UNIVERSITY OF APPLIED SCIENCES UTRECHT

MASTER OF INFORMATICS

MASTER'S THESIS

Influencing Factors towards Non-Compliance in Information Systems

Carelessness and Shadow IT in the corporate workplace

Author:

Taco Dols

Date:

October 24, 2009

University of Applied Sciences Utrecht
Faculty Science and Engineering
P.O. box 182
3500 AD UTRECHT
The Netherlands

Image: © 2008 Moebius Technology

Abstract

IT organizations and CEO's are –and should be- very concerned about the lack of data confidentiality and the usage of 'shadow IT' systems by employees. Data breaches may result in monetary loss, public embarrassment for the company or even fines or imprisonment for senior management. This makes it essential that employees comply with the IT security policies.

This paper presents a study which aimed to identify factors which influence the usage of Shadow IT, carelessness and non-compliance towards data security. Since Shadow IT and non-compliance can be the result of reduced spending on IT projects, the study was also focusing on finding out if it is the perception of employees that their company displays an increased focus on IT control and IT investment selectivity. Significant factors were selected using a review of the existing literature, and then tested in a survey among employees of PricewaterhouseCoopers in The Netherlands and Belgium.
Desk research identified factors, which cause employees not to follow the IT security policies, including:

- Carelessness. Surveys indicated that most data breaches are often caused by careless or ignorant employees. Carelessness is caused by an incorrect assessment of the risk involved.
- Lack of awareness and lack of training and education. Businesses with IT security training programs in place have reduced levels of risk.
- Lack of Business – IT alignment. Poor accessibility, slow responsiveness, lack of dedication and knowledge of the users' business are drivers for employees to look for IT solutions outside the company IT department.
- Increased attention for IT Governance has been tested as a driver for non-compliant behavior towards IT Security. Stricter IT Governance results in stricter policies, stronger security measures and tighter budgets.
- Different national cultures. Research by Hofstede was used when analyzing links between national cultural dimensions and information security behavior.

The survey, which was conducted in The Netherlands and in Belgium, asked the respondents to agree or disagree with 16 statements on awareness, carelessness and compliance with IT security policies. The results showed differences in attitude and behavior between nationality, gender and age. The survey results did not establish clear links with poor Business – IT alignment or with reduced capacity or funding for IT projects (IT Governance).

Dutch survey respondents showed higher assertiveness and more non-compliant behavior than Belgians. Employees from both countries would equally break the IT security policies if their boss asks them.

Women showed different IT security behavior then men. Older employees showed more compliance with these policies than younger employees.

Against expected outcomes, employees did not feel the impact of increased IT governance. Most respondents just didn't know if less budget for IT initiatives was available than before. It was not a motive for non-compliant behavior. Overall, respondents are satisfied with the technology the IT department provides to them. However that doesn't prevent them to often bend or bypass the IT security rules whenever they are not convenient.

Based on desk research and survey results, a framework has been presented to assist in developing programs for effective security awareness training and developing, improving, monitoring and/or developing or rethinking the IT security guidelines.
The outer layer of the model shows the influencing factors researched in this thesis.
The middle layer gives the cycle for setting up policies, conducting training, monitor compliance and review of policies.
The core of the framework shows the four key elements of effectively communication the policies to the end users: What, How, Why and Where.

Preface

This thesis is the final work of my Master study at the Utrecht University of Applied Sciences. It serves as documentation of my research during the study, which has been made from December 2007 until October 2009. It presents the results of a study towards aspects of data security awareness with corporate employees. It specifically looks at aspects such as the usage of shadow IT and possible cultural different attitudes towards data security.

It was a true learning experience and I had fun digging into the many, many books and documents on this subject but it was also a road paved with delays and unexpected problems.

For their help, I would like to thank the following persons in particular:
Wiebe de Witte, thesis speculator, for his advice and feedback, and for his motto “As 't net kin sa't moat, dan moat it mar sa it kin” (If it cannot go as it should, then it should go as it could.)
I also would like to thank my former manager Ronald Hunse for allowing me two weeks off in august 2008 to work on the thesis and to Desire Schück for setting up the survey for me in NetQ.
Then a big thank you to Hans Weerd, Information Security Officer at PwC, for his efforts to get Germany, UK, Switzerland and Spain on board to participate in the survey. Unfortunately, due to various reasons, I only managed to get approval for sending out surveys to The Netherlands and Belgium.
This brings me to thank Gilbert Silvius and the other members of the exam committee to allow the thesis to be completed based on the results of those two countries.

Finally I would like to thank my wife for her encouragements to take on this study and putting up with me for the past three years, spending many evenings away from home or hidden behind my computer.

Utrecht, October 24, 2009
Taco Dols

Contents

Figures and Tables

Chapter 1

1. INTRODUCTION

"… The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network…"

Article 17 of the European Union Data Protection Directive, 1995, p.31-50

1.1 BACKGROUND

Information security is a widely discussed topic these days (For example Brooke 2004, Gordon 2005, NewDilligence 2006, Ponemon 2007, IronPort 2008). Despite years of investments in technology and processes, truly protecting data remains a distant goal for information security officers (Al Awadi and Renauld 2007). Figuring out what, when and how to protect, in combination with requirements of regulatory compliance, has become very complex and has created the need for a new approach, which includes establishing meticulous risk fundamentals and which requires using a holistic technical understanding (Richards 2008).

New technological developments such as Software-as-a-service, Web 2.0 technologies and multi-media hardware like iPhones increase the number of possibilities for sensitive information falling in the wrong hands. Regulations, statutes, and contractual expectations overwhelm IT managers with audit requests and build up the pressure to do something about the problem. To make matters worse, some companies are decreasing their investments in security, at least in some areas, in order to save money (Forrester 2009), and recent lay-offs increase the risk of disgruntled employees taking off with sensitive data (Gage 2009).

The risk is real and the problem is huge: In a survey of 1000 IT managers in the U.S. and Europe in January 2009, almost all respondents, 98%, said their organization has experienced tangible loss as a result of a cyber attack incident and 31% experienced theft of customer or employee personally identifiable information. Another 25% were hit with theft of corporate data (Symantec 2009). And according to a recent study by the Verizon Business RISK team (2009) more electronic records were breached in 2008 than the previous four years combined, and 93 percent of the 285 million(!) breached records were accessed by organized crime. The percentage of breaches involving financial service organizations, including accounting firms, targeted attacks, and customized malware all doubled in 2008.

Threats come from many sides: malicious outsiders, malicious insiders (employees), and negligent insiders. Some argue that careless and negligent employees pose the greatest security threat to a company (Ponemon 2006, Krom 2006, Whitty 2006, Moreau 2007).

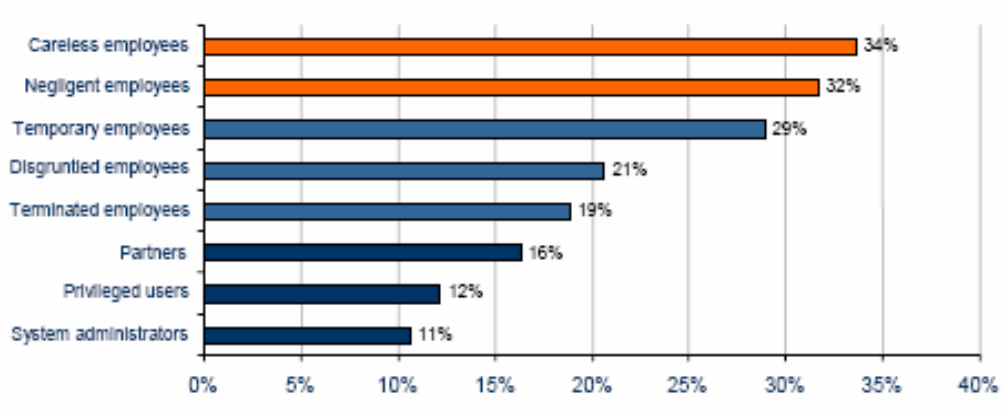


Figure 1: Ponemon Institute research result among 461 IT professionals
"Which categories of your staff pose the greatest risk of an insider threat?"

Other research suggests that insiders account for only two in ten data breaches in the past 5 years (Verizon 2009).

This thesis will try to identify the factors that negatively influence data confidentiality for these insiders or employees. For example the carelessness with which employees approach data security and the usage of 'shadow' IT systems by these same employees.

1.2 TRENDS

The two examples above may seem very distinct topics, yet they have in common that the employees seem to lack awareness of possible risks and lack of awareness of company policies for information security. Also, both topics find themselves in the media spotlight lately. Several trends can be accredited to this increased attention.

First, a decrease can be seen in 'traditional' attacks by viruses, spyware and malware (CSI/FBI 2005, IronPort 2008). Instead, an increase is seen in more sophisticated attacks like phishing and social engineering. Malicious outsiders ("hackers" and "cyber-criminals"), faced with increased security and countermeasures companies have put into place, seem to have shifted their focus. The attackers now seem to have two new targets that allow them to easily evade firewalls, antivirus, and even intrusion prevention tools: 1] end-users who are easily misled and 2] custom-built applications. This is a major focal shift from prior years when these attackers limited most of their targets to flaws in commonly used software. (SANS 2007)

Second, trend research indicates that more and more people perform parts of their work tasks from home (Hotopp 2002, CPB 2004). Evidence suggests that this so-called "teleworking"' has boosted worker productivity and innovative performance throughout the

EU economy (Reichwald *et al.* 1998, SIBIS 2002). Working from home is however largely beyond the control or supervision of the IT department. This also includes the transport of sensitive or confidential company information home on data carriers such as laptops, USB sticks and shared internet storage.

Third, a research done by Dutch Internet magazine Webwereld.nl (2008) among 2389 employees and management in The Netherlands showed that management thinks that unintentional (23%) or intentional (9%) distribution of confidential information by own employees poses the biggest security risk at the moment. One in six companies actually experienced such events. These results are backed up by research done by the Ponemon Institute (2006 & 2007). As mentioned before, research (Verizon 2009) states that insiders only account for one in five data breaches, but when one includes misuse of access privileges, violation of IT security policies, user error and omission, employees are a contributing factor in nearly all data breaches.

Fourth, IT technology seems to become less and less the main driver of innovation. One does not buy software anymore, one buys functionality. The public does not want to be bothered with where the technology is located and how it is composed. This is similar to Telecommunications where one doesn't want to worry about the enormous technical complexity of calling a colleague in another part of the world, but just expect this to work. The technology part is shrouded in a 'cloud' of mystery. The term cloud is also used as a metaphor for the Internet. This trend is therefore often related to as Cloud Computing.

Cloud computing can broadly be defined as Internet-based development -and use of- computer technology. Cloud computing services usually provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. This concept incorporates software as a service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS) as well as other recent technology trends like Web 2.0, where the common theme is reliance on the Internet for satisfying the computing needs of the users.(Desisto *et al.* 2008). But with the ever increasing bandwidth available to internet users, a number of "free" online (office) applications have emerged in the last three years.

Google Docs for example is a free, Web-based word processor, spreadsheet, and presentation application. It allows users to create and edit documents online while collaborating in real-time with other users. Google Docs was released early 2006. This was quickly followed by ZoHo Office Suite, ThinkFree Office and SimDesk in 2006, and ShareOffice in 2007, offering similar or better functionality (Wikipedia 2008). Even Microsoft joined in with its introduction of Microsoft Office Live Workspace in March 2008.

It is clear that a company IT department has no control over or ability to secure such data flows. This was made painfully clear in 2008 when users of the Google Docs word-processing program couldn't access documents for around an hour on July 8, Amazon's S3 online storage service experienced outages for eight hours on July 20, and Apple's MobileMe service left one percent of its users without e-mail for 10 days between July 18 and July 28 (Choney 2008). In fact, cloud computing has "*unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing*", Gartner says (Heiser, Nicolett 2008).

1.3 RESEARCH JUSTIFICATION

Often employees are unaware of the existence of security policies or do not see the relationship between the policy and their daily tasks and see it more as a nuisance (Höne and Eloff 2002). The essence of IT security governance is to determine sufficient levels of control that still support business objectives. Too much governance will inhibit innovation and the ability to react quickly to new opportunities. Too little governance will expose the business to unnecessary risks. The balance needs to be just right (Brooke 2004). Finding factors that influence the employee behavior towards data confidentiality could result in finding that valuable balance.

1.4 RESEARCH IDEA

The initial idea was to measure the effects of 'shadow IT' on business. Shadow IT is a technology term for any application or transmission of data relied upon for business processes, which is not under the jurisdiction of a centralized IT or IS department (Sherman 2004). It creates 'unofficial' and uncontrolled data flows and may include transportation of data on USB sticks or CD's, even if company policy does not allow this. Besides the obvious and often documented risks involved with the usage of Shadow IT, there could also be positive effects due to, for example, increased flexibility.

In addition to looking at 'what', it could also be useful to look at the 'why'. One viewpoint could be that increased focus on justification of IT spending (IT governance) unwillingly promotes the usage of shadow IT systems. There are strong indications that "*some business units initiate IT projects outside of corporate IT because of significant reductions in IT spending and an increasing demand for IT to address infrastructural issues, including but not limited to security, regulatory compliance, technology migration/updates, and service level maintenance*" (Moreau 2007). This also suggests a possible relationship with IT Governance.

This is another interesting idea on which to form the second basis of this thesis.

1.5 RESEARCH QUESTIONS

The research idea leads to the following overall research question:

Which factors influence the usage of Shadow IT and carelessness towards data security?

When looking at the concept of IT security, often a distinction is made between technical risk factors and human risk factors (Ponemon 2007, Sherman 2004, Schaffner 2007). This thesis research will help to identify some of those human risk factors. For example, cultural different attitudes towards the perception of risk might be one of those factors. (Rundmo *et al.* 2004, Hofstede and Hofstede 2005).

As stated in the previous paragraph, Shadow IT might result from reduced spending on IT projects, so in order to answer the overall question, one first needs to ask two sub-questions to establish if:

- *it is the perception of employees in general that their company displays an increased focus on IT control and investment selectivity*, and if so,
- *That this increased focus results in reduced or delayed spending on IT projects which they feel limits them to perform their work effectively and competitively*.

A number of questions need to be answered beforehand in order to get a common understanding of the topics discussed:

- *Which security risks can be derived from literature?*
- *Are national cultural differences aspects of importance?*
- *What other influencing aspects can be defined and which will be tested?*
- *How can awareness be defined and can levels of awareness be identified?*
- *What forms of shadow IT can be defined?*

Obviously, many more questions could have been developed, but a relevant selection has been made in order to keep the size of both the desk research and the questionnaire within the limits of 'goodwill' of the respondents.

1.6 RESEARCH APPROACH AND RESEARCH STRATEGY

The possibility to identify the influencing factors will depend on many factors and may differ from organization to organization and nationality to nationality. This makes it likely that an answer containing all possible factors is not to be found and/or answers covering all questions will not be possible. However, the research method chosen must be able to provide fundamental, general findings (facts).

For this a research flow is designed which depicts the approach for this survey.

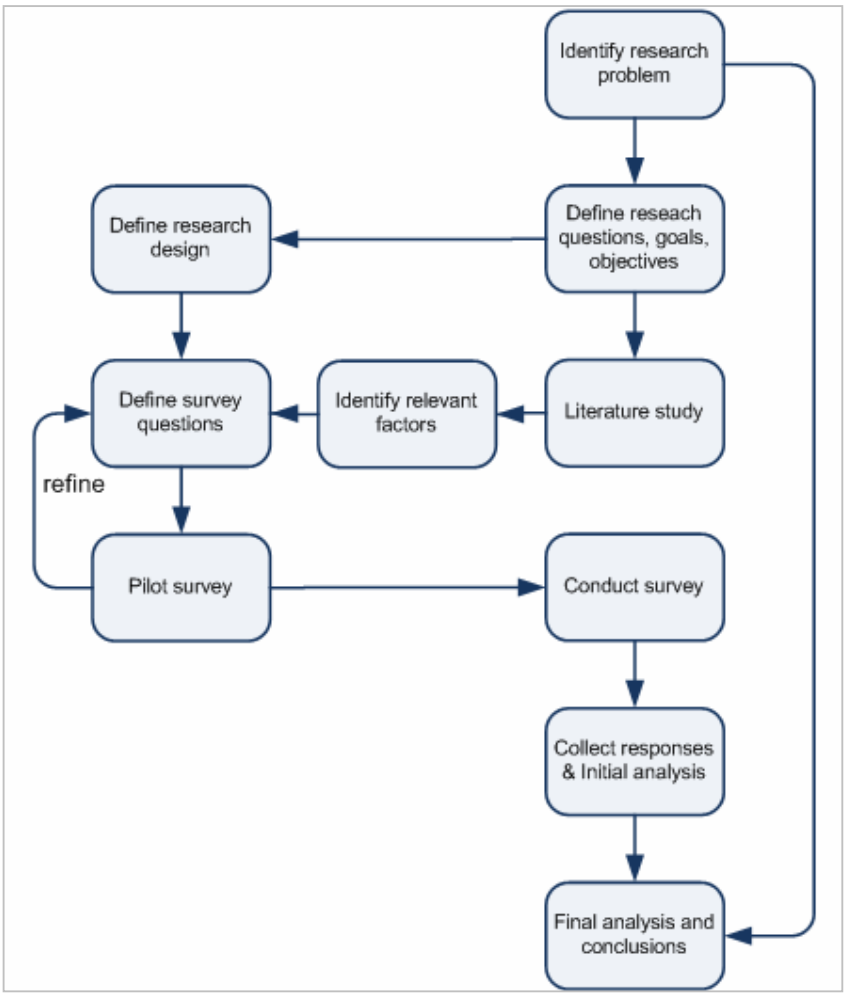


Figure 2: Research design flowchart

As the topics are of a contemporary nature, one of the challenges is to find research papers that relate to the topic and to design a questionnaire in a way that is most likely to answers the questions. When looking at the available knowledge and subject data, the most appropriate research approach is one of induction: Theory will be developed from collected

data rather than the other way around. The assessment is that a quantitative method is preferable in the goal to reveal behavior and attitudes within a defined research area, although the chosen research strategy, the survey, is usually associated with the deductive research approach (Saunders 2003).
In this case the survey research area is defined as two PwC countries within the 'EuroFirm' group: The Netherlands and Belgium (see paragraph 3.4).

In quantitative studies, researchers look at possible relationships between variables and pose these relationships in terms of questions or hypotheses (Creswell 2003). According to Creswell, a reasonable strategy in exploring these questions is by use of a survey approach. Surveys include cross-sectional and longitudinal studies using questionnaires or structured interviews for data collection, with the intent of generalizing from a sample to a population (Saunders 2003).

The survey is preceded by a review of existing literature in an attempt to gain knowledge about the research subject. This is necessary because "*explanatory research requires data to test a theory or theories.[…] You therefore need to have reviewed the literature carefully, […] and conceptualized your own research clearly prior to designing your questionnaire*" (Ghauri, Grønhaug 2002).
From that, the challenge will be to construct a self-administered, on-line questionnaire good enough to obtain and reveal the key findings.

In table 1 the choices made have been highlighted.

Research Philosophy	Positivism	Interpretivism	Critical Theory	Other
Nature of the data	Quantitative	Qualitative	Mixed Qual/Quants	
Research Approaches	Deductive	Inductive		
Research Strategies	Experiment	Survey	Case Study	
Research Purposes	Explanatory + Predictive	Descriptive	Exploratory	Exploratory + Explanatory
Time Horizon	Cross Section	Longitudinal		
Data Collection Methods	Secondary Data	Interviews	Questionnaires	Observ-ations
Some Research Traditions	Grounded Theory	Action Research	Ethnography	"Organiz-ational"

Table 1: Research possibilities Grid (Watson 2000 referring to Saunders et al. 2003)

1.7 RESEARCH OBJECTIVES

The objectives of this research are both generic as company specific:

- to get a general insight in the current knowledge and perspectives on the subject;
- to get insight in the extent to which (PwC) employees (are aware that they) take unnecessary IT risks including the use of shadow IT;
- to get insight in the reasons why (PwC) employees take unnecessary IT risks including the use of shadow IT;
- to identify conditions which increase or influence human risk-taking behavior towards sensitive information.

With these results, (PwC) corporate risk and security managers can for example develop tailor-made policies and communication plans. IT managers and budget holders can start projects and reserve budget for IT facilities the (PwC) employees indicate they use but are not yet provided or supported by their IT organization. Another possibility is to block certain features, programs or ports if they pose direct or indirect security risks to the company.

Other benefits may appear during the research and analysis and may include developing a risk assessment tool which can identify conditions which increase the human risk factors.

Chapter 2

2 THEORETICAL FRAMEWORK

"Federal agencies are required to provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of that agency."

United States Government Computer Security Act of 1987

2.1 INTRODUCTION

This study focuses on employees as sources of corporate data breaches and data loss. This focus is established for good reasons: A large international study (Whitty 2006) confirms the findings of a study by the Dutch Military IT Organization (Krom 2006) that many employees take unnecessary risks with their desktop PC's and laptops. Especially mobile users take more risks with the usage of uncontrolled data flows.
Noticeable in the "Trust and Risk in the Workplace" study by Dr. Whitty were the differences per country which may imply there are work attitudes and/or cultural aspects to consider as well.
So first this chapter will look at specific terms and definitions used in order to get a common understanding on what is meant by terms like "Risk", "Shadow IT" and "IT Governance".
Then the thesis is going to explore the existing literature (research papers, studies and other publications) on the subjects of Shadow IT and Carelessness with IT Security.
Finally the subject at the root of the issues, the IT Security policies themselves, is being discussed.

2.2 DEFINITIONS AND TERMS

In order to avoid ambiguity in the terms and topics that this thesis covers, this paragraph will provide the definitions, available research and examples of:

- Risk perception and risk-taking behavior (§2.2.1)
- Compliance (§2.2.2)
- Shadow IT (§2.2.3)

2.2.1 Risk perception and Risk-taking behavior

For an individual, there are many definitions of risk that vary by specific application and situational context. It is proportional to both the expected loss and to the probability of occurrence: greater loss and greater event likelihood result in a greater overall risk. (Holton 2004)
When looking at risk from a philosophical standpoint, it is said that when there is a risk, there must be something that is unknown or that has an unknown outcome. Therefore, knowledge about risk is knowledge about lack of knowledge. This combination of both knowledge and lack of knowledge contributes to making issues of risk complicated. (Stanford 2008)

The ability to assess risk is considered as one of the keys in human decision making, and many methods have been developed to support this assessment.
In information security, a risk is usually defined as a function of three variables:

- the probability that there is a threat
- the probability that there are any vulnerabilities
- the potential impact.

If any of these variables approaches zero, the overall risk approaches zero. (Wikipedia 2008) This concept was shown in practice by a study by Weirich and Sasse (2001), which showed that users will not make good security decisions unless they believe they are at risk.

When describing attitudes towards risk, these are often found in the domain of social and behavioral sciences. It is said that employee behavior which results in IT security incidents is more of a social problem that a technical one (Cook and Levi 1990). Therefore, assessing risk must consider cognitive bias (awareness; see paragraph 2.3.2) and cultural bias (national cultures; see paragraph 2.3.5). Also, no group of people assessing risk is immune to group thinking (organizational culture; see paragraph 2.3.5).

Most definitions of risk-taking behavior focus on situations where people put themselves at risk to something. Some risks are the result of our own behaviors, and risks vary in the degree that they can be controlled by our actions. The concept of risk is sometimes said to incorporate the possibility of gain.
Risk taking behavior can be defined as the voluntary participation in behaviors that contain, or are at least seem to contain, a significant degree of risk. People adopt different approaches to risk, their "risk orientation". (Llewellyn and Sanchez 2007).
Obviously and as a topic of this research more common, people can also be unaware they are taking risk, or that their actions put others at risk. This awareness, which may include the lack of awareness of rules and policies which reduce risk, has been the topic of some research.

2.2.2 Compliance

Most companies are very concerned about meeting the requirements of the Sarbanes-Oxley Act (2002). The act mandates that management has effective internal controls. This includes the key operating (IT) systems that run the businesses. The IT Management Reform Act (Clinger-Cohen 1996) for government agencies is seen as guideline for public companies on how to report on IT to comply with Sarbanes-Oxley (Bloem and Van Doorn 2004).
Besides Sarbanes-Oxley (SoX), many other compliance-centric initiatives like

- GAAP (General Accepted Accounting Principles, the standard framework of guidelines for financial accounting),
- IFRS (International Financial Reporting Standards),

- HIPAA (Health Insurance Portability and Accountability Act),
- BASEL II (International Standards for Banking),
- FISMA (Federal Information Security Management Act of 2002),
- ITIL (IT Infrastructure Library), COBIT (Control Objectives for IT),
- TQM (Total Quality Management) etc.

have an increasing influence on the way IT is made available to employees.

To reverse this perspective, one could assume that increased focus on IT Governance has resulted in an increasing number of IT projects to be cancelled or delayed. This assumption can be made since the Clinger-Cohen Act prescribes the use of IT Portfolio management and the preparation of business cases as a way to assess the financial viability of IT projects. When business cases, including ROI and TCO, do not add up, Business Units take matters into their own hands, which results in Shadow IT (Moreau 2007).
It seems that the creation of policies and procedures, issuing of warnings or seeking dialog with managers will not stop shadow IT. The perceived benefits appear to be just too attractive to users and their managers (Schaffner 2007).

2.2.3 Shadow IT

“Shadow IT” or “Rogue IT” is usually defined as the ‘unofficial’ usage of IT hardware and software in the workplace and a term used in IT for any application or transmission of data relied upon for business processes but which is not under the jurisdiction of a centralized IT department. The IT department did not develop it, is or was not aware of it, and does not support it. It creates ‘unofficial’ and uncontrolled data flows, which makes compliance difficult. On the other hand, Shadow IT is by some considered an important source for innovation and such systems may turn out to be "prototypes" for future approved IT solutions (Anthes 2007).
Also groups or departments performing IT functions like development, maintenance or support of applications, but who are not actually part of the IT organization, are referred to as Shadow IT groups or Shadow IT systems.

The existence of Shadow IT implies a failure on the part of IT to provide all of the services to meet their clients’ needs. Shadow IT doesn’t usually attempt to replace the ‘core’ IT processes (like networking or security) or ‘core’ applications (like ERP or CRM)(Raden 2005a).

Some other examples of unofficial data flows are:

- the transportation of sensitive information on USB sticks or other portable data storage devices (not encrypted and not issued by the IT organization). Examples hit the media almost every day with examples where such USB sticks are lost or stolen causing public embarrassment, or worse.
- the use of Gmail or other online e-mail services to send, store or receive company or client information which results in increased possibility of viruses and spyware, issues of data control and integrity. Having email stored where IT cannot locate it can raise serious legal issues if it involves subject matter caught up in a lawsuit. Likewise there are certain legal requirements regarding data privacy.
- the use of Google Docs or other online document sharing to share documents or files with colleagues or clients. This should not be confused with Google Apps, a SaaS suite of applications including secure web mail which has specifically been set up for (small) businesses.

Also, many sources indicate that

- the use of MSN Messenger or other online messaging software to communicate with clients or colleagues and/or
- Skype or other online VOIP software to communicate with colleagues or clients,

are forms of Shadow IT. However, these type of applications which are downloaded onto end-user PC's systems and who are sometimes specifically programmed to bypass organization firewall security, are lately referred to as 'Greynet'.

Greynets can be defined as real-time communication applications, often installed by end-users without the expressed permission of IT. They sometimes use highly evasive techniques to by-pass existing security infrastructure. Like Shadow IT, they can be useful to the business, but can also introduce risks to the business if left unmanaged (NewDiligence 2006).

Besides Messaging and VOIP software, activities include media streaming (web radio, live sports broadcasts), RSS newsreaders, peer-to-peer file sharing (Limeware, Kazaa, etc.) and peer-to-peer collaboration (e.g. Webex web conferencing).
The problems with Greynet programs are linked to those of Shadow IT:

- Greynet programs may open doors to viruses and other malware and thus create network security risks;
- they may create privacy issues allowing information to leak outside;
- Greynet programs create compliance issues by creating a 'parallel' communications network which is not monitored or retrievable by network administrators, and

- they may create issues on local PC's through the consumption of local system resources or cause interference with other programs;
- They can occupy valuable bandwidth from the company's networks and thus influencing overall network performance.

All of these issues increase risk (compliance, data leakage), time and costs for the support IT groups. Worthwhile mentioning, but not a topic for research in this thesis, is the loss of meaningful production time due to non-work related distractions (Prince 2007).

2.2.3.1 Why Shadow IT and Greynet systems are created

Generally it is believed that employees use shadow IT systems because they think there is no other way to get the data they need to do their jobs. This is most visible in the area of Business Intelligence (BI), which is believed to be the largest segment of Shadow IT. Many employees still perform their analysis, reporting and information sharing with MS Excel spreadsheets and MS Access databases, even if IT-supported BI tools are available to them. This can be explained by the fact that they know how to use these applications (or, reversely, find the supported BI tool to difficult to use), they perceive it as a "free" solution to use, they can easily exchange information with everyone and, usually it gets them the results they need. (Sherman 2004). As for Greynets: even when a company puts a secure enterprise IM system in place, users will still resort to greynet applications to connect with family, friends and business contacts who are not using the internal communication software. This is mainly because IM systems such as 'consumer IM' Windows Live Messenger and 'business IM' IBM Lotus Sametime are not interoperable.

Additionally, a RSA study (2007) confirms that 35% of employees feel they need to work around a security measure or protocol to be able to do their work efficiently. 63% send documents to their home e-mail address to continue work from home, even when they are aware that this is probably not allowed.

2.2.3.2 Why Shadow IT and Greynet are an underestimated problem

Besides the aforementioned problems with compliance to governmental issued regulation, Shadow IT usually results in lack of documentation, no backup/fallback plans, non-adherence to programming or hardware standards, security and data confidentiality, lack of testing, resource inefficiencies and problems with software licensing (Schaffner 2007).
Raden (2005b) defines some additional implications of Shadow IT:

- *Inconsistent Business Logic*: If a 'shadow IT' spreadsheet application includes its own definitions and calculations, it is likely that over time inconsistencies will arise from the

accumulation of small differences from one version to another and from one group to another, as spreadsheets are often copied and modified. Errors that occur from lack of understanding or incorrect use of the spreadsheet are aggravated due to a lack of testing and version control.

- *Inconsistent Approach*: Even when the definitions and formulas in the spreadsheet are correct, the methodology for doing analysis can be wrong.
- *Wasted Investment*: Shadow IT applications sometimes prevent full ROI from investments in systems that are designed to perform the functions now replaced by Shadow IT. The best example in this would be the previously depiction of data warehousing (DW) and BI projects. They are initiated with good intentions, but end-users stick to excel and consistent usage of DW and BI in the organization never really starts off.
- *Inefficiencies*: Besides being a driver for innovation, Shadow IT can be a barrier to innovation by blocking the establishment of more efficient work processes. Data might be exported from a BI system to a spreadsheet to perform the critical part of data analysis.
- *Barrier to Enhancement*: Although some Shadow IT uses the latest available technology trends such as SaaS, Shadow IT can act as a brake on the adoption of new technology. Because e.g. spreadsheets are deployed to fill critical needs, they must be replaced carefully. But lacking adequate documentation, controls and standards, that process is slow and error-prone.

