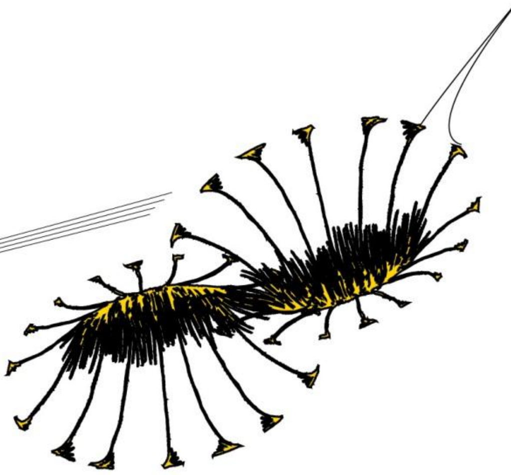
Security without risk?

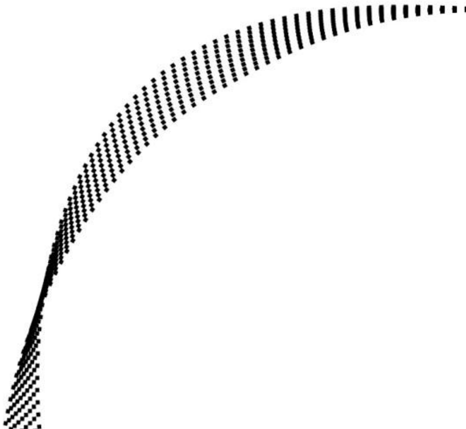
Investigating information security among Dutch universities



Master thesis

Business Information Technology
University of Twente

Kasper van der Leeden
December 2010



UNIVERSITEIT TWENTE.

Master thesis

Title:	Security without risk? Investigating information security among Dutch Universities
Date:	December 9th, 2010
Author:	K. (Kasper) van der Leeden
Student number:	s0014370
Institution:	University of Twente, Enschede, The Netherlands
Faculty:	School of Management and Governance
Master:	Business Information Technology

Graduation Committee

Supervisor:	Dr. Ir. A.A.M. (Ton) Spil
Institution:	University of Twente, Enschede, The Netherlands
Faculty:	School of Management and Governance
Research group:	Information Systems and Change Management
Supervisor:	Dr. V. (Virginia) Nunes Leal Franqueira
Institution:	University of Twente, Enschede, The Netherlands
Faculty:	Faculty of Electrical Engineering, Mathematics and Computer Science
Research group:	Information Systems

External Supervisor

Supervisor:	Ir. F. (Erik) Nijboer
Institution:	University of Twente, Enschede, The Netherlands
Department:	ICT Service Centre

Acknowledgements

First of all, I would like to thanks my supervisor. The feedback at various stages, sometimes regarding the general focus of the research and other times in-depth discussions how concepts fitted together, were invaluable to this research and helped greatly to improve the quality of this work.

Secondly, an investigation of information security practices at the TU Eindhoven. TU Delft, Wageningen U&R and the Open University could not have been performed without their cooperation. Many thanks go out to these universities and I hope that this work will also be beneficial to the information security practices at these universities.

Last but certainly not least, I would like to thanks the employees of ICTS who have granted me insight into the resolution processes and the state of user awareness at the University of Twente.

Management Summary

Research goal

While the University of Twente has a lot of experience with resolving the information security incidents, the organisational process of performing *information security* is relatively new. This thesis set out within this context to investigate the current status of information security at the University of Twente and at other universities in the Netherlands in order to answer the question: "*What is the status of information security at the University of Twente and other universities in the Netherlands and how can information security practices at the University of Twente be improved?"*

Research setup

This research includes an examination of literature in the field of information security which revealed that r*isk management, information security controls, information security incident management* and *analysing and acting upon incidents* are crucial steps in information security. Using literature as base, the status of information security at the University of Twente and several other universities in the Netherlands was investigated by means of case studies. The universities chosen for these case studies were the TU Eindhoven, the TU Delft, Wageningen University and Research and the Open University. The universities were deliberately chosen to include universities which show great resemblance to the University of Twente (TU Eindhoven and TU Delft) but also universities which show less resemblance to account for possible differences.

Conclusions

Based on the literature and the case studies, it was found that:

- none of the investigated universities performs a risk analysis on the subject of information security .
- none of the investigated universities try to quantify the impact of incidents which occur.
- the information security controls at the universities follow best practices in the field of Information Security.
- individual practices at the different universities show that the best practices for universities have not yet been discovered.
- at most universities, the information security incidents are not investigated in terms of vulnerability or threat involved, making it very difficult to correctly adjust the information security practices.
- user awareness among all universities is perceived as low.

For the University of Twente is can be concluded that:

- the registration process of incidents is limited by the application in use.
- reporting solely the frequency of incidents does not show where the problems in information security are located
- some incidents are reported directly to Workstation Support for resolution and are not registered at information security incident management

Recommendations

In order to improve information security at the University of Twente, clarity is needed where to focus the information security practices. It is therefore recommended to:

- perform an information security risk analysis at the University of Twente
- investigate incidents in terms of vulnerabilities, threat and impact
- register incidents in one single application instead of two separate ones

Table of Contents

Introduction

For many organisations, information is an important resource. Information can give insight into how an organisation is performing, how the competition is performing or how a market is developing. According to Ward and Peppard (2002) “most organizations in all sectors of industry, commerce and government are fundamentally dependant on their information systems”.

To ensure this information is available, correct and remains confidential, organisations perform information security. Information security is an organisation process aimed at reducing information security risks to an organisation. Unfortunately, despite various technical, organisational or human-related solutions (controls) information security remains difficult to perform and most organisations will be experiencing information security incidents.

While performing information security may reduce the risk to an organisation, information security can be a costly process. On the other hand, it may be worthwhile as information security incidents can also be costly; costing time and money to resolve or damaging the reputation of the organisation. Therefore organisations need to make a trade-off between the costs of protection versus the costs of possible incidents. A key determinant in this trade-off is *Risk*.

While the risks for the University of Twente is not yet investigated, is can be concluded that there are many information security incidents: between January 2009 and March 2010 over 1600 complaints were received by ICTS (the IT department of the University of Twente). Many of these complaints concern possible copyright infringement (*fraud*), viruses or complaints about spam. These incidents happen within the current implementation of information security at the University of Twente and while applying information security controls and resolving incidents has been performed for a long time at the University of Twente; information security is a process with is still being designed and implemented and policies regarding information security have been formally approved during the time this research took place.

