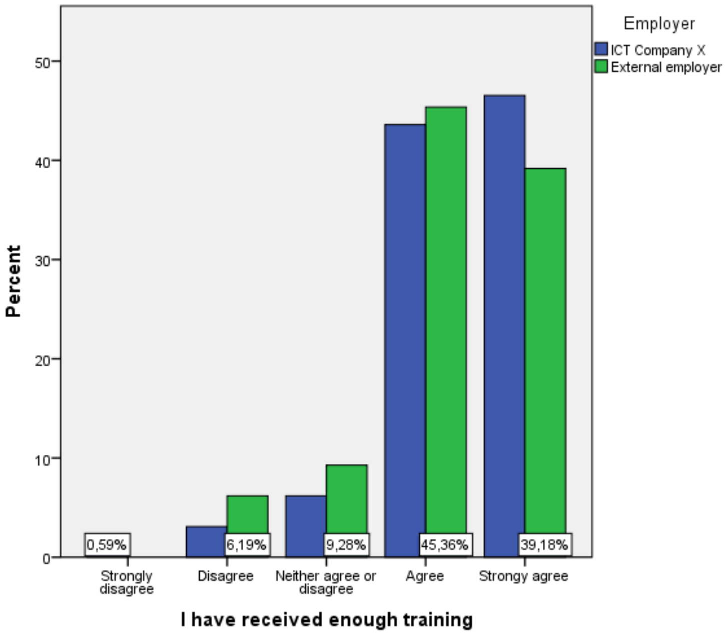
  ICT Company X: Average 3,6 / Median 4 / SD 1,4

  External employer: Average 3,6 / Median 4 / SD 1,4

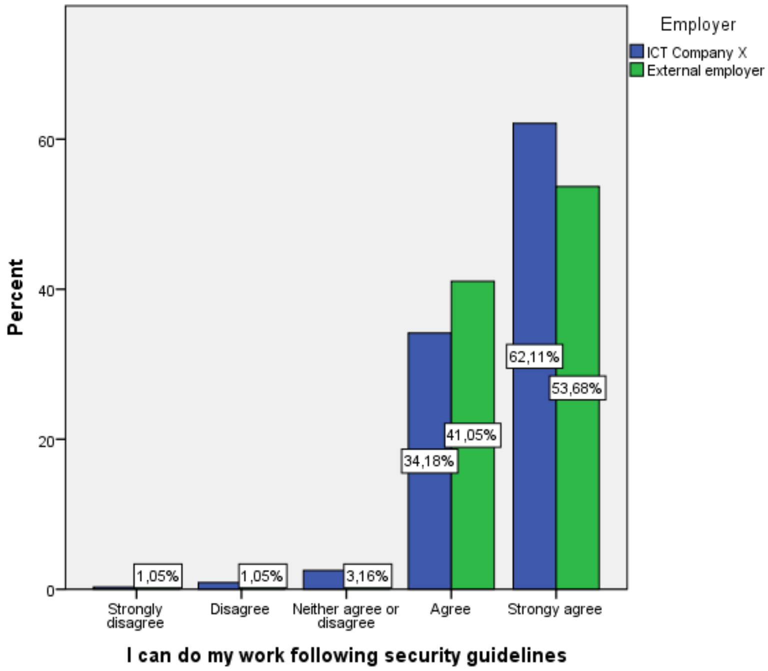
9. I think that the work environment in ICT Company X is safe. N 775 (678 ICT Company X and 97 External employer)



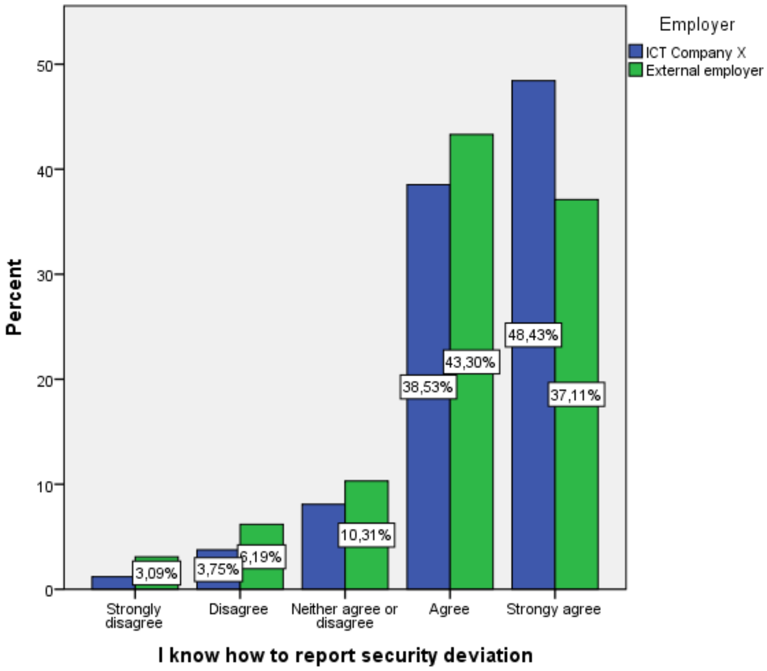
10. I have received enough training and guidance to security related issues in ICT Company X. N 776 (169 ICT Company X and 97 External employer)



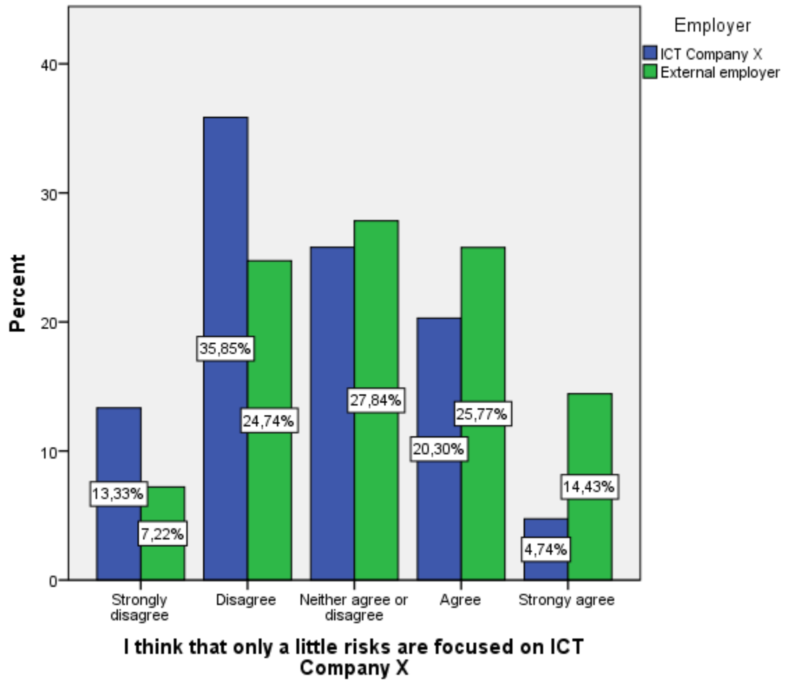
12 I can work by following ICT Company X's security requirements. N 768 (673 ICT Company X and 95 External employer)