A study by NewDilligence (2006) among 778 IT managers and 385 end users to the effects of Greynet showed that 83% of end-users admitted using one or more Greynet applications on their work computer. About 40% had installed Greynet applications that were explicitly not sanctioned or approved by their IT departments. Age seemed to play a role: younger employees were more likely to have installed Greynet applications without IT's permission. Because younger workers have typically "grown up" with computers, they may have a greater tendency to customize their machines, even in the workplace. According to the survey, 39% of users believe they should be allowed to install the applications they need on their work computers, independent of IT control or policy, while 53% of users report they tend to disregard security policies that limit installing and using Instant Messaging and file sharing applications. Despite all the security technology installed the IT department to block malicious attacks, the user is often the biggest vulnerability, especially on the real-time, socially-networked Web (Cabri 2007).

2.3 IDENTIFICATION OF FACTORS

Table 2 below summarizes the factors identified in **bold**. Details are given in the next paragraphs.

Authors	*Factor identified*
Ponemon (2007)	Their survey among 893 IT professionals in the USA showed that respondents consider **careless** and negligent insiders (i.e. employees) to pose the greatest threat to an organization's information assets.
RSA (2007)	This security experts group surveyed government and corporate employees in Boston and Washington D.C. and confirmed the findings that the biggest threats in a workplace are *"often unintentional, often resulting from **carelessness** or ignorance of individuals within the organization or company"*. (RSA 2007)
Spafford (2004)	In this publication, George Spafford argues that regulatory compliance problems start when IT systems, that have been created by customers themselves and/or are maintained outside of the formal IT organization, have been forgotten or ignored but suddenly show up in audits. He states: *"The existence of Shadow IT within an organization is symptomatic of **a lack of alignment between business units and IT** and, possibly, even senior management and IT."*
Booz Allen Hamilton (2004)	This consultant company identifies Shadow IT as those people performing IT functions but who are not actually part of the IT organization. They state "*The problem here is not the existence of shadow staff, but the inadequacies in the normal service delivery model that prompted the business unit to circumvent it."* This also points **to lack of business – IT alignment**.
Raden (2005a) -and- (2005b)	Raden identifies **self-developed BI analysis tools** in Microsoft Excel by end users as a form of **Shadow IT** and also explains why end users do this and why this is a risk to companies. Also the author states that Shadow IT results from of a number of factors: Budget cuts for IT **[IT governance], Lack of IT/business alignment**, User Independence and Timing.
Moreau (2007)	Moreau states that *"to deal with IT projects that don't go through proper channels, IT security officers need to understand why they exist. There is a gap between the abilities of [the information technology department] and*

Authors	*Factor identified*
	business needs[…]" So again **poor alignment between business and IT** is identified as a factor of importance. A link is also made with a lack of funding on IT projects due to **stricter IT governance**.
Schaffner (2007)	Schaffner lists 5 reasons why employees turn to Shadow IT systems (#) and Shadow IT staff (*): Better accessibility#, better responsiveness#, ease of use#, more dedication* and knowledge of the users' business*. These all are signs of **poor business – IT alignment.**
Lutchen (2004)	Lutchen concludes **that poor IT governance** (*"a reduced ability to leverage the investment portfolio")* is one of the main reasons for limiting the business value of IT and *"the inability to connect the dots across all of the various drivers creates serious business risk[…]"*
Cumps *et al* (2007)	Cumps also links to **IT governance** and **Business-IT alignment**: " m*aking sure that IT investments are in sync with the organization's business objectives proves to be more challenging than initially expected, especially in today's fast-changing, dynamic environment*"
Al Awadi and Renaud (2007)	The authors first establish that employees forms an integral part of information security and cannot be isolated from it. Furthermore they found that *"In particular we should consider specific as well as generic human aspects, […] also **specific issues such as culture** and personal beliefs."* So National culture is identified as a factor.
Björck and Jiang (2006)	The two authors use Hofstede's **cultural dimensions** to compare different attitudes towards information security behavior. They find significant differences in security behavior and attitude.
Chaula (2006)	Chaula's study concludes that "*Results show that **culture** affects the way people approach IS security.*"
Mathieson (1991)	Mathieson studies and tries to predict why sometimes people do not use the Information systems provided to them (and may opt for Shadow IT systems). When examining the Theory of Planned Behavior he identifies **Culture** as one of the reasons why people refuse to use an IT system.
Witty and Wagner (2005)	In their study they conclude that **lack of awareness** due to lack of awareness training is an important factor for increased security risk.
Hung *et al* (2007)	Hung argues that techniques to achieve **Business-IT Alignment**, such as portfolio management, are usually not easy to implement. Success to

Authors	*Factor identified*
	implement such techniques can only be achieved with the full participation, and commitment of the business.

Table 2: Summary of identified factors

In summary of the previous table, this research will focus on these influencing factors:

1. Carelessness (§2.3.1)
2. Lack of security awareness (§2.3.2)
3. Stricter IT governance (§2.3.3)
4. Poor alignment between Business and IT (§2.3.4)
5. Cultural differences (§2.3.5)

With the identified factors, a conceptual model on which to base the rest of the chapters can be sculpted:

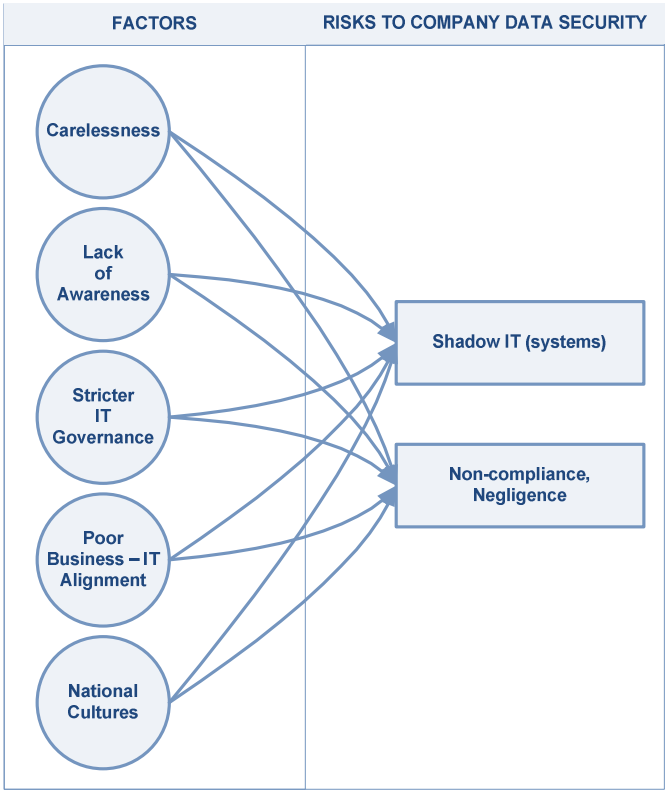


Figure 3: conceptual framework

The next paragraphs will further explore some of the identified factors deemed important to this thesis.

2.3.1 Carelessness

Carelessness and ignorance can be the result of an incorrect assessment of the risk involved. Therefore paragraph 2.2.2 looked at aspects involving risk perception.
For a typical IT organization, risk is different from that of an individual.
Traditionally, the following types of risk can be identified:

- Strategic risk, including reputation risk and marketplace risk, which covers areas such as due diligence, policy breaches, privacy, competition, country legislation etc.
- Financial risk, including credit risk and compliance risk, which covers areas such as portfolio risk, liquidity and credit rating, and
- Regulatory risk, including fraud risk and operational risk, which covers areas such as fraud, both internal as external, identity theft and compliance. (Nelsestuen 2007)
  In this thesis, the regulatory risk for a company is the main focus.

Gartner (Hunter and Blosch 2003) states that recently, new types of risk have emerged:

- The interconnection of businesses, which increases dependencies and exposures to theft and misuse of information. Mismanaging these relationships is a new risk outside the traditional purview of IT.
- Executive criminality, which has produced many corporate failures and new legislation aimed at reducing such abuses.
- Consumer demand for privacy protection, where for example large thefts of sensitive personal information have led consumers to demand privacy protection from their governments. Not complying with these new privacy laws is a new legal risk.
- IT failures, with new legal liabilities likely in the near future.

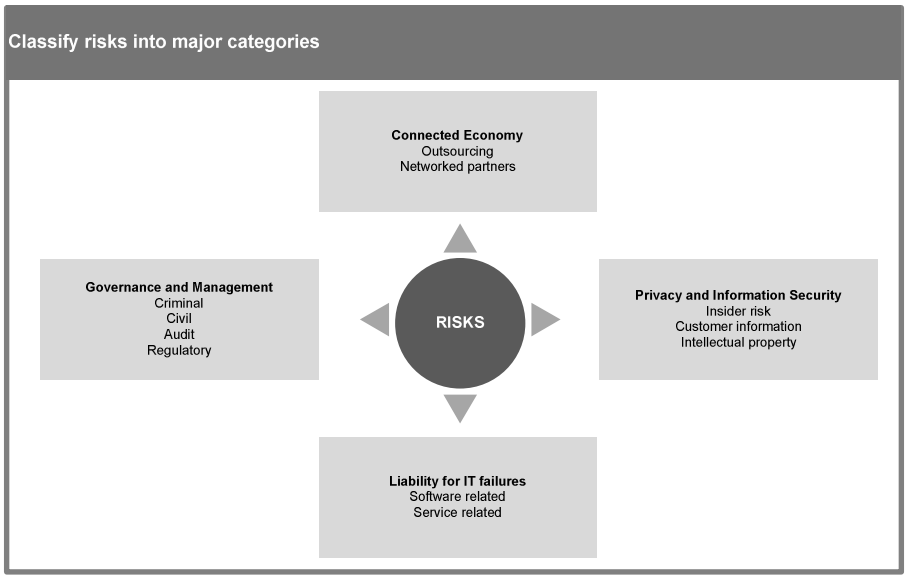


Figure 4 Major categories of risk
source: Gartner EXP Research, July 2003: "Managing the new IT risks"

2.3.2 Awareness

In the context of this thesis, (information security) awareness can be described as the state where users in an organization are aware of their security 'mission' (usually described in end-user 'code of conduct' and/or security guidelines). Where Mathieson (1991) stated the obvious that Information Systems can only be useful if people use them, the same can be said for information security guidelines. Therefore, information security awareness is of the highest importance, as the defined guidelines and procedures can be misinterpreted or not practiced by end-users, which results in losing their usefulness (Straub and Welke 1998).

Problems relating to awareness are complex and in order to create a systematic distinction, two categories should be defined: framework and content. Most research has been focusing on creating frameworks (for example Perry 1985, NIST 1995 and Morwood 1998). An example of a framework will be given in figure 4. An example of the content category is how to motivate employees to comply with information security guidelines (Siponen 2000).

Reversely, increasing awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. And although research has shown that end-users think giving security awareness training to be one of the least-effective approaches to manage IT risk, businesses with such training programs in place have shown to have reduced levels of risk (Witty and Wagner 2005).

The National Institute of Standards and Technology confirms that awareness can be created through education: explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously (NIST 1995). The NIST has created in its handbook "An Introduction to Computer Security" a framework that makes a distinction between security awareness, training and education.

Comparative Framework

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Videos -Newsletters -Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion Seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Eassay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Figure 5: NIST Comparative Framework (NIST 1995)

However later studies (Parker 1998, Spruit 1998 referenced by Siponen 2000) show that other factors, such as attitude, motivation and commitment, play an important role as well.

2.3.3 Relationship with IT Governance

IT Governance is a part of Corporate Governance that focuses on IT systems, performance and risk management. In the last few years, IT governance is a hot topic due to compliance regulations like Sarbanes-Oxley (SOX 2002) in the USA and Basel II (Basel II 2004) in Europe (see paragraph 2.3.1).

When one looks for definitions of IT governance in books or on the internet, they generally have the following activities in common:

- Control of the work performed by IT professionals
- Compliance with internal policy or regulation
- Justification of IT spending
- Accountability and transparency
- Connecting with the needs of customers, the broader organization, and other stakeholders.

These activities (control, compliance, justification of spending) could suggest some relationship with shadow IT and non-compliance by those same customers: stricter IT security policies, stricter enforcement of those same policies and less money for customer

'pet projects' could lead to those customers setting up their own systems and evade policies and controlling measures.

In addition, many publicized examples where IT projects have run out of control have had a negative impact on the performance of organizations (Lutchen 2004). IT Governance has in many ways also become a synonym for 'IT Cost Control' as IT management struggles to make clear how the IT investment portfolio is actually generating business value. And making sure that IT investments are in sync with the organization's business objectives proves to be "*more challenging than initially expected, especially in today's fast-changing, dynamic environment*" (Cumps *et al.* 2007). This is because historically, from a business point of view, IT has been one of the least understood expenditures and also one of the most poorly managed.
As IT managers have often failed to weigh IT business risk against cost, this has resulted in increased expenditure and reduced ability to leverage the investment portfolio value (Lutchen 2004). After the millennium bug was 'exterminated' and the Internet Bubble had burst, CEO's stepped in and significant IT budget cuts were made.
This in combination with issues like increased demands for regulatory compliance have resulted in growing IT project backlogs, which has limited IT's ability to be responsive to the needs of business units, many of whom are dependent on IT projects to achieve business objectives.

To summarize: the assumption for this thesis is, that there is a relationship between IT Governance and non-compliance with company IT security rules and guidelines, that is, when rules get stricter and budgets get tighter, employees increasingly bend these rules and find (unsafe) alternatives to satisfy their IT needs.

2.3.4 The Business- IT Alignment Challenges

As stated before, one of the influencing factors why employees do not comply with IT security policies is believed to be lack of alignment between the business and the IT staff which supports it. It is therefore sensible to also look at factors that inhibit effective business-IT alignment ("BITA").

In this thesis, Venkatraman's approach to BITA is used (Henderson and Venkatraman 1993). In this approach ICT has to be in line with the organizational strategy and design. Four ICT architectures are relevant:

- Functionality: what information systems are in use and which tasks these systems are performing (operational systems, financial systems, office automation software, etc.);

- Data: every information system keeps data, that is part of an organizational information model;
- IT infrastructure: hardware (computers, servers) and communication technology (networks, routers, etc.) ;
- IT staff: the level of sophistication of data-management, and the size and complexity of the IT-infrastructure, results in a larger or smaller IT-department with more or with less specific IT-functions (e.g. data-manager, network manager, helpdesk, etc.).

Techniques to achieve BITA, such as portfolio management, balanced scorecards and other business metrics are well established and proven, although usually not easy to implement. Failure to implement such techniques cannot be blamed totally on IT as they can deliver only 'capabilities'. Turning those capabilities into business benefits can be done only with the full participation, commitment and engagement of the business. Without that engagement, any attempt to "align" IT and the business will most likely fail (Hung *et al.* 2007, IBM 2008).

Other failure factors seem to be (Jahnke 2005):

- Business managers should determine the "what" and IT should determine the "how". In practice IT does both. Conversely, IT is usually not involved with the business planning process.
- There is still a widespread belief that IT is only a cost center and cannot make a difference in business outcomes (profit, market share, ROE, ROA, etc.).
- As a cost center, IT is often the target for outsourcing which makes alignment between IT and business even more difficult.
- IT may lack the necessary credibility which is the crux of successful alignment between IT and business.

Luftman (1999) also presents influencing factors (both positive and negative) for effective alignment:

	ENABLERS	INHIBITORS
1	Senior executive support for IT	IT/business lack close relationships
2	IT involved in strategy development	IT does not prioritize well
3	IT understands the business	IT fails to meet commitments
4	Business - IT partnership	IT does not understand business
5	Well-prioritized IT projects	Senior executives do not support IT
6	IT demonstrates leadership	IT management lacks leadership

Table 3: Enablers and Disablers for effective B-IT A (Luftman 1999)

According to Luftman a certain minimum level of maturity is needed to have effective BITA. Luftman calls this “strategic alignment”. Combining the strategic alignment model from Henderson and Venkatraman (1993) with these enablers and inhibitors, he developed his Business & IT Alignment Maturity model. In this model six criteria are used to determine the maturity of the alignment of IT and business (Luftman 1999):

1. Communications maturity
2. Value measurement maturity
3. Governance maturity
4. Partnership maturity
5. Scope & Architecture maturity
6. Skills maturity

Finally, implementation of Business and IT alignment rules and guidelines itself is also affected by cultural aspects. Silvius (2008) has matched the above six criteria from Luftman in a matrix against Hofstede’s cultural dimensions (Hofstede 1980). These cultural dimensions will be discussed in depth in the next paragraphs.

Silvius concludes that “…*cultural aspects in general are likely to have an impact on the different variables of BI[T]A maturity assessment. The effect of cultural dimensions on BI[T]A maturity scores is not straightforward; the cultural dimensions most likely influence the variables of BI[T]A maturity in different directions*.” (Silvius 2008).

The conceptual mapping of Hofstede’s dimensions of culture on Luftman’s variables of BIA maturity can be found in appendix C.

2.3.5 The Cultural Issue: How to address

Research on cultural related aspects on information security is hard to find in literature. These human factors have rarely been investigated (Al-Awadi and Renaud 2006), but the importance of information security in organizations these days makes it clear that technology alone cannot lead to sufficient solutions (Slay 2003).

In other words, the human aspects cannot be isolated from technology in information security. Therefore it is needed to not only consider traditional human-computer interaction issues but also specific issues such as culture and personal beliefs.

In the previous paragraphs it has been shown repeatedly that the human element seems to be the 'Weakest Link' in IT security, and that cultural different attitudes towards IT security need to be taken into account. In this context one needs to make a distinction between national cultures and organizational cultures. The difference between both is that national culture represents values that are dominant in the whole nation and organizational culture represents values that are dominant in a particular organization. Robbins (2005) argues that national culture, organizational culture and employee behavior can be correlated and that national culture influences employee more than organizational culture. Therefore, knowledge about national culture is vital if accurate prediction of employee behavior in an organization is sought. In this view, if an organization plans to develop an effective security culture, it should not be developed in isolation of national culture and the organizational culture (Chaula 2006).

The respondents of the survey (see chapter 3) are all of PwC, and more specifically within the 'Euro-zone' region. They share many corporate policies on how business should be conducted and how to act and behave towards clients and towards colleagues. Employees are largely performing the same type of activities and have been recruited to fit within the corporate 'culture'. The assumption is therefore that the organizational culture is similar to an extent that no clear differences would be found. The focus will therefore be on national culture. In the next paragraphs, I will briefly describe two of the leading researchers in this area and will attempt to relate these to the problems of non-compliance with IT security policies.
Research has not often established a connection between these dimensions and information security. Björck and Jang (2006) in their study "Information Security and National Culture" make a first attempt in this direction and Al-Awadi and Renaud (2006) establish a link between trust (in IT) and national culture.

2.3.5.1 Hofstede

Hofstede (1980) analyzed a large database of employee values scores collected by IBM between 1967 and 1973 covering more than 70 countries, from which he first used the 40 largest only and afterwards extended the analysis to 50 countries and 3 regions. In the editions of Hofstede's work since 2001, scores are listed for 74 countries and regions, partly based on replications and extensions of the IBM study on different international populations. Subsequent studies validating the earlier results have included commercial airline pilots and students in 23 countries, civil service managers in 14 counties, 'up-market' consumers in 15 countries and 'elites' in 19 countries. From the initial results, and later additions, Hofstede developed a model that identifies four primary Dimensions to assist in differentiating cultures.

These four national culture dimensions are:

- *Power distance* (PDI) The basic issue involved within this dimension is human inequality. A national culture characterized by high power distance is more willing to accept inequalities (e.g. those between a manager and her/his subordinates) within an organization than cultures with low power distance.
- *Uncertainty avoidance* (UAI) This dimension deals with natural human uncertainty about the future and in what way people try to cope with the domains of technology, law, and religion. National cultures with a low degree of uncertainty avoidance are better equipped to handle future uncertainties without assisting rules.
- *Individualism vs. Collectivism* (IDV) This dimension describes the relationship between the individual and the collectivity that prevails in a society. In countries such as the USA, individualism is seen as a blessing and a source of well-being while in others, such as China, it is perceived as alienating.
- *Masculinity vs. Femininity* (MAS) This dimension deals with the emotional and social roles of the genders. Survey results indicate that women generally attach more importance to social goals such as relationships, helping others, and the physical environment, and men attach more importance to ego goals such as careers and money.

In his later work (Hofstede 2001), Hofstede introduces a fifth dimension: The

- *Long-term vs. short-term orientation* dimension (LTO). He describes long-term orientation as "*characterized by persistence, ordering relationships by status and observing this order, thrift, and having a sense of shame, whereas short-term orientation is characterized by personal steadiness and stability, protecting your 'face', respect for tradition and reciprocation of greetings, favors, and gifts."(ibid.)*

Hofstede argues that depending on the location and the level of society one looks at, individuals are influenced by a mix of underlying values and learned practices.

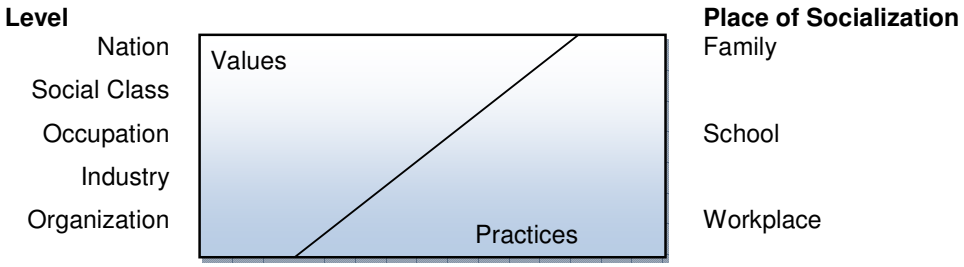


Table 4: The balance of values vs. practices (Hofstede, 2001)

At the national level cultural differences reside mostly in values and less in practices. At the organizational level, cultural differences reside mostly in practices and less in values. The differences in the values vs. practices balance can be explained by the different places of learning ('socialization') for values and for practices.

Values are acquired at an early age, and this takes place mainly in the family, and later at school. By the age of 10, most of a child's basic values have been 'programmed' into his or her mind. Organizational practices are learned through socialization at the workplace, thus as adults. For the occupational values the place of socialization is mainly the school or university, between childhood and adulthood (Dahl 2004).

2.3.5.2 Trompenaars and Hampden-Turner

Trompenaars and Hampden-Turner (1997) also classified cultures along a mix of behavioral and value patterns. They identify seven value orientations, some of these nearly identical to Hofstede's dimensions. Their value dimensions are:

- *Universalism vs. particularism* can be considered comparable to Hofstede's UAI. Companies from universalistic cultures negotiating with a business partner in for example China must recognize that relationships matter and take time to develop. They form the basis of the trust that is necessary in order to do business.
- *Communitarianism vs. Individualism* can be considered comparable to Hofstede's IDV. Companies from individualistic cultures such as the USA will face difficulties in introducing methods of individual incentives such as individual performance-based rewards and one-on-one assessments in communitarian cultures such as Japan.
- *Neutral vs. Emotional* This describes the extent to which feelings are openly expressed.
- *Diffuse vs. Specific* describes the range of involvement. Managers from specific cultures such as The Netherlands tend to criticize subordinates directly and openly without

regarding their criticism as a personal matter. In a diffuse culture such as China, this will be seen as an unacceptable loss of face.

- *Achievement vs. Ascription* can be considered comparable to Hofstede's PDI dimension. In many traditional cultures such as India, individuals derive their status from birth, age, gender or wealth. A person with ascribed status does not have to achieve to retain his status: it is accorded to him on the basis of his being. India with its deeply rooted caste system is a clear example of such an ascriptive society. Therefore, sending a young manager to run a subsidiary in Mumbai will generate difficulty.
- *Human-Time relationship* describes attitude towards punctuality, personal vs. business relationships, work-life balance etc.

2.3.5.3 GLOBE aspects

In relation to security awareness and behavior the GLOBE research project defined another nine National culture dimensions (GLOBE 2003, referenced by Chaula 2006):

- Assertive Orientation (People are generally dominant)
- Power Distance (Followers are expected to obey their leaders without question)
- Uncertainty avoidance (Most people lead highly structured lives with few unexpected events)
- Humane Orientation (People are generally very tolerant of mistakes)
- Institutional Collectivism (Leaders encourage group loyalty even if individual goals suffer)
- In-group collectivism (In this society, children live with parents until they get married.)
- Gender Egalitarianism (Boys are encouraged more than girls to attain a higher education)
- Future orientation (More people live for the present than for the future) and
- Performance orientation (Employees are encouraged to strive for continuously improved performance)

A lot of similarities can be found between these dimensions and those of Hofstede and Trompenaars. Interestingly, in the GLOBE research a link is made between Gender equality and social equality: Social values related to forms of equality such as economic independence and equal opportunities have serious impact on IS security. In a system where there is a big gap in economic conditions, it is more likely that the rate of security incidents will be high. For example in many cases fraud is committed motivated by financial gain. Also, it was found that low UAI results in shallow or non- holistic approaches to security. High PDI can result in poor communication on security issues between management and employees and a low degree to which employees are ready to report unethical conduct by colleagues.

2.3.5.4 *Summary cultural aspects*

Trompenaars and Hampden-Turner's 'non-Hofstede' dimensions seem to be more like behavioral aspects rather than values in themselves, while the GLOBE aspects seem to borrow dimensions from both. This thesis will therefore limit itself to the five dimensions as defined by Hofstede.

As said before, research has not yet linked behavioral aspects towards IT security with national culture. However research by Al-Awadi and Renaud (2006) to links between trust and Hofstede's IDV, PDI and UAI shows that a person from an individualistic society tends to trust IT more easily than one from a collectivist society. On the other hand, high PDI and high UAI societies trust IT less. Reversely, the level of trust in IT is high when there is low PDI and low UAI.

And according to Gartner (Witty *et al.* 2001), trust is "*the result of applying a combination of authentication, authorization, integrity and non-repudiation controls, in other words: trust results from the effective application of information security techniques.*" The established connections between IDV, PDI, UAI and trust will therefore be used in this thesis when analyzing the link between IDV, PDI, UAI and information security behavior.

2.4 IT SECURITY POLICIES

Finally this thesis will explore the issues with the IT policies, guidelines and measures themselves as a source of non-compliant behavior.

2.4.1 Security Policy Ineffectiveness

It would seem logical that organizations focus on creating security policies that are strictly enforced and that they educate employees on the importance of complying with these policies. What the Ponemon survey (2007) shows however is that many employees are uncertain or don't know about the existence of such policies. Additionally, even if they are aware of these policies, many perceive their organizations as being apathetic towards enforcement.

Wold (2004) and Mathisen (2004) have also shown that when companies develop information security policies, in many cases these policies are not practiced or followed by the users.

This apathy is confirmed by a large study (PricewaterhouseCoopers 2007) among 7.200 IT, security and business executives in more than 119 countries. 63% of respondents state they

do not audit or monitor user compliance with security policies, and only 48% measured and reviewed the effectiveness of security policies and procedures in the last year.
More apathy was encountered during tests performed as part of a study by DeWitt and Kuljis (2006). This apathy seemed to be due to the users' persistent attitudes towards security. When questioned, the users who did know the purpose of [the tests] did not put their theories into practice because they simply did not care about the consequences. Some participants also indicated that their data was not important to anyone but themselves, and therefore not worth taking effort to protect. Participants also indicated that completing the task at hand was more important than protecting their security and it was observed on several occasions that they would try to use [security software], but if they were unsuccessful in their first attempt they would bypass it to open files without protection (*ibid.*).

2.4.2 Effectuation of IT Security Policies

Much research has been done to assess how to effectuate IT security policies (for example Wills 2002, Mathisen 2004 and Siponen 2004). Wold (2004) explored the key factors that influence the effectiveness of (corporate) information security policies. His survey study was carried out among 41 large Norwegian companies.
The study defined six key factors which improve the effectiveness of information security policies: Engagement from management; learning and awareness; cultural aspects; personal bonding; measuring-reporting-follow up; and focus on attainable security objectives. He concluded that human-related factors were most important when designing and implementing information security policies.

Other research has focused on possibilities to measure and quantify IT security performance (for example Kahraman 2005 and Ostowan 2006). Kahraman has created a balanced scorecard to measure security performance which is divided into three main parts:
An Organizational view, looking at policies and procedures, an "Evaluating minds" section which incorporates human factors, and a technical view which includes access control, auditing, monitoring, viruses, backups and configuration management. Although measures in all of these three areas are important, the author states that:

"*…The human factor in the information systems can affect security in many ways. In fact, the security depends on the human factor[…] It's easy to manipulate people rather than technology as most of the time organizations overlook that human element.*"(Kahraman 2005)

2.4.3 Usability of Security Features

As stated in paragraph 1.3, IT security policies should guarantee sufficient levels of control while still supporting the business objectives. Too stringent rules will inhibit the ability to respond effectively to new opportunities (Brooke 2004). Recently, there has been a growing realization that besides policies, usability problems of security features are hindering the security effort as well.

Promoters of usability want to make it easy to use a system while security people favor making it hard to access a system (Nielsen 2000). For example, it is common opinion that people in general, and employees in particular are faced with an overload of too many different passwords, PIN codes and login names. Users are asked to change their passwords often and to use strong passwords (many characters) that are hard to remember and guess. To simply cope with the problems of remembering all those different passwords, users may try to use the same PIN or password as often as possible and/or store them in their phone or write them down on a piece of paper (Clear 2002, referenced by Chaula 2006).

Alternative authentication methods such as behavioral and physiological biometrics are proposed to authenticate users to systems (Davis *et al.* 2004). However this requires much effort and investment. Effectiveness and usability of security features (as opposed to security policies) will remain out of scope as subject for research in this thesis, but will be an interesting area for further research.

2.5 SUMMARY ON THEORETICAL FRAMEWORK

The previous paragraphs have discussed several topics which can be related to intentionally or unintentionally not following IT security policies. Not following policies includes the use of shadow IT.

Shadow IT

This term can be divided in three broad groups:

The use of hardware and (online) software which is not approved or supported by the IT department, the use of Greynet systems, such as MSN Messenger, Skype and Limeware, and the use of Shadow IT 'Support Systems', where IT support is provided by non-IT staff.

Compliance

The Sarbanes-Oxley Act (2002) mandates that management has effective internal controls which include the key operating (IT) systems that run the businesses. The Clinger-Cohen Act prescribes the use of IT Portfolio management and the preparation of business cases as a way to assess the financial viability of IT projects. This may result in IT projects to be cancelled or delayed.

Risk

It was found that an employee may assess something to be risky, as a function of Probability x Vulnerability x Impact. If any of these three factors is perceived as zero, the overall assessment will be that no risk is involved in the actions. This follows the framework by NIST (1995) that education about potential risk is important as it allows for a more accurate assessment. Other research (NewDiligence 2006) however shows that many employees knowingly disregard IT security policies even if aware of the potential risk.