Looking at the current practices of information security at the University of Twente, the key question is: “where are we and where should we go next?” In order to investigate this, this thesis will investigate the current status of information security at the University of Twente. The ‘problem’ of information security is however only not a problem for the University of Twente faces but to all organisations including other universities. As these universities may already have found solutions to the problem the University of Twente is facing, is it very interesting to also investigate how similar institutions are performing information security and compare their situation to the University of Twente. The thesis will be an investigation of information security practices among Dutch universities with special interest in possible improvements for the information security practices at the University of Twente.

1 Methodology

1.1 Research problem

In order to investigate the information security practices among Dutch universities, the following research problem is defined:

What is the status of information security at the University of Twente and other universities in the Netherlands and how can information security practices at the University of Twente be improved?

1.2 Research objectives and setup

This research problem contains three parts. It includes 1) the status of information security at the University of Twente, 2) information security at other universities in the Netherlands and 3) an analysis the information security practices at these universities and recommend improvements for the University of Twente.

Therefore, the objective of this thesis is to:

- investigate the University of Twente and determine the status of its information security in terms of practices and incidents
- learn the status of information security practices and incidents at other universities in the Netherlands and compare them with the status at the University at Twente
- recommend improvements for information security practices at the University of Twente

1.3 Scope

Information can exist in many forms, therefore information security can applies to many objects. As the current scope of information security at the University of Twente is limited to digital information, so is the scope of this thesis. This enables this thesis to investigate improvements to the current practices of the University of Twente rather than investigating what changes to the organisational structure may be necessary to apply to different forms of information.

1.4 Research questions

1. **What is information security?**
    - What are the relevant aspects of information security given the scope of this research?
    - What is information security risk and how identified risks can be treated?
    - What kind of information security incidents exist?
    - How can the impact of information security incidents be determined?
    - What is the role of the “user awareness” in information security?

2. **How is information security being performed at the University of Twente?**
    - How are information security risks at the University of Twente determined?
    - How is the University of Twente reducing information security risks?
    - Which information security incidents are occurring at the University of Twente?
    - What kinds of users are involved in these incidents?
    - What is the impact of the information security incidents at the University of Twente?

3. **What is the status of information security at other universities in the Netherlands?**
   - How are information security risks at these universities determined?
   - How are the universities reducing information security risks?
   - Which information security incidents are occurring at these universities?
   - What kinds of users are involved in these incidents?
   - What is the impact of the information security incidents at these universities?

4. **How is user awareness involved in the information security incidents at the University of Twente?**

5. **How can information security be improved at the University of Twente?**

1.5 Master thesis structure

The research questions have been designed so that first the relevant literature on the subject of information security is investigated. That this literature is applied in practice by studying the University of Twente and other universities in the Netherlands by means of case studies, and based on these findings investigate user awareness and possible improvements for the University of Twente. The structure of this thesis will follow the same structure as the research questions; every research question being addressed in a separate chapter. This thesis will finish off with conclusions and recommendations. An overview of chapters can be found in Table 1 below.

Research question	**Objective**	**Chapter**
1 - What is information security?	Literature review	Chapter 2 – Information security
2 - How is information security being performed at the University of Twente?	Case study of the University of Twente	Chapter 3 – Information security at the University of Twente
3 - What is the status of information security at other universities in the Netherlands?	Case study of four universities in the Netherlands	Chapter 4 – Information security at four universities in the Netherlands
4 - How is user awareness involved in the information security incident at the University of Twente and the interviewed universities in the Netherlands?	Observations based on interviews at the University of Twente and four other universities in the Netherlands	Chapter 5 – User awareness of information security
5 - How can information security be improved at the University of Twente?	Comparing the practices at the University of Twente to the practices at the four other universities in the Netherlands	Chapter 6 - Improving information security at the University of Twente
	Conclusions & recommendations	Chapter 7 – Conclusions
		Chapter 8 – Recommendations
	References & Appendices	References List of interviewees List of figures List of tables Appendices

Table 1: Structure of master thesis

1.6 Abbreviations

Within this thesis, several abbreviations may be used. An overview of these abbreviations can be found in the list below.

CERT	Computer emergency response team
“CIA”	*Confidentiality*, *Integrity* and *Confidentiality* – The three main security attributes of information.
ICTS	ICT-Service centre, the IT department of the University of Twente
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information technology
NIST	National institute of Standards and Technology
VPN	Virtual Private Network

1.7 Literature

Literature on information security was primarily retrieved from Elsevier’s *Scopus* database[1], extended with searches in other database when the full-text articles or references within those articles were not available within the *Scopus* database. In rare cases the websites of the original authors were used to retrieve the full-text article or referenced articles when these articles were not available in the Scopus database or other databases. A search in the Scopus database with the keyword *information security* yielded a wide variety of results which included many technical aspects like cryptography and technical vulnerabilities. While these aspects are relevant to the field of information security, this research was more interested in the practices and processes related to information security. An important part of the information security is concerns the question of which information to protect, which is determined in a process called ‘risk analysis’. Keyword searches were thus also executed on ‘information’ in combination with ‘risk analysis’ and in combination with ‘value’ as the value of information may help in determining whether the costs of protecting the information can be justified. One of the keywords that stood out during the investigation of literature was the concept of ‘awareness’ as human factor may have a great influence on information security. In addition, the keyword of ‘information’ was also interchanged with ‘information technology’ or ‘IT’.

In conclusion, keyword searches were executed on the following keywords: *information security, information security awareness, IT security, IT user security, information value, information risk analysis*. Over 700 articles were scanned based on title and abstract. This yielded about 90 articles which require closer examination and 36 of those articles, which include journal articles, articles from conference proceedings, articles in periodicals and PhD theses have been kept. Some provided useful insight or information for this research while others provided useful background information. On these articles, backwards and forward citation searches were executed which were subject to the same process of selection.

[1] http://www.scopus.com/home.url

1.8 Case studies

In addition to the literature, this research will look at information security as it is being performed at both the University of Twente and several universities in the Netherlands by means of case studies. Case studies try to examine *"(a) a contemporary phenomenon in its real-life context, especially when (b) the boundaries between phenomenon and context are not clearly evident."*. While, as will be shown in literature, information security involved a number of related concepts, how the University of Twente and other universities in the Netherlands deal with these concepts is not yet clear. (Yin, 1981)

These case studies therefore try to investigate the phenomenon of information security as it is performed currently among these universities based on practices found in literature. Case studies depend on "information from multiple sources of evidence. The evidence may include direct observations, interviews, documents, archival files, and actual artifacts"(Yin, 1997). At the University of Twente, the data will be retrieved from various sources. These data sources will be described for the University of Twente and the other universities in the next section.