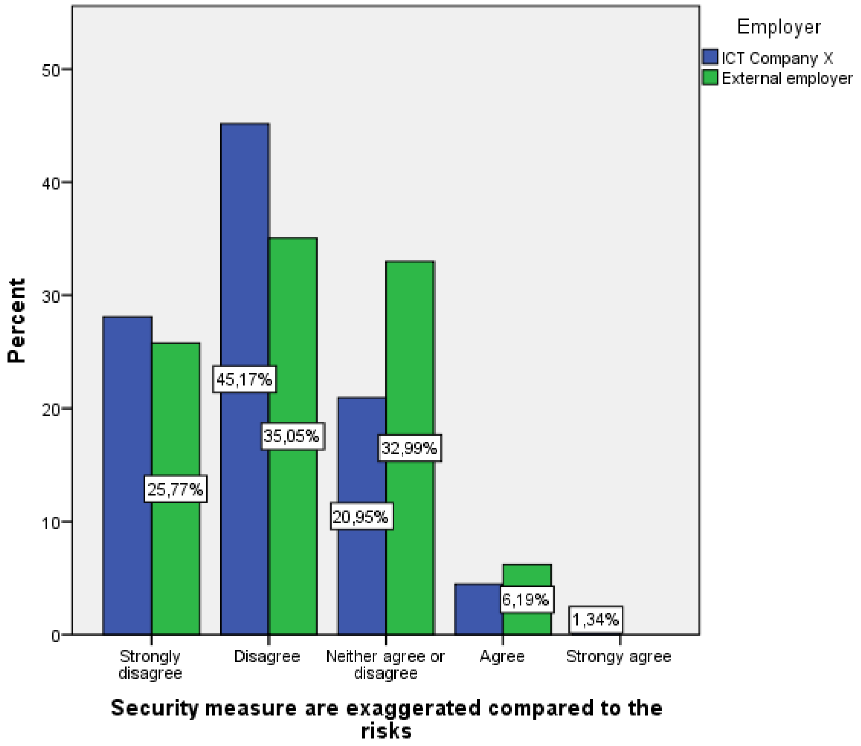
13 I know how to report a security deviation. N 764 (667 ICT Company X and 97 External employer)



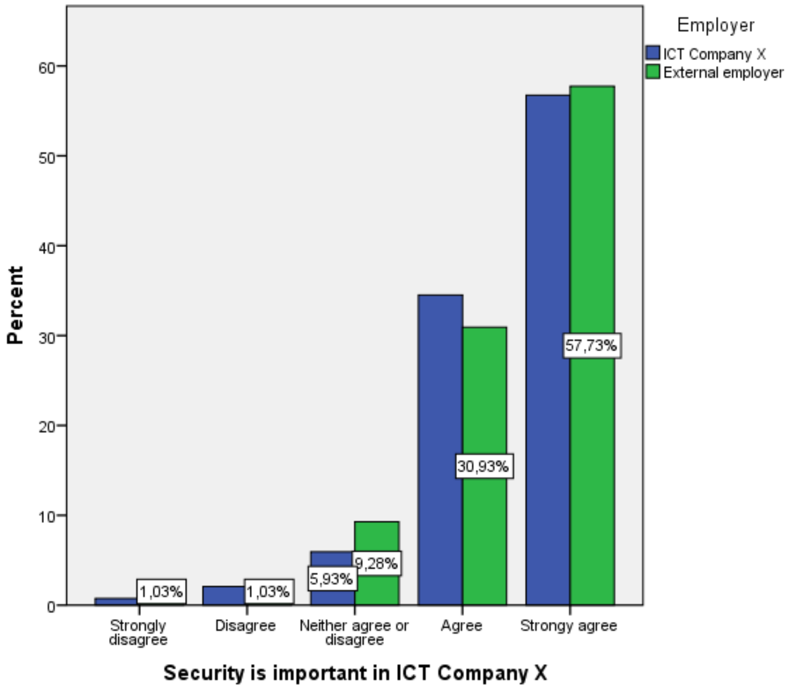
14 I think that only a little security risks are focused on the business of ICT company X in its field. N 772 (675 ICT Company X and 97 External employer)



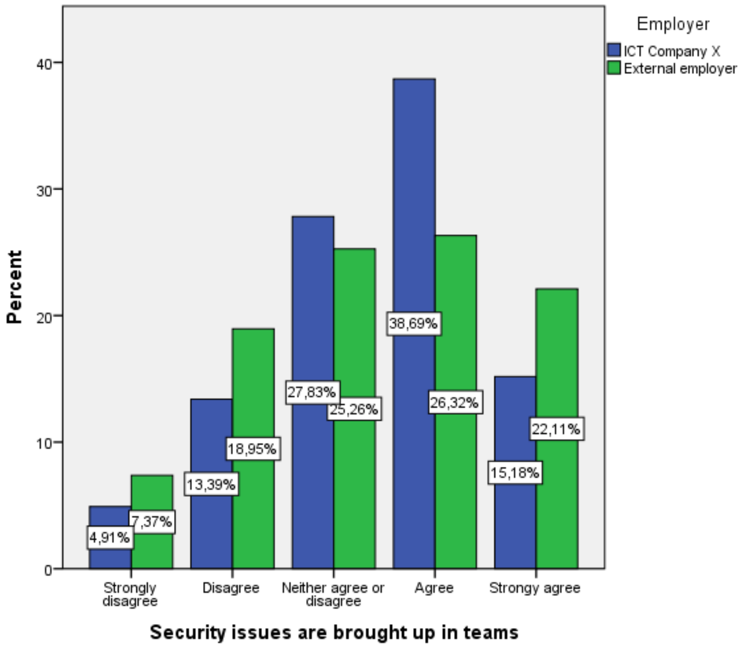
15 I think that ICT Company X's security measures are exaggerated compared to security risks. N 770 (673 ICT Company X and 97 External employer)



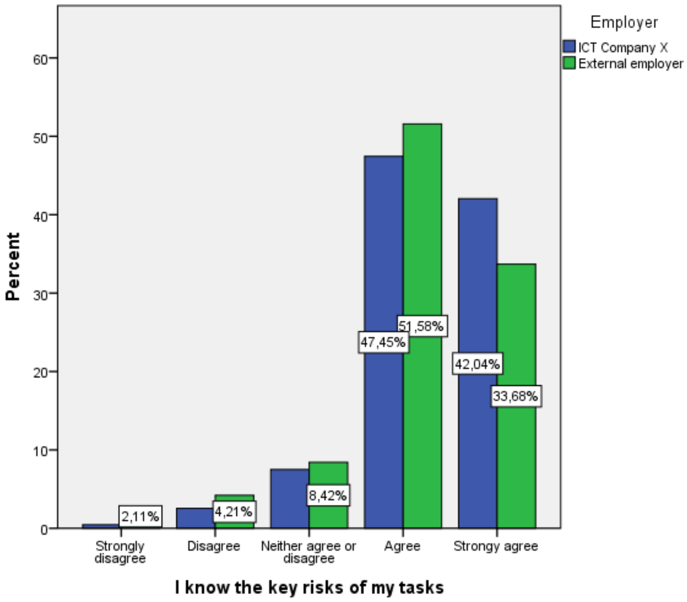
16 Security is important in ICT Company X. N 772 (675 ICT Company X and 97 External employer)