It was also found that risk taking behavior, or the attitude towards taking risk, is partly a culturally defined aspect (Cook, Levi 1990). National culture plays an equal or even more important role as the organizational culture (Chaula 2006).

Influencing factors

Reviewing of the existing publications revealed five recurring factors which influence the usage of shadow IT systems (and thus leading to answering the main research question):

- Carelessness, which may result from an incorrect assessment of the risk involved,
- Poor alignment between Business and IT (BITA), which may lead to employees creating their own IT solutions and systems,

- Lack of security awareness, closely related to Carelessness but distinct because employees just don't know what is allowed or what the policies are,
- Cultural differences where compliance with policies is affected by cultural beliefs, and
- Stricter IT governance, closely related to poor BITA, where reductions on IT spending (projects, support etc.) may lead to employees setting up their own IT projects and support systems.

These identified influencing factors will be tested via a survey among PwC staff in The Netherlands and Belgium in the next chapters.

Carelessness

Carelessness and ignorance can be the result of an incorrect assessment of the risk involved. Traditionally, risk consisted of Strategic risk, financial risk, and regulatory risk. Recently new types have emerged: the interconnection of businesses, executive criminality, consumer demand for privacy protection, and IT failures.

Awareness

Awareness was defined as being aware of the security mission. Awareness can be created through education, however other studies show that factors such as attitude, motivation and commitment play an important role as well.

IT Governance

IT Governance is a part of Corporate Governance that focuses on IT systems, performance and risk management. Stricter IT security policies, stricter enforcement of said policies and stricter IT cost control may result in less money for customer 'key business' projects which in turn could lead to those customers setting up their own systems and evade policies and controlling measures.

Business-IT alignment

Finally problems aligning Business objectives with IT were discussed. Common reasons for, and examples of alignment failure were given. It was found that IT only can deliver the capabilities. Turning those into business benefits is up to the business themselves. Inhibitors and enablers for effective BITA were given which need a level of 'alignment maturity'.

Cultural differences

The human aspects cannot be isolated from technology in information security and it seems to be the 'Weakest Link'. Cultural different attitudes towards IT security need to be taken into account. Hofstede has done extensive research in this area and has defined 4 cultural dimension with can be used to assess or predict employee behavioral differences. It is

argued that National culture is much more dominant than the organizational culture of a company.

IT Security Policies

Some time was spent on exploring the issues around IT security policies, making them work in 'real life', and IT security measures and their possible ineffectiveness.

chapter

3

3 THE SURVEY

"The Commission shall prescribe rules requiring each annual report required by section 78m (a) or 78o (d) of this title to contain an internal control report, which shall:

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."

Sarbanes-Oxley Act, Section 404.

3.1 SCIENTIFIC APPROACH

When describing the scientific approach of this study one needs to look at the choice of philosophical perspective, and the choice of methodology.

3.1.1 Philosophical perspective

The choice of philosophical perspective is related to the question of how scientific knowledge is generated and judged as being acceptable. There are mainly three perspectives acting as guiding frameworks for how knowledge should be produced: Positivism, Realism and Interpretivism (Saunders et al. 2003). Although not commonly associated with IT, Realism seems to be the proper philosophical approach as it is based on the believe that there are large-scale social forces and processes that affect people without them necessarily being aware of such influences on their behavior. As said before by Cook and Levi (1990): IT security incidents are more of a social problem that a technical one. The definition of risk and cultural different attitudes towards the perception of risk appear to be in the domain of social constructionism. (Rundmo et al. 2004, Stanford encyclopedia of Philosophy 2008)

3.1.2 Methodological perspective

The methodological perspective can be seen as a link between the philosophical perspective and the practically applied research design. There are two main approaches within methodological theory: the qualitative and quantitative approach.

The quantitative approach is the search for large numerical relationships and statistical analysis, whereas the idea of the qualitative approach is to get insights via interpretation and verbal analysis (Saunders et al. 2003). The quantitative approach is the most appropriate for the survey.

Another important categorization of methodological approaches is the distinction between induction and deduction. Induction is based on empirical findings and seeks to generalize findings of the studied phenomena to laws and theories. Deduction on the other hand is an approach where theories and hypotheses are tested against reality and then verified or falsified. Based on the explorative nature of this study, an inductive methodology is being used to seek knowledge and insights based on the different patterns related to national cultures.

3.2 CRITICAL REVIEW

Three important issues can be listed regarding the methodology which will be utilized for this study.

The first issue is the usage of only one company as test subject: the survey results, analysis and conclusions are not adequate to make generalizations about relationships between the concepts of national culture, IT governance, data security behavior and awareness. However it is not the purpose of the study to prove such relationships. This study aims to explore differences in attitude towards data security awareness, despite the research subject being a single company.
Others may challenge the universality of the results themselves because these are based on the study of a single company, as they did in relation to Hofstede's research. However most researchers (Alden et al. 2005; Abrams et al. 1998; Soutar et al. 1999) found those results valid because they were correlated with other (general and demographic) data. And Yin (1994) also states that "*even a single company case can be sufficient enough to make certain generalizations*".

Secondly, this study used a 'shotgun-approach' in identifying possible factors, which results in each factor not being examined in-depth. Others have studied these factors individually, for example cultural differences on data security behavior (Björck and Jiang 2006).

Thirdly, the type of questions asked in the survey may lead to (socially) desirable answers being given, although the chosen method of a self-administered online survey is less likely to be affected by this than a face-to-face interview (Dillman 2000).

3.3 SURVEY QUESTIONS

The questionnaire examines respondent's knowledge and understanding of the IT security policies as well as the percentage of respondents who actually comply with these policies. There are two main sections to the questionnaire. The first section deals with more general and demographic questions and the second section deals with technical security questions. However, due to the flow of questionnaire, questions related to these two sections are occasionally mixed. Before distributing, the questionnaire was tested on 4 end-users.

The guidelines used while designing the final questionnaire were (Brace 2004):

- Keep the language simple
- Keep the number of questions to a minimum
- Limit each question to one idea or concept
- Not asking leading questions
- Avoid wording in a manner that suggests an answer
- Allow all possible answers
- Organize the pattern of the questions
- Separate demographic questions from other questions
- Ask easier questions first
- Let opening questions arouse interest
- Group similar questions together
- Place the emotional question at the end of the questionnaire

3.3.1 General questions

The following five questions are attribute variables which contain data about the respondent's characteristics.

No.	Question	Type	Values	Factor measured	Comments
1	Gender	Single Select	[M/F]	n/a	*This question is both an easy introduction, but might also serve to test differences between males and females and Hofstede's cultural Masculinity vs. Femininity dimension.*
2	Country of origin / Nationality	Single Select	Belgium, Netherlands, Spain	Cultural differences	*Initially Spain was included in the list of surveyed countries. However due to company politics the survey eventually was only allowed in The Netherlands and Belgium.*
3	Age group	Single Select	[18-23] [24-29] [30-35] [36-41] [41+]	n/a	*This is another introduction question, and might show a behavioral distinction between the young, Internet savvy persons and the older generation for whom computers and Internet are more of a learnt skill. Research (NewDilligence 2006, Mogull 2007, Kaplan 2008) seems to confirm this.*
4	PwC laptop	Single Select	[Y/N]	n/a	*Study shows (Whitty 2006) that mobile users are more likely to take more risks with the usage of uncontrolled data flows. However it is expected that over 90% of the interviewed persons have a laptop computer.*
5	I have been with the company xxx years	Single Select	[<1 yr] [1-3 yr] [4-6 yr] [>6 yr]	n/a	*A relation might be found between number of years/months with the company, and familiarity with the company IT Security policies and guidelines.*

Table 5: General Survey questions

3.3.2 Specific questions

The next questions relate to the respondents' familiarity with the existing IT security policies. They are rated on a semantic differential scale. This scale has opposite ends of the scale marked with two different or opposing statements. Respondents are then asked to indicate the area in which they fall on the scale.

Unlike the Likert scale (rating 1 to 5), the semantic option does not have to have a "statement" that is semantically identified for each rating along the scale. This method will plot the differences between individuals' connotations for words and thus map the psychological 'distance' between words. It is typically recommended to use a seven–point scale for these types. It is also good to keep the statements on the opposite ends short and precise (Brace 2004).

Every question is related to one ore more of the identified factors in chapter 2.

No.	Question	Type	Values	Factor measured	Comments
6	Please rate your familiarity with the security policies for your organization.	7-step semantic differential	Very Familiar to Very Unfamiliar	Lack of security awareness	*It is likely that the results will show a correlation between familiarity with the policies and the actual adherence to these policies.*
7	Do you practice these policies?	7-step semantic differential	Always to Never	Carelessness, Cultural differences	*Unfamiliarity with the policy will most likely result in not practicing the policy. However, a far more interesting outcome will come from the combination high familiarity and low practice. This indicates that the rules are willfully ignored or bend, This can also be linked to Hofstede's (2001) Individualism vs. Collectivism dimension: Strong individuals are more likely to 'go their own way' to reach their goals.*
8	Compared previous years, I find that IT security policies have become more strict.	7-step semantic differential	Strongly agree to Strongly disagree	Stricter IT Governance	*This question is designed to find out if employees perceive policies to have become more strict. A correlation is expected with the level of practice of the policies.*
9	I sometimes feel that IT security prevents me to work efficiently.	7-step semantic differential	Strongly agree to Strongly disagree	Stricter IT Governance, Cultural differences	*This question acts as a validation for the previous question. It is an opinion variable, which means that the question records the feeling about something or what they think or believe is true or false (Dillman 2000). Low UAI countries would be expected to agree with this statement.*
10	My IT department provides me with the technology I need to perform my tasks.	7-step semantic differential	Strongly agree to Strongly disagree	Stricter IT Governance, Poor alignment between Business and IT	*This question aims to assess a link between compliance to rules and the feeling that respondents have towards not having the necessary IT resources to perform their tasks. Low UAI countries would be expected to agree with this statement.*

11	I sometimes need to bend the rules in order to get work done.	7-step semantic differential	Strongly agree to Strongly disagree	Stricter IT Governance, Poor alignment between Business and IT	*This question aims to assess a link between compliance to rules and the feeling that alignment between business (objectives) and IT is inadequate.*
12	I sometimes feel that less budget is available for IT (projects) than before.	7-step semantic differential	Strongly agree to Strongly disagree	Stricter IT Governance	*This question is to answer the research question "Is it the perception of employees in general that their company displays an increased focus on IT control and investment selectivity", which is in fact also one of the factors identified in chapter 2:*
13	If the IT security rules make no sense to me, I sometimes ignore them.	7-step semantic differential	Strongly agree to Strongly disagree	Lack of security awareness, Poor alignment between Business and IT	*This question aims to assess a link between compliance to rules and the feeling that alignment between business (objectives) and IT is inadequate. It might also indicate that security (awareness) education is inadequate. Low UAI countries would be expected to agree with this statement.*
14	If my Partner or manager asks me to bend the IT security rules, I will do so.	7-step semantic differential	Strongly agree to Strongly disagree	Cultural differences	*Hofstede (2001) links this behavior to the cultural aspect of Power Distance.*
15	If I notice a colleague not following the IT security guidelines, I will address this with him/her.	7-step semantic differential	Strongly agree to Strongly disagree	Cultural differences, Lack of security awareness	*Hofstede (2001) links this behavior to the cultural aspects of Individualism and Power Distance.*
16	I store or transport documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick (excluding PwC-issued encrypted devices).	7-step semantic differential	Often to Never	Lack of security awareness, Carelessness	*In this question a link is made with behavior which falls under the Shadow IT practices. Low UAI countries would be expected to agree with this statement.*
17	I use Google Docs or other on-line collaboration software to store or share work with colleagues.	7-step semantic differential	Often to Never	Lack of security awareness, Carelessness	*In this question a link is made with behavior which falls under the Shadow IT practices. Low UAI countries would be expected to agree with this statement.*
18	I should be able to install the applications I need on my work computer.	7-step semantic differential	Strongly Agree to Strongly Disagree	Lack of security awareness, Poor alignment between Business and IT	*This question tries to investigate the attitude towards the use of Greynet applications (see paragraph 2.4). In a recent study (NewDilligence 2006) almost 40% of end-users agreed with this statement.*

19	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	7-step semantic differential	Strongly Agree to Strongly Disagree	Lack of security awareness, Stricter IT Governance	*This question aims to assess a link between compliance to rules and the feeling that alignment between business objectives and IT security objectives is inadequate.*
20	I sometimes send documents (that could be considered to contain sensitive/confidential information) to a home/private email account so I can work from home.	7-step semantic differential	Strongly Agree to Strongly Disagree	Lack of security awareness	*In this question a link is made with behavior which falls under the Shadow IT practices.*
21	I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)	7-step semantic differential	Strongly Agree to Strongly Disagree	Lack of security awareness, Carelessness	*This question tries to investigate the attitude towards the use of Greynet applications (see paragraph 2.4). In a 2006 study (NewDilligence 2006) almost 53% of end-users agreed with this statement. Initially the question started with "I tend to disregard company policies[…]" but this question was altered because it was too leading and suggestive.*
22	I sometimes download non-PwC software for convenience, speed and productivity improvements. I don't review them with IT since because:	Multiple select	[I never download software], [I always check with IT], [they simply say "No"] , [They don't respond in any reasonable timeframe], [I was not aware of this policy/requirement], [Other]	Lack of security awareness, Poor alignment between Business and IT	*In this question a link is made with behavior which falls under the Shadow IT and Greynet practices. It also links with Business – IT Alignment issues.*

Table 6: Specific survey questions

Responses to these questions would provide enough data to answer the appropriate research questions.

3.3.3 Survey samples

In this survey, the populations are precisely defined as the employees of PwC (excluding temps, trainees, hired consultants etc.) in the countries of The Netherlands and Belgium.

Initially permission was also asked from the German IT Director to execute the survey in Germany, however he denied because of a data breach which just had occurred in their domain. Then permission was asked in the United Kingdom, they denied because parts

of their IT infrastructure is outsourced to CapGemini. Then Switzerland was approached but after consultation they denied because they had just recently launched an annual customer satisfaction survey and didn't want to overload the users with questionnaires. Finally Spain was asked if the survey could be conducted in their country. After a long time they responded that the English language would pose a problem getting valid responses. It was offered to translate the survey but eventually they decided not to go ahead with this. This only shows that this was a sensitive topic and that one of the risks described in the thesis proposal ("limited access") in fact materialized.

A subset (sample) of the Dutch and Belgium population is to be studied, which is representative of the population. In order for the conclusions made from the sample to be extended to the population as a whole, the extent to which the chosen sample is representative needs to be examined.

The margin of error is a statistic expressing the amount of random sampling error in (survey) results. That is, the larger the margin of error, the less confidence one should have that the surveys' results are close to the "true" figures of the whole population. Specifically, the p-value represents the 'probability of error' that is involved in accepting the observed result as "representative of the population." For example, a p-value of .05 indicates that there is a 5% probability that the relation between the variables found in the sample is purely coincidental. Typically, in many research areas, results that yield $p \leq .05$ are considered (borderline) statistically significant (StatSoft 2008).

Territory	Population (n)	p-Value	sample size
PwC Netherlands	5800	.05	361
PwC Belgium	1200	.05	292

Table 7: sample sizes calculated with 95% confidence level (p=.05).
Source: *http://www.journalinks.be/steekproef/*

One note needs to be made about the sample size and the actual response rate. Obviously it was not expected to receive 100% response on the surveys. With an expected response of about 40% (see paragraph 4.1.1) , in order to have a valid number of responses, the Dutch tested base would effectively be nearly 20% instead of 6% and for the Belgians 60% instead of 24% of the population. It was agreed with the IT Directors of these countries that that would be a too high impact on the user organization and to stick with the calculated sample sizes.

3.4 PROFILE OF THE SURVEYED ORGANIZATION

PricewaterhouseCoopers (PwC) was formed in 1998 from a merger between Price Waterhouse and Coopers & Lybrand. It has a history that dates back to the nineteenth century. Both accounting firms originated in London during the mid 1800s.

Currently, it performs industry-focused services in the fields of accounting (assurance), tax, human resources, transactions, performance improvement and crisis management. It also provides services to educational institutions, government, non-profit organizations, and international relief agencies. Recently (2002) PwC has sold the "PwC Consulting" branch to IBM. Worldwide, PwC operates through 850 offices in over 150 countries, with over 146.000 employees.

GTS (Global Technology Solutions) is the internal IT support and solutions provider for PwC. Its goal is to provide Partners and staff with an effective and efficient primary point of contact for a timely and consistent response on computing and technology related inquiries. It reviews and monitors technical errors that occurs in the production environment and mitigate the recurrence of similar issues and incidents and attempts to maximize the reliability and promote the efficiency of GTS Firm-wide services. This is accomplished through systematic and defined processes (ITIL), controls (ISO/IEC 27001) and best practices in process re-engineering and communication.

3.4.1.1 The Netherlands in general as a country and as a culture

Within Europe, several cultural streams are found, each with its distinct cultural dimensions. For instance, The Netherlands in general is said to be in the Germanic region, together with Germany, Austria and Switzerland, but also Britain and Scandinavian countries (*Source: Wikipedia*).

With respect to national culture, the Hofstede dimensions for the Netherlands are very similar to that of German and some Scandinavian countries. The Netherlands highest dimension is Individuality (IDV) at 80, which is the fourth highest in the world. This high Individualism ranking for the Netherlands is indicative of a society with more individualistic attitudes and relatively loose bonds with others. Among high IDV countries, success is measured by personal achievement. The Dutch tend to be self-confident and open to discussions on general topics; however, they hold their personal privacy off limits to all but the closest friends. Due to the importance of the individual within the society, individual pride and respect are highly held values. (Nath and Sadhu 1988)

The second highest Hofstede dimension for the Netherlands is Uncertainty Avoidance at 53, compared to a world average of 64. Uncertainty avoiding cultures try to minimize the possibility of uncertain, unexpected situations by strict laws and rules, safety and security measures.

The lowest Hofstede dimension for the Netherlands is Masculinity at 14. This relatively low MAS Index value may be indicative of a low level of differentiation and discrimination between genders. In this culture, females are treated more equally to males in all aspects of society. This low Masculinity ranking may also be displayed as a more openly nurturing society.

At 38, the Power Distance Index is well below the world average (55). This indicates that the Dutch are less likely to accept and expect that power is distributed unequally.

3.4.1.2 Belgium in general as a country and as a culture

Belgium, through it's language 'barrier' is split in a Flemish and Walloon part which represents respectively the Germanic and Latin culture. As the PwC offices are mostly located in the Walloon part, for this thesis the Latin culture is applied, which is shared with the French, Spanish, Portuguese and Italian. It is characterized as having a medium to high IDV, a high PDI, a high UAI and a medium MAS (Nath and Sadhu 1988).

The cultural (Hofstede) analysis for Belgium shows a very high Uncertainty Avoidance Index (UAI) of 94, compared to the average European countries' score of 74. High Uncertainty Avoidance indicates the society's low level of tolerance for uncertainty. In an effort to minimize or reduce this level of uncertainty, strict rules, laws, policies, and regulations are adopted and implemented. The ultimate goal of this population is to control everything in order to eliminate or avoid the unexpected. As a result of this high Uncertainty Avoidance characteristic, the society does not readily accept change and is very risk adverse.

The Power Distance Index (PDI) is 65, well above the Netherlands (38), and can be compared to France and most South-American countries. This indicates that Belgians accept that there is a high level of inequality (more versus less), but defined from below, not from above. It suggests that Belgium's level of inequality is endorsed by the followers as much as by the leaders.

Individualism (IDV) scores relatively high at 75, so this indicates a society in which the ties between individuals are loose: everyone is expected to look after him/herself and his/her immediate family.

Masculinity (MAS) scores 54, about the world average and well above The Netherlands (14). This indicates that the men are assertive and prone to 'macho' behavior, and a relatively large gap between men's values and women's values.

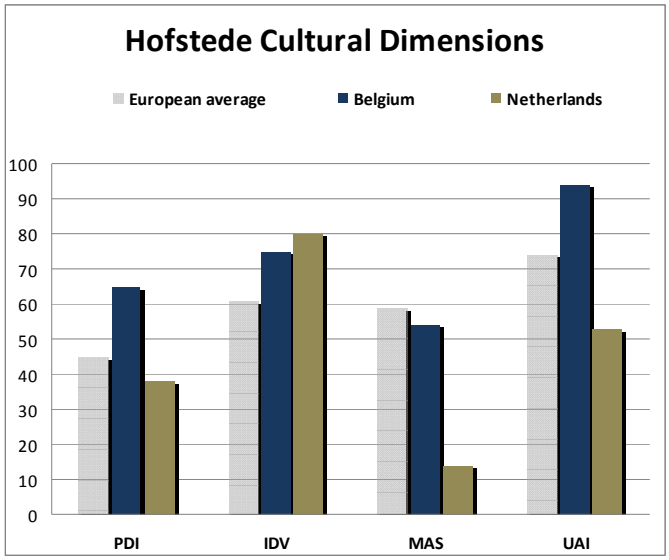


Figure 6: Cultural dimensions
PDI: Power Distance Index
IDV: Individualism
MAS: Masculinity
UAI: Uncertainty Avoidance Index

3.4.2 The Dutch PwC organization

The Dutch environment consists of over 5.800 workstations (mostly laptops), divided over 17 offices in the Netherlands. It has a central Lotus Notes environment in which over 50.000 databases are shared and a storage volume of over 23 Terabyte. It offers a company-wide Portal to its employees and interconnectivity between the Dutch and European networks, offices and VPN remote access. It uses a "high availability and secure" data center. The Dutch IT environment is supported by 180 employees.

3.4.3 The Belgian PwC organization

The Belgium PwC environment consists of over 1200 employees with an average age of 28. IT supports 1.200 workstations, divided over 4 offices in Brussels, Antwerp, Liège and Ghent. Like the Netherlands PwC, it has a central Lotus Notes environment. It offers interconnectivity between the Belgian and European networks, offices and VPN remote access. The Belgian IT department consists of 40 employees.

Chapter

4

4 RESEARCH RESULTS

"The irony of Sarbanes-Oxley is that what the SEC now demands is what good executives have been asking for all along. Every good leader wants to know what their true numbers are and how their management team knows those numbers are accurate. They need someone to monitor what IT systems and processes touch the data that filters down to financial reports, and they want to be assured that appropriate governance is in place for all those systems and processes."
Gwen Thomas, Sarbanes-Oxley Practice Lead for CIBER Inc.

4.1 INTRODUCTION TO RESULTS

The questionnaire consists of 5 grouping variables and 17 test variables.
A comparative research question involves differences between two or more groups with respect to a particular variable, distinguished on the basis of a given characteristic such as gender or age. These characteristics are called the grouping variables. (Baarda *et al.* 2004) Combined with the variables the thesis want to test the groups against, this gives (5 x 17 =) 85 possible (paired) dimensions to test.

The grouping variables are:
Gender: Do men show different behavior and attitudes than women?
Nationality: Are the Dutch displaying other behavior and attitudes than Belgians?
Age: Do younger employees show (significant) different behavior and attitude than older employees?
Laptop users: To what extent do laptop users show (significant) different behavior than desktop users?
Number of years with company: Somewhat related to age; this is to test if 'old-timers' show other behavior and attitudes than 'new joiners'

4.1.1 Response rate

The respondents have been asked to fill out a questionnaire by means of an Internet connection to a web-page from NetQuestionnaires. They have been invited trough an inter-company Lotus Notes email with a hyperlink. This method is called the Computerized Self-Administered Questionnaire (Babbie 2003). Screenshots of the survey pages can be found in appendix B.

The invitation to participate in this survey was sent out to 653 randomly selected employees: 361 in The Netherlands and 292 in Belgium.

country	selected	actual sample size*	responded	response rate
NL	361	360	139	38,6%
BE	292	289	134	46,4%
Total	653	649	273	42,1%

Table 8: Survey response rates
*Out of the invitations 4 delivery failures were received indicating these persons already had left the company.

It can be argued that the non-respondents would have, in some way, a bias towards the topic. For example, people who knowingly breach security would not respond to avoid detection or possible repercussion. To minimize this effect absolute anonymity was guaranteed and care was given not to ask leading or 'company desirable' questions. For more details see paragraph 3.3.

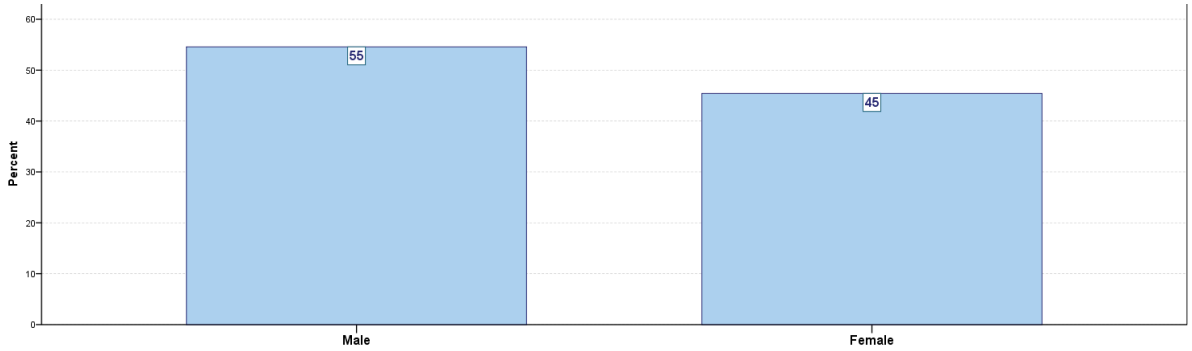
No incentive (gifts etc.) was given, no reminders were sent. Nearly 4 out of 10 Dutch participants and nearly 5 out of 10 Belgians have responded and filled out the survey.
To assess if this is an acceptable response rate depends on several factors: (Hamilton 2003)

- Research purpose: High Response rates are less important if the purpose is to gain insight.
- Type of statistical analysis: Some statistical procedures require a minimum sample size.
- How the survey is administered: Acceptable response rates vary by how the survey is administered:
    - Mail: 50% adequate, 60% good, 70% very good
    - Phone: 80% good
    - Email: 40% average, 50% good, 60% very good
    - Online: 30% average
    - Classroom paper: > 50% = good
    - Face-to-face: 80-85% good

As this survey (average response 42.1%) is a mix of e-mail and online survey, a response rate of average between 30 and 50% can be considered good.

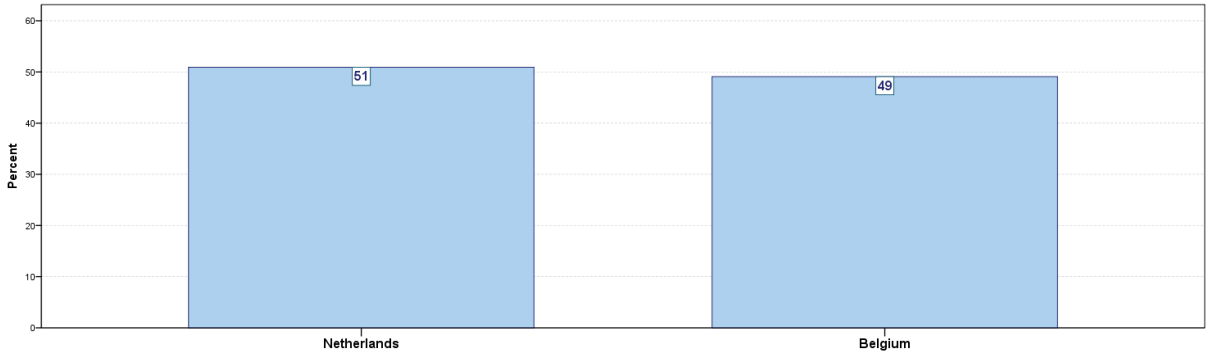
4.2 DESCRIPTIVE STATISTICS

Gender



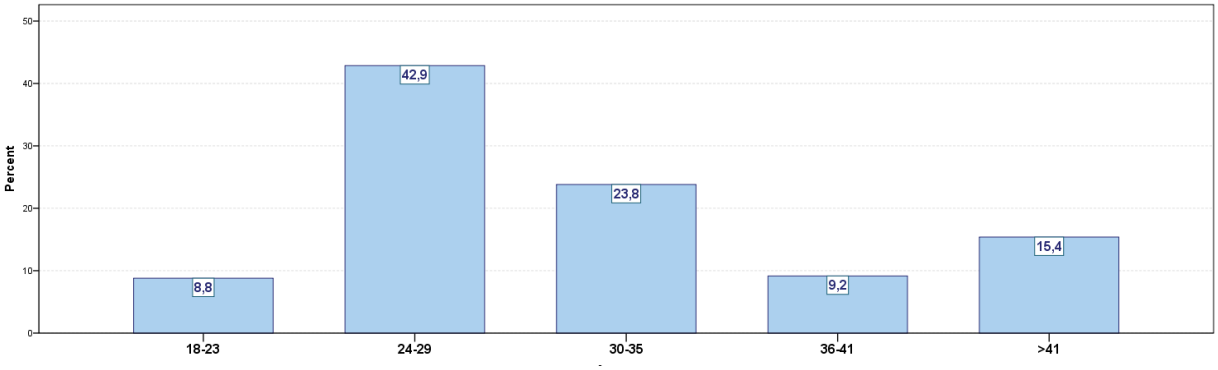
The grouping variables show a good balance between countries and gender. According to the PwC annual report, 41% of Dutch PwC staff is made up by females. For Belgium no data is available, but globally the split is 50-50.

Country



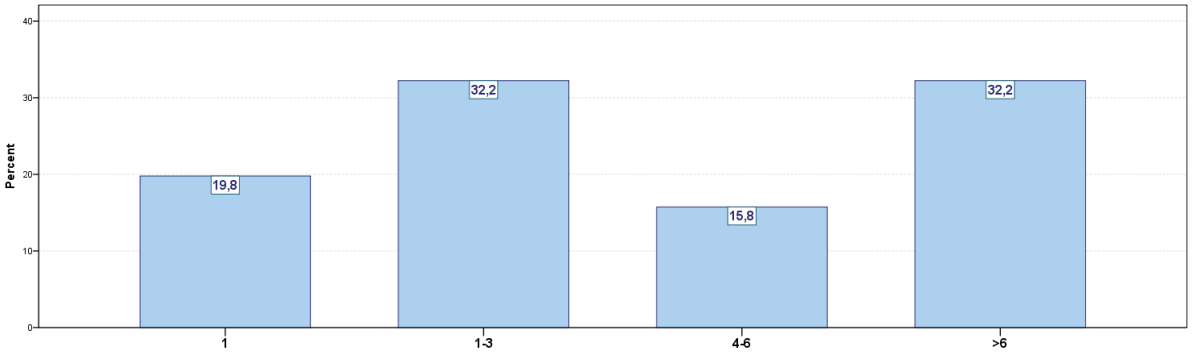
Since more surveys were sent to the Dutch PwC branch, which is bigger than the Belgian one, it was to be expected that more responses came from The Netherlands. However responses are in balance.