1.8.1 Information sources at the University of Twente

The research will include both general information on the organisation as well as information on specific information security incidents. The information on the organisation is retrieve from publicly available sources like the information security policies as presented on the website of the University of Twente[2]. Information on past incidents contains user information which is considered private information and therefore not publicly available. While this linking of data is necessary to the resolution process; it is considered personal information and not disclosed anywhere else. For purposes of analysis for this research personal user data was used to distinguish between students and employees, but only on a group level are the results presented in this thesis.

In addition to documented data, the research also relies on interviews because some procedures are not well documented or additional background information is desired on a subject. Therefore interviews were held with the assistant information manager of the University of Twente, two members of the information security team and several members involved with the various IT support groups at the University of Twente. An overview of interviewees is included at the end of this thesis. The interviews at the University of Twente were semi-structured. As, with case studies, the boundaries between phenomenon and context are not always clear, this choice allowed for more detailed examination of subject brought up during the interview; while this maintaining a link with the overall structure as will be presented in literature.

1.8.2 Information sources on universities in the Netherlands

The data on several other universities in the Netherlands was mainly gathered by means of semi-structured interviews. The interviews were designed based on the findings in literature and the finding in the case study at the University of Twente. These interviews consisted of questions regarding 7 subjects, which will be presented in section 0, and were designed to take approximately 1.5 hours. As with the interviews at the University of Twente, a list of interviewees is included at the end of this thesis.

[2] http://www.utwente.nl/secr/im/, accessed 01-07-2010

2 Information security

Security, in general, is often concerned with 'protecting something'. In those terms information security may be defined as *the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximizing return on investment and business opportunities".* (ISO/IEC, 2005) Security, however, can also be understood in terms certainty or assurance. Social security is not necessarily about protecting someone but ensuring that people can live despite some social misfortune.

Information security can best be seen in terms of ensuring certain attributes of information rather than protecting and information security, at a minimum, is concerned with ensuring the *confidentiality, integrity and availability* of information; often referred to as the *CIA* of information. Cooper (2009) describes these attributes as:

- *Confidentiality* involves protecting resources from unauthorized access and/or disclosure.
- *Integrity* involves protecting against unauthorized changes (accidental or intentional) to data.
- *Availability* ensures that information is accessible by users when needed.

The extent to which an organisation focuses on information security depends on the desired level of protection of information which influences the amount of time and money an organisation needs to invest in information security. This is most clear for ensuring availability: when an application is only running on one server the application is unavailable when there is a hardware failure. When this is undesirable, this may be solved by have multiple servers running the same application so that the application will only be unavailable when a problem occurs with all servers simultaneously. However, there are more costs when acquiring and maintaining multiple servers. In information security there are clearly costs. While the fact that there are costs involved in information security, Albrechtsen (2008) even describes it as a very *"resource demanding"* process, but he also states that can be process well worth investing in as *"information security breaches may cost even more*". These costs can include costs of repairing damage, loss of reputation, costs of lawsuits or missed income (e.g. loss of patentable information). Information security is thus a trade-off.

One of the difficulties in information security is the existence of tension between the information security attributes. Oliver (2002) it is *"a well-known phenomenon in security: security is widely regarded as a balance between confidentiality, integrity and availability. Without the need for availability, the confidentiality problem is trivially solved by 'unplugging' the database"*. Not only is 'unplugging' often not a viable option, the demands on information are increasing as users are getting used to the internet and expect information to be accessible from more and more locations.

Another difficulty in information security is the question: "how to protect information?". The view on information security solutions *"has traditionally been technology-oriented"* (Albrechtsen, 2008) and the answers to the question "how to protect information" was thus answered with new or better technology. However, it was found that users were quite adapting at circumventing technical solutions. For example, implementing the best virus scanner in the world does not help is the users disables it. While solutions for this problem may exist in the technical domain, the practice of writing down passwords cannot easily be solved by technical means.

In sector 2.6 this human factor will be examined in more detail and it will be shown that one possible explanation of this behaviour is security places a burden on the user causing them to make an implicit trade-off between the burden of information security and the risk the user perceives.

This concept of "risk" is crucial to information security. As information security can be "*resource demanding"* (Albrechtsen, 2008) organisation do not perform information security without reason. An organisation performs information security to prevent a level of perceived risk from becoming actual incidents. To explain how information security works, section 2.1 will first present a conceptual framework with the relationships between the various concepts. After section 2.1, the remainder of this chapter will look at the various concepts in more detail.

2.1 Conceptual model

Information security is a very broad subject and there are many important concepts. The three concepts of most interest to this thesis are: *Risk, Security Controls* and *Incidents*. In section 0 it was mentioned that there will be costs if information security is not achieved. Risk is the estimation of these costs. Risk management, which will be discussed in section 2.2, is the organisational process which assesses the risks and decides how to treat those risks. When it is decided to reduce the risk, it is necessary to design security controls. These controls can be:

- Technical, e.g. a firewall
- Organisational, e.g. organisational policies
- human-related, e.g. training, education or awareness campaigns

While security controls often reduce the risk to an organisation, they often do not succeed in completely eliminating the risk. As a result, information security incidents may occur. Not every risk will become an incident, but every incident does show that there is a specific risk that is not (completely) covered by the security controls. To continue to improve information security, it is necessary for the organisation act upon incidents, either by reassessing the security controls or the risks to the organisation.

To achieve continuous improvements in information security, the relationship between these concepts should be view as a cyclical process and as a cyclical improvement process it can be modelled in terms of the Plan-Do-Check-Act circle by W. Edwards Deming, as shown in Figure 1.

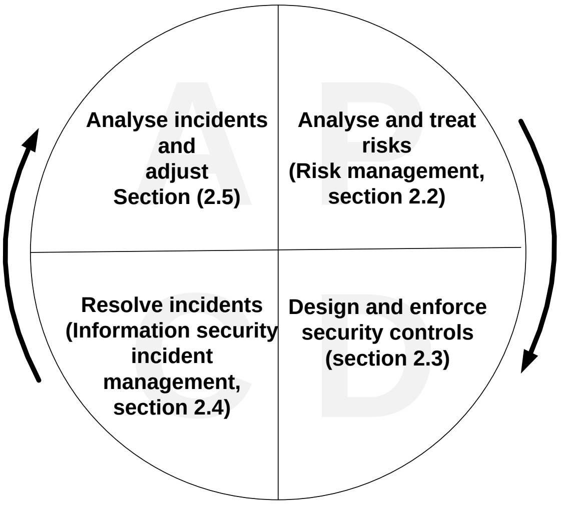

Analyse incidents and adjust Section (2.5)
Analyse and treat risks (Risk management, section 2.2)
Resolve incidents (Information security incident management, section 2.4)
Design and enforce security controls (section 2.3)
A
B
C
D

Figure 1: Relationship between the concepts in information security (modified Deming circle)

This model also shows the logical flow between the concepts which will be used to structure the sections to come. These sections will describe the process of risk management (section 2.2), security controls (section 2.3), information security incident management (section 2.4) and analysing the information security incidents (section 0). In addition, section 2.6 will described the human factors in information security.