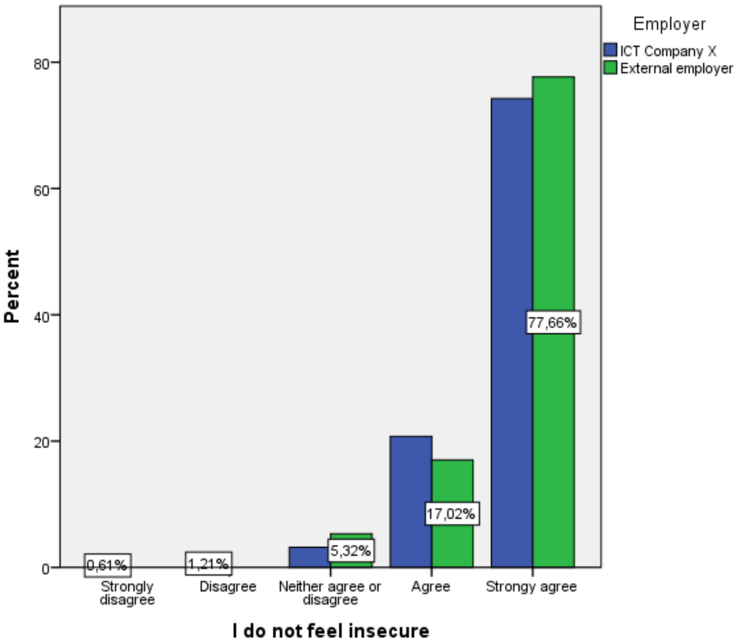
17 My team brings up security related issues regularly. N 767 (672 ICT Company X and 95 External employer)



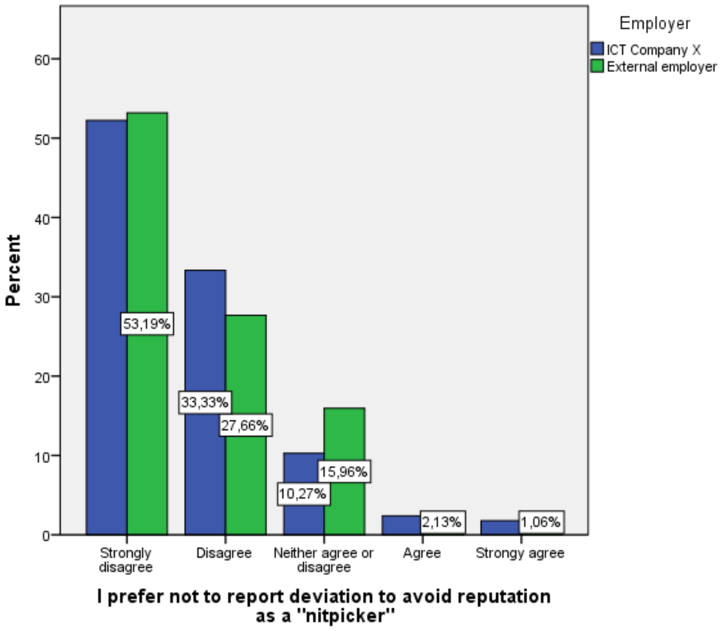
18 I know the central security risks in a scope of my own tasks. N 761 (666 ICT Company X and 95 External employee)



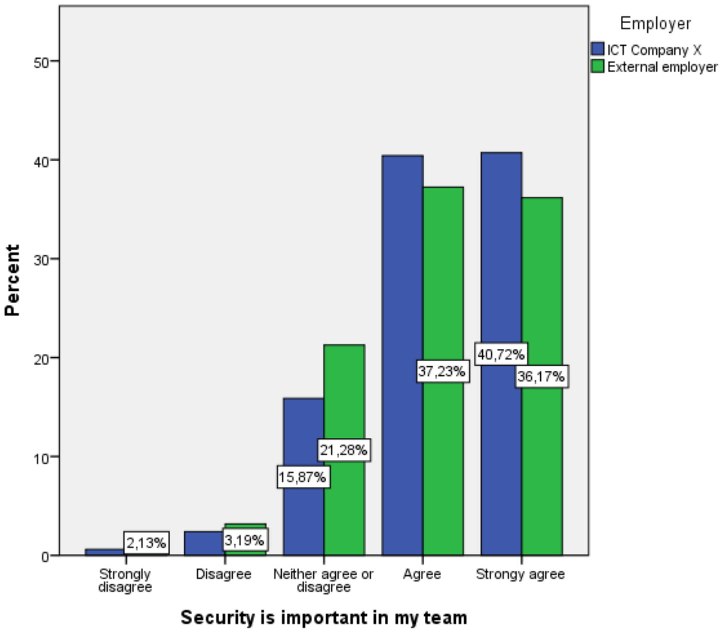
19 I do not feel insecure. N754 (660 ICT Company X and 94 External employer)



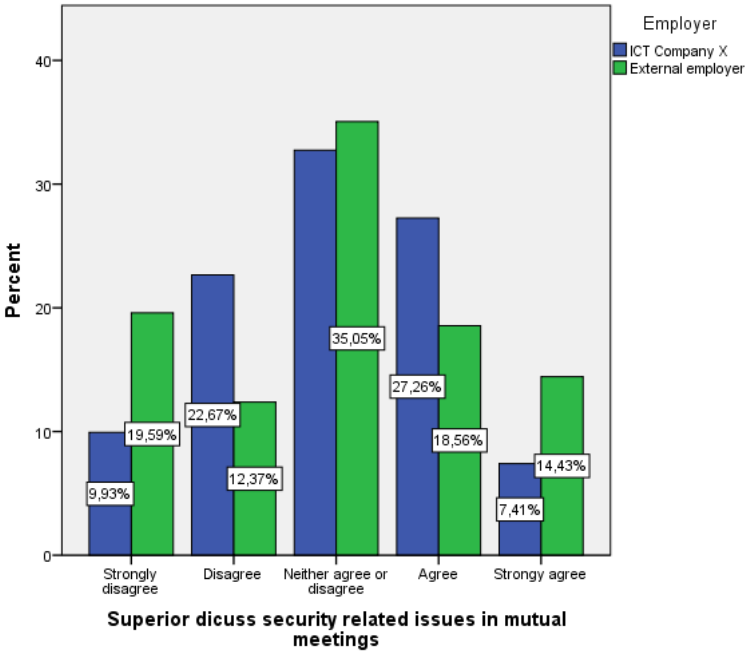
20 I prefer not to report security deviation I have noticed to not get reputation as a nitpicker. N 766 (672 ICT Company X and 94 External employer)