Age group



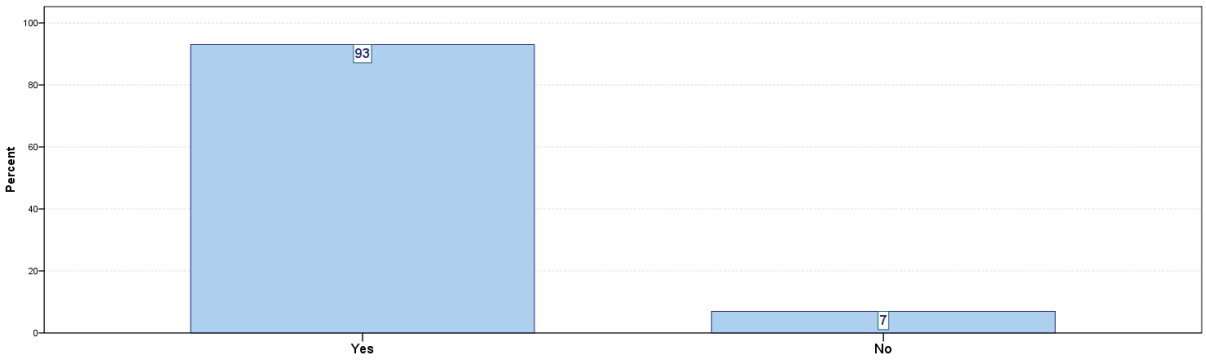
PwC is a young organization with an average age of around 28 years. This is reflected in the employee responses. This group has grown up with computers and internet, may show different behavior and may need to be approached differently from the 'older' generation.

I have been …. year(s) with the company



The relatively young workforce is also with the company for a shorter time. Notably, over half of the respondents are under 4 years with the company.

Has a PwC laptop

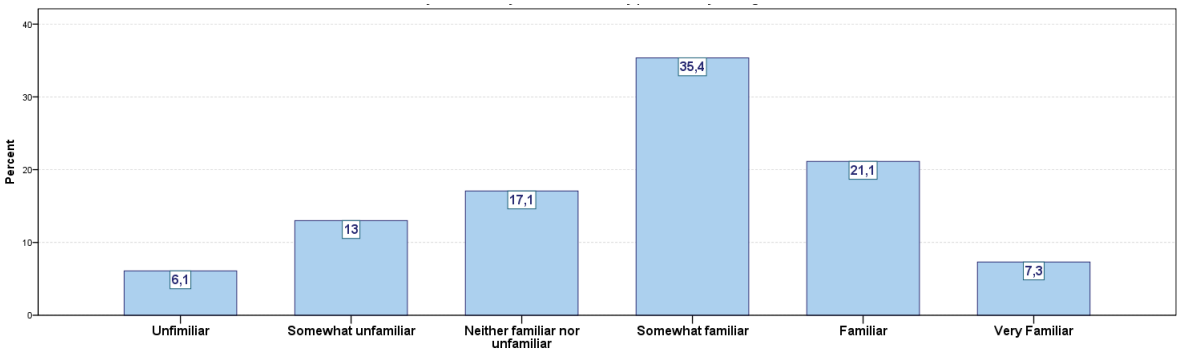


The majority of respondents have a company laptop. Some research shows that these 'mobile users' are more likely to loose data.

4.3 TESTING VARIABLE STATISTICS

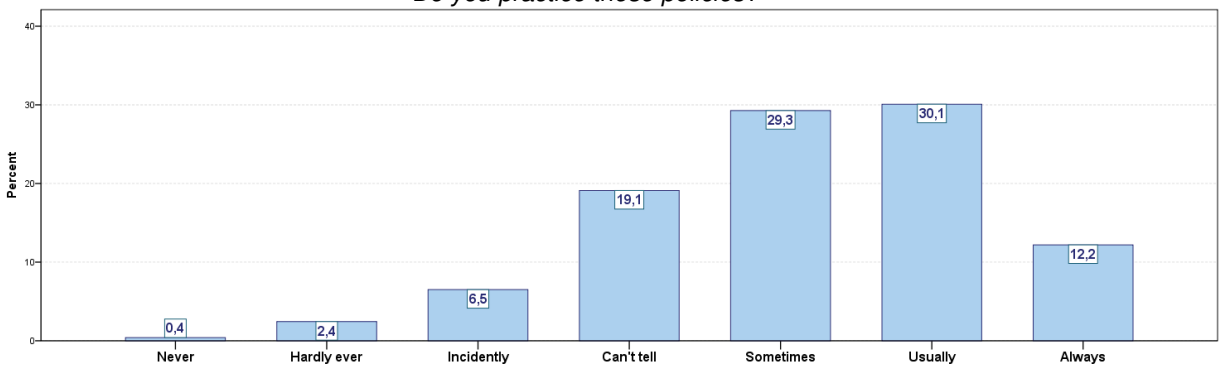
The following graphs are the 'plain' survey results from the testing variables. They give a general picture of the attitudes towards IT and IT Security and serve as an anchor point when making cross-reference analysis in the next paragraphs.

Please rate your familiarity with the security policies for your organization.



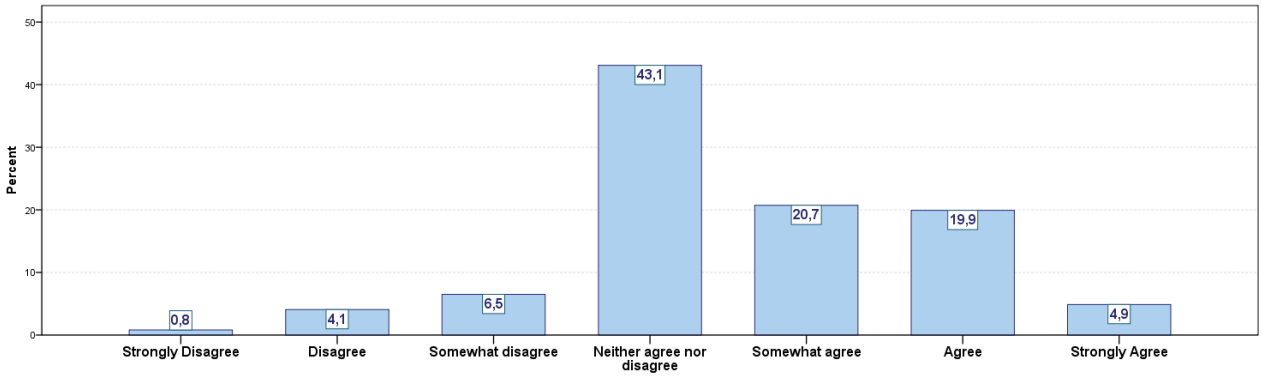
Only a little over half of the respondents are somewhat to very familiar with the policies.

Do you practice these policies?



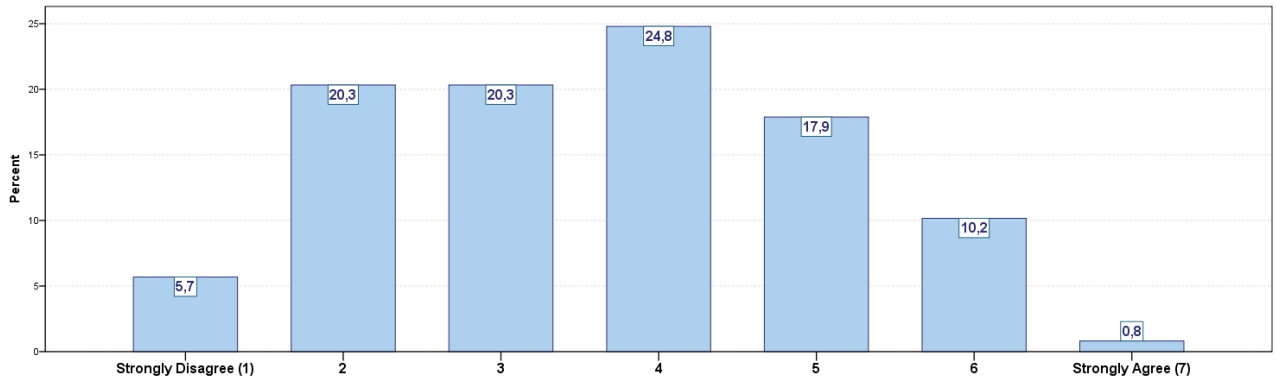
Over 25% do not (knowingly) follow the IT security policies strictly.

Compared previous years, I find that IT security policies have become more strict.



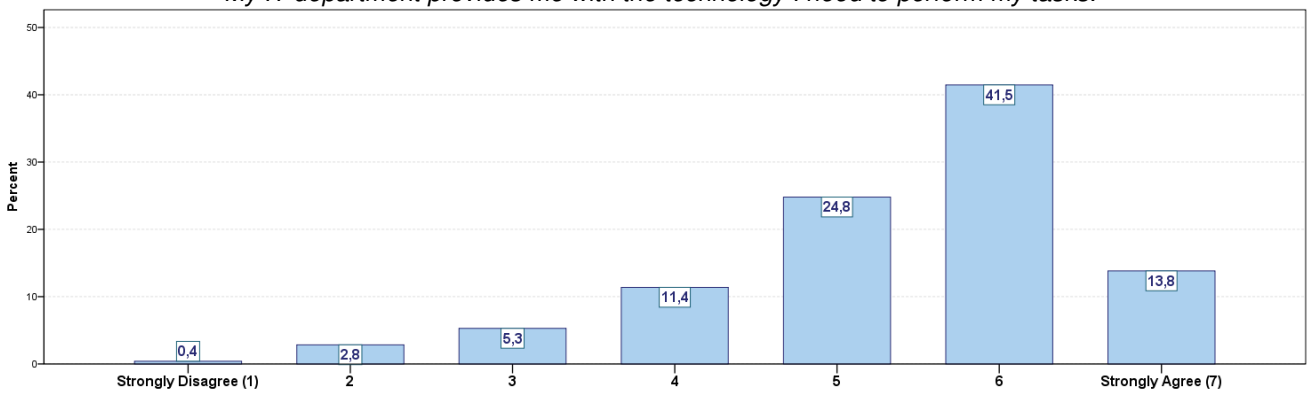
About 40% of respondents do not know if policies have become stricter, and another 46% think they have.

I sometimes feel that IT security prevents me to work efficiently.



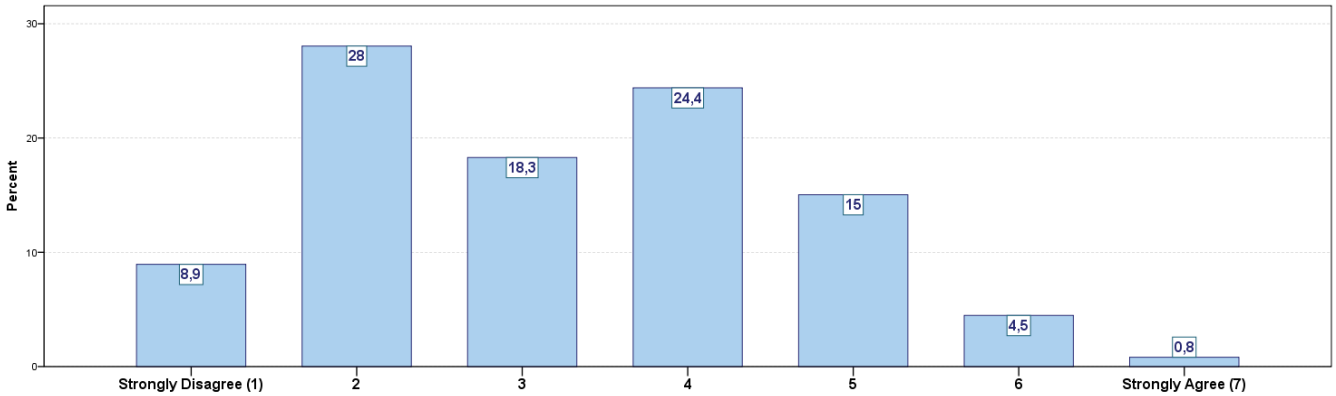
However, only about 30% feels that these security policies prevent them from working efficiently.

My IT department provides me with the technology I need to perform my tasks.



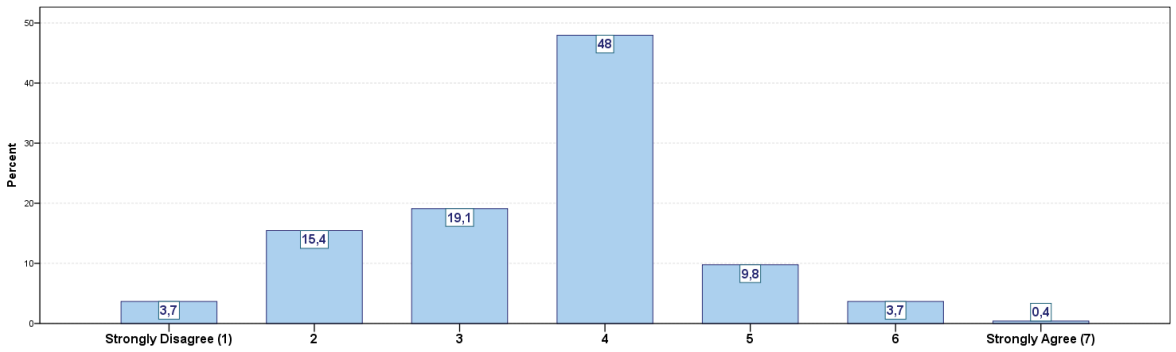
Three out of four are satisfied with the IT equipment provided to them.

I sometimes need to bend the rules in order to get work done.



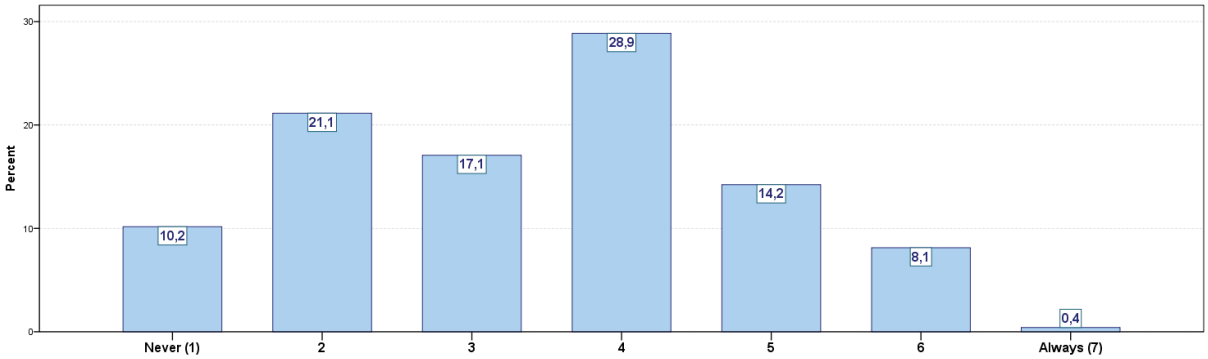
Yet one in five bends or evades the IT security rules to perform their daily tasks!

I sometimes feel that less budget is available for IT (projects) than before.



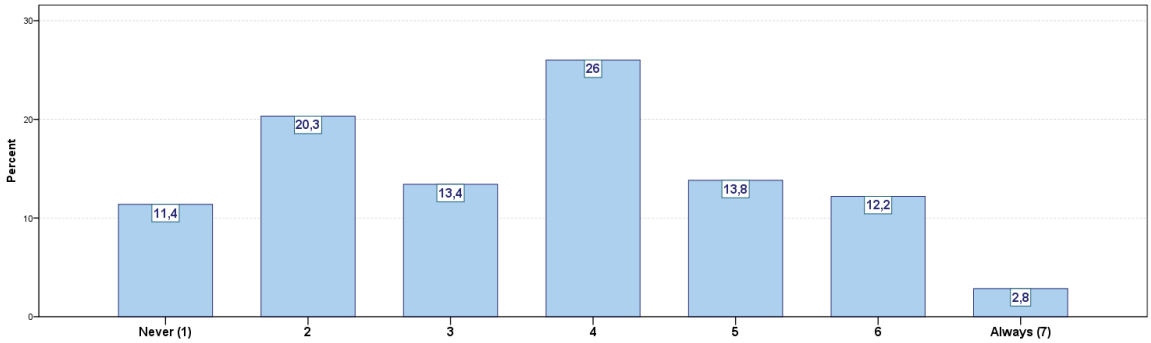
Hardly any of the respondents observe reduced IT budgets. It does not seem a reason for non-compliant behavior.

If the IT security rules make no sense to me, I sometimes ignore them.



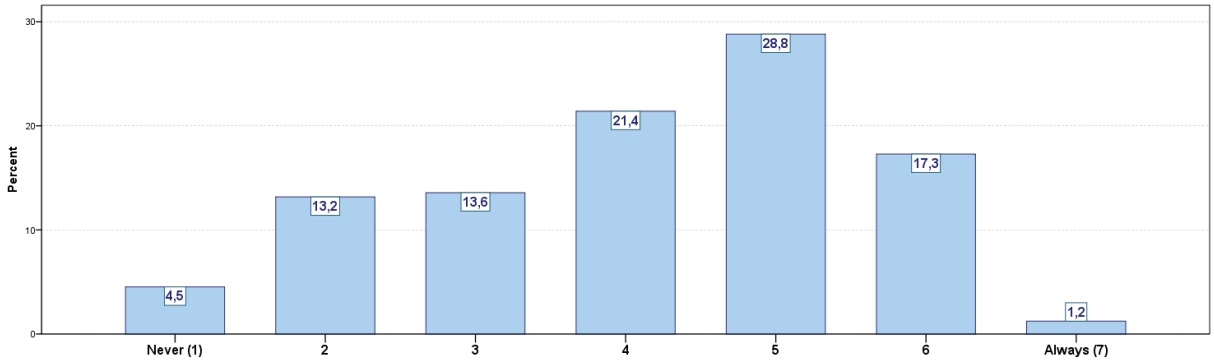
In line with the "I sometimes need to bend the rules…" question, one in five ignores the rules if they don't seem to make sense.

If my Partner or manager asks me to bend the IT security rules, I will do so.



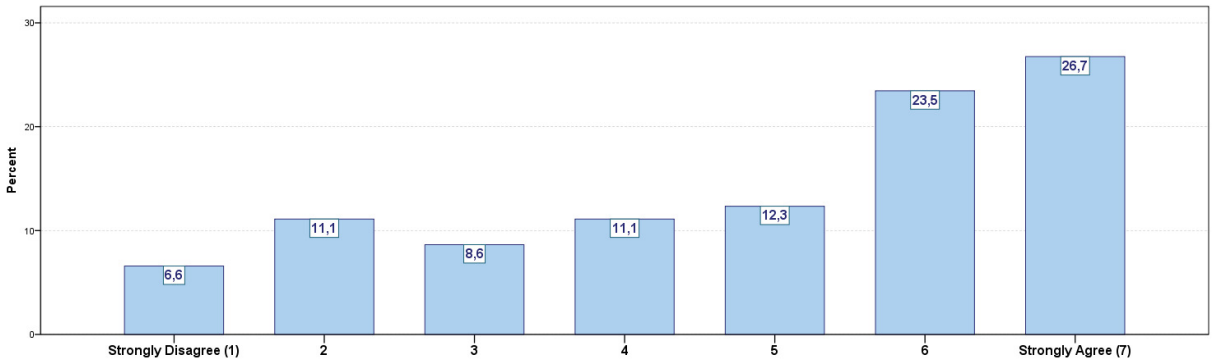
Over half of respondents would bend or break the rules if asked by a manager. This is also part of the organizational culture, which is not researched in this thesis.

If I notice a colleague not following the IT security guidelines, I will address this with him/her.



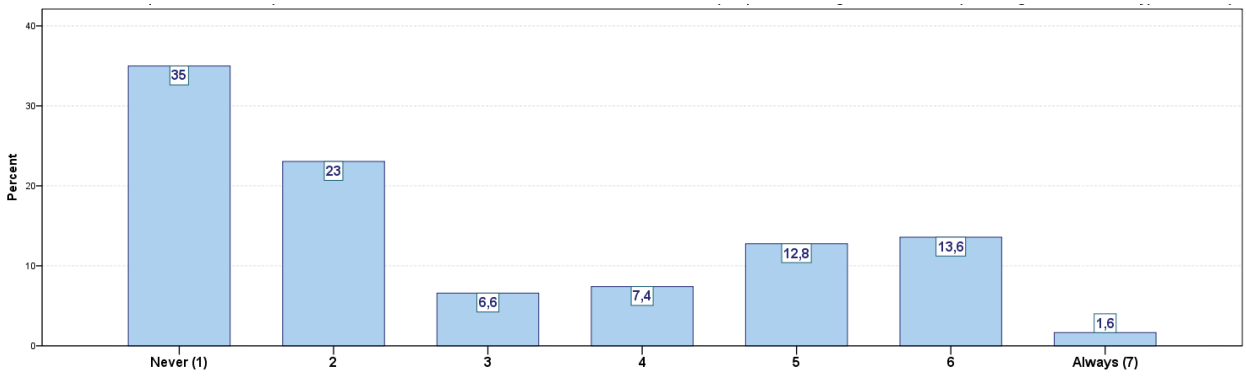
Again about half of respondents would probably not address observed breaking of the rules with colleagues.

I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)



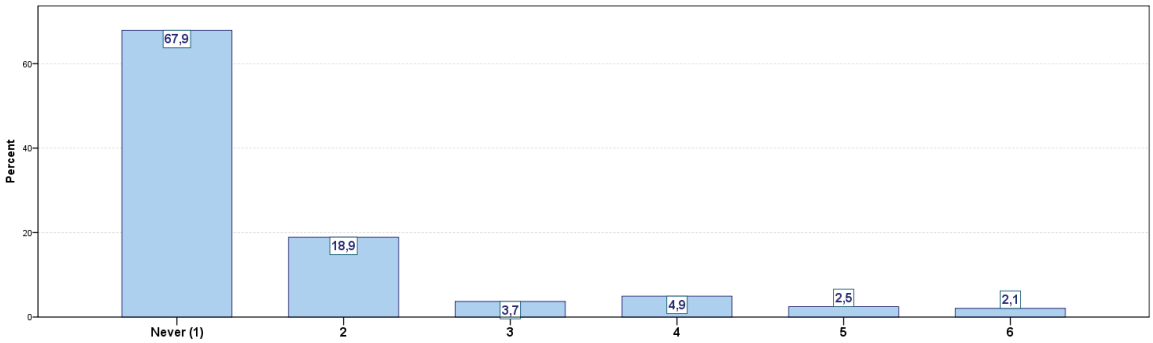
Over half of respondents are aware that they should not IM and P2P software on their work computer. Yet the 16% who aren't aware can put the company at severe risk of data breaches and should not be ignored.

I store or transport documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick (excluding PwC-issued encrypted devices).



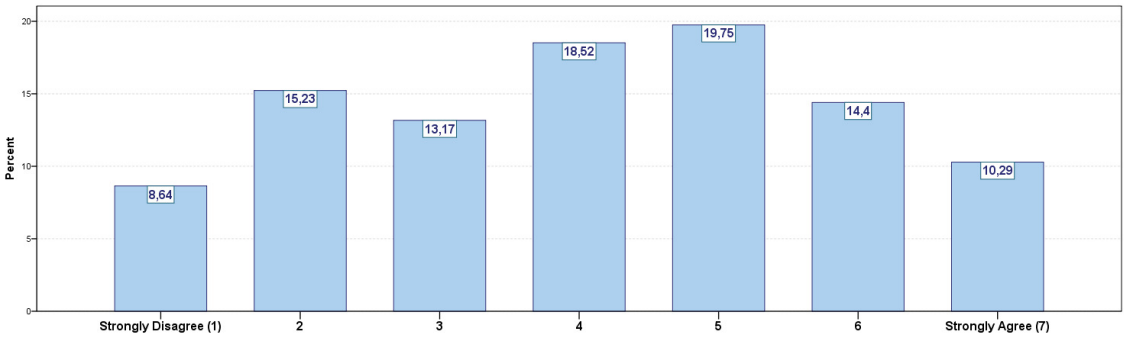
The results show that carrying data on an unsecured data stick is still quite common, although some of the PwC employees (but not all) are provided with an PwC-issued, secure device.

I use Google Docs or other on-line collaboration software to store or share work with colleagues.



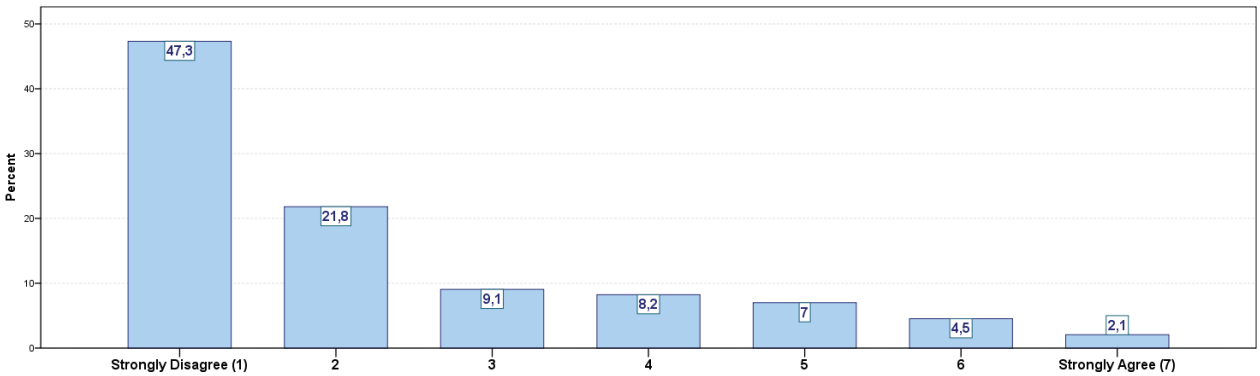
The usage of uncontrolled, web-based applications to share work is not yet common and control or preventing such usage should not have highest priority.

I should be able to install the applications I need on my work computer.



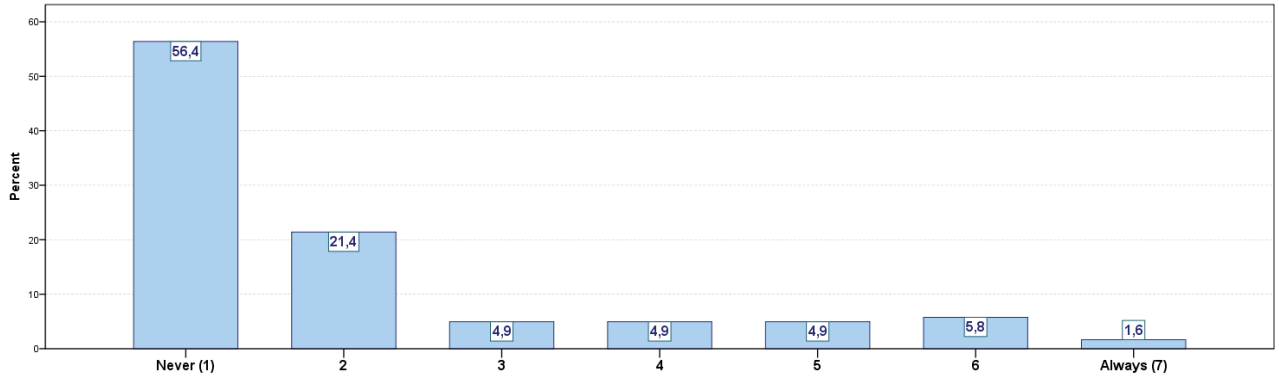
The survey shows an even distribution of answers to the question whether one should be able to install any software needed. Still two in five tend to agree with the statement.

I sometimes need to share my passwords with colleagues so they can assist me with my tasks.

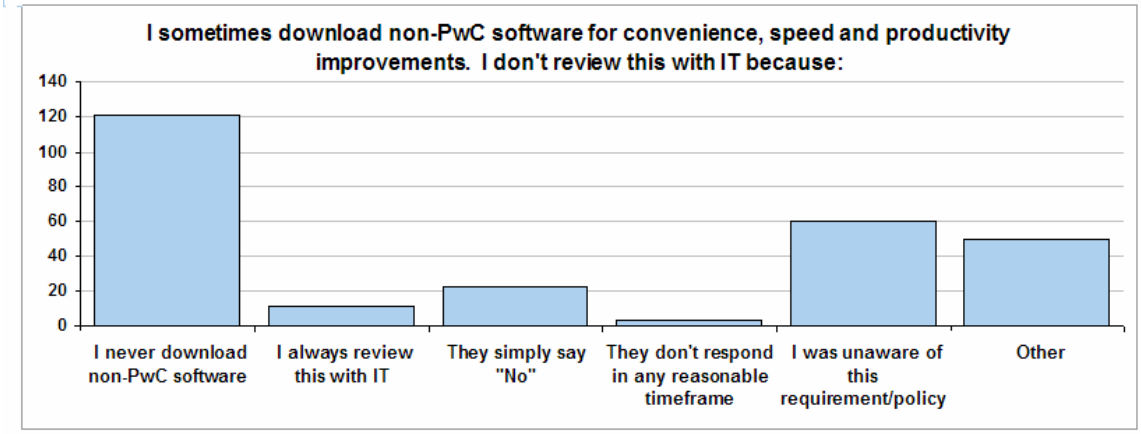


The question on sharing passwords got a 'desired response': when the IT director of Belgium requested the insert *"excluding identified GTS personnel"* this might have triggered some respondents to conclude that they should disagree with this statement.

I sometimes send documents (that could be considered to contain sensitive/confidential information) to a home/private email account so I can work from home.



As with the previous question, the added insert *"that could be considered to contain sensitive/confidential information"* may have prompted a desired response. On the other hand, with 95% of respondents having a laptop computer, the need to send e-mail to private account is lower than several years ago.



The final question was a multiple selection option on reasons if, and why, employees download and install potentially harmful software on their PC. The last four options combined exceed the first two combined which makes this a potential source of risk. Unawareness with the policy is most prominent but easy to address. However this question cannot be used in

comparison with the other results in variance analysis and will not be included for that purpose in the rest of this chapter.