2.2 Risk management

Risk in information security is the predicted of the costs that will occur when information security is not achieved. Risk in the context of information systems can be defined as a combination of:(Nunes Leal Franqueira, 2009)

i) The likelihood that a given threat agent will exploit or trigger a particular information system vulnerability

ii) The resulting impact of this exploitation for an organization, if successful

2.2.1 Likelihood

This likelihood was given as *the likelihood that a given threat agent will exploit or trigger a particular information system vulnerability*. For a risk to occur there needs to be a combination of a *vulnerability* and a *threat* (agent) (Nunes Leal Franqueira, 2009)[3]. The aspects of vulnerability, threat and threat-agent can be described as (adapted from 3):

[3] These given definitions are based on the work of Stoneburner, Goguen and Feringa and the NIST Glossary of Key Information Security Terms. For more information on these definitions and sources, please see Nunes Leal Franqueira (2009).

- A **vulnerability** is a very broad concept and is defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat agent
- A **threat** is a potential for a threat-agent to successfully exploit a vulnerability.
- A **threat agent** is a human agent who actively exploits a vulnerability while performing an attack

An organisation will usually have little influence on the threat agent although, as will be shown in section 2.6, it may be that the threat agent is a member of the organisation; in which case the organisation may have some influence. The organisation however can influence the vulnerabilities that exist and try to treat those with security controls.

2.2.2 Impact

The second factor influencing the risk is the impact of exploitation of the risk on the organisation. Impact, when related to risk, is an expected value of the consequences that information security incidents may have. These incidents can have various consequences the ISO (ISO/IEC, 2008) and National Institute for Standards and Technology (NIST, 2002) standards on risks for information technology describe as the tangible and intangible consequences of the violation of the security attributes, like *confidentiality*, *integrity* and *availability,* of information.

NIST 800-30 describes the analysis as a “Business impact analysis” which accounts for the:

- Loss of confidentiality
- Loss of integrity
- Loss of availability

The tangible consequences can consist of lost revenue, cost of repairing and effort required to correct the problem while the intangible consequences can consist of loss of public confidence, loss of credibility and damage to an organisation’s interest (NIST, 2002). The exact type and amount of cost related to a risk depends entirely on the individual organisation.

As Figure 2 below shows, risk exists when there are both vulnerabilities and threats to those vulnerabilities. The amount of risk is determined by the likelihood and impact that is expected for those risks.

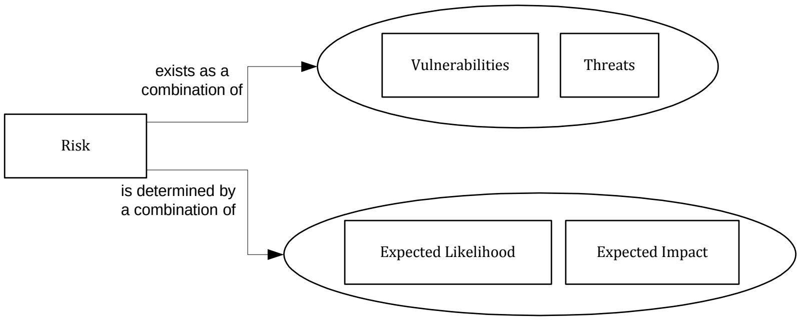
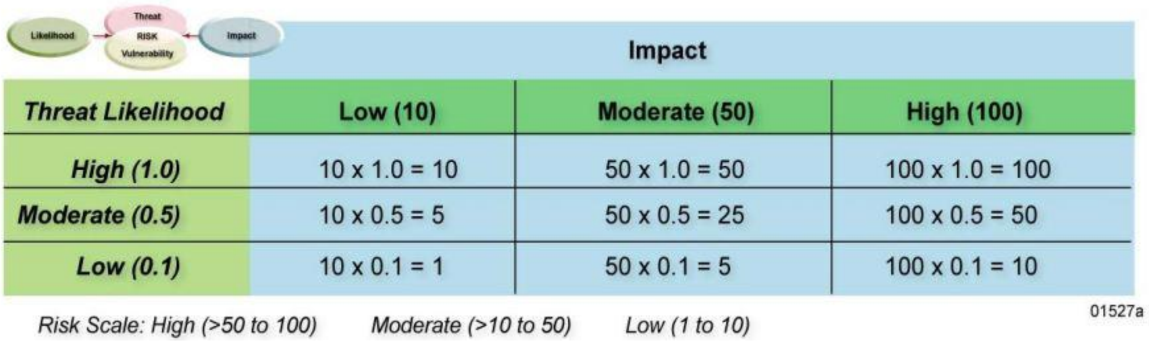


Figure 2: Risk in terms of vulnerabilities, threat, expected likelihood and expected impact

2.2.3 Determining risk

In an ideal world, both the likelihood and impact would be quantifiable. If, for example, there are 2 known vulnerabilities which, if not treated are expected to translate into 10 incidents each. If each such incident would have an impact on €10.000, than the risk to the organisation would be 2 x 10 x € 10.000 = € 200.000. Unfortunately, both factors are often very hard to predict: the likelihood depends on threat agents (over which the organisation has little control) and the impact can contain intangible parts which are difficult to quantify.

When quantifying the impact is not possible, a more subjective method can be chosen like a likelihood-impact matrix as shown in Figure 3. In this case both the likelihood and the impact may be determined in terms of high, medium or low and given the values at the likelihood and impact (determined by the organisation) in indication of risks may be calculated.


Likelihood
Threat
RISK
Vulnerability
Impact

	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

Risk Scale: High (>50 to 100) *Moderate (>10 to 50)* *Low (1 to 10)*

01527a

Figure 3: example likelihood-impact matrix from (NIST, 2002)

Determining the amount of risk as a part of the risk management process is important because this allows an organisation to decide how to treat those risks.

2.2.4 Treating risk

When the amount of risk is determined, an organisation can look how to treat the risks. Treating risk can be done in 4 ways (ISO/IEC, 2005):

1) Apply appropriate controls to reduce risk.
2) Knowingly and objectively accept risks, providing they clearly satisfy the organization’s policy and criteria for risk acceptance.
3) Avoid risks by not allowing actions that would cause the risk to occur.
4) Transfer the associated risks to other parties, e.g. insurers or suppliers.