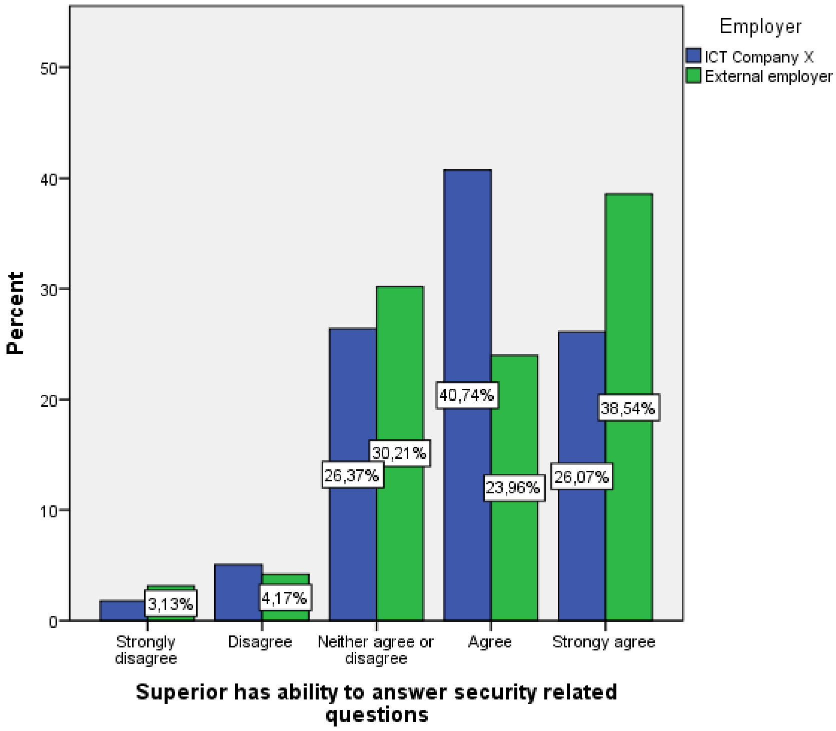
21 My team thinks that security is important. N 762 (668 ICT Company X and 94 External employer)



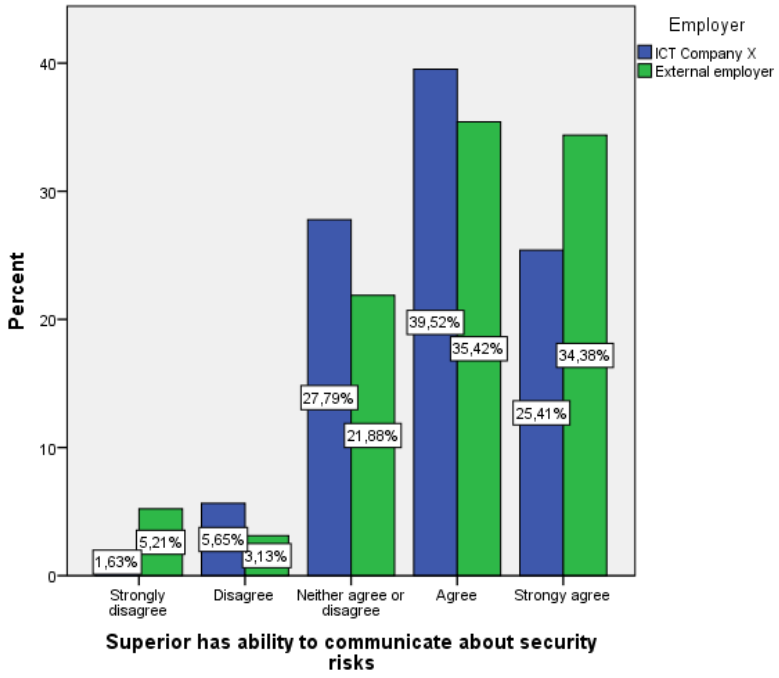
22 My superior brings up to the conversation security related issues in mutual meetings, for example, in goal setting palaver. N 772. (675 ICT Company X and 97 External employer)



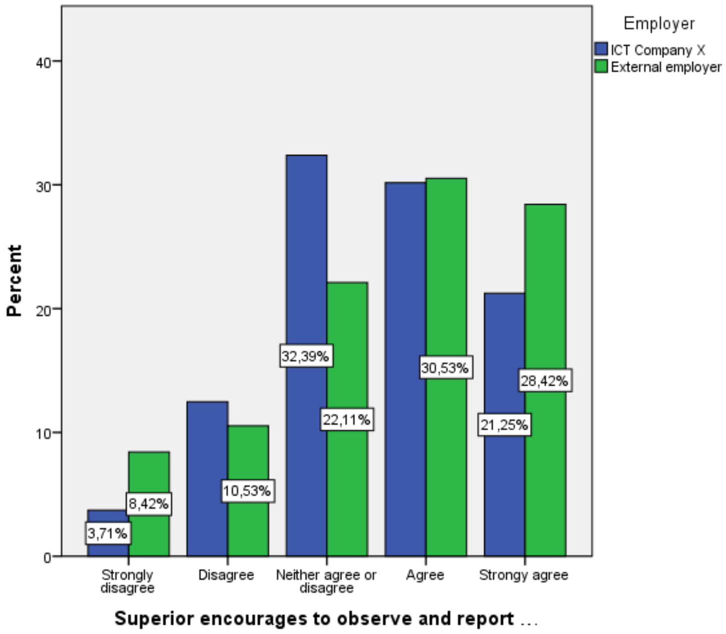
23 My superior has ability to answer my security related questions. N 771 (675 ICT Company X and 96 External employer)



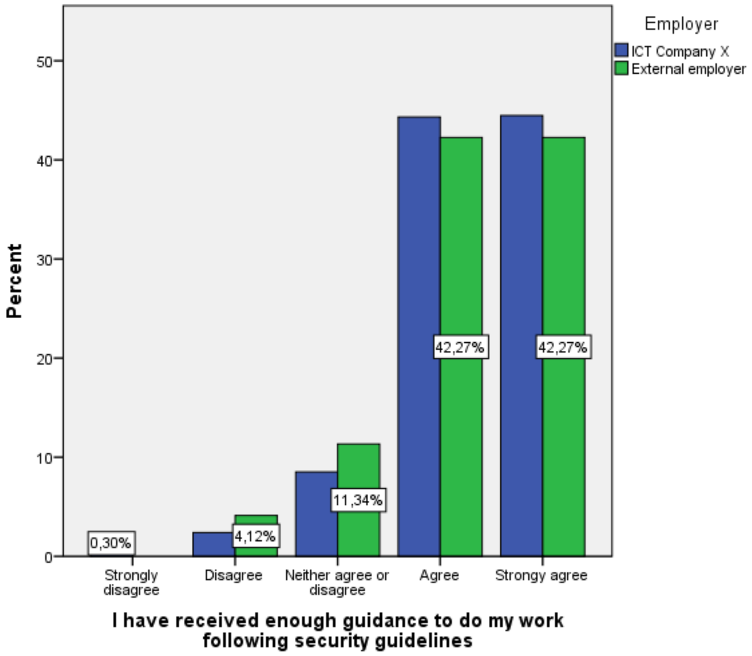
24 My superior has ability to communicate security risks influencing our operations. N 769(673 ICT Company X and 96 External employer)



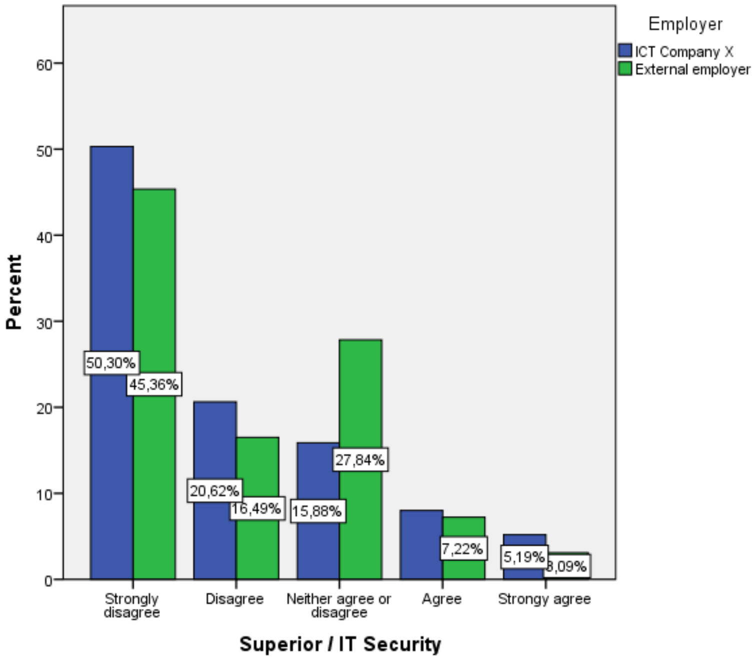
25 My superior encourages me to observe and report security deviations. N 768 (673 ICT Company X and 95 External employer)