4.4 CROSS-REFERENTIAL ANALYSIS

The next page shows table 7 indicating which testing variables are cross-referenced against grouping variables. Out of the 85 possibilities, a selection of 40 combinations have been selected and analyzed in depth because they were expected to show interesting results based on desk research and common sense. This detailed analysis can be found in Appendix D. A summary of results is given in the next paragraph.

testing variables / grouping variables (p-values)	Gender	Nationality	Age group	time with company	laptop owner
Is familiar with policies	.220 [A]	.019 [B]	.014	.003 [C]	.361
Practices these policies	.694 [D]	.691 [E]	.011 [F]	.007	.849 [G]
Finds that policies have become more strict	.899	.886 [K]	.004	.005 [L]	.417
Finds that security prevents them to work efficiently	.026	.075 [M]	.196 [N]	.095	.061
Needs to bend the rules sometimes in order to get work done	.316	.059 [O]	.018	.425	.250
Sometimes need to share password in order to get work done	.147	.286 [P]	.310 [Q]	.215	.000
Feels that IT provides what is needed	.774	.262 [R]	.819	.544	.581
Feels that less budget is available	.106	.395 [S]	.513	.282 [T]	.637
Will bend rules if manager asks to do so	.472 [U]	.101 [V]	.000	.062	.720
Will address colleague if sees that rules are ignored	.001 [W]	.570 [X]	.054	.100	.599
Sometimes ignore rules if they make no sense	.436	.050 [Y]	.028 [Z]	.008	.438
Has stored data on USB sticks etc.	.293 [AA]	.315 [BB]	.128 [CC]	.156	.131 [DD]
Has used Google docs	.725	.769 [EE]	.335 [FF]	.167	.407
Has send document to home e-mail	.998 [GG]	.593 [HH]	.590	.579	.075
Has sometimes downloaded software	Xxx [II]	Xxx [JJ]	Xxx [KK]	xxx	Xxx
Should be able to install any software needed	.068	.291 [LL]	.024 [MM]	.013 [NN]	.003
Is aware of MSN, Kazaa policies	.601	.815 [H]	.070 [I]	.011	.520 [J]

Table 9: Matrix of which variables were tested

.000	indicates correlation is significant at the P<0.50 level
x	indicates selected for detailed analysis in appendix D.

4.4.1 Analysis details

When we look at the goal of this thesis, it is useful to look at some of the results in a little more detail. This may also include analysis where there is no significant correlation or difference observed.
The mere fact that two (or more) of the variables are correlated, does not say much. It just means that in the sample, the values of those variables are distributed in a consistent manner and systematically correspond to each other for the observations.
Below statements aim to clarify the meaning of the correlation, but it is important to remember that the answers to the questions are mostly self-perception; actual knowledge of the topic or subject was not tested.

Familiarity with IT Security rules

1. The Dutch are more familiar with IT Security rules then Belgians.
2. Older respondents are more familiar with IT Security rules than younger respondents.
3. The longer one is with the company, the more familiar one is with the IT Security rules.

Practicing IT Security policies

1. Older respondents practice IT Security rules more than younger respondents.
2. The longer one is with the company, the more compliant one is with the IT Security rules.

Finds that policies have become more strict

1. Younger employees (age) find that policies have become stricter.
2. The longer one is with the company, the more one feels that the IT Security rules have become stricter.

Finds that security prevents them to work efficiently

1. 37% of men agree with this statement compared to only 19% of women.

Needs to bend the rules sometimes in order to get work done

1. One in three respondents in the age group 30-35 agrees with this statement.
2. Both the under-23 group and the over-41 group typically do not bend the rules to get work done.

Sometimes need to share password in order to get work done

1. Desktop users need to share passwords more often than laptop users.

Feels that IT provides what is needed

1. All respondents are equally satisfied with what IT provides to them; only 8% are dissatisfied.

Feels that less budget is available

1. There is no distinct group which has a strong opinion on this; 86% just don't know or tend to disagree.

Will bend rules if manager asks to do so

1. The under-30 group is most likely to bend the IT security rules if asked by a manager.

Will address colleague if sees that rules are ignored

1. Women are much less likely to address colleagues who are not following IT security rules.

Sometimes ignore rules if they make no sense

1. The Dutch are more likely to ignore the IT Security rules if they don't make sense.
2. In all age groups under-35, about one in four will ignore the rules if they don't make sense. In the over-35 groups, this is only one in twelve.
3. Interestingly, of employees who have joined the company recently (under 3 years) one in four will sometimes ignore rules if they don't make sense, while of employees who have been with the company 3-6 years, one in three will do so. Of those employees longer than 6 years with the company, only one in ten are non-compliant if rules don't make sense.

Has stored data on USB sticks etc.

1. There is no distinct group which has a strong opinion on this; yet overall about one in four have (occasionally) stored and transported confidential data on unsecured USB sticks.

Has used Google docs

1. There is no distinct group which shows significant different behavior on this but 95% has not used this way of sharing information online.

Has send document to home e-mail

1. At the p=.05 level there is no significant correlation between the grouping variables. On a slightly less significance level p=.075 level we find that desktop users will do or have done this more often than laptop users, which makes sense as a portable device like a laptop theoretically eliminates the need to send documents to a home PC.

Should be able to install any software needed

1. 65% of employees under 23 feel they should be allowed to install any application needed on their PC. This percentage decreases when going up in the age groups; in the over-41 group less than 20% agrees with the statement.
2. Employees who are between 1 and 4 years with the company clearly agree with this statement (61%), while this number decreases as they are longer with the company (31% for 'over 6 years' group)
3. Laptop owners (46%) agree with this statement more than desktop owners do. (20%)

Is aware of policies regarding the use of 'Greynet' applications on the work floor like MSN, Kazaa etc.

1. There is no distinct difference between any of the grouping variables.
2. More than half of all respondents say they know that it is not allowed. That is not to say that they do not use it.

4.4.2 Summary

In summary it is observed that age of the respondent is a major factor for the different outcomes. In general, older employees are more aware, more compliant and happier with what they got from IT to do their work. The same applies to those who have been with the organization for a longer time.

As expected from theory, differences are observed between Dutch and Belgian respondents. In general, Belgian PwC employees are more compliant and happier with what they got from IT to do their work than Dutch PwC employees, and the last group is more likely to bend or break the rules. There are not many differences between male and female respondents; female PwC employees do find it more difficult to address security issues with colleagues. Detailed conclusions from these findings can be found in chapter 5.

4.5 CAUSE AND EFFECT ANALYSIS

In chapter 1 several contributing factors were discovered which may lead to the use of shadow IT:

- Carelessness
- Poor alignment between Business and IT
- Lack of security awareness
- Cultural differences
- Stricter IT governance

It is worthwhile to cross-reference this with the forms of shadow IT and other precarious IT behavior which were identified in chapter 2 and tested in the survey. So a split in the specific questions is made between what respondents do (actions, behavior) and what they know, feel or think (attitude, beliefs).

For the purpose of this thesis, these 'actions' have been defined as:

- Bending the IT security rules
- Ignoring IT security rules
- Storing and/or transporting sensitive material on USB sticks
- Using Google Docs or other unsecured collaboration software for work purposes
- Sharing passwords with others
- Sending confidential documents to home computer

The next page shows the 60 possible correlations in a table. The full table of all 120 cross-referential analyses can be found in Appendix E.

Shadow IT / Careless behavior	Carelessness/negligence			Shadow IT		
testing questions	Needs to bend the rules sometimes in order to get work done	Sometimes need to share password in order to get work done	Sometimes ignore rules if they make no sense	Has stored data on USB sticks etc.	Has used Google docs	Has send document to home e-mail
❶ Is familiar with policies	.078	.636	.109	.419	.675	.475
❷❺ Practices these policies	.081	.005	.010	.301	.499	.133
❶❷ Is aware of MSN, Kazaa policies	.601	.390	.002	.407	.180	.192
❹ Finds that policies have become more strict	.021	.870	.098	.320	.920	.403
❹❺ Finds that security prevents them to work efficiently	.000	.992	.001	.635	.522	.711
❸❹ Feels that IT provides what is needed	.041	.396	.124	.451	.868	.014
❹ Feels that less budget is available	.006	.955	.307	.188	.103	.873
❺ Would bend rules if manager asks to do so	.001	.199	.000	.122	.588	.813
❶❺ Would address colleague if sees that rules are ignored	.025	.116	.000	.033	.237	.747
❶❸ Should be able to install any software needed	.008	.879	.075	.376	.747	.574

Table 10 : Cross referencing influencing factors with behavior (p=0.05)

❶| Awareness ❷| Carelessness ❸| Poor BITA ❹| Stricter IT Governance ❺| Culture

Two things need to be noted about above table:

First, nationality (cultural differences) isn't included in above table, although it is part of the five identified factors. There are two reasons for this: first, Nationality was already included in the first cross-referential analysis so it would duplicate 11 of the previous outcomes. Secondly, culture doesn't really fit in either category as it is not something people experience consciously or do deliberately. In the table, it would be in fact a third dimension which complicates interpretation.

However, when creating two separate tables, one for Belgium and one for The Netherlands, different outcomes are noted. In 6 cases, the outcome for The Netherlands was significant, while it wasn't for Belgium, in 4 cases Belgium outcomes were significant and Dutch outcomes weren't, and finally in 8 cases outcomes for both countries were equally significant. Although interesting, the results are probably too fine-grained to base any conclusions on.

Secondly, one could argue about the position of the following two questions in the table:

- *Would bend rules if manager asks to do so?*
- *Would address colleague if sees that rules are ignored?*

Are these things people (would) do or is it something they feel/think? When looking at the exact phrasing, the question is asking an opinion and therefore fits better in the testing questions section.

To the right the conceptual model is shown, now with an overlay of the questions and behavioral aspects from the table.

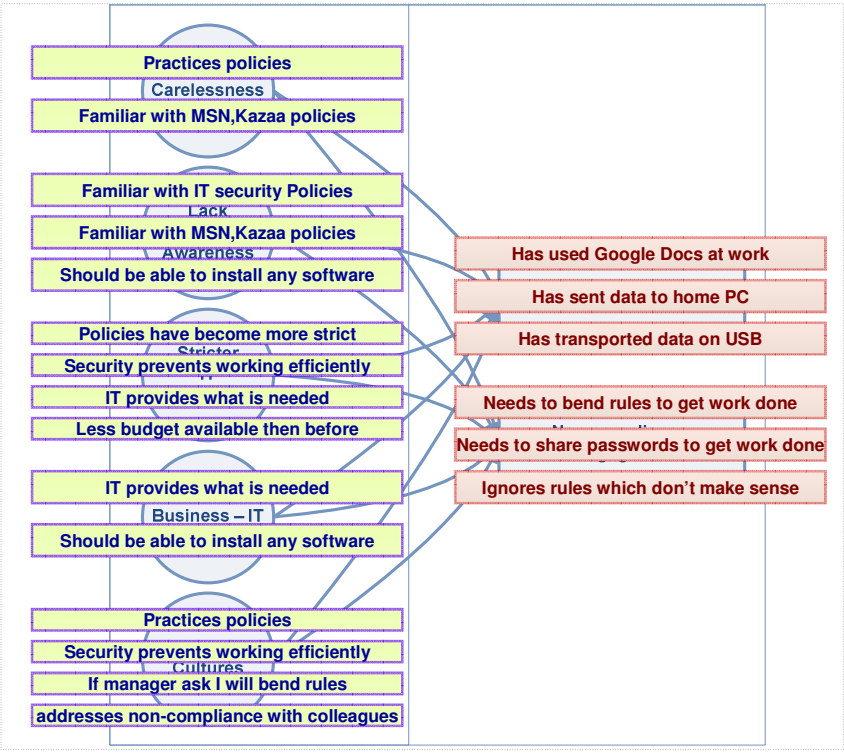


Figure 7: Results analysis projected on Conceptual model

4.5.1 Analysis details

When looking at the results of table 8, it is first needed to again establish what is being measured and secondly what the results represent.

All responses represent a numeric value, or score, of 1 (never, strongly disagree) to 7 (always, Strongly agree).

The cross-tab analysis looks at the linear relationship between scores of variable A (contributing factors) against variable B (insecure behavior towards IT policies and data).

It shows the two-sided significance of the relationship, or in other terms, if variable A scores low, what is the likelihood that variable B also scores low? At a 95% confidence level, any

Pearson's Chi-Square test (p-value) of 0.05 or lower indicates that the relationship is real and not by chance. The grey areas in table 8 show the significant relationships.
When looking at the table in a first glance, some observations can be made:

- In general, insecure behavior —like sharing passwords, storing data on unsecured USB sticks, using unsecured online document sharing and sending confidential mails to home PC's— seems not to be influenced significantly by what the respondents think or feel about the services IT provides to them.
- 'Bending' or ignoring the rules seems like a valid excuse when 'work needs to be done' or when 'rules do not make sense'.
- Effectively people who bend the rules (i.e. willingly ignore or circumvent the IT Security policies) seem to point to others (IT department, managers) or the situation (less money available etc.) for their behavior.
- Familiarity with the policies does not seem to affect (reduce) incompliant behavior.
- Online applications like Google docs are hardly used (5%) and their usage is not influenced by any of the identified factors.
- Someone who 'sometimes – to always' needs to bend the rules to get work done, also finds that policies have become more strict, that security prevents them to work efficiently, feels that less budget is available than before and will bend the rules if manager asks to do so, and finally feels that the should be able to install any software needed. This outcome was somewhat to be expected: if all the preconditions were perfect, there would be no need to bend the rules.

Note that the significant correlation (p=.041) between "[A] my IT dept. provides me with the tools I need to perform my job" and "[B] I sometimes need to bend the rule to get work done" is a 'reverse' correlation: the less respondents agree with statement A, the more they agree with statement B.

The same logic does not seem to apply between statement "[A] I sometimes need to bend the rule to get work done" and "[B] If I notice a colleague not following the rules, I will address this with him/her". One would expect that if respondents do not bend the rules themselves, they would address others (colleagues) who do. However 47% of respondents who disagree with statement A, almost never (40%) address this with peers.

4.5.2 Summary

It is difficult to summarize the effects observed in the previous paragraphs: in some cases inconsistent behavior is observed with unexpected outcomes. The most important finding is that, although the respondents indicate that they are familiar with the IT security rules, this doesn't prevent them from ignoring them if circumstances provide a valid excuse (in the eyes of the culprits).

This then points to the fact that respondents know *what* the rules are, but lack the insight in *why* the rules are there and *how* to use them effectively.

The other finding is that in general, insecure IT behavior doesn't seem *directly* influenced by lack of alignment between what business wants and IT can deliver nor by stricter (enforcement of) IT Security rules.

Chapter

5

5 CONCLUSIONS AND RECOMMENDATIONS

"Change is good. You go first."

Dilbert (Cartoon created by Scott Adams, American cartoonist, born 1957)

5.1 CONCLUSIONS

This paragraph will combine all findings of chapters 2,3 and 4 and draw conclusions from them. This includes a check if the research questions have been answered and if research objectives have been met.

5.1.1 General conclusions

In paragraph 1.5 the research question was defined: *which factors influence the usage of Shadow IT and carelessness towards data security*. This will be discussed in paragraphs 5.1.1.1 and 5.1.1.2.
The sub-questions were: *is it the perception of employees in general that their company displays an increased focus on IT control and investment selectivity, and if so, that this increased focus results in reduced or delayed spending on IT projects which they feel limits them to perform their work effectively and competitively.* The literature study in chapter 2 resulted in several indicators that this was the case (for example Moreau 2007; Shaffner 2009). This will be discussed in paragraph 5.1.4.

Also, some sub-questions were defined:

Which security risks can be identified?

Paragraphs 1.1, 2.1; 2.2 have given many examples. Monetary loss, public embarrassment, personal fines or even imprisonment are some of many possible consequences.

Are National Cultural differences aspects of influence?

The last section of paragraph 5.1.3 will go into detail about that.

What other influencing aspects can be defined and which ones will be tested?

Literature defined 5 influencing factors which have been tested in the survey. Table 9 on the next page summarizes those and other factors.

How can awareness be defined and can levels of awareness be identified?

This question was addressed in paragraph 2.3.1. In short, and in the context of this thesis, it is the state where users in an organization are aware of their security 'mission'. Information, knowledge and insight are levels of measurement. Other factors, such as attitude, motivation and commitment, play an important role too.

What forms of shadow IT can be defined?

This was explained in paragraph 2.2.4. Shadow IT takes many forms: unofficial data flows inside and outside the company network perimeter, self developed applications, Greynets, shadow IT groups outside of company IT.

5.1.1.1 *Factors influencing usage of shadow IT and carelessness*

As to the finding which factors influence usage of shadow IT:

Literature indicated that low awareness and incorrect assessment of risk in the IT dimension were found to be an influencing factor. When the survey asked questions covering the same theme, it was surprising that none of the themes showed a valid homogeneity within the questions.

Identified factors from the literature review and result after testing in survey:

Factor	Result
National culture *	A moderate factor; in 2 out of 16 test questions culture was an influencing factor
Stricter IT governance (stricter IT Cost control, IT budget cuts, Project investment selectivity)	A minor factor
Awareness of IT security policies *	A minor factor
Carelessness (Incorrect assessment of risk involved)	A major factor
Poor Business - IT Alignment	A minor factor

Table 11 : Summary of identified influencing factors

Suspected factors (not identified in literature) after testing in surveys:

Factor	Result
Age	A major factor; in 7 out of 16 test questions, age group was an influencing factor
Gender	A minor factor; in 2 out of 16 test questions culture was an influencing factor
Years with the company	A major factor; in 7 out of 16 test questions, age group was an influencing factor A factor but not a strong one
Senior management setting example	A moderate to major factor; over half of respondents would break the rules if asked by a manager.

5.1.1.2 Factors influencing carelessness towards data security

National culture

Research of existing literature shows national cultures to be factors of importance, in this survey it was only identified as a medium to minor factor. Had the third survey country been included, the outcome may have been more important. In this last subject, the thesis will explore what (other) impact culture can have in the thesis perspective.

In low 'Power Distance' countries such as the Netherlands (with a score of 38) employees and managers consider each other as essentially equal. In these cultures, *"the hierarchical system is just […] established for convenience"* (Hofstede and Hofstede 2005).
Before conducting the survey, it was expected that the Dutch respondents would show higher assertiveness than Belgians, such as ignoring IT security rules "if they don't make sense" but also refusing to execute tasks if they feel these are against personal beliefs and less resistance towards addressing issues with peers. In general, these expectations were not confirmed in the survey. This can be explained by the about equal IDV rating for each country, which also influences this behavior.
Perhaps most significant, 9 out of 10 (males or females) would ignore rules if told so by the manager. It is therefore extremely important that these managers set the correct example and not put employees in this position.

Research by Hofstede (2005) shows that feminine cultures such as The Netherlands extend their need for quality of life into the workplace as well. Leisure and personal activities, such as reading the news and watching television, may be tolerable at work. This is not so in more masculine cultures such as Belgium, where one would find a stricter task orientation. Employees in feminine cultures are also likely to take work home just to be with their families (Mooij 2000). This poses the most risk as can be seen in the many reports in the media where in the transfer from workplace to home confidential data is lost or stolen.

Uncertainty Avoidance can be defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations" (Hofstede and Hofstede 2005). The Dutch have a very low UAI compared to the Belgians. Low UAI cultures are less rule-dependent and more trusting. This may lead to experimentation with new online applications or software. Also, companies in low UAI are less likely to impose company rules on ICT usage, and if they do, it's likely that people will challenge or break such rules for pragmatic reasons (Veiga *et al.*,2001, referenced by Sørnes *et al.* 2004). However the survey did not find strong indications of this behavior.

Stricter IT governance

In this thesis, desk research gave indication that employees feel the impact of increased IT governance. This would result in stricter policies, stronger security measures and tighter budgets. As a result it was predicted that employees would show more non-compliant behavior to work around these limitations, and therefore expose the company to more risk.

Six questions have been asked in the survey on these topics, four covering the rules and policies, two with regards to the budgets. Combined with the grouping variables Nationality, Age (group) and Time with company this resulted in 10 outcomes to be studies.

The survey results did not confirm the desk research expectations. Although about half the respondents did feel that policies had become stricter, this did not 'force' them in non-compliant behavior like bending the rules or sharing passwords. Also, most respondents just don't know if less budget for IT initiatives is available than before so it is not a motive for other non-compliant behavior. Overall, PwC employees in both countries are actually very satisfied with the technology the IT department provides to them.

Awareness of IT security policies

It was found that (un)familiarity with the security policies is an influencing factor, but not as strong as one would expect. That is, respondents indicating familiarity with the security policies may still display insecure behavior, and respondents indicating unfamiliarity with policies may show more careful behavior.

The survey shows that respondents in general do not really know if security policies have become stricter, but lean towards the perception that they have. However they do not feel that there is less budget available then before and are happy with the IT means provided to them.

Men indicate that they feel they are more familiar with IT security policies than women. However this does not mean they also show more compliant behavior; some outcomes even point to the contrary. Also notable is that on average, one in three men and women indicate they are not familiar with IT security policies.

Three out of four Dutch respondents indicate that they are to some extent familiar with the existing security policies. For the Belgians, this is only one in two. On the other hand, half of the Dutch indicate they sometimes need to bend or bypass the IT security rules in order to get work done. The Belgians do only slightly better.

The older employees assess themselves to be more compliant with the IT Security policies than the younger employees. As the age of the employee increases they feel less that IT security prevents them from working efficiently.

Education (the 'what') and availability of IT Security Guidelines (the ‘where’) should therefore be the priority and the framework of paragraph 5.2 could assist in making that effective. Making end users aware of their security responsibilities and teaching them correct practices helps these users change their behavior (NIST 2001).

Carelessness

Carelessness was a difficult dimension to test. It is closely related to awareness because it is usually an unconscious process. Those who knowingly bypass rules because they don’t care about the consequences were tested with two questions. Around 20% of respondents show this type of behavior. They need to be thoroughly educated on the impact such behavior may have on their company, clients, colleagues or themselves.

Poor Business - IT Alignment

Over 75 percent of respondents were happy to very happy with what IT tools and infrastructure are provided to them. In effect all questions testing a poor match between what business wants/needs and IT can deliver did not confirm that poort BITA is a factor for non-compliance with IT security rules.

Other factors: IT as an obstruction

The older one gets, the more one tends to disagree with the statement 'IT security prevents me from working efficiently'. It’s the age group 30-35 that feels strongest that IT security prevents efficient working.

Four in ten Belgians sometimes need to bend or bypass the IT security rules in order to get work done, against half of the Dutch. Overall, Belgians are most satisfied with the technology provided by their IT department and don’t see IT as an obstruction.

The Dutch are more likely to ignore rules if they make no sense to them and the younger generation (under 30) is more likely to ignore rules if they make no sense than the over 30 group.

Education on the 'why' is therefore very important and motivates those being trained to care about IT security, and to remind them of existing security policies. Explaining the possible disastrous effects to the organization, clients, and employees when IT security fails because of policies not being followed motivates people to take that security seriously.

Other factors: Senior Management should set example

If a Partner or manager asks a Belgian employee to bend the IT security rules, he/she will more likely do so than a Dutch employee. It was found that overall, 87% of men and 91% of women could/would at one point bend the IT security rules if asked to do so by a superior.
Men are more likely than women to address colleagues if they observe them not following security guidelines. This is possible one of the most significant outcomes of the survey. As both The Netherlands and Belgium have relatively low PDI and relatively high IDV, It was expected that risk arising from following 'illegal' instructions by Senior Management would not be a big problem. It is therefore essential to have management buy-in in awareness programs and they should lead by example.

Specific usage of Shadow IT

The survey shows that one in three of the Dutch 'occasionally' to 'always' transport data on USB sticks, against two in five of the Belgians.

Although most respondents in general do 'never', 'hardly ever' or 'rarely' transport sensitive data on USB sticks, the age group 24-29 clearly stick out with their 'sometimes', 'usually' and 'always' answers.

The survey shows that online collaboration outside of the enterprise network is not something very common yet. Shadow IT in the form of IT support groups/structures outside the view and control of the internal IT department was not research or tested.

5.1.2 Evaluation of objectives

To round off the conclusions, in paragraph 1.7 the research objectives were given, and it can now be tested if these have been met:
First, this thesis aimed to obtain a general insight in the current knowledge and perspectives on the subject; the better part of chapter 2 has been devoted to that.

Secondly, it was the aim to get insight in the extent to which (PwC) employees (are aware that they) take unnecessary IT risks including the use of shadow IT and to get insight in the reasons why (PwC) employees take unnecessary IT risks including the use of shadow IT; for this the survey was defined, executed and analyzed. Based on the findings, certain generalizations can be made.

Finally, the research set out to identify conditions which increase or influence human risk-taking behavior towards sensitive information. Several contributing factors were found to increase risk-taking behavior and non-compliance, including:

- Cultural aspects, mostly national and in lesser extent organizational;
- Carelessness or willfully ignoring the rules;
- Bad alignment between IT provisioning and Business requirements and objectives;

And indications that these factors have some effect as well:

- Age and time with the company;
- Senior Management not leading by example;
- IT not taking leadership and responsibility for security awareness program development and training;
- Poor usability of available security features;
- No monitoring of compliance to IT security guidelines;

It must be noted that not all identified factors were tested in the survey, and not all the tested factors showed the expected results.

5.1.3 Limitations of the research

Before rounding off the conclusions, this thesis wants to put the result in the context of the limiting factors encountered.
First, the small sample size, which was requested by the IT Directors of the two PwC countries, has most likely influenced the survey outcomes. Where 653 results were needed to get a reliable representation of the population, the survey only delivered 273 results. The significance of the outcomes has to be viewed within this limiting perspective.

Secondly, a third PwC territory to research would have benefited the outcomes, particular those relating to cultural differences. Unfortunately this was not allowed.

Finally, as stated earlier in this thesis, IT security is a vast area to explore and test, and has many links with behavioral sciences. This thesis has limited itself to some influencing factors found in current publications and research. This list is in no way comprehensive. The conclusions drawn from the outcomes have to be viewed within this limiting perspective.

5.2 RECOMMENDATIONS

In the introduction the need for a new ‘ holistic’ approach towards IT security was mentioned, which includes establishing meticulous risk fundamentals. This part of IT governance is sometimes also described as IT assurance. These recommendations can act as part of this holistic approach.

When trying to define practical application of the research in this thesis, only universal recommendations can be given. This is in part because the survey outcomes, analysis and conclusions were based on a small sample size.

Forrester (Jaquith 2009) recommends three key steps IT security officers should take to succeed. This research gives reason for some extra steps, also taking into account the largely unexplored area of national cultures.

It is essential that business management not only leads by example but also takes ownership for adherence to security policies. This responsibility should not (only) lie with the IT department,but (also) with the business units themselves. The survey shows that this is perhaps the most surprising as well as the most risky issue within PwC. If even in countries with a low power distance such as The Netherlands eight out of ten employees would willingly and knowlingly break the IT security rules if asked by their manager, one could expect even higher scores in countries such as Japan or India.

IT should take ownership for basic data security tools that require no customization, such as laptop harddisk encryption and automatically updated antivirus software. Both are relatively simple to implement and offer effective protection while not impeding productivity. In addition, IT security should offer data flow monitoring services to the ‘business’. This recommendation is confirmed in this thesis: the survey shows that if IT security rules are too obstructive or restrictive, many employees will start looking for ways to bypass these rules.

Following the previous two recommendations, one should encourage the business side, so not the IT security manager, to drive business data protection initiatives. For tools like data encryption, and data loss prevention, IT security's role should be limited to providing expert advice, try to achieve consistency by setting standards, and consulting with business units as they deploy solutions. This will prevent business units and their leadership to see IT security as an annoyance or nessecary evil, and thus make it easier for them to set the right example to their employees without jeapordizing the business goals.

IT and Business management should take a fresh and unbiased look at how users work and think. Best practices for security programs usually depend on succesfull security awareness

education, and typically that part of employee training is usually forgotten, skipped or put on hold. When developing IT Security awareness programs, one should tailor these to appeal to younger staff and/or specifically for women. Awareness training should be an essential part of introduction training when joining the company.

When developing security awareness programs, take into account that the national cultural aspects are stronger than the organisational culture. This may result in different policies, training methods and monitoring practices per country, even if dealing with the same company. For example, in the Netherlands, the training developer may need to spend more time on explaining the 'why' of the policies so they would make more sense to the employees.

In addition to the necessity to educate employees on the need to think about security, IT should focus on making controls both invisible and inescapable.. In particular, the enterprise should promote strategies that reduce the need for sensitive data on 'portable' devices like laptops and USB sticks and/or provide their employees with secured, encrypted devices. The survey shows that resondents now feel they need to bypass some security policies in order to get work done.

Management should not ignore the new 24 hour economy: working life and company life blend into each other. In feminan cultures especially, Business and IT Security may need to accept a certain level of personal and leisure activities during regular working hours; in return they can expect employees to also work in evenings and in weekends. Blocking non-business websites like Facebook or Gmail at work may not only demotivate people, but also may trigger them to look for ways to bypass security. In addition, the company needs to make it easy for them to perform those business activities outside regular working hours (from home or hotel) in a controlled and secure manner.

5.2.1 Framework

For a general overview, a model has been developed which tries to put many of the variables in relation to each other. A framework is a support structure for describing a set of concepts, methods and technologies.

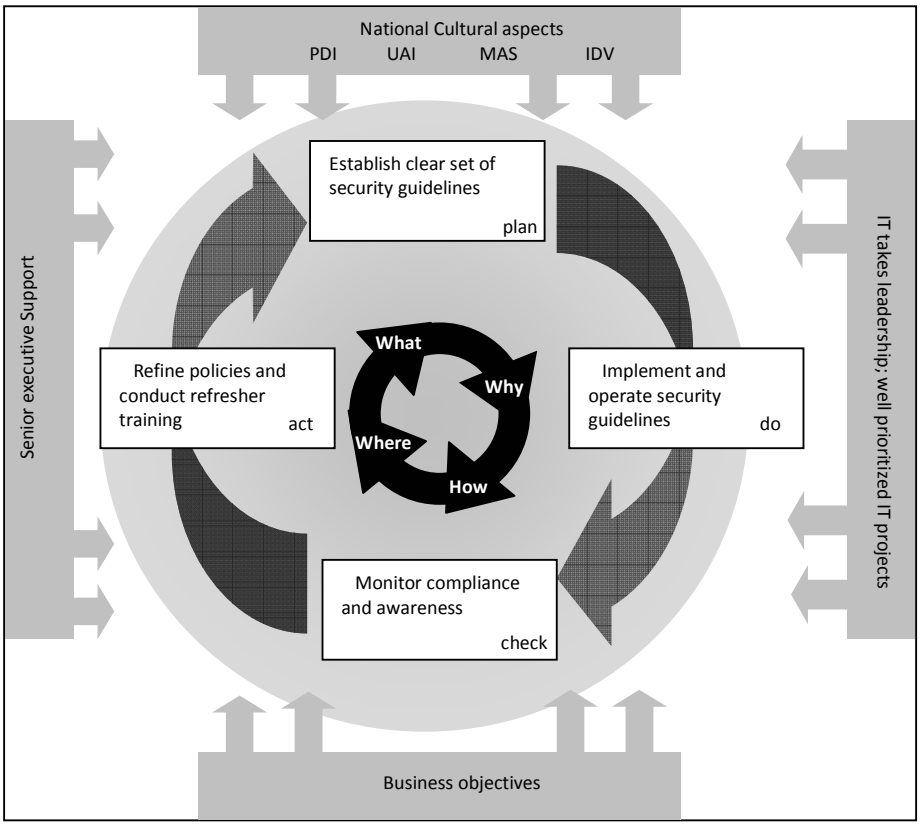


Figure 8: Framework for developing, implementing and monitoring security guidelines

This model might be used when developing, improving, monitoring and/or rethinking the IT security guidelines.

The framework combines several best practices. As the theoretical study and research suggest, in order to reaching optimal effectiveness, what is needed is a multidisciplinary, holistic approach (see paragraph 1.1: Richards 2008).