Which treatment method to choose depends in part on the specific situation of an organisation. As risks can be related to the specific business of an organisation, avoidance is not always a viable choice. Regarding the other treatment methods, the trade-off of costs of protection versus the expected impact will often be the determining factor. This trade-off is very obvious when transferring the risk to an insurer but also when transferring to risk to suppliers or outsourcing part of your business.

While the particular risk(s) are covered for the organisation, the organisation is charged for that service. When not avoiding or transferring risk, the risk remains at the organisation and it has to decide what to do with it: reduce or accept (again based on the trade-off between costs of protection and the expected impact). When the decision is made to reduce the risk, information security controls need to be designed, implemented and enforced. These security controls are discussed in the next section.

2.3 Information security controls

Information security *"is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions"* (ISO/IEC, 2005). The policies, processes, procedures, organizational structures are examples of organisational controls, while software and hardware solutions (e.g. firewalls) are technical solutions. In section 2.6, the role of the human factor in information security will be examined and that section will show that the human factor can also contain or introduce (e.g. by disabling a virus scanner) vulnerabilities. Addressing these issues, e.g. by training or educating user can be a form of human-related controls. Security control, as mention in section 2.1, can be:

- Technical controls
- Organisational controls
- human-related controls

These controls usually work on vulnerabilities by eliminating vulnerabilities from the organisation or by preventing threat agents from exploiting the vulnerabilities. In some cases, the controls may also work directly on the threat (agents). It was already mentioned that the threat agents in some cases might be a member of the organisation. When, through for example policies, it is known that the punishment for the member of the organisation is severe, maybe he or she will cease to be a threat agent.

One very important control in information security is the information security policy. Higgins (in (Doherty & Fulford, 2006)) notes that *"without a policy, security practices will be developed without clear demarcation of objectives and responsibilities"*. The information security policy is used to "*provide management direction and support for information security in accordance with business requirements and relevant laws and regulations"* (ISO/IEC, 2005). In their work, Doherthy and Fulford (2006) agree with this in the sense that the information security policy should be aligned with strategic goals of an organisation. So while the information security policy is a form of security control, it is very important as it gives direction any other security control.

To support the cyclical approach to information security, the ISO standards 27002 and 27005 standard specify the need for periodical review. The world is constantly changes and so may be the business objectives of an organisation to cope with those changes. The risks to an organisation may change due to (ISO/IEC, 2008):

- New assets
- Changing asset values
- New threats
- New or increased vulnerabilities
- Increased impact
- Information security incidents

The information security policy review should include, among other things (ISO/IEC, 2005):

- Trends related to threats and vulnerabilities
- Reported information security incidents.

Both specify the information security incidents as important information to risk management process as well as the review of information security policy. The information security incidents can show that the risks the actual impact of incident differs from the expected risk (for better or for worse) which may lead to a reassessment of the risks. It can show that certain information security controls are not functioning properly. The information on incidents can be gathered in the information security incident management process.

2.4 Information security incident management

Information security incident management has two important functions. The first one is resolving information security incidents. An incident is *"a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* (ISO/IEC, 2005). An information security incident is a realisation of a specific risk.

When an incident happens, there was a specific combination of a vulnerability and a threat which lead to that incident. In addition, incident has an actual frequency and actual impact, which may differ from the likelihood and expected impact when the risk was determined. The relationships between incident, vulnerability, threat, frequency and impact are shown in Figure 4.

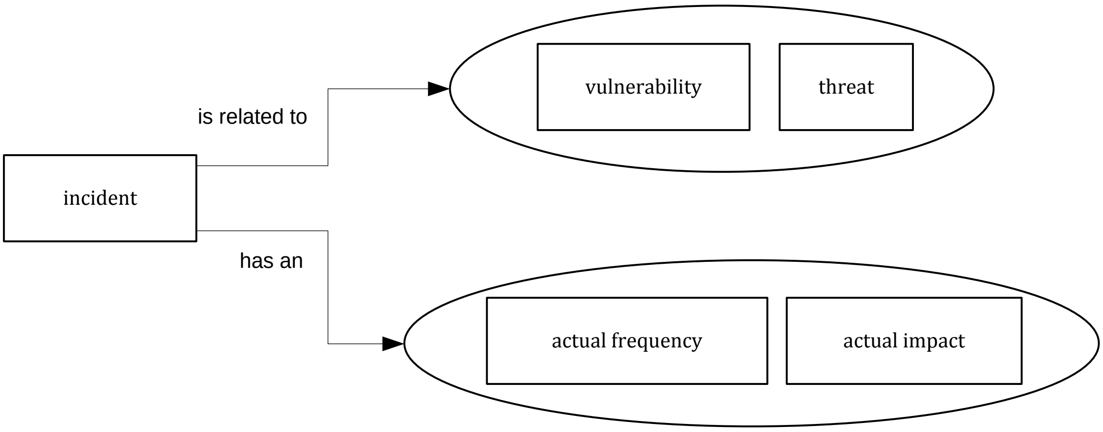


Figure 4: Information security incidents in terms of vulnerability, threat, actual impact and actual frequency

These incidents can concern *“breaches of any law, statutory, regulatory or contractual obligations, and of any security requirement”* (ISO/IEC, 2005). While the ISO standard gives some examples of incidents, a comprehensive overview of the types of information security incidents is given in the eCSIRT framework for incident reporting. This framework provides a classification of incidents in 25 different types, grouped in 9 high level classes. An overview of the framework can be found in Appendix A.

The second important role of incident management is to generate reports on these incidents to enable the risks and information security controls to be reassessed. According to ISO 27002 *“[t]here should be mechanisms in place to enable the*

- ➢ *types,*
- ➢ *volumes,*
- ➢ *and costs*

of information security incidents to be quantified and monitored” (ISO/IEC, 2005). This information provides feedback on the current situation of information security within an organisation and the evaluation of information security incidents *“may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process”* (ISO/IEC, 2005). This information can only be reported with the incidents are investigated and the results are recorded. Based on this information, the actual impact of incidents may be compared to the expected risks. The outcome might show that incidents are occurring more frequently or have a greater impact than expected. It might also be that there are incidents that were not expected. When investigating these incidents, it might also be important to investigate the specific vulnerability involved as this information is required to adjust the security controls.

2.5 Analysing information security incidents

When the investigation on incidents shows that the actual incidents and expect risk do not match, it can be that the risks were misjudged or that the situation has changed (e.g. new vulnerabilities have been introduced) or it may be that the security controls fail to reduce the risk to the expected level. In both cases it is important to further analyse the incident in terms of vulnerability and threat involved. If these show that these factors are new, they should be taken into account in a new risk analysis. Should they not deviate from what is expected, the security controls may not be functioning correctly. In that case, before analysing the risks again, it might be necessary to adjust the security controls.