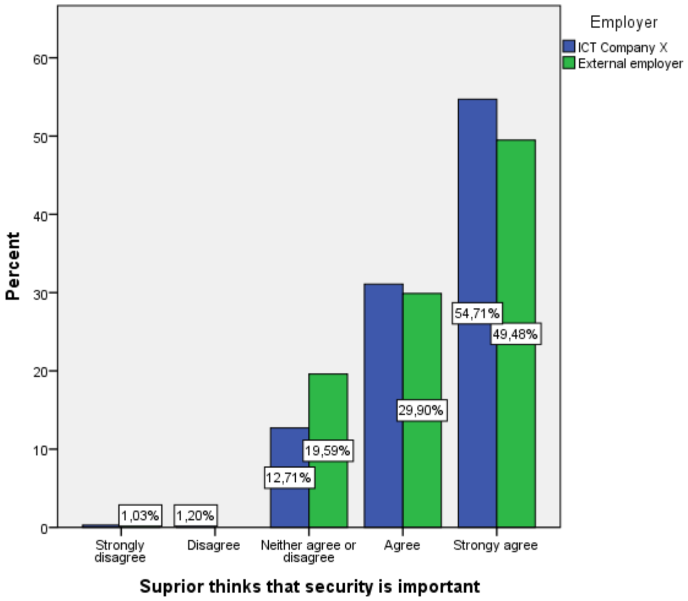
26 I have received enough guidance to do my tasks following security guidelines of ICT Company X. N 767 (670 ICT Company X and 97 External employer)



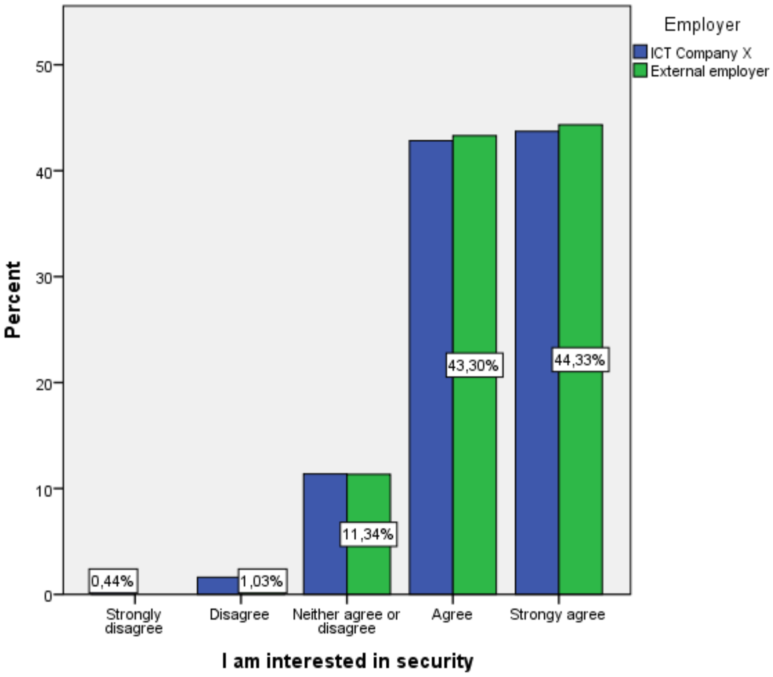
27 My superior thinks that IT Security is not one of our team's responsibilities. N 771 (674 ICT Company X and 97 External employer)



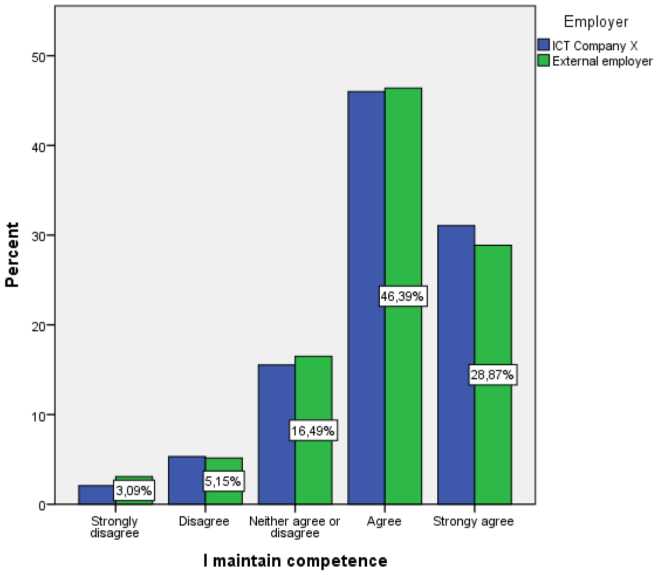
28 My superior thinks that security is important. N 766 (669 ICT Company X and 97 External employer)



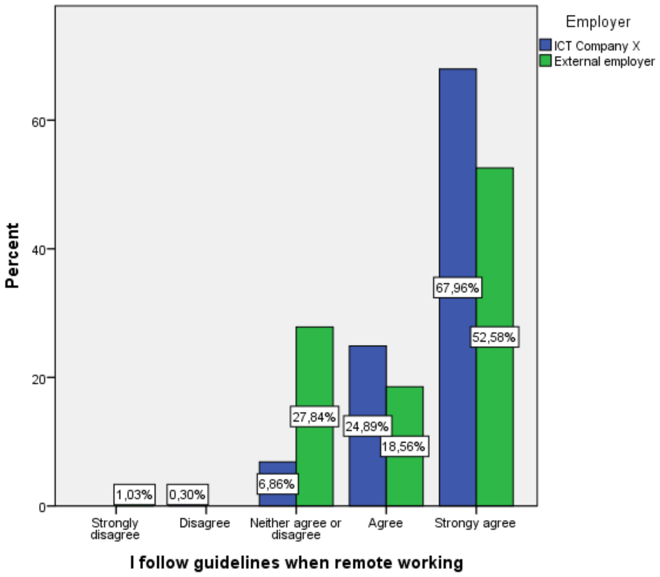
29 I am interested in security at the workplace. N 774 (677 ICT Company X and 97 External employer)