5.2.1.1 Model Basis

The model's basis is built on the 'Plan – Do – Check – Act' continuous improvement circle developed by Deming (1986) or the Six Sigma 'Define – Measure – Analyze – Improve - Control" cycle (Motorola 2006) but also includes Hofstede's Cultural dimensions and Luftman's (1999) Enablers of Strategic Alignment. Finally, the center shows the attributes of the Comparative Framework (NIST1995) most important components of creating security

awareness. Every IT security policy or guideline should include the why, how, where and when component.

5.2.1.2 Outer layer

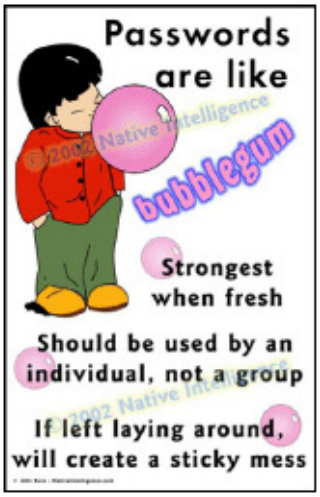
The outer layer of the model shows the influencing factors researched in this thesis. They include the Hofstede national cultural dimensions PDI, UAI, MAS and IDV, which give indications on how employees behave, learn and are motivated. Another group in the outer layer shows leadership by the IT organization, actively seeking alignment with the business and the business objectives. This also includes carefully evaluating IT projects, not solely based on ROI if essential security processes or business needs need to be addressed.
This is again emphasized in the bottom section of the outer layer. The business objectives influence the way IT security policies are created, monitored and enforced. Making clear in what way the policies and guidelines meet or enhance business goals, will promote acceptance and adherence of said policies. This will also make it easier for the final group in the outer layer: senior management. It cannot be stressed enough that they should set the right example to their staff and not put these employees in a position where they need to bend the rules or evade security measures in order to meet the requests or tasks given to them by management.

5.2.1.3 Middle layer

The middle layer gives the cycle for setting up policies, conducting training, monitor compliance and review of policies. It starts with defining a clear set of rules, policies and guidelines, which is carefully matched and discussed with the business stakeholders. Then these policies need to be made available to the target audience via various sources: Initial training (First Day at the Office training), refresher training, intranet, booklets, posters, flyers etc.

Also, if employees view security as just bothersome rules and procedures, they are more likely to ignore them. The guidelines and policies should therefore be made easily accessible, easily to comprehend and easy to remember. Sometimes such information is presented in cartoon style or as (video) sketches.

Figure 9: "Pinkey"



&

Figure 10: "Bubblegum"

Figures 7 and 8 : Examples of security Awareness posters (Native Intelligence 2002, NIST)

PwC itself has produced short feature films for its clients (e.g. the movie "the Crisis") to educate its customers on risks of inadequate Corporate Governance. It would be recommended to create such videos for their employees as well.

It is not effective to establishing rules and guidelines which are not enforced or monitored. Therefore checks need to be built in and reported to Business leadership. Also surveys to collect feedback on many factors surrounding the policies (awareness, compliance, availability, clarity etc.) helps in evaluating where the training and awareness programs should be adjusted.

5.2.1.4 The inner layer

The circle in the center of the framework depicts the 'core' of the model with the four key elements of effectively communication the policies to the end users:

- What: to provide insight and inform the users so they are able to recognize what the policies are and where to apply them. This creates the awareness on even simple things such as locking computers or doors.
- How: training on how to be compliant. These can be viewed as more or less 'technical' skills such as 'how do I create a secure password' and 'how do I back up my data'.
- Why: Sometimes guidelines do not make sense in the view of the employee. Explaining why is often forgotten or explained in terms end users do not understand or cannot relate to. The thesis has shown that policies which do not make sense are often ignored or bypassed.

- Where: the literature study and survey have shown that it is also very necessary that the policies are easily available. This may include communicating the highlights in multimedia form such as posters, banners in intranet sites, screensavers on PC's etc. Another option is the setup of a dedicated security awareness website. This website could consist of different sections with the different areas that need to be covered. As an example, the University of Tennessee implemented a very impressive security awareness website complete with videos, examples, and helpful external links (http://security.tennessee.edu/).

5.2.2 Future research

Topics for future research can be viewed in different perspectives. First, this thesis is limited to analyze the security awareness and compliance of the employees working in PricewaterhouseCoopers based mainly on the National cultural behavior and the alignment of business and IT. Future research could expand on companies and countries surveyed, as well as in-depth research on the topics just briefly mentioned in this thesis.

Also, as stated earlier in this thesis, IT security itself is a broad field and it contains many areas to explore and test. In this thesis technical (risk) factors including implementing security measures on network and hardware level have not been explored nor has employee's actual knowledge on IT security measures been compared with their self-perception. Yet another perspective is that in this thesis, analysis is made on employees working in the accounting and tax advisory sector. However the Financial services sector is a vast sector and it has many sub-sectors in it. Comparative research on those sub domains can also be conducted as a future research.

References

Abrams, D, Ando, K and Hinkle, S 1998, *Psychological Attachment to the Group: Cross Cultural Differences in Organizational Identification and Subjective Norms as Predictors of Workers' Turnover Intentions,* Personality and Social Psychology Bulletin, 24 (10), 1027-1040.

Al Awadi, M and Renaud, K 2007, *Success Factors in Information Security Implementation in Organisations* , IADIS International Conference e-Society 2007. Lisbon, Portugal. 3-6 July 2007

Alden, D, Steenkamp, J and Batra, R 1999, *Brand positioning through advertising in Asia, North America, and Europe: the role of global consumer culture*, Journal of Marketing, Vol. 63 No.1, pp.75-87.

Anthes, G 2007, *The right road to Innovation,* CIO magazine Canada, 1 september 2007, available from <http://www.itworldcanada.com/a/Leadership/c4376db0-7fec-484c-99ec-73bc382ea50d.html>

Baarda, D, Goede, de, M and Dijkum, van, C 2004, *Introduction to Statistics with SPSS: a guide to the processing, analysing and reporting of (research) data*, 2nd edition, Houten: Wolters-Noordhoff

Babbie, E 2003, *Survey Research Methods*, 3rd Edition, Belmont, California., Wadsworth Pub. Co. USA

Basel II 2004, *International Convergence of Capital Measurement and Capital Standards: a Revised Framework*, Available from: < http://www.bis.org/publ/bcbsca.htm>

Björck, J and Jiang, K 2006, *Information Security and National Culture*, MSc thesis, KTH Royal Institute of Technology, Stockholm, Sweden

Bloem, J and Doorn, van, M 2004, *Realisten aan het roer: Naar een prestatiegerichte governance van IT* (in Dutch), ViNT (Sogeti) kleine Uil , Groningen

Brace, I 2004, *Questionnaire Design : How to Plan, Structure and Write Survey Material for Effective Market Research*, London, Sterling, VA: Kogan page

Brooke, P 2004, *From the Top: Security Governance: Balancing Your Organization's Goals and Risk, Ensure well-directed security investments.*, American Financial Group publication, April 15, 2004, available from <http://nwc.securitypipeline.com>

Burgess, T 2001, *A General Introduction to the design of questionnaires for survey research*, University of Leeds, Available from <URL http://www.leeds.ac.uk/iss/documentation/top/top2.pdf>

Cabri, F 2007, *FaceTime Reports IM & P2P Malware is Packing a Bigger Punch*, FaceTime Press release, January 16, 2007, Available from <http://www.facetime.com/pr/pr070116.aspx>

CBS (Central Bureau for Statistics) 2004, *De Digitale Economie 2004* (in Dutch), Centraal Bureau voor de Statistiek, Voorburg / Heerlen, Netherlands

Chaula, J 2006, *A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance*, PhD thesis, Stockholm University, Stockholm

Choney, S 2008, *When 'cloud computing' turns dark and stormy*, August 6, MSNBC, available from < http:// www.msnbc.msn.com/id/26040510/>

CIO magazine 2004, *Shining the Light on Shadow Staff: Booz Allen Hamilton*, January edition, Available from <http://www2.cio.com/consultant/report2085.html>

Clear, T 2002, Design and Usability in Security Systems: Daily Life as a Context of Use, ACM SIGCSE Bulletin, Vol. 34, Issue 4

Clinger/Cohen Act 1996, The Information Technology Management Reform Act, Available from <http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html>

Coles, R and Hodgkinson, P 2008, *A Psychometric Study of Information Technology Risks in the Workplace*, University of Leeds paper, February issue of Risk Analysis (Vol 28, No 1, 2008).

Collins, J. 2001, Good to Great; Why some companies make the leap… and others don't, HarperCollins Publishers Inc, New York, NY

Cook, K and Levi, M 1990, The Limits of Rationality, University of Chicago Press

Creswell, J 2003, Research design. Qualitative, quantitative and mixed methods approaches, Thousand Oaks, CA: Sage.

Cumps, B, Martens, D, De Backer, M, Haesen, R,Viaene, S, Dedene, G,Baesens, B and Snoeck, M 2007, *Predicting Business/ICT Alignment with AntMiner+*, Katholieke Universiteit Leuven. KUL. Faculty of Business and Economics

Dahl, S 2004, Intercultural Research: The Current State of Knowledge. , Middlesex University Discussion Paper No. 26.

Davis, D, Monrose, F and Reiter, M 2004, On user Choice in Graphical Password Schemes, Proceedings of the 13th USENIX Security Symposium, San Diego

Deming, W 1986, Out of the Crisis, MIT Center for Advanced Engineering Study. ISBN 0-911379-01-0.

Desisto,R, Plummer, D, and Smith, D 2008, Tutorial for Understanding the Relationship Between Cloud Computing and SaaS, Gartner Research Paper, Available from <http://www.gartner.com/resources/156100/156152/tutorial_for_understanding_t_156152.pdf>

DeWitt, A and Kuljis, J 2006, Aligning Usability and Security: A Usability Study of Polaris, Symposium On Usable Privacy and Security (SOUPS) July 12-14, 2006, available from <http://cups.cs.cmu.edu/soups/2006/proceedings/p1-dewitt.pdf>

Dillman, D 2000, Mail and Internet Surveys: The Tailored Design Method (2nd edn), New York, Wiley.

Empirica 2000, Telework Data Report (Population Survey) – Ten Countries in Comparison. Project Report, Available from: < http://www.ecatt.com/ecatt/>

Fallows, D 2005, How Woman and Men Use the Internet, Pew Internet & American Life Project, report available from <http://www.pewinternet.org>

Gage, D April 2009, “Somber year for RSA Conference on cybersecurity”, San Francisco Chronicle

Hunter, R and Blosch, M, July 2003, “Managing the New IT Risks”, Gartner EXP research publication, Stamford, USA

Ghauri, P and Gronhaugh, K 2002, Research methods in Business Studies: A practical guide, 2nd edition, Harlow, Financial Times Prentice Hall

GLOBE 2003, The GLOBE Research Program, Available from <http://www.haskayne.ucalgary.ca/mg/GLOBE/public>

Gordon, L, Loeb, M and Lucyshyn, W 2005, Computer crime and Security Survey, Computer Security Institute/FBI San Francisco Bureau, available from < http://www.gocsi.com or www.fbi.gov>

Hamilton, M 2003, Online survey response rates and times: background and guidance for industry., Tercent, Inc. whitepaper, available from <http://www.supersurvey.com/papers/supersurvey_white_paper_response_rates.pdf>

Harris Interactive for Websense Inc. 2006, Web@Work Survey 2006, Report available from <http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/IT_Decision_Makers.pdf>

Heiser, J and Nicolett, M 2008, Assessing the Security Risks of Cloud Computing, Gartner Research Paper, available from <http:// www.gartner.com/DisplayDocument?id=685308>

Henderson, J and Venkatraman, N 1993, Strategic alignment: Leveraging information technology for transforming organizations, IBM Systems Journal, Vol. 32, no. 1.

Heuser, L, Alsdorf, C and Woods, D. 2007, International Research Forum 2006, April 2007, Evolved Technology Press, New York, NY

Hofstede, G 2001, Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations, Sage Publications, London, UK

Hofstede, G 1980, Culture's consequences : international differences in work-related values., Beverly Hills, Sage Publications.

Hofstede, G and Hofstede G J 2005, Cultures and Organizations: Software for the Mind, 2nd edition, McGraw-Hill, New York, NY

Holton, G 2004, Defining Risk, Financial Analysts Journal, 60 (6), 19–25.

Höne, K and Eloff, J 2002, What makes an Effective Information Security Policy?, Network Security, Volume 2002, Issue 6, 1 June 2002, available from < http://www.sciencedirect.com >

Hotopp, U 2002, Teleworking in the UK, Labour Market trends, vol.110, no. 6. UK Department of Trade and Industry

Hung T, Ching, R and Ja-Shen, C 2007, 'Performance Effects of IT Capability and Customer Service: The Moderating Role of Service Process Innovation', *International Conference on Wireless Communications, Networking and Mobile Computing,* September 2007. WiCom 2007.

Iarossi, G 2006, *Power of Survey Design*, Publisher: The World Bank

IBM 2008, Transforming the IT infrastructure to generate business advantage: the CIO agenda to enable innovation that matters., IBM Whitepaper, available from <http://www-935.ibm.com/services/us/cio/outsourcing/optit_wp_gts_transforming.pdf>

IronPort 2008, *Cisco 2008 annual security report*, Available from <http://www.ironport.com/report/_media/Final_Cisco2008_Annual_Security_Report.pdf>

Jahnke, A 2004, 'Sound Off - Why Is Business-IT Alignment So Difficult?', *CIO magazine*, available from <http://www.cio.com/article/32322/Sound_Off_Why_Is_Business_IT_Alignment_So_Difficult_?page=1>

Jaquith, A 2009, 'Data Security: Whose Job Is It Really? Forrester believes CISOs must revisit the need to centrally control data security'., *Forrester Research via CSO Magazine*, 30 March 2009, available from <http://www.csoonline.com/article/487261/Data_Security_Whose_Job_Is_It_Really_?page=1>

Kahraman, E 2005, *Evaluating IT security performance with quantifiable metrics*, MSc thesis, Stockholm University, Sweden

Kaplan, D 2008, The next generation, SC Magazine US, April 2008 edition, available from < http://www.scmagazineus.com/The-next-generation/article/108410/>

Krom, E 2006, *Briefing Veiligheidsbewustzijn*, Defensie Telematica Organisatie, available from <http://www.isaca.nl/index.php?download=Briefing_Veiligheidsbewustzijn.swf>

Lenth, R 2001, *Some Practical Guidelines for Effective Sample-Size Determination*, University of Iowa, Available from <URL http://www.stat.uiowa.edu/techrep/tr303.pdf>

Llewellyn, D and Sanchez, X 2007, 'Individual differences and risk taking in rock climbing' , *Psychology of Sport and Exercise* doi:10.1016/j.psychsport.2007.07.003

Luftman, J 1999, 'Assessing Business Alignment Maturity', *Communications of AIS*, Volume 4, Article 14 1

Lutchen, M 2004, *Managing IT as a business : a survival guide for CEOs.*, Hoboken, N.J., J. Wiley.

Mathieson, K 1991, 'Predicting user intentions:comparing the technology acceptance model with the theory of planned behaviour', *Information System Research*, Vol. 3 No. 2

Mathisen, J 2004, *Measuring Information Security Awareness*, MSc thesis, Gjøvik University College, Norway

Mogull, R 2007, *Gmail, iPhones and Wiis: Preparing Enterprise Security for the Consumerization of IT*, Gartner research paper, available from <http://www.gartner.com/resources/146800/146879/gmail_iphones_and_wiis_prepa_146879.pdf>

Mooij, de, M 2000, 'The future is predictable for international marketers: Converging incomes lead to diverging consumer behavior', *International Marketing Review*, 17 (2)

Moreau, D 2007, Aligning IT Security and Operations: Four Ways to Close the Gap, ConfigureSoft whitepaper, available from < http://www.configuresoft.com/downloads.aspx>

Morwood, G 1998, Business continuity: awareness and training programmes, Information Management & Computer Security, Vol. 6 No. 1

Motjolopane, I and Brown, I 2004, 'Strategic business-IT alignment, and factors of influence: a case study in a public tertiary education institution', *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries.*

Motorola University 2006, *What is Six Sigma?*, available from <http://www.motorola.com/content/0,,3088,00.html>

Nath R, and Sadhu, K 1998, *Comparative Analysis. Conclusions, and Future Directions, in Comparative Management -A Regional View*, Cambridge MA: Ballinger Publishing Company

Nelsestuen, R 2007, *Financial Services Strategies and IT Investments*, Towergroup whitepaper August 1, 2007

NewDiligence 2006, *Employee Use of Greynets: 2nd Annual Survey of Trends, Attitudes & Impact*, FaceTime Report, available from <http://www.facetime.com/pdf/SecondAnnualGreynetsSurvey_Nov06.pdf>

Nielsen, J 2000, *Security & human factors*, Available from <http://www.useit.com/alertbox/20001126.html>

NIST Handbook, The 1995, *An Introduction to Computer Security*, NIST special publications 10-95

Odubiyi, J. 2006, 'Develop your organisation's power Distance Index to attract and retain employees', *EzineArticles.com*, available from <http://ezinearticles.com/?Develop-Your-Organizations-Power-Distance-Index-to-Attract-and-Retain-Employees&id=389405>

Ostowan, B 2006, *Towards a Framework to Measure User Compliance with Computer Security Practices*, MSC thesis, Department of Computer and Systems Sciences, Stockholm University, Sweden

Parker, D 1998, *Fighting Computer Crime; A New Framework for Protecting Information*, Wiley Computer Publishing, New York, NY.

Perry, W 1985, *Management Strategies for Computer Security*, Butterworth Publisher, Boston, MA.

Ponemon Institute LLC 2006, *National Survey On Managing The Insider Threat, Research Report,* September 25, Available from < http://www.arcsight.com>

Ponemon Institute LLC 2007, *Data Security Policies Are Not Enforced, US Survey of IT Practitioners*, Research Report December 4, Available from <http://www.redcannon.com/documents/ RedCannonPonemonReport.pdf>

PricewaterhouseCoopers 2007, 'The Global State of Information Security Survey', Publication available from *CIO magazine, CSO magazine* and PricewaterhouseCoopers

Prince, B 2007, Risky Employee Behavior on Web Threatens Corporate Networks, eweek.com January, available from <http://www.eweek.com/c/a/Security/Risky-Employee-Behavior-on-Web-Threatens-Corporate-Networks/>

Raden, N 2005a, Shedding Light on Shadow IT: Is Excel Running Your Business?, Available from: <http://www.hiredbrains.com/proclarity.pdf>

Raden, N 2005b, 'Shadow IT: A Lesson for BI', October edition, *BI Review Magazine*, Data Management Review and SourceMedia, Inc.

Reichwald, R, Möslein, K, Sachenbacher, H, Englberger, H and Oldenburg, S 1998, Telekooperation.Verteilte Arbeits- und Organisationsformen. , Berlin et al.: Springer.

Richards, K January 2008, The Future of Information Security: 2008 and Beyond, Available from: <http://www.cio.com/article/168352/The_Future_of_Information_ Security_2008_and_Beyond>

Robbins, S 2005, *Essentials of Organisational Behaviour* (8th edition), New York: Prentice Hall

RSA 2007, *The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk*, Available from: < http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf>

Rundmo, T, Oltedal, S, Moen, B and Klempe, H 2004, *Explaining risk perception. An evaluation of cultural theory*, Norwegian University of Science and Technology, Trondheim

SANS Institute 2007, *SANS Top-20 2007 Security Risks*, Available from <http://www.sans.org/top20/2007/top20.pdf>

Saunders, M, Lewis, P and Thornhill, A 2003, *Research Methods for Business Students*, Prentice Hall, Financial Times

Schaffner, M 2007, IT Needs To Become More Like "Shadow IT", Available from <http://www.typepad.com>

Schweber, A 2007, Employees take unnecessary risks with laptops, June 11, Available from <http://blog.absolut.com>

Sherman, R 2004, Shedding light on Shadow Systems, DM Direct, Athena IT Solutions

SIBIS (Statistical Indicators
Benchmarking the Information Society) 2002, Measuring the Information Society in the EU, the EU Accession Countries, Switzerland and the US, Available from <http://www.sibis-eu.org/files/Sibis_Pocketbook_updt.pdf>

Silvius, G 2008, 'The Impact of National Cultures on Business & IT Alignment', *Communications of the IIMA (CIIMA)*, ISSN: 1543-5970, Volume 8 Issue 2, International Information Management Association Inc., San Bernadino CA

Siponen, M 2000, *A conceptual foundation for organizational information security awareness*, Information Management &Computer Security 8/1 [2000] 31±41, MCB University Press

Slay, J 2003, 'IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings', *The Emerald Research Register* 20(3): 98-104.

Sørnes,J, Stephens, K, Sætre, A, and Browning, L 2004, 'The Reflexivity between ICTs and Business Culture: Applying Hofstede's Theory to Compare Norway and the United States', *Informing Science Journal*, Volume 7

Soutar, G, Grainger,R and Hedges, P 1999, 'Australian and Japanese Value Stereotypes: A Two Country Study', *Journal of International Business Studies*, 30 (1), 203-217.

SoX (Sarbanes-Oxley) 2002, Public Company Accounting Reform and Investor Protection Act, Available from: < http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107>

Spafford, G 2004, The Dangers that Lurk Behind Shadow IT, February 4, Available from <http://www.earthweb.com>

Spruit, M 1998, 'Competing against human failing', *15th IFIP World Computer Congress, `The Global Information Society on the way to the next millennium'", Proceedings of the SEC'98*, TC11, Vienna.

Stanford Encyclopedia of Philosophy 2008, *Risk*, Available from < http://plato.stanford.edu/entries/risk/>

StatSoft Inc 2008, Elementary Concepts in Statistics, Available from <http://www.statsoft.com/textbook/stathome.html>

Stone, B 2007, 'Firms fret as office e-mail jumps security walls', *International Herrald Tribune*, January 11, available from <http://www.iht.com/articles/2007/01/11/technology/web.0111email.php?page=1>

Straub, D and Welke, R 1998, 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, Vol. 22 No. 4

Symantec 2009, *2009 Managed Security in the Enterprise Report*, available from <http://www.symantec.com/content/en/us/about/media/managed_security_ent_US_12Mar09.pdf>

Trompenaars, F and Hampden-Turner, C 1997, *Riding the waves of culture* (2nd edition), McGraw-Hill, New York, United States

Veiga, J, Floyd, S, and Dechant, K 2001, 'Towards modelling the effects of national culture on IT implementation and acceptance' , *Journal of Information Technology*, 16 (3)3, 145-158.

Verizon Business RISK 2009, *2009 Data Breach Investigations Report*, Available from <http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf>

Wang, X, June 2009, Application Security Technology Adoption Trends in 2009, Forrester Research paper

Watson, C 2000, Formulating and clarifying the research topic, Powerpoint presentation, available from <www.colinwatsonleeds.co.uk>

Webwereld 2008, *Webwereld Security Onderzoek* , IDG Nederland in coperation with Nuzakelijl.nl and Security.nl. Available from <http://www.webwereld.nl>

Weirich, D and Sasse, M 2001, *Pretty good persuasion: A first step towards effective password security for the real world.*, New Security Paradigms Workshop. Cloudcroft, NM, USA: ACM Press.

Whitty, M 2006, *Report Surf Control: Trust and Risk in the Workplace*, Queen's University, Belfast

Wikipedia 2008, Risk, Available from < http://en.wikipedia.org/wiki/Risk>

Wills, L 2002, Security Policies: Where to Begin., Available from <http://www.sans.org/reading_room/whitepapers/policyissues/security_policies_where_to_begin_919>

Wimmer, R 2001, Sample Size Calculator, Available from <http://www.wimmerdominick.com>

Witty, R and Wagner, R 2005, *Awareness Training Is Necessary to Support Your Information Security Program*, Gartner Research, 31 January 2005, Available from < http://www.gartner.com/resources/125800/125896/awareness_training_is_necess_125896.pdf>

Witty, R, Girard, J, Graff, J, Hallawell, A, Hildreth, B, MacDonald, N, Malik, W, Pescatore,J, Reyanolds, M, Russell, K, Wheatman, V, Dubiel, J and Weintraub, A 2001, *The Price of Information Security*, Gartner Strategic Analysis Report, Available from <http://www.gartner.com/DisplayDocument?ref=g_search&id=331017>

Wold, G 2004, *Key factors in making Information Security Policies Effective*, MSc thesis, Gjøvik University College, Norway

Yin, R 1994, *Case study research: Design and Methods*, Sage Publications,Thousand Oaks, California, USA

A Appendix : Acronyms

Acronym

BASEL II - Basel Committee on Banking Supervision (BCBS) accord on banking laws and regulations

BITA - Business vs. IT Alignment

BPO - Business Process Outsourcing

COBIT - Control Objectives for IT

FISMA - Federal Information Security Management Act of 2002

GAAP - General Accepted Accounting Principles

HIPAA - Health Insurance Portability and Accountability Act

ICT - Information and Communication Technology

IDV – Individuality vs. Collectivism index (Hofstede dimension)

IFRS - International Financial Reporting Standards

IS - Information Systems

ISO - International Standard Organization

IT - Information Technology

ITIL – Information Technology Infrastructure Library

MAS – Masculinity vs. Feminimity (Hofstede dimension)

PDI - Power Distance Index (Hofstede dimension)

PIN - Personal Identification Number

PwC - PricewaterhouseCoopers

ROE - Return On Equity

ROI – Return On Investment

RSS - Really Simple Syndication (Web feed format used to publish frequently updated works)

SoX - Sarbanes-Oxley Act

TCO – Total Cost of Ownership

TQM - Total Quality Management

UAI - Uncertainty Avoidance Index (Hofstede dimension)

VOIP – Voice-Over-Internet Protocol

B Appendix: Screenshots of the online Survey

PRICEWATERHOUSECOOPERS

Nederland

Survey on PwC IT Security

Dear participant,

Thank you for taking the time to complete this survey. This survey is part of a Master's thesis by PwC employee Taco Dols. Your feedback is important to PwC in order to get a good view of behavior and attitude towards IT data security.
This survey consists of 22 questions and should only take about 5 minutes of your time. Your answers will be completely anonymous.

Instructions:
- Please answer honestly; the results will be collected and analyzed anonymously.
- Most answers will rate on a scale from 1 to 7, where value 4 can be considered a 'neutral' answer.

For example:
Familiar 1 2 3 4 5 6 7 Unfamiliar
these values would read as:

1. Familiar 2. Reasonably familiar 3. Somewhat familiar 4. Neither familiar nor unfamiliar
5. Somewhat unfamiliar 6. Reasonably unfamiliar 7.Unfamiliar

If you have any questions on this survey, please contact me at taco.dols@nl.pwc.com or call +31(0)30219 4471

Please return this survey by December 15, 2008
Click on 'next' to start the survey

Survey on PwC IT Security

0%

General questions

1. **Gender:**

- Male
- Female

2. **Country :**

- Netherlands
- Switzerland
- Belgium

3. **Age group**

- 18-23
- 24-29
- 30-35
- 36-41
- >41

4. **PwC laptop**

- Yes
- No

5. **I have been: ... year(s) with the company**

- <1
- 1-3
- 4-6
- >6

Next

Survey on PwC IT Security

23%

Specific questions

6. **Please rate your familiarity with the IT security policies for your organization.**
Very Unfamiliar (1) 2 3 4 5 6 Very Familiar (7)

7. **Do you practice these policies?**
Never (1) 2 3 4 5 6 Always (7)

8. **Compared previous years, I find that IT security policies have become more strict:**
Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

9. **I sometimes feel that IT security prevents me to work efficiently.**
Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

10. **My IT department provides me with the technology I need to perform my tasks.**
Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

11. **I sometimes need to bend the rules in order to get work done.**
Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

12. **I sometimes feel that less budget is available for IT (projects) than before.**
Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

13. **If the IT security rules make no sense to me, I sometimes ignore them.**
Never (1) 2 3 4 5 6 Always (7)

14. **If my Partner or manager asks me to bend the IT security rules, I will do so.**
Never (1) 2 3 4 5 6 Always (7)

Back Next

* connectedthinking™

Survey on PwC IT Security

64%

15. **If I notice a colleague not following the IT security guidelines, I will address this with him/her.**

Never (1) 2 3 4 5 6 Always (7)

16. **I have stored or transported documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick (excluding PwC-issued encrypted devices)**

Never (1) 2 3 4 5 6 Always (7)

17. **I have used Google Docs or other on-line collaboration software to store or share work with colleagues.**

Never (1) 2 3 4 5 6 Always (7)

18. **I should be able to install any applications I need on my work computer.**

Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

19. **I sometimes need to share my passwords with colleagues (excluding identified GTS personel) so they can assist me with my tasks.**

Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

20. **I sometimes send documents (that could be considered to contain sensitive/confidential information) to a home/private email account so I can work from home**

Never (1) 2 3 4 5 6 Always (7)

21. **I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)**

Strongly Disagree (1) 2 3 4 5 6 Strongly Agree (7)

22. **I sometimes download non-PwC software for convenience, speed and productivity improvements. I don't review this with IT because: (You may choose more than one option)**

- [ ] I never download non-PwC software
- [ ] I always review this with IT
- [ ] They simply say "No"
- [ ] They don't respond in any reasonable timeframe
- [ ] I was unaware of this requirement/policy
- [ ] Other

Back Submit

* connectedthinking™

C Appendix: Matrix Hofstede and Luftman

The potential effect of Hofstede's dimensions of culture on Luftman's variables of BIA maturity.