2.6 Human Factors

Human factors in information security were traditionally regarded as *"unpredictable"* (Ashenden, 2008) and as a result information security has (traditionally) been treated from a *"technology-oriented"* (Albrechtsen, 2008) perspective. In this perspective, the role of information security managers often *"has been that of the technical specialist with a command and control approach to management"* (Ashenden, 2008).This view is however changing: Kruger and Kearney (2006) state that *"[t]he effective management of information security requires a combination of technical and procedural controls to manage information risk. The value of controls usually depends on the people implementing and using them and in information security this is no different. Controls can be circumvented or abused by employees who ignore security policies and procedures."*

One possible reason for this behaviour may be found in the work of Herley (2009). Because technical security controls often place an additional burden on the users: remembering difficult passwords, changing it often, locking/unlocking your workstation, Herley (2009) states that within information security the user makes an implicit trade-off which is consistent with the calculation of risk: *"what is the risk I get involved in an incident and how much time does it take to recover from that incident?"* According to him, usually only a very small number of users get involved in an incident and that the annoyance of recovery is quickly overcome and that complying with security every day takes much more time.

Not every user will immediately ignore security, but they are likely to comply with security to a certain extent. In the research on a 'compliance budget' (Beautement, Sasse, & Wonham, 2008) it was found that (in)compliance with the security policies is a choice of users which is influence by, among other, the additional 'costs' (mentally or physically) a user has to endure to comply with the security measures. In the meantime, other research on human aspects in information security focuses on the awareness of users. Siponen & Oinas-Kukkonen (2007) state that when users lack awareness, they may be inclined to work around 'troublesome' security measure and it may be easier for user to become victim to social engineering attacks *(where human faults or weaknesses are used to carry out such an attack*). Therefore, according to Albrechtsen (2008), the *"non-technological aspects of information security now must be considered in addition to technological aspects"*, although it is also not necessary to raise the knowledge to a specialist level: *"One cannot require that employees should be security experts; but one can expect users to be aware of information security and perform simple, not time-consuming actions"* (Albrechtsen, 2008).

One of the goals of information security should be to create *“the correct mindset, and ensuring that people are working for (or at least with) security rather than against it”* (Furnell & Thomson, 2009). The first step in creating this mind-set may be creating ‘awareness’ among users. Marks and Rezgui (2009) say that *“most* [information] *security managers pay more attention to technical aspects and solutions, such as firewalls, routers, and intrusion detection software, and tend to overlook socio-organizational issues such as the hazards caused by end users’ lack of IS awareness.”*

Information security awareness is about *“ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with”*(Kritzinger & Smith, 2008) and it deals *“with the use of security awareness programs to create and maintain security-positive behavior as a critical element in an effective information security environment”* (Kruger & Kearney, 2006). It is of crucial importance *“as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness” and should help to* minimize *“user-related faults, nullify them in theory, and maximise the efficiency of security techniques and procedures from the user point of view”* (Siponen, 2000).

Malcolmson (2009) even talks about an information security culture. Although she also notes there is not yet a generally accepted definition of what an ‘information security culture’ exactly is, a working definition she gives is: *“Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact”* (Malcolmson, 2009). Furnell & Thomson (2009) also recognize the concept of culture, but what is clear from their work is the fact that there are multiple levels of compliance regarding information security and awareness is a part of it in the process of getting the organisation to comply with the desired level of security.

Compliance	Culture	The ideal state, in which security is implicitly part of the user’s natural behaviour.
	Commitment	Security is not a natural part of the behaviour, but is provided with appropriate guidance/leadership then users accept the need for it and make an associated effort
	Obedience	Users may not buy into the principles, but can be made to comply via appropriate authority (i.e. implying greater level of enforcement than simply providing guidance).
	Awareness	Users are aware of their role in information security, but are not necessarily fully complying with the associated behaviour as yet.
Non-compliance	Ignorance	Users remain unaware of security issues and so may introduce inadvertent adverse effects.
	Apathy	Users are aware of their role in protecting information assets, but are not motivated to adhere to good information security practices.
	Resistance	Users passively work against security, opposing those practices they do not agree with.
	Disobedience	Users actively work against security, with insider abusers intentionally breaking the rules and circumventing controls.

Table 2: Levels of security compliance based upon individual behaviours (Furnell & Thomson, 2009)

It can also be noted from the table of Furnell & Thomson that while it is possible for users to become threat agents by deliberately working against security, it is also possible for user to inadvertently introduce hazards into the environment. The unintentional adverse effects can be introduced because of a lack of knowledge and this is described as a state of 'ignorance' by Furnell & Thomson (2009). This can be countered by creating awareness and while users may still choose not to fully comply with the security policies, the hazards that are introduced unintentionally can be decreased. Therefore, it is useful to distinguish between incidents that have been caused by intentional and unintentional human actions.

While users in this section have been shown can contribute, or cause, incidents in various ways, users are not the only cause of incidents Kraemer, Carayon and Clem (2009) state that there are many organisational and human factors causing vulnerabilities and that the human, organisational and technological causes are interlinked.

To deal with information security, either in a technological, organisational or human-related manner, it is important to know the source of the threat. When the threat originates outside the border of the organisation, one has to make sure to properly lock the (virtual) doors. The incidents, however, are certainly not only caused by external users. Insider threats have been identified as an important source of threats and while the number of security incidents by this group is usually lower than those caused by outsiders, the impact is usually more profound (Nunes Leal Franqueira et al., 2010) & (Willison & Siponen, 2009). The distinction between *insiders* and *outsiders* is usually based on the authorization to access a system or some information. Nunes Leal Franqueira et al. (2010) however recognize a third group of people who may have authorized access but who are not fully trusted by the organisation, namely *External Insiders.*

The three categories of users are explained as in the work of Nunes Leal Franqueira et al. (2010) as:

- **Insiders** are individuals that are trusted and have (some) authorized access over the organisation's assets.
- **Outsiders** are individuals that are not trusted and have no authorized access over the organisation's assets
- **External Insiders** are individuals that are not trusted and have (some) authorized access over the organisation's assets.

While the groups of outsiders is organised homogeneously (none of users within this group should have access to an organisation's assets) this is not necessarily true for the groups of insiders or external insiders. For example, a human resource employee may need access to the payroll data of the employees. This information is often considered private and other employees should therefore have no access to this information. Organisational structure and roles thus influence who should have access to which organisational assets and information security needs to ensure this is realised.

2.7 Summary

Information is an important resource to organisations. Information security is not just tasked with protecting that information but ensuring that authorised users *are* and that unauthorised users *are not* allowed to view or modify information. At the same time information security is tasked with ensuring that the information is available to the authorised users. In section 0, these attributes were defined as the confidentiality, integrity and availability of information.