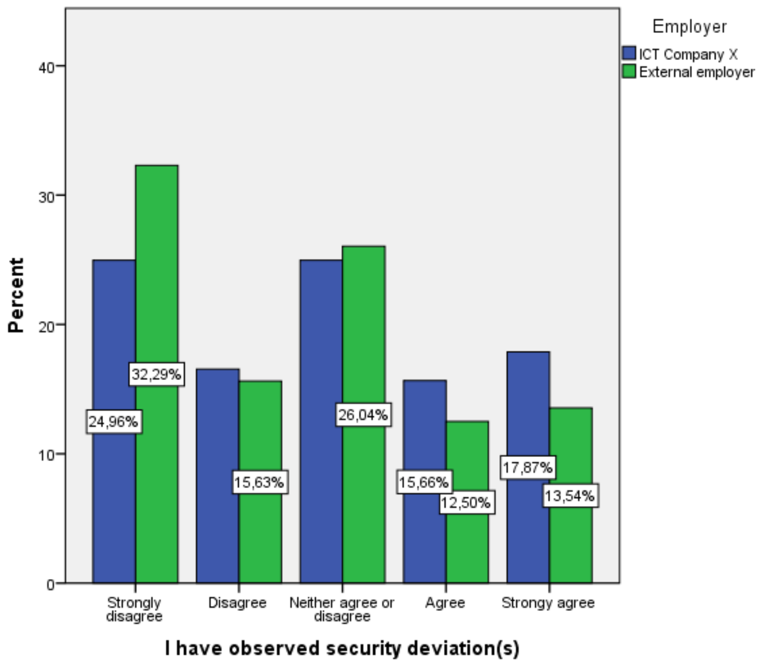
30 I maintain my security awareness by reading instructions, for example from internal website. N 773 (676 ICT Company X and 97 External employer)



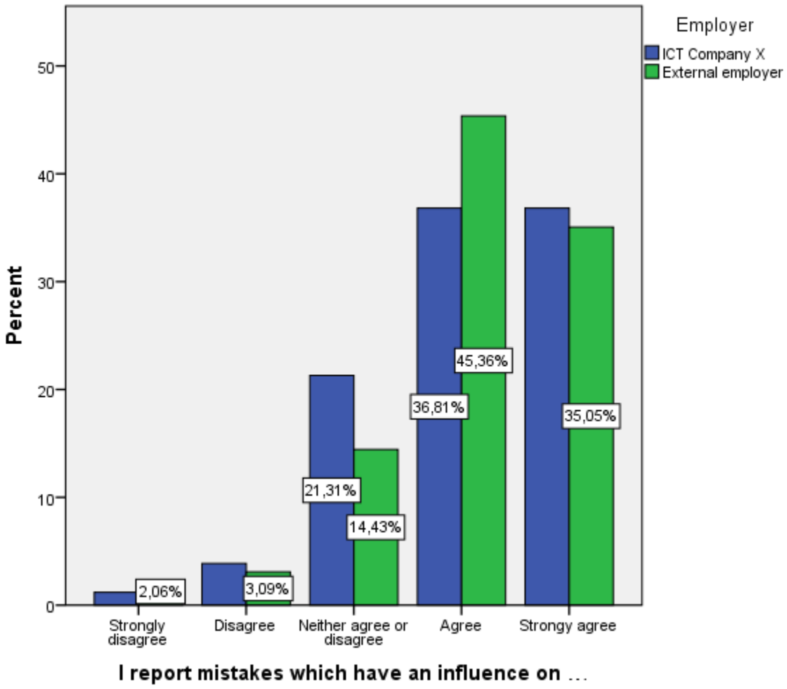
31 I follow ICT Company X’s security guidelines also when I am not working in the company’s premises. N 768 (671 ICT Company X and 97 External employer)



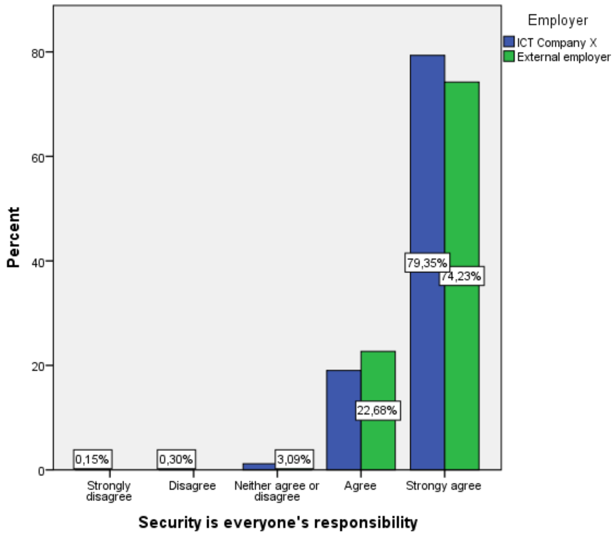
32 I have observed at least one security deviation during the past half years. N 773 (677 ICT Company X and 96 External employer)



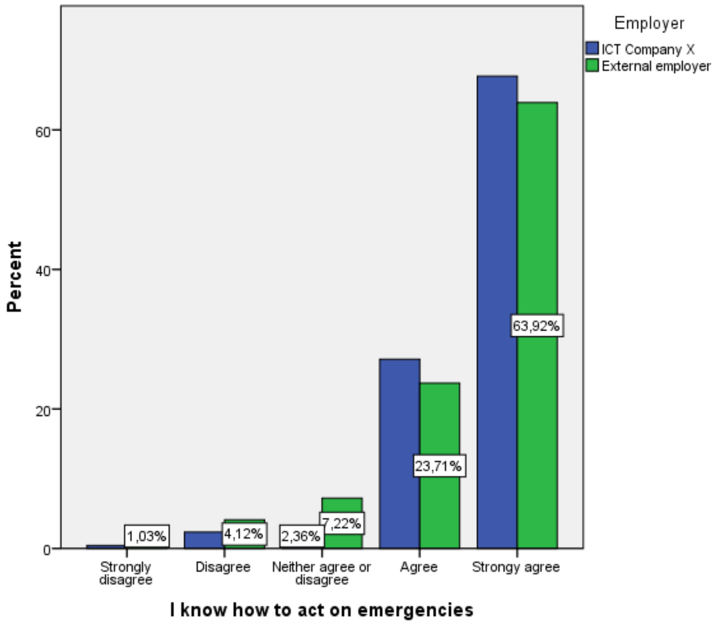
33 I report the mistakes that have an influence on security, regardless if I did the mistake by myself. N 768 (671 ICT Company X and 97 External employer)



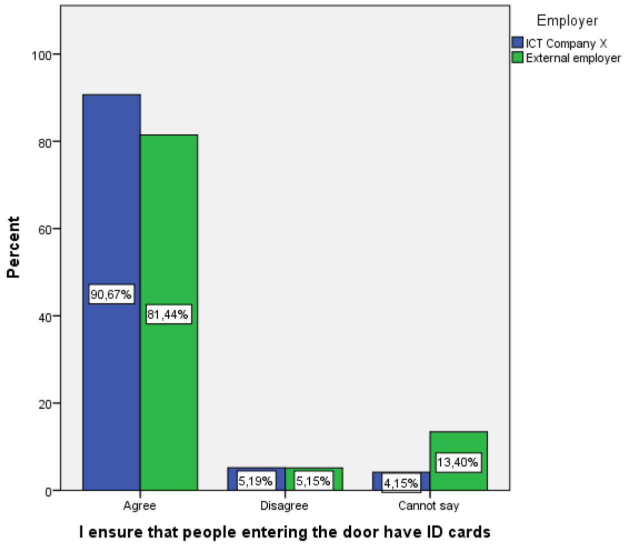
34 I think that everyone working in premises and/or processes of ICT Company X are responsible for security. N 770 (673 ICT Company X and 97 External employer)