A. J. Gilbert Silvius

Business & IT Alignment maturity criteria	Dimensions of national culture: Power Distance Index	Individualism vs. Collectivism	Masculinety vs. Femininity	Uncertainty Avoidance Index	Long Term Orientation
Communications maturity	Based on the findings of Semes et al. (2004) it can be concluded that a low PDI score indicates close working relationships between hierarchical levels and assertive behavior by subordinates. This can be expected to result in a higher Communications maturity because of more intensive and less formalized communication.	In individualistic societies, the task will normally prevail over personal relationships (Hall, 1976; Walls, 1993). A high IND score could therefore indicate a much task oriented communication that will result in a high maturity score, but lacks personal warmth that may be important in case of problems.	Hofstede's (2000) findings support the claim that one-way communication will be more prominent in masculine countries, while two-way communication prevails in feminine countries. It should therefore be expected that a high MAS culture scores relatively lower on Communications maturity.	A high UAI culture can be expected to score relatively lower on Communications maturity because of its tendency towards certainty which does not stimulate open and informal communication	A high LTO culture can be expected to score high on Communications maturity because of its orientation on developing relationships (Hall, 1976; Walls, 1993).
	PDI ↑ → Communications maturity ↓	IND ↑ → Communications maturity ↑	MAS ↑ → Communications maturity ↓	UAI ↑ → Communications maturity ↓	LTO ↑ → Communications maturity ↑
Value measurement maturity	Following the motivation stated under ' Communications', a lower PDI score can be expected to result in less need for creating transparency, procedures and reports that enhance Value measurement, therefore resulting in a lower maturity on this factor.	Individualistic cultures will normally show a high appreciation of value and performance. It should therefore be expected that these societies score relatively high on Value measurement maturity.	A high "masculine" culture values value assertiveness and focus on material success, while "feminine" countries value modesty, tenderness, and quality of life (Hofstede, 1991). A high MAS score can therefore be expected to score high on Value measurement maturity.	Following the argumentation of Semes et al. (2004), a high UAI culture can be expected to avoid uncertainty about value, resulting in a higher score on Value measurement maturity.	A short term orientation will result in more focus on short term performance, therefore a low LTO culture can be expected to score high on Value measurement maturity.
	PDI ↑ → Value measurement maturity ↑	IND ↑ → Value measurement maturity ↑	MAS ↑ → Value measurement maturity ↑	UAI ↑ → Value measurement maturity ↑	LTO ↑ → Value measurement maturity ↓
Governance maturity	Again based on the findings of Semes et al. (2004) that concluded that a low PDI score indicates close working relationships between hierarchical levels and assertive behavior by subordinates, it should be expected that in cultures with a low PDI there is less need for formalised governance processes, resulting in a relatively lower Governance maturity.	In Hofstede's study, the United States scores highest (most individualistic) of all nations on this dimension. The United States also developed strongly in governance as a reaction to fraudulous actions of individuals. It should therefore be expected that High IND cultures also score high on Governance maturity.	Because of it's orientation on material success, performance and measurement stated above, a high MAS culture can be expected to score high on Governance maturity.	Following the argumentation of Semes et al. (2004), a high UAI culture can be expected to score high on Governance maturity because of its tendency to require certainty	A high LTO culture can be expected to pair with a high Governance maturity because of the guidance that is provided with governance. On the other hand, a short term orientation will result in more focus on short term performance which also requires a high Governance maturity. Therefore no straightforward indication can be found for the relationship between LTO and Governance maturity.
	PDI ↑ → Governance maturity ↑	IND ↑ → Governance maturity ↑	MAS ↑ → Governance maturity ↑	UAI ↑ → Governance maturity ↑	LTO ↑ → Governance maturity ?
Partnership maturity	Following the motivation given under ' Communications', a lower PDI score can be expected to result in a higher Partnership maturity because of more intensive, less formalized and richer communication	In individualistic cultures personal task prevail collective tasks (Veiga, et al., 2001). A high IND culture should therefore be expected to result in a lower Partnership maturity. On the other hand, Van Birgelen et al. (2002) found that in an individualistic culture people therefore seem to be more innovative and trusting in exchange relationships with external parties, which could be reflected in a higher Patnership maturity.	In more feminine cultures individuals don't like to stick out, be unique or conspicuous, unlike the more assertive and career-seeking individuals found in masculine cultures (Semes et al., 2004). This ' live and let live' approach could enhance partnerships between individuals, departments or organizations. A less MAS culture should therefore be expected to result in a higher Partnership maturity.	Given the fact that 'partnership' in general is based more on trust than on certainty, it should be expected that a high UAI culture scores relatively lower on Partnership maturity.	A high LTO culture can be expected to score high on Partnership maturity because of its appreciation for the long term collective goals and interests (Veiga, et al., 2001).
	PDI ↑ → Partnership maturity ↓	IND ↑ → Partnership maturity ?	MAS ↑ → Partnership maturity ↓	UAI ↑ → Partnership maturity ↓	LTO ↑ → Partnership maturity ↑
Scope & Architecture maturity	Given the chcracteristics of this factor, no indication was found to indicate how the PDI relates to the Scope & Architecture maturity.	Given the more collective nature of architecture it can be expected that a high IND culture should reflect in a relatively low score on Architecture maturity. On the other hand, the findings of Van Birgelen et al. (2002) mentioned above provide indication that a more individualistic culture reflects in a higher Architecture maturity because of it's openness to exchange relationships with external parties.	Because of it's tendency to appreciate individual performance and success, a more masculine culture should be expected to score lower in Scope & Architecture maturity, which has a non-individual character.	A high UAI culture can be expected to score high on Architecture maturity because of its tendency to create certainty and security, amd the slower rate of adoption of new technologies found by Png et al. (2001)	A high LTO culture can be expected to score high on Architecture maturity because of the long term character of these assets.
	PDI ↑ → Scope & Architecture maturity ?	IND ↑ → Scope & Architecture maturity ?	MAS ↑ → Scope & Architecture maturity ↓	UAI ↑ → Scope & Architecture maturity ↑	LTO ↑ → Scope & Architecture maturity ↑
Skills maturity	The high level of assertiveness that is expected to result from a low PDI score is stimulating entrepreneurship and initiative in lower organisational levels and can therefore be expected to result in a high Skills maturity.	A high IND culture can be expected to result in a high Skills maturity because of its appreciation of individual skill development	Because of it's orientation on work and material success (Hofstede, 1991), a high MAS culture should be expected to result in a higher Skills maturity. On the other hand, a more " feminine" culture can be expected to stimulate a more diverse skills development that in fact could also result in a higher Skills maturity score.	Based on the findings of Livonen et al. (1998) it can be expected that a high UAI decreases the pace of individual learning and will result in a lower Skills maturity	A high LTO culture can be expected to score high on Skills maturity because of the long term character of skills development.
	PDI ↑ → Skills maturity ↓	IND ↑ → Skills maturity ↑	MAS ↑ → Skills maturity ?	UAI ↑ → Skills maturity ↓	LTO ↑ → Skills maturity ↑

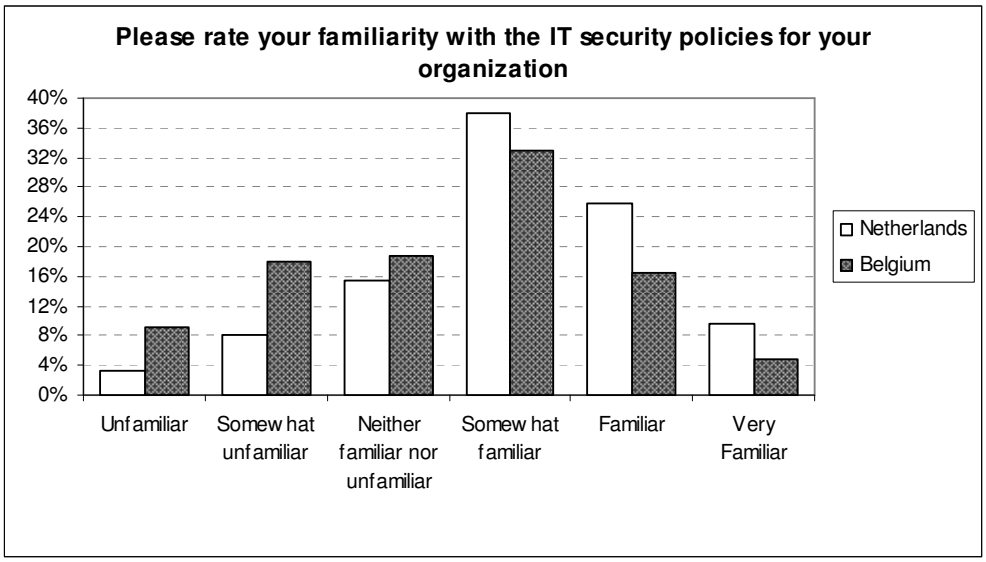
D Appendix: Detailed analysis of survey results

[A] Gender <> Is familiar with policies

There is no significant difference (p=.220) in answers between males and females. In all, 69,1% of males indicate they are somewhat to very familiar with the security policies where only 57,3% of women do.

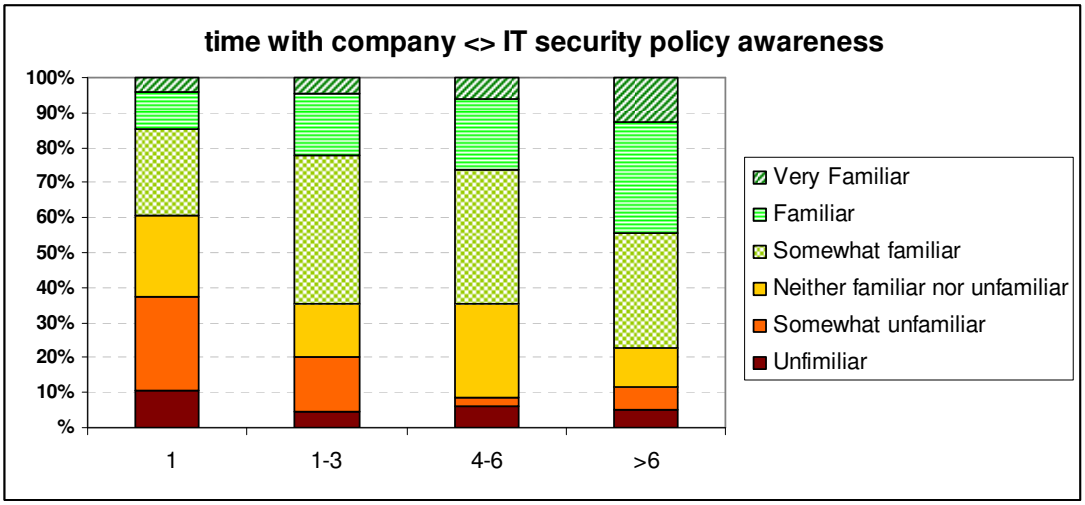
[B] Nationality <> Is familiar with policies

Of the Dutch respondents, 73,4% state that they are Somewhat to Very Familiar with the existing security policies. For the Belgians, this is significantly (p=.019) lower: 54,1%! The chart shows the distribution of the given answers:



[C] Time with company <> Familiarity with the IT security Policy

A very strong relationship (p=.003) was found between familiarity with the policies and the time the respondents are with the company. It appears that of the many things a new employee needs to learn in the first years with the company, IT security policy awareness is no priority.



[D] Gender <> Do you practice these policies?

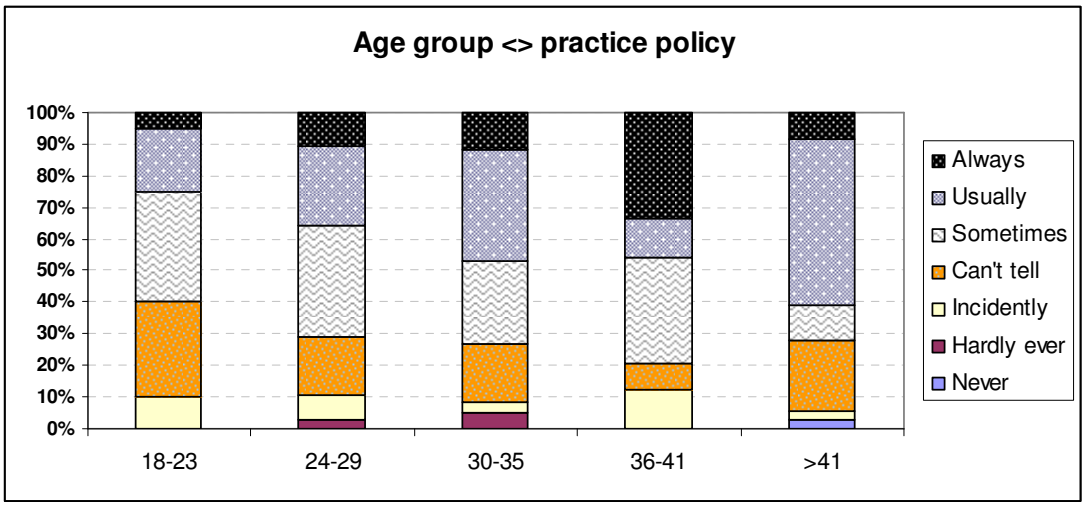
No significant difference (p=.694) is observed between the opinion between men and woman. Both groups sometimes, usually or always practice the policies (Males 71,3%, Females 71,8%)

[E] Country <> Do you practice these policies?

As the survey shows there is a difference between familiarity with policy between The Netherlands and Belgium. And since there is some (albeit not fully statistical significant) homogeneity between awareness and practicing policy, differences are expected here as well. Of the Dutch respondents, 73,4% Sometimes to Always practice the policies. For the Belgians, this is 69,7%. However when correlation is measured over all possible answers (p=.691) or between the Sometimes to Always answers (p=.441) one finds no significant difference between Belgians and Dutch respondents.

[F] Age group <> Do you practice these policies?

A significant relationship (p=.011) was found between age and adherence to policies: The older, the more compliant with the policies one seems to become.



When looking at the composition of the age group, one sees that over 75% of respondents fall in the under-36 category where less than half usually or always comply with the security policies.

Age group

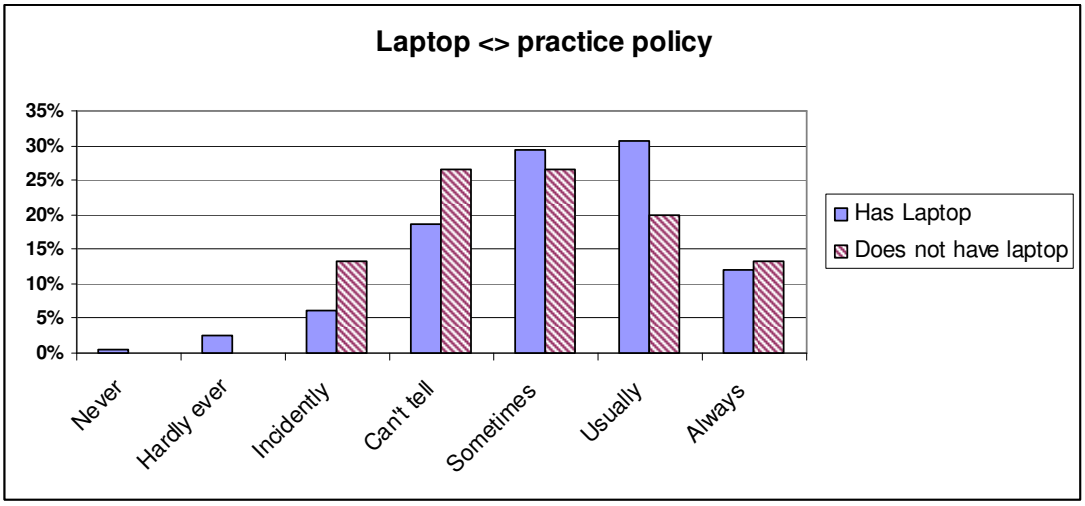
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-23	24	8.8	8.8	8.8
	24-29	117	42.9	42.9	51.6
	30-35	65	23.8	23.8	75.5
	36-41	25	9.2	9.2	84.6
	>41	42	15.4	15.4	100.0
	Total	273	100.0	100.0	

[G] laptop owner <> compliance with IT security policies

93% of the interviewed employees are in the possession of a company laptop. This makes it difficult to compare distinct behavior between owners and non-owners of a company laptop. Therefore there is no significant (p=.849) difference in adherence to IT security policies between laptop users and others.

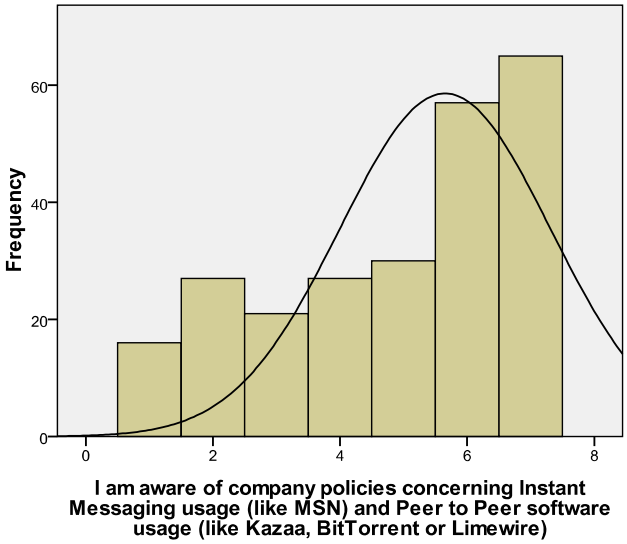
PwC laptop

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	254	93.0	93.0	93.0
	No	19	7.0	7.0	100.0
	Total	273	100.0	100.0	



[H] Country <> Is aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)

No significant difference between the responses of both countries (p=.815) was found but when looking at the percentages, it is noticeable that in both countries, over ¼ of respondents are unaware of such policies although these types of software have been found to pose great risk of (accidentally) exposing sensitive data.



[I] Age groups <> Is aware of company policies concerning Instant Messaging usage and Peer to Peer software usage

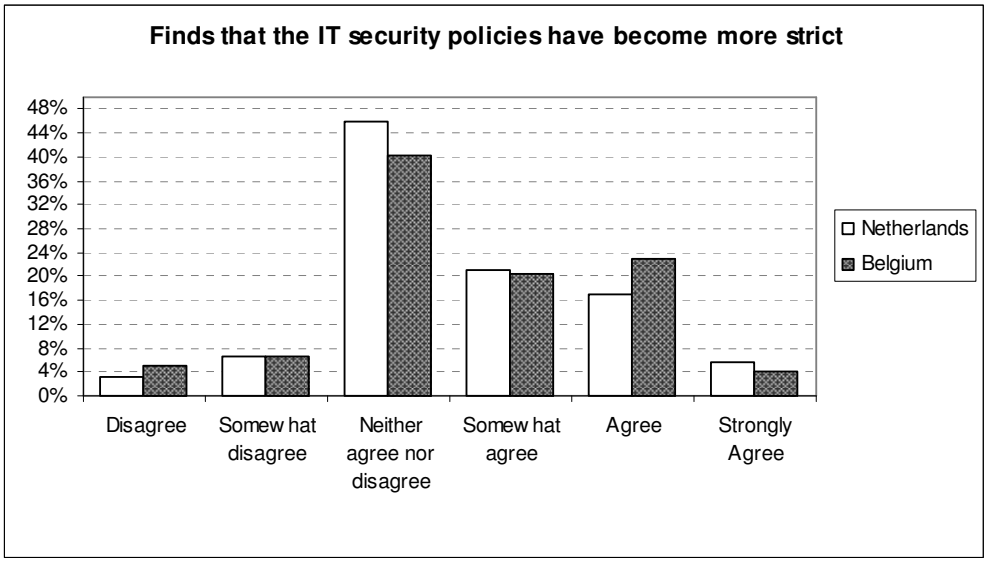
There is some but no significant relation (p=.070) between awareness of policies regarding usage of Kazaa etc. between the age groups. When looking at the statement itself, it was found that most respondents are aware of such policies.

[J] Has laptop <> Is aware of company policies concerning Instant Messaging usage and Peer to Peer software usage

There is no significant difference between laptop and non-laptop users in awareness of these policies (p=.520)

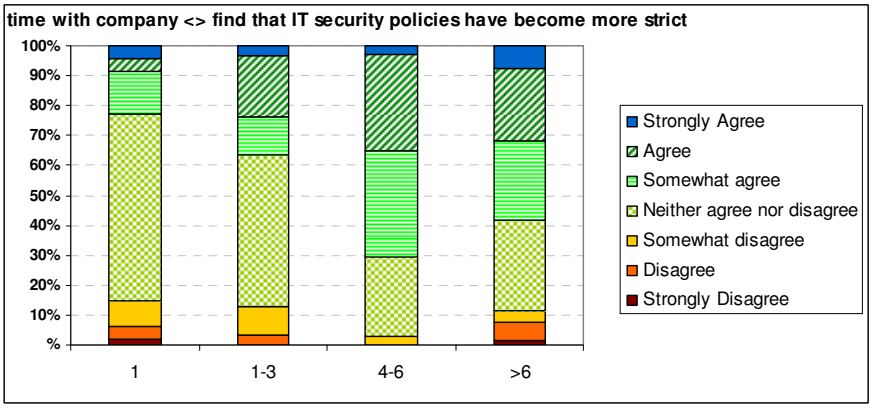
[K] Nationality <>, finds that, compared previous years, IT security policies have become stricter

There is no difference between Dutch and Belgians (p=.886) towards this statement. However more Belgians (47,5%) than Dutch (43,5%) somewhat to strongly agree that policies have become more strict.



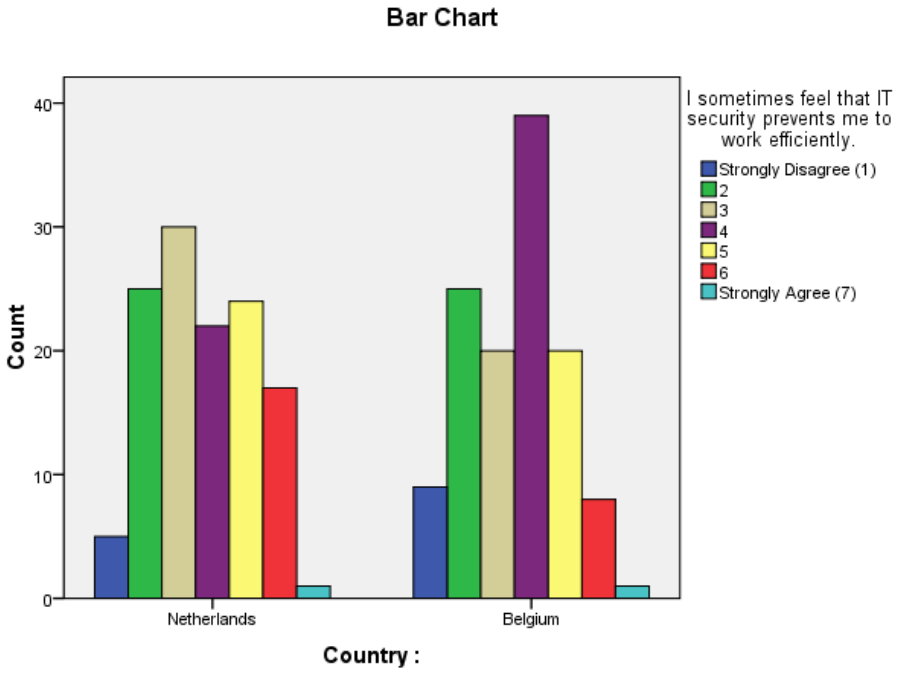
[L] Time with company <> finds that, compared previous years, IT security policies have become stricter

Obviously, the longer one is with the company, the better one can judge if policies have become stricter. It is therefore no surprise that there is a strong correlation (p=.005) between the two variables. Notably in the group '4-6 years with the company', 7 out of 10 somewhat to strongly agree with the statement that policies have become more strict.



[M] Nationality <> finds that security prevents them from working efficiently

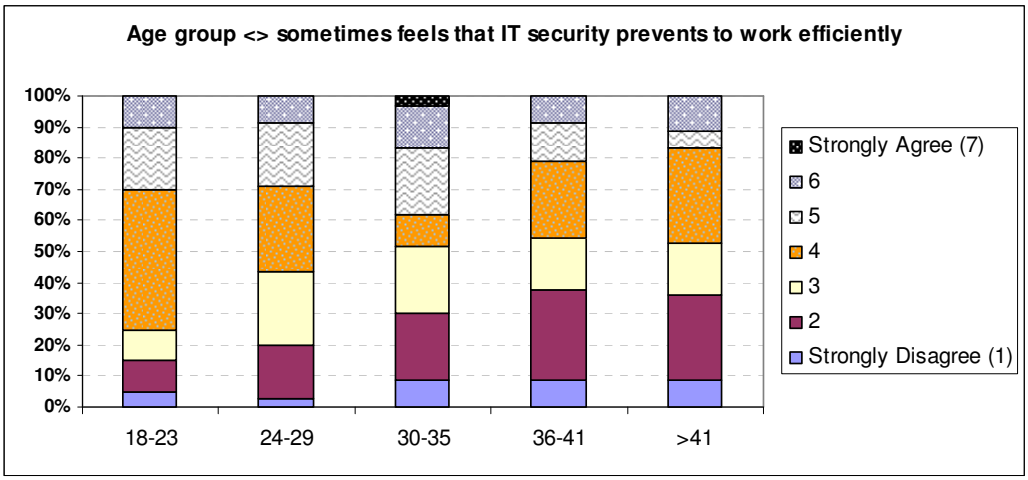
There is some, but no significant correlation between nationality and the feeling that IT security prevents efficient working (p=.075). Overall it can be stated that more people disagree with the statement than agree with it.



[N] Age group <>Finds that IT security prevents them from working efficiently

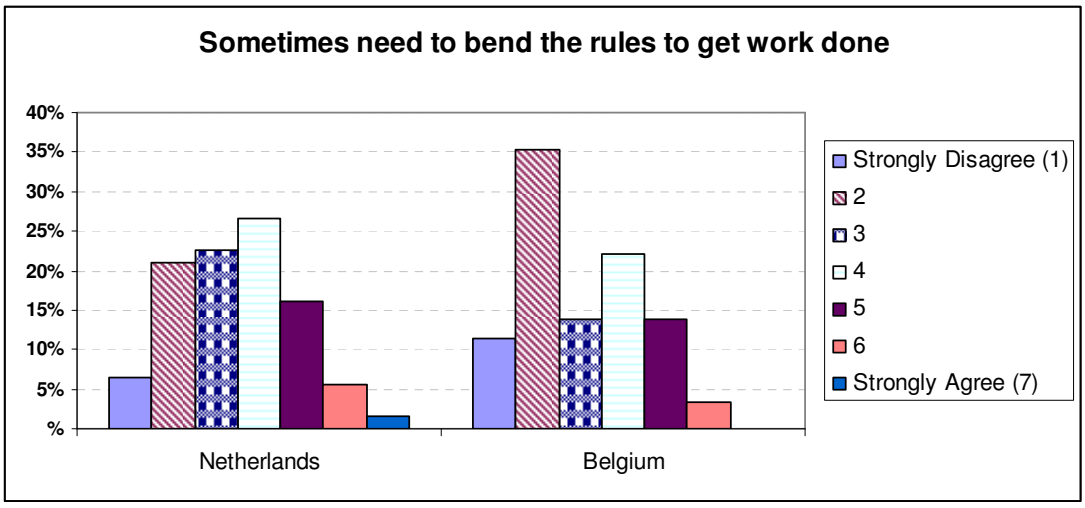
No strong significant (p=.196) relationship is seen between the age groups versus this statement.

Perhaps surprisingly, the older one gets, the more one tends to disagree with the statement. It was expected that younger employees, with their familiarity with PC's and the Internet, to agree most with this statement, but it's the age group between 30-35 feels strongest that IT security prevents efficient working.



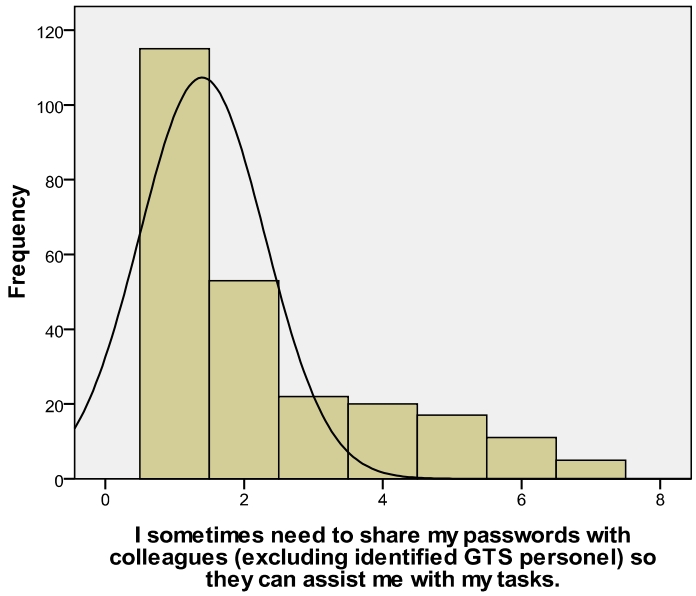
[O] Nationality <> needs to bend the rules sometimes to get work done

An almost significant difference (p=.059) was found between Dutch and Belgian respondents. 60% of Belgians somewhat to strongly disagree with the statement against 50% of Dutch.



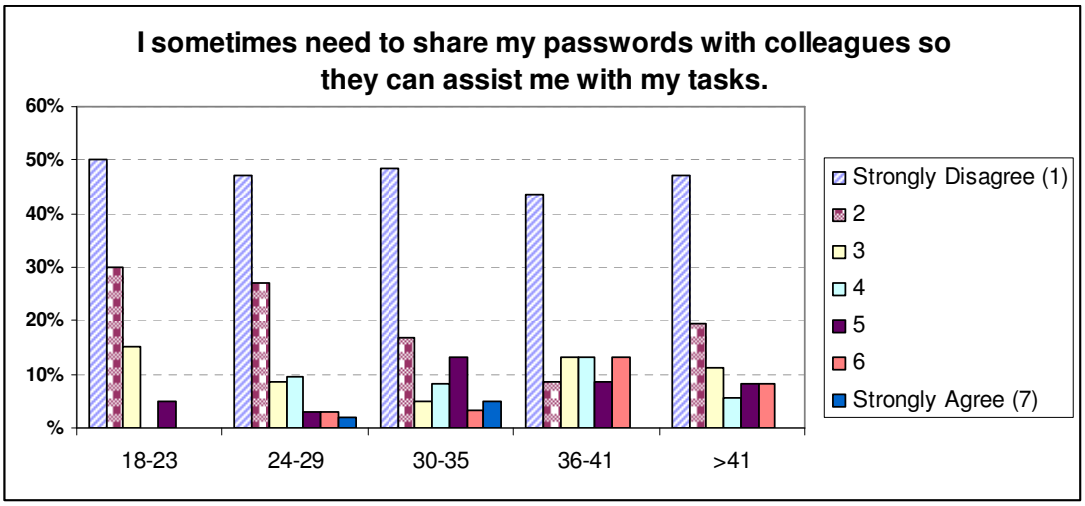
[P] Nationality <> sometimes needs to share passwords with colleagues so they can assist with tasks.

No significant difference was found between Belgians and Dutch (p=.286). When looking at the statement itself, it quite clearly shows that sharing passwords is no necessity for the respondents: 86% do not agree with this statement, about half of which strongly disagree with the statement.



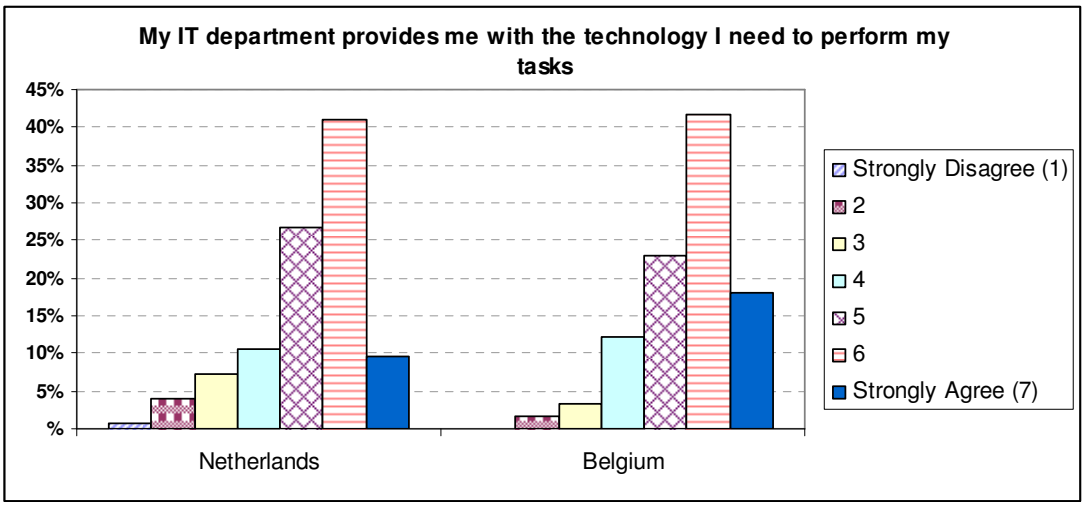
[Q] Age group <> sometimes needs to share passwords with colleagues so they can assist with tasks

There is no statistically significant (p=.310) difference between the age groups. Most do not need to share their passwords; respondents above 30 are more likely to agree with the statement.