Information security is necessary because there are risks that threaten the information security attributes. As shown in section 2.2, key terms when looking at risks are: vulnerability, threat, likelihood and impact. Risk exists in a situation where there is weakness to the system (vulnerability) and someone willing to exploit that weakness (threat). As a part of risk management, an organisation can try to assess these risks and the expected amount risk to the organisation. With that information, an organisation can decide how to treat that risk. The organisation can try to *avoid* or *transfer* the risk. If these options are not feasible, an organisation can decide to either *reduce* or *accept* the risk. With all of these options, there are costs involved. These costs can be from investing in security controls or paying insurers for the risk. If the risk is accepted, the costs are the impact; should incidents occur. Information security is thus a trade-off between the costs of protection versus the costs of information security incidents.

Based on the method of risk treatment, information security controls can be designed. Section 2.3 described that there are three types of controls: technical, organisational and human-related. One of the cornerstones in information security is an organisational control: the information security policy. This policy should provide a link with the organisational goals (e.g. why is there a need to reduce the risk) and give direction to the other security controls.

Throughout the year, an organisation will likely have to deal with information security incidents. Incidents can occur because security controls are not perfect or because risks were accepted or not included in the analysis. Information security incident management, as described in section 2.4, is tasked with resolving those incidents. To be able to improve information security, the play an even more crucial role: investigate the incidents in terms of vulnerability and threat, and determine the actual frequency and impact of the occurrences. This information can be reviewed and used to either review the risk management processes or the information security controls, as described in section 0.

In the last section of this chapter, the human factor in information security was discussed. It was determined that there are three groups of users: insiders, outsiders and external insiders; depending to the authorization the user has and whether they are trusted by the organisation. These users, as shown by Furnell & Thomson, can work deliberately against security, deliberately in compliance with security or unintentionally against it. Factors influencing the behaviour of a specific user may be the level of awareness of the user, a concept called the compliance budget and the implicit trade-off a user makes regarding information security during their daily business.

3 Information security at the University of Twente

Like all universities, the University of Twente is a place where knowledge is created and transferred. To support those processes there is a significant amount of IT at the University of Twente, including e-mail servers, files servers, and servers hosting educational, financial, administrative or educational applications. Like many universities (Marks & Rezgui, 2009), the University of Twente provides relatively open access to the internal network. This network can be accessed by workstations at the university, but also by (private) notebooks and workstations at home. While the distinction between type of computer is important when analysing the incidents and their impact, the distinction between a workstation and a notebook is not always important. In those cases 'computers' will be used a term to refer the collection of both notebooks and workstation.

Before looking how the University of Twente addresses the aspects of Risk Management, Information security controls, Information security incidents management and the analysis and adjustment, first the human factors at the University of Twente. While there is no detailed information about the awareness or the motivation of the users to comply with security or not, the user groups within the University of Twente can be identified. Knowledge on these user groups will be important for the remainder of this chapter.

3.1 Humans factors at the University of Twente

The types of user which were mentioned in section 2.6 are insiders, outsiders and external insiders. At the University of Twente the majority of the population consists of students and employees. These users are registered at and trusted by the University of Twente; therefore these accounts can be considered insiders.

When looking at the accounts, there are more users than students and employees who can access the facilities at the University of Twente. There are accounts for guests and third-parties. The difference between these accounts is that a guest account can be created and activated immediately, but is only active for a week. Accounts for third-parties have to be requested and approved and usually last for a longer time. In addition, users from the Saxion school in Enschede and users connected to the Eduroam federation can use their (external) credentials to access the facilities at the University of Twente. All of these accounts can be considered external insiders. With Eduroam and Saxion accounts the university has no control over accounts at all. With the guest and third-party accounts the University of Twente may have some technical control over these accounts, but does not entirely control the lifecycle. For example, third-party accounts may be introduced for former-employees for specific reasons. The account will be terminated if the account is not used for 6 month or the director of the IT departments decides to terminate it[4]. This account could exist for a long time and the user is in control for a major part. Therefore these accounts can be seen as external insiders.

[4] http://www.utwente.nl/icts/bezoekers_derden/thuisaansluitingen/ex_medewerkers/, accessed December 9th, 2010

In the Table 3 below, the accounts are shown with the number of account active on May 31st, 2010.

Insiders		
Group	**Account**	**Active accounts** (31-05-2010)
Students	s-accounts	10356 accounts
Employees	m-accounts	4239 accounts
External insiders		
Third-parties	d-accounts	1038 accounts
Guests (active for one week)	t-accounts	62
Eduroam	Eduroam account	Unknown
Saxion	Saxion account	Unknown

Table 3: Overview of active accounts (gathered on 31-05-2010)

Other users than those in the tables above should have no access to the facilities and are therefore considered to be *outsiders*.

3.2 Risk management

This section will look at the risk management process at the University of Twente. In addition to the analysis of risk, this section will look at the possible sources of the risks in terms of the (network) connections used and the possible impact of the risks. Information on the connections used or the impact will help to decide upon the treatment of the risks.

3.2.1 Risk analysis

Risk management has the task of assessing the risks and deciding how to treat these risks. While this process is recognized at the University of Twente as an important process for information security, the risks for the university have not yet been assessed. In addition, the impact of risks depends on the information involved and which information security attributes were compromised. However, there is no overview of the information which is present at the University of Twente and therefore no estimation of the impact should incidents happen to this information.

3.2.2 Types of connections at the University of Twente

The University of Twente provides workstations (or notebooks) for their employees. These computers are managed by the University of Twente, although the employee may have administrator privileges on these computers. In addition, employees can introduce private notebooks on the network. The University of Twente also has student homes located on the campus which introduce more private computers to the network of the university. While there still are some workstation (managed by the university) meant for students, the number is decreasing. At the same time, the number of studies which require the student to use a private notebook is increasing. To work from a location outside of the university the University of Twente has VPN facilities. This shows that there are many ways for users to access the facilities and the IT department only manages a small part of it. In many cases, information security thus relies on the individual user instead of the university.

Later, it will be shown that the type of connection used influences the impact of the incidents that have occurred at the University of Twente, therefore a complete overview of the connections that (end)users use to access the facilities is:

- WLAN
- VPN,
- Campusnet
- Faculties
- Other

There workstations (or notebooks) for employees are grouped within the category of *faculties*. There are also workstations at student homes. *Campusnet* is the term for computers registered at student homes or other private notebook using the cabled network. Notebooks using the wireless connection are grouped as *WLAN* and computers at home connecting through the VPN network are grouped as *VPN*. Lastly, there is the group of others of any connection that could not be traced back to one of the other sources.