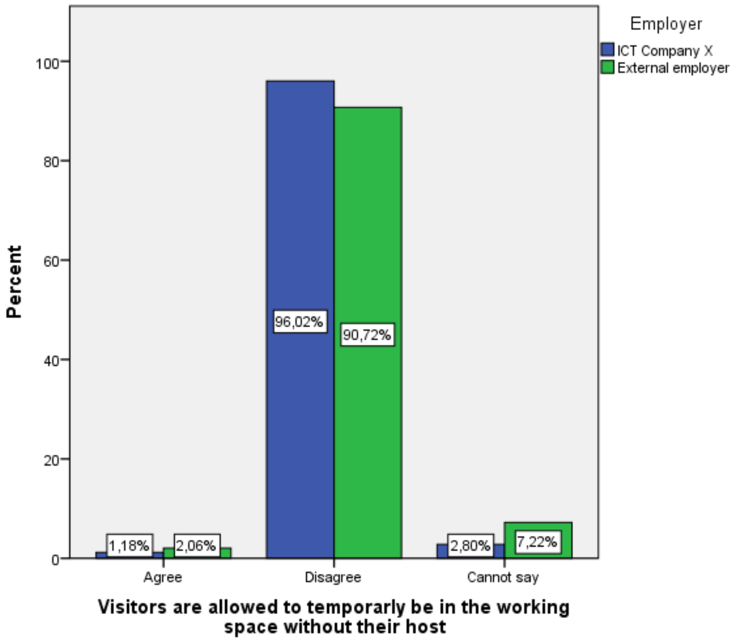
35 I know how to act in exceptional situations, for example during a fire alarm. N 775 (678 ICT Company X and 97 External employer)



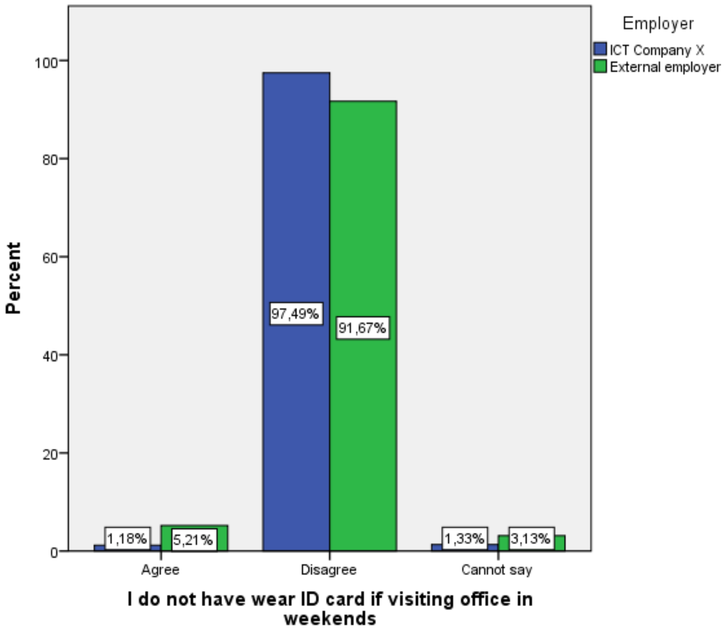
36 I ensure that people entering with the same opening of the door are wearing their ICT Company X ID cards, at the workplace. N 772 (675 ICT Company X and 97 External employer)



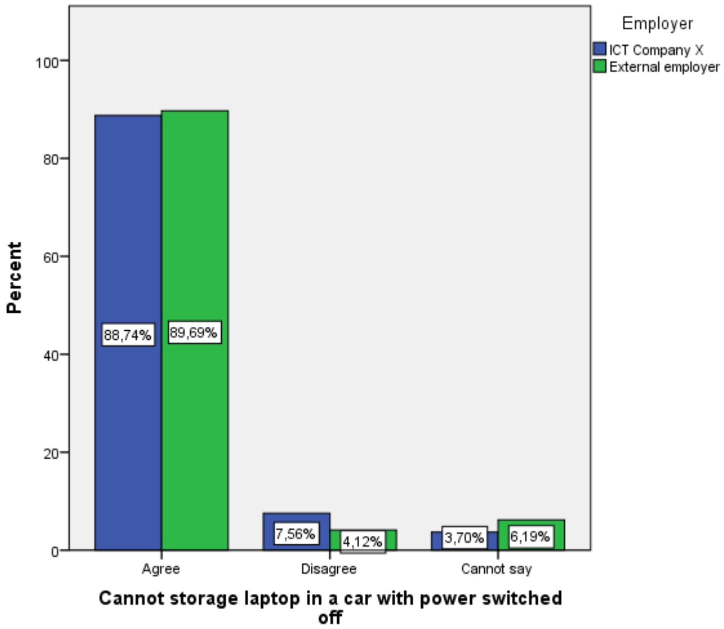
37 Visitors are temporally allowed to be in the working area of ICT Company X without their host. N 775 (678 ICT Company X and 97 External employer)



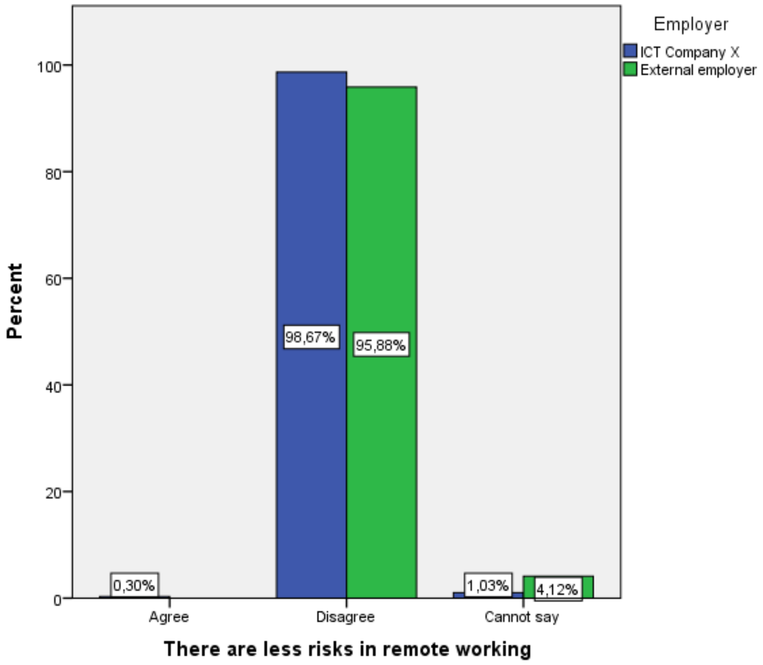
38 I do not have wear ICT Company X’s ID card when I am visiting the premises during a weekend. N 772 (676 ICT Company X and 96 External employer)