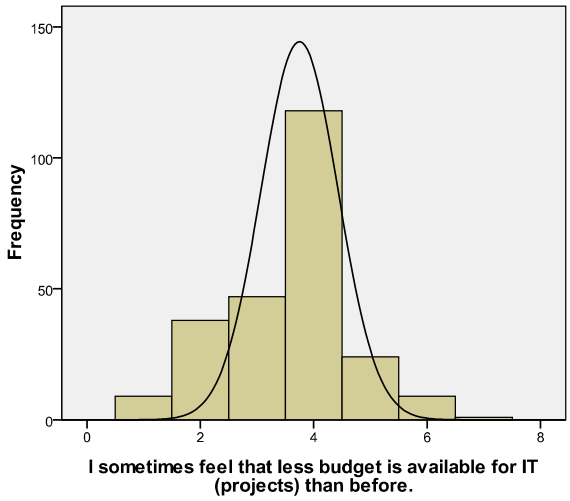
[R] Nationality <> IT department provides the technology needed to perform the tasks

Although no significant difference was observed between the Dutch and the Belgians (p=.262), overall, Belgians are most satisfied with the technology provided by their IT department.



[S] Nationality <> feels that less budget is available than before

There is no significant difference between the two nationalities. (p=.395). When looking at the statement itself, it is clear that about half just don't know, and the remaining half tends to disagree with the statement.

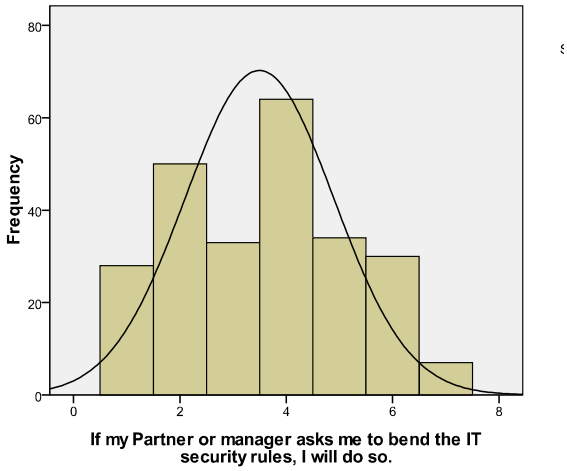


[T] Time with company <> feels less budget is available than before

There is no significant difference between the time-with-company groups. (p=.282).

[U] Gender <> If Partner or manager asks to bend the IT security rules, will do so

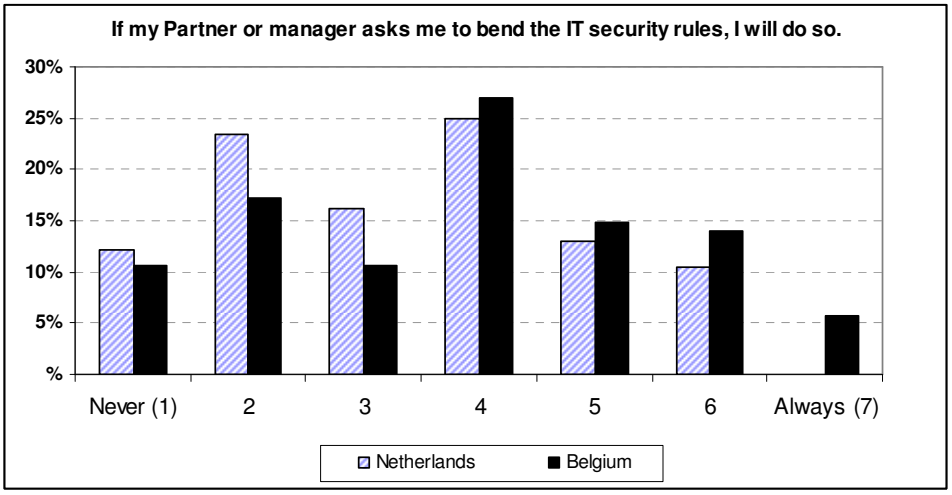
There is no significant difference in the behavior of men and women (p=0,472). However, 50% of males would never, hardly ever of incidentally bend the rules if manager asks them, while only 39,1% of women would. As the first selection option (never) excludes all others, it can be concluded that 86,8% of men and 90,9% of women could/would at one point bend the IT security rules if asked to do so by a superior.



1= Never 2=Hardly ever 3=Incidentally 4=Depends 5=likely 6=Usually 7=Always

[V] Nationality <> If Partner or manager asks to bend the IT security rules, will do so.

Unlike the predicted outcomes from the Hofstede cultural dimensions, there is no significant difference between The Netherlands and Belgium at 95% confidence level (p=.101). Still, as the graph below shows, the Latin culture (Belgium) has a much higher Power Distance Index, they generally will be more likely to accept authority and therefore a higher percentage will 'do as they are asked'.

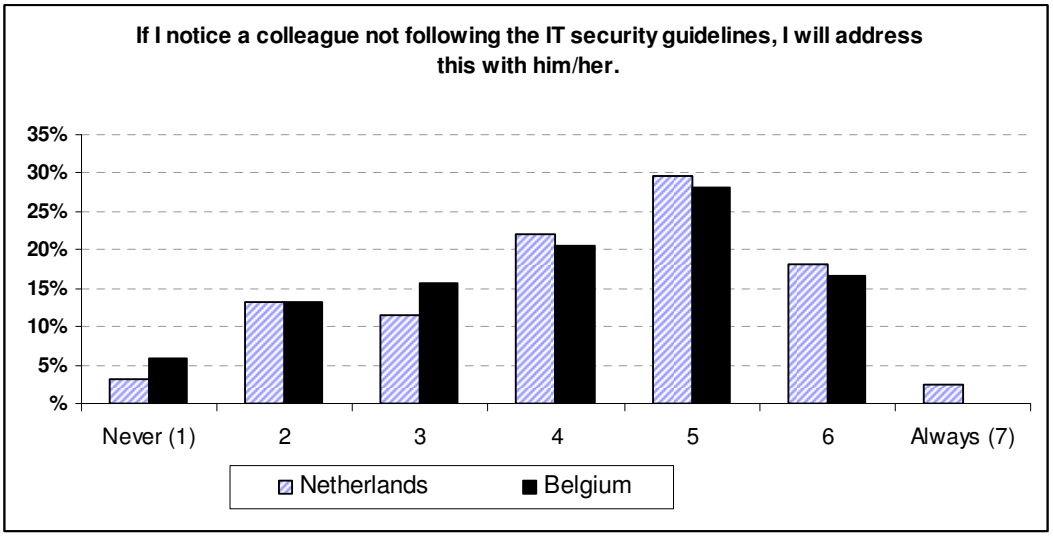


[W] Gender <> If I notice a colleague not following the IT security guidelines, I will address this with him/her.

A significant difference is observed between men and women (p=.001). Men are more likely to address colleagues if they observe them not following security guidelines. 29,9% of women would never or hardly ever speak to a colleague about their behavior, against 11,1% of men.

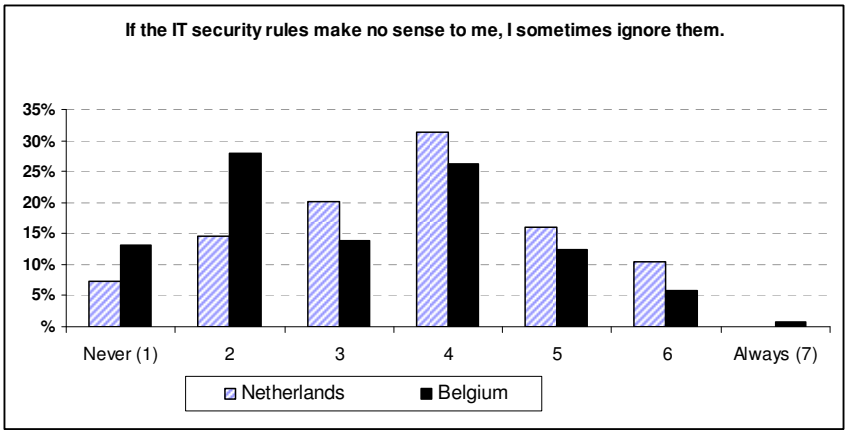
[X] Nationality <> If I notice a colleague not following the IT security guidelines, I will address this with him/her.

A slightly different distribution among the answers was found, but no significant difference (p=.570) between both countries. This is not really surprising as both countries about score equal in Hofstede's Individualism Index. Countries with higher PDI are less likely to address such issues with an equal, which can explain the difference in the 'never' and 'always' scores. There is no significant difference between Dutch and Belgian females (p=.310) or Dutch and Belgian males (p=.717).



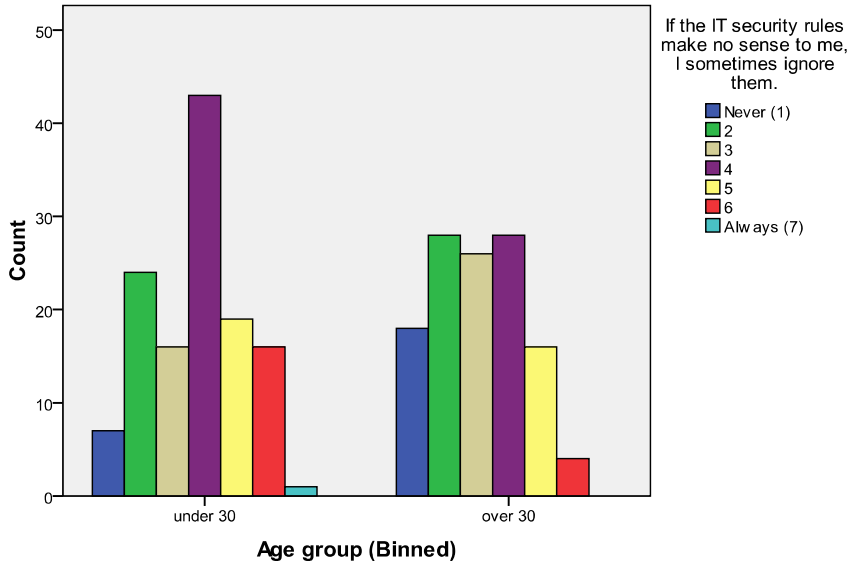
[Y] Nationality <> sometimes ignore rules if they make no sense to me

As predicted from the Hofstede cultural dimensions, there is a significant difference between The Netherlands and Belgium (p=.050). As the Latin culture (Belgium) has a higher Power Distance Index (PDI), they generally will be more likely to 'do as they are told'. However making autonomous decisions is also associated with Individuality (IDV) which is about equal for both countries.



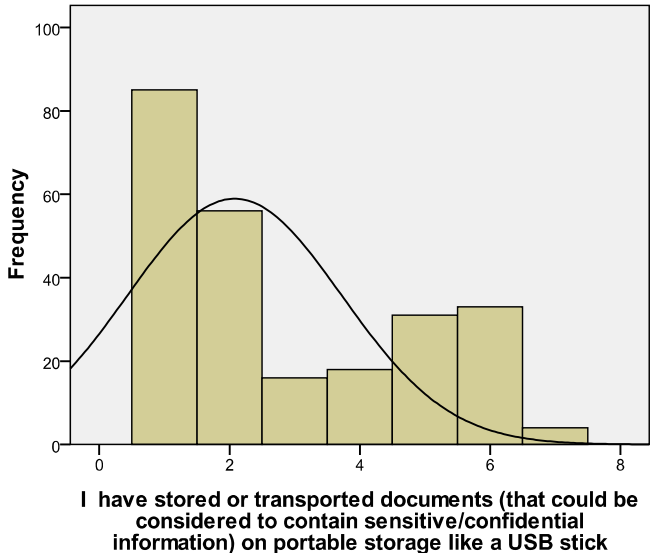
[Z] Age group <>sometimes ignore rules if they make no sense to me

There is a significant difference between adherence to the rules between the age groups (p=.028): the younger generation (under 30) is more likely to ignore rules if they make no sense than the over 30 group.



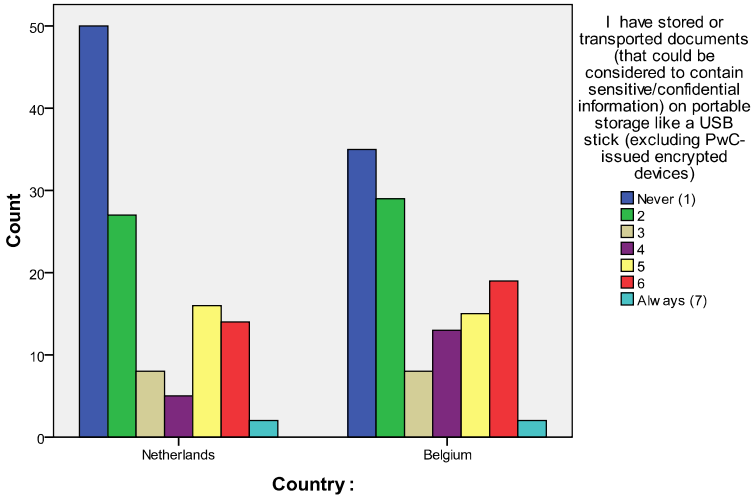
[AA] Gender <> Has stored and transported sensitive data on (unsecured) USB sticks

There is no significant difference between males and females (p=.293). When looking at the frequencies, it can be noticed that there is a large group (58%) that does not transport documents on unprotected devices. This can partially be explained by the fact that (in the Netherlands) most employees are provided with a secure, encrypted USB stick for these purposes, and should have no need to use an unencrypted device. At analysis [BB] a difference was seen (although barely significant) between Belgium and The Netherlands. Also noticeable is that there is another group (28%) who admit they do this on a somewhat regular basis. It could be assumed that unfamiliarity with policy could lead to transporting data on a unprotected USB stick. A cross-tab analysis shows however no significant relationship between familiarity with policy and transporting data on USB sticks (p=.419)



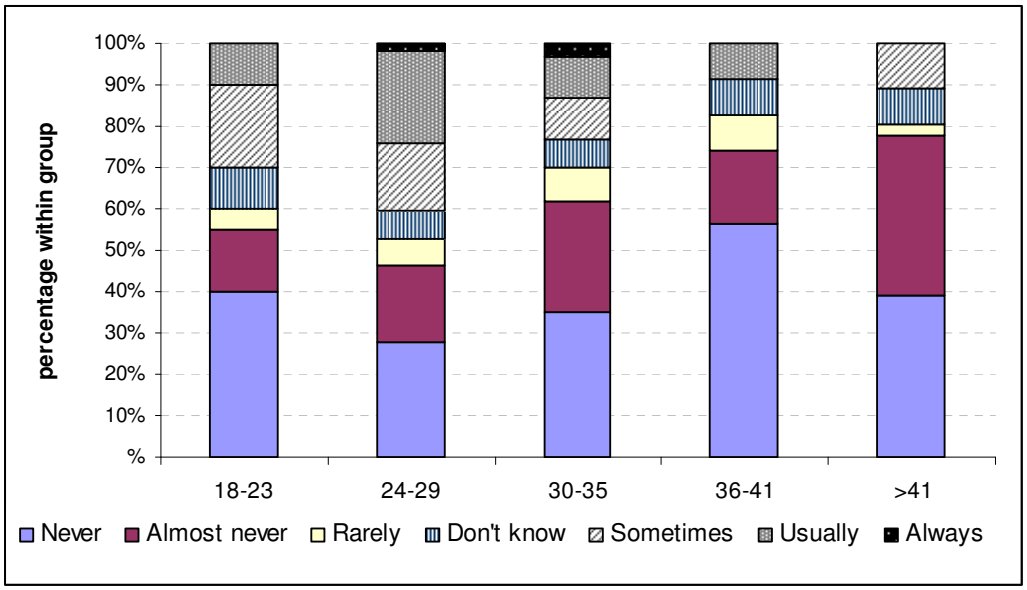
[BB] Nationality <> Has stored and transported sensitive data on (unsecured) USB sticks

More Belgians than Dutch admit transporting data on unsecured USB sticks, but the difference is not significant at a 95% confidence level (p=.315). In percentages the responses show that 30.3% of the Dutch occasionally to always (answers 4 – 7) transport data on USB sticks, against 40.5% of the Belgians.



[CC] Age group <> has stored or transported sensitive / confidential information on portable storage like a USB stick

With a p=.128 there is some, but no significant difference in behavior between the age groups.



Although most respondents in general (64,6%) do never, hardly ever or rarely transport sensitive data on USB sticks, the age group 24-29 clearly stick out with their sometimes, usually (22%!) and always answers.

[DD] Laptop owner <> has stored or transported sensitive / confidential information on portable storage like a USB stick

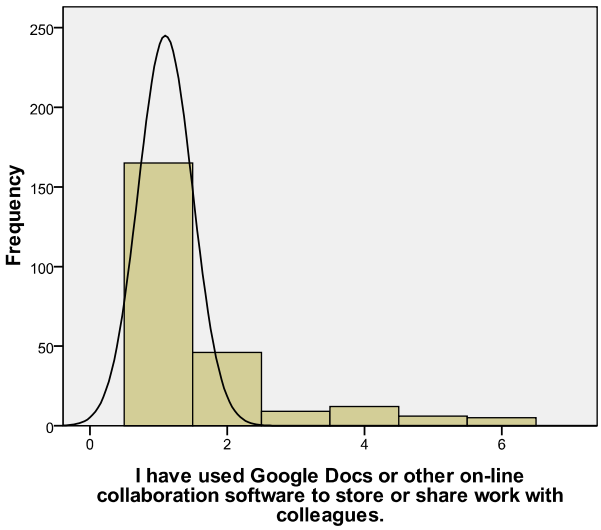
As said before, only 15 out of 243 respondents do not own a company laptop. With a significance of p=.025 there is a difference between laptop owners and non-laptop owners: Maybe surprisingly, non-laptop owners do not have or feel the need to use USB to store or transport data (no scores on sometimes, usually or always answers). 68% of the laptop owners do.

[EE] Nationality <> has used Google Docs or other on-line collaboration software to store or share work with colleagues

- and –

[FF] Age group <> I have used Google Docs or other on-line collaboration software to store or share work with colleagues.

With a p=.769 between The Netherlands and Belgium and a p=.335 between the age groups, there is no difference among them. Also, when looking at the frequencies, online collaboration outside of the enterprise network is not something the security manager should worry about.

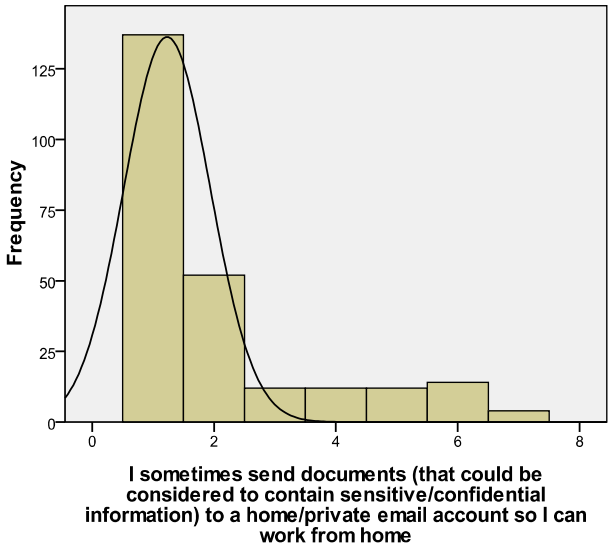


[GG] Gender <> sometimes sends sensitive / confidential information to a home/private email account as to work from home

- and –

[HH] Nationality <> sometimes sends sensitive / confidential information to a home/private email account as to work from home

There is no difference (p=.998) between male and female respondents, nor is there a difference between the Dutch and the Belgians (p=.593). When examining the frequencies, sending sensitive documents to home e-mail addresses is not something the security manager should worry about too much.

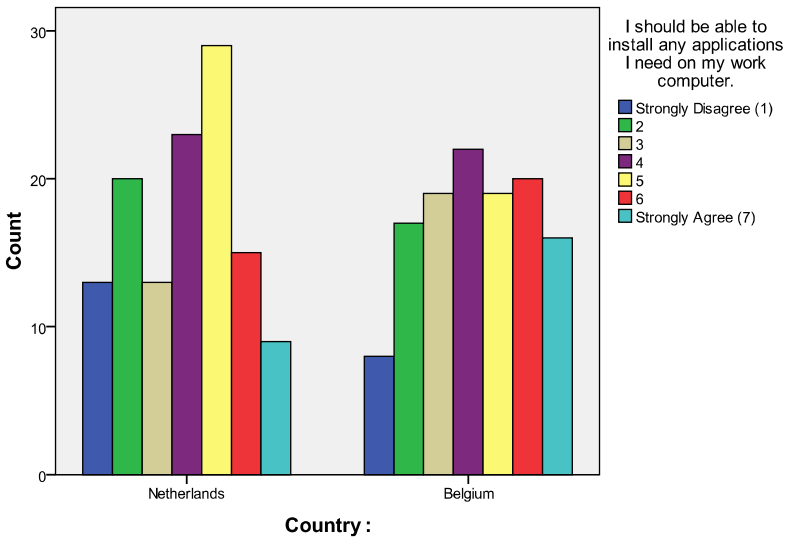


[II] "Has sometimes downloaded software which wasn't reviewed with IT" versus gender
[JJ] "Has sometimes downloaded software which wasn't reviewed with IT" versus nationality and
[KK] "Has sometimes downloaded software which wasn't reviewed with IT" versus age

These results required special analysis. Due to the (unintentionally incorrect) setup of the survey by the survey builder, each possible answer cannot be matched against a grouping variable directly, using cross tab analysis.
The answers to the statement "I sometimes download software, but don't review this with IT because" can summarized as follows:

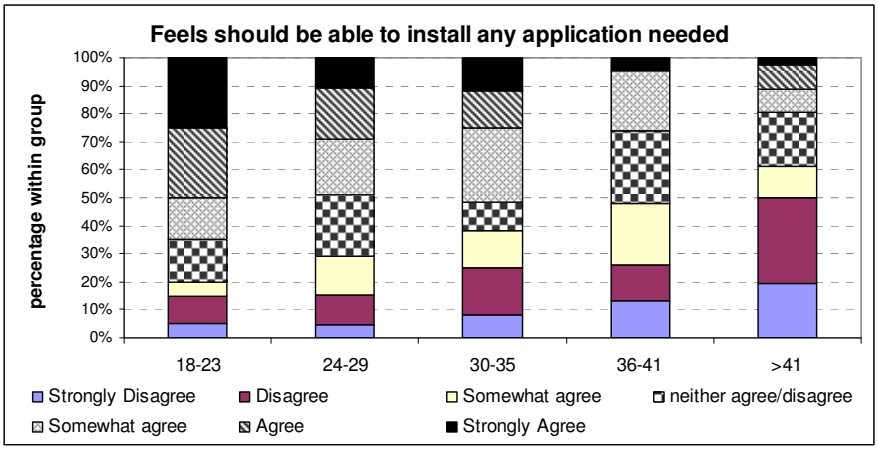
- Nearly half the respondents (49.8%) indicate they never download software, or only after they review this with IT, (4.59%).
- 1% of respondents assume or have experienced IT to say ' no' to such requests,
- only 1.2% would not review the request with IT because they feel it takes to long for IT to respond to such requests,
- 24.7% was unaware that that requirement existed to check with IT and finally
- 14.8% indicate there are other reasons why they don't check with IT before downloading software.

[LL] Nationality <> should be able to install any application needed on work computer.
Obviously, IT security does not agree with this statement as installing unchecked software might interfere with system stability, network performance and data security and integrity. Although the graph shows some interesting variations, there is no statistical difference between the Dutch and Belgians (p=.291). Overall, the Belgians feel stronger about this statement, which might be surprising as Hofstede suggests that the country with the higher PDI and lower IDV would be more compliant with the rules as they are.



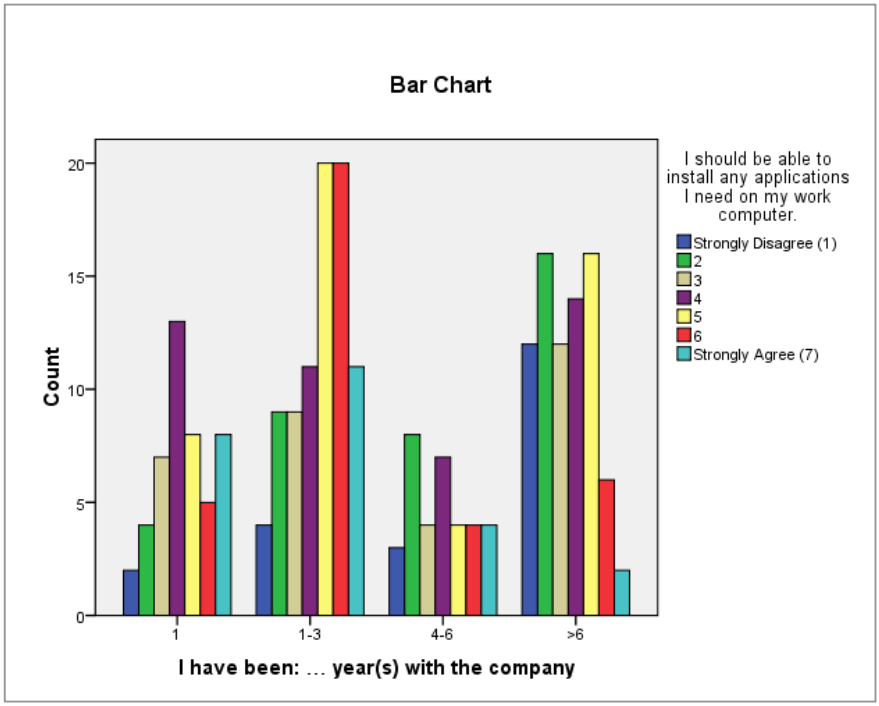
[MM] Age group <> should be able to install any application needed on work computer.

As was discovered before, on this question there is a significant difference between the age groups (p=.024). The younger one is, the more one tends to agree with the statement.



[NN] Time with company <> should be able to install any application needed on work computer.

Similar to analysis [MM], question there is a significant difference between the age groups (p=.013). The younger one is, the more one tends to agree with the statement.



E Appendix: Correlations of all testing variables

Correlations

n=246 Pearson Correlation **Sig. (2-tailed)**	Do you practice these policies?	I find that IT security policies have become more strict:	IT security prevents me to work efficiently.	My IT department provides me with the technology I need	I sometimes need to bend the rules in order to get work done.	I sometimes feel that less budget is available for IT (projects) than before.	If the IT security rules make no sense to me, I sometimes ignore them.	If my Partner or manager asks me to bend the IT security rules, I will do so.	If I notice a colleague not following the IT security guidelines, I will address this with him/her.	I have stored or transported documents on portable storage like a USB stick	I have used Google Docs or other on-line collaboration software to store or share work with colleagues	I should be able to install any applications I need on my work computer.	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	I sometimes send documentsto a home/private email account so I can work from home	I am aware of company policies concerning Instant Messaging usage) and Peer to Peer software usage
Please rate your familiarity with the IT security policies for your organization.	,472** .000	,240** .000	-.014 .822	,176** .006	.024 .703	-.031 .631	-.056 .386	-,194** .002	,247** .000	-.085 .187	-.064 .320	-,129* .045	-.115 .075	-.121 .060	,216** .001
Do you practice these policies?	,206** .001	-,136* .033	,269** .000	-,179** .005	-.089 .164	-,233** .000	-,227** .000	,224** .000	-.070 .276	-.118 .066	-.103 .110	-.086 .179	-,157* .014	,260** .000
Compared previous years, I find that IT security policies have become more strict:	,162* .011	.119 .063	,13737* .031	.090 .162	.074 .250	-.037 .563	,13636* .034	.013 .836	-.014 .823	.039 .544	.008 .905	-.058 .368	,148* .021
I sometimes feel that IT security prevents me to work efficiently.	-,145* .023	,505** .000	,188** .003	,301** .000	,154* .016	.008 .904	.019 .766	.035 .587	,183** .004	.004 .951	.004 .956	-.037 .570
My IT department provides me with the technology I need to perform my tasks.	-,232** .000	-.067 .298	-.083 .192	.010 .880	.032 .619	-.034 .593	-.013 .835	-.043 .506	-.057 .379	-.111 .084	,174** .006
I sometimes need to bend the rules in order to get work done.	,156* .015	,388** .000	,280** .000	.033 .608	,152* .018	,163* .011	.098 .127	.032 .623	.121 .059	-.082 .205
I sometimes feel that less budget is available for IT (projects) than before.	.078 .222	,146* .022	.070 .275	-.091 .159	.108 .093	-.043 .503	.095 .140	-.031 .633	-.021 .739
If the IT security rules make no sense to me, I sometimes ignore them.	,332** .000	-,151* .018	,310** .000	.112 .082	,221** .001	-.077 .231	.083 .196	-,152* .018
If my Partner or manager asks me to bend the IT security rules, I will do so.	-,190** .003	,186** .004	.031 .626	,130* .042	.028 .658	-.023 .726	-,236** .000
If I notice a colleague not following the IT security guidelines, I will address this with him/her.	.038 .551	.058 .366	-,128* .047	-.007 .913	-.059 .363	.020 .760
I have stored or transported documents on portable storage like a USB stick	,247** .000	,175** .006	-.111 .086	,201** .002	-.102 .114
I have used Google Docs etc. to store or share work with colleagues.	.083 .199	.072 .263	,277** .000	-.054 .400
I should be able to install any applications I need on my work computer.	-.015 .817	.084 .191	-.045 .483
I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	.089 .167	-.003 .959
I sometimes send documents to a home/private email account so I can work from home	-.044 .492

0.125

Grey area indicates significant at the p=.05 level

Accepted by the Faculty of Science and Engineering of the University of Applied Sciences Utrecht in partial fulfillment of the requirements for the degree Master of Informatics.

_____

Adviser

_____

(Registrar

The views expressed in this thesis are those of the student and do not necessarily express the views of the University of Applied Sciences Utrecht. Permission is granted to the University of Applied Sciences Utrecht to make this thesis available for use by its own patrons, as well as those of the broader community through inter-library loan. This use is understood to be within the limitations of copyright.

_____

(Student) Signature

_____

Date