3.2.3 Impact of risks

The University of Twente, as described in the information security policy of the University of Twente (UT, 2010), has chosen the information security attributes of *confidentiality, integrity* and availability. Violation of these attributes can have a number of consequences which can be both tangible and intangible in nature. According to the assistant information manager of the University of Twente, the tangible impact of incidents would be the most useful for the university at the present time.

The incidents in information security will usually not cause direct material damage, although the eCSIRT framework as mentioned in 2.4, does recognize *sabotage* as an incident type. But even when a physical machine or the digital information (e.g. by a virus) is damaged, the University of Twente can recover from the incidents. New machines can be installed and the information (on the servers) can be recovered from the backups which are made regularly, but recovery takes times. This ‘time’ factors work on the impact of incidents in two ways: 1) ICTS employees spend time on resolving the incidents and 2) during that time a user may not be able to use his or her computers, becoming impaired in his or her daily work. While this impairment can be categorized as ‘lost revenue’ on terms of NIST SP800-30, but the ISO standard on risk (ISO/IEC, 2008) may have a clearer description: “impairment of business performance”. Using this term, the tangible costs for the University of Twente can be summarized as:

- Impairment of business performance.
- Cost of repair

Other, intangible, impact types that can be associated with the goals of the information security policy of the University of Twente (UT, 2010) are:

- Violation of legislation and/or regulation
- Loss of goodwill/negative effect on reputation
- Breach associated with personal information
- Breach of confidentiality

The (intangible) costs of the impact types depend on various factors among which the exact information which has been compromised. Without a complete overview of information present at the university, it is virtually impossible to determine in the associated impact with these types.

Without a risk analysis, it is hard to determine the impact of the risks. What can be done is, look at the previous incidents and based on those incidents determine the impact those incidents have had on the University of Twente. As this impact depends on the incidents which have been seen and how they were resolved by information security incident management, the impact will be discussed at the section on incident management at the University of Twente (section 3.4).

3.3 Information security controls

As an information security control, the University of Twente has an information security policy. In addition, there are a number of policies and documents which have been derived from the information security policy:

- Detailed security policies regarding:
    - The introduction and removal of hardware and software at the University of Twente
    - ICT-account
    - Security domains
    - Network security
    - Server security
    - Workstation security
    - E-mail security
- Code of conduct for employees.

Normally, it can be expected that the information security policy is created based on an information policy; the information policy describing which goals the university has in terms of information and the information security policy describing how that is going mitigate the risks. While the University of Twente has an Information and ICT plan (UT, 2008), this document described the goals for the University of Twente regarding ICT projects rather than information. Therefore the information security policy has no link to the risks to the University of Twente.

While the information security policy should be derived from a risk analysis and treatment and there should be a link to the information policy, not all is lost. In information security there are many best practices regarding controls; for example introducing password protection and network segmentation. In his book, Stefanek (2002) describes 205 best practices in information security. By applying these best practice controls many incidents in information security will be prevented, even without an information security policy or a risk analysis. The disadvantage of applying best practices without a risk analysis is that an organisation will be performing information security without guidance which practices are necessary.

The controls in information security were, in section 2.1, described as technical, organisation or human related. In addition to the organisational controls mentioned earlier there are several controls, which include:

- Virus scanners on workstations and network drives
- Standard policies on workstations
- Virus and spam detection on the e-mail facilities
- 'Honeypots' to detect malicious behaviour in the network
- Central firewall between the network of the university and the rest of the world

Many of the connections in the network, however, are privately managed and virus scanners and policies need to be managed by the individual user. To increase the chance of the individual user to adhere to the policies and manage facilities like a virus scanner there may be human controls in the form of education, training or raising awareness. At the University of Twente two information security awareness campaigns have been executed as a form of human controls.

3.4 Information security incidents management

Information security incident management has the task of resolving incidents, but also reporting the frequency and impact of the incidents to risk management. This section will shortly look at how the incident are detected and resolved as well as the incidents that have taken place in the recent past. After that the impact of these incidents will be determined based on the resolution process.

3.4.1 Incident detection and resolution

Before incidents can be resolved, they need to be detected. This detection is done in the form of complaints of possible incidents being received by the IT department of the University of Twente. Most of these complaints originate from *outsiders*, reporting that they are receiving spam from computers within our network, experiences some form of attack or seeing copyrighted material being distributed though our network. From there the incidents are processed which involved the information security team of the University of Twente (CERT-UT) and possibly a local support group of 'workstation support'. The CERT-UT team will trace the source of the malicious behaviour to the individual computer and registered owner of the computer. Depending on the type of incident, actions may be taken to stop further abuse and/or notify members of the 'workstation support' group to take on-site actions, like helping the user to solve the incident or to re-install the computer.

By request of the information management department, reports about information security incidents should follow the eCSIRT framework for incident reporting. This framework will thus be used in this thesis. The eCSIRT framework distinguishes between general incident classes and more detailed incident types. The incidents are currently reported on the level of incident class. At high level, the eCSIRT framework recognizes the following incident classes:

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusions

- Availability
- Information Security
- Fraud

In cases of a computer within the network of the University of Twente is involved in incidents regarding abusive content, malicious code or intrusion attempts, then the computer is exhibiting unwanted behaviour to other computers inside or outside of the network of the University of Twente. To prevent further breaches of information security, these computers are (remotely) disconnected from the public network. While this prevents further abuse, this also prevents the user from being able to use the computer and limits his or her ability to perform their duties. The 'workstation support' group is notified to resolve these incidents as quickly as possible.

It can also happen that the personal account data of a user is compromised. Should this be detected, the account is blocked and 'workstation support' group is notified to help the user to reset the account data. The University of Twente is experiencing many cases of fraud, more specifically the distribution of copyrighted material. These complaints are registered and the 'workstation support' group is notified to stop this behaviour in cooperation with the user. While cases of fraud are information security incidents, they do not endanger further comprise of information so no immediate actions are taken to terminate the connection of the computer.

The task of the CERT-UT team is thus to analyse the incidents, prevent further compromise of information security and distribute the cases to the correct support group for resolution.

3.4.2 Information security incidents at the University of Twente

To assess the status of information security at the University of Twente, this section will take a look at the past incidents at the University of Twente. While there are a number of quarterly reports on the incidents, these reports only include the number of incidents that have occurred with a certain incident class (as given in section 3.4.1). To get more detailed information it was important to investigate the incidents in relation to the users and connection types, therefore all incidents were re-investigated.

The main source of information is an application called "Application for Incident Response Teams". This application contains all incidents received by the ICTS department, including information on the incident, the computer and the user involved. The "