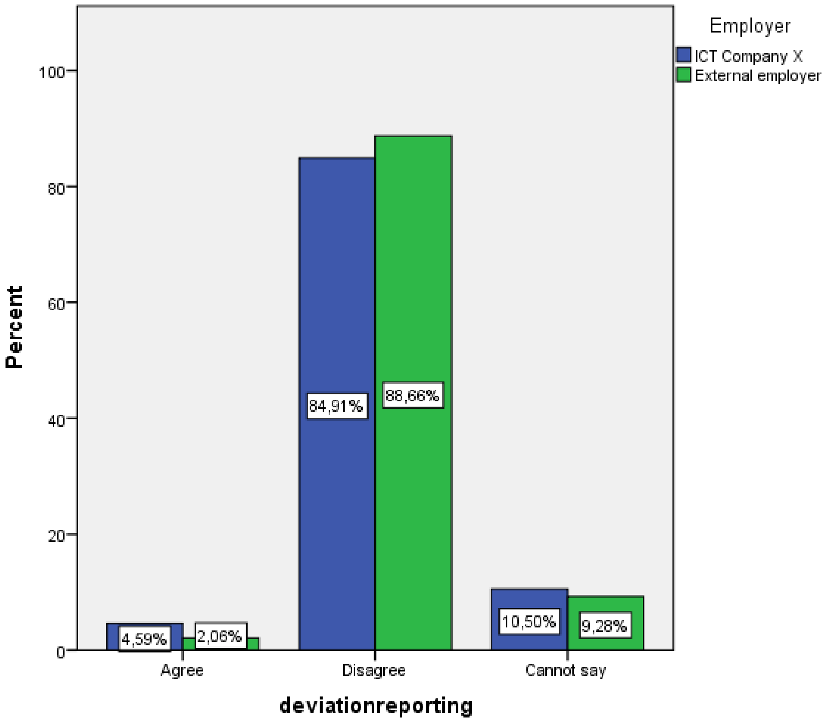
39 It is not allowed to storage laptop at car, even though the power has been switched off. N 772 (675 ICT Company X and 97 External employer)



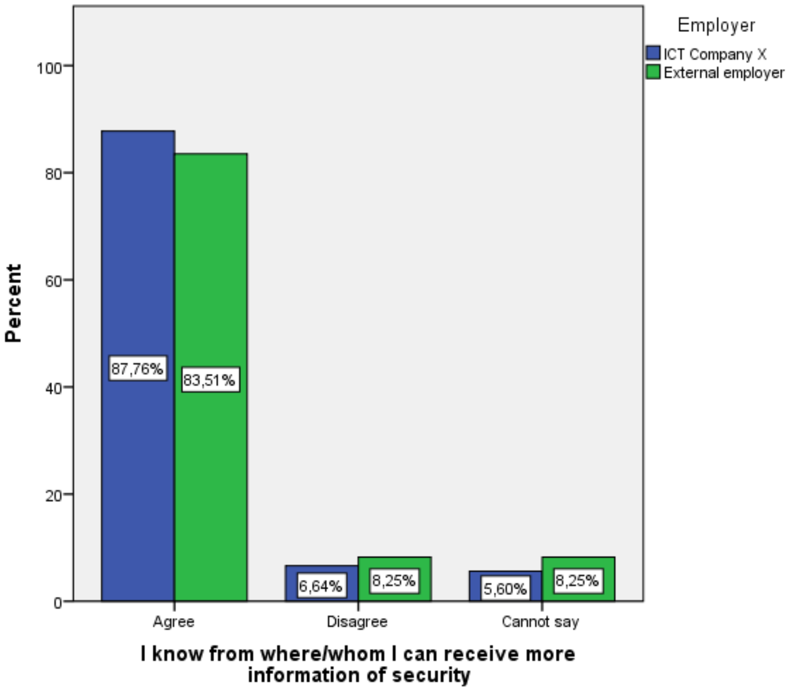
40 When I am working from distance I do not need to worry about the confidentially of the information, because there are less risks. N 774 (677 ICT Company X and 97 External employer)



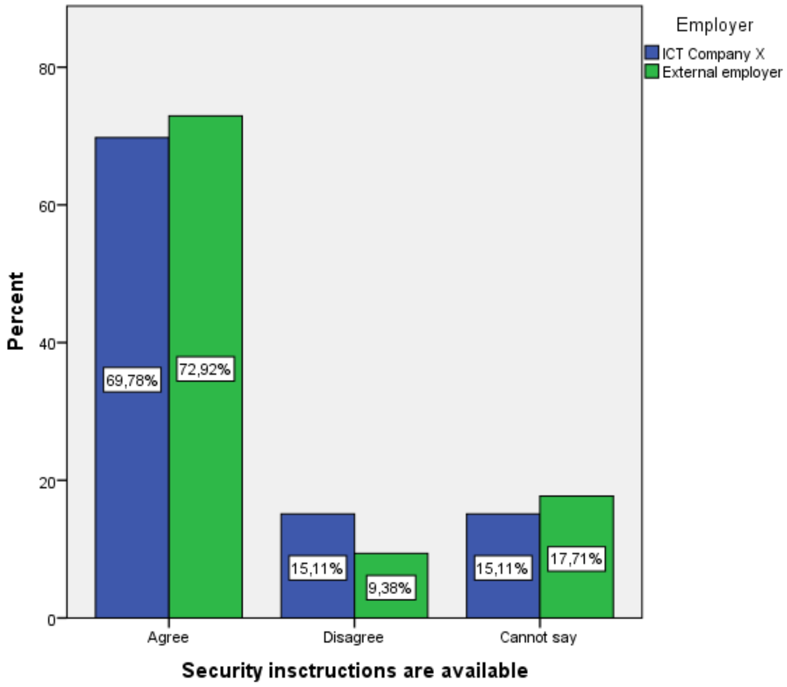
41 Reporting security deviation can cause nitpicker reputation. N 773 (676 ICT Company X and 97 External employer)



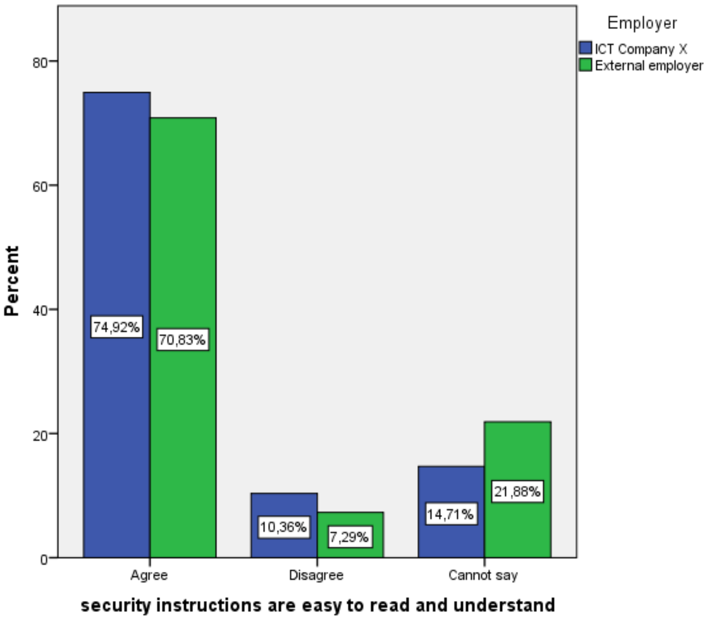
42 I know from where/whom I can approach for guidance in security issues. N 775 (678 ICT Company X and 97 External employer)



43 Security related instructions are easily available. N 771 (675 ICT Company X and 96 External employer)



44 Security related instructions has been written clearly and they are understandable. N 762 (666 ICT Company X and 96 External employer)


Employer
ICT Company X
External employer
Percent
80
60
40
20
0
74,92%
70,83%
10,36%
7,29%
14,71%
21,88%
Agree
Disagree
Cannot say
security instructions are easy to read and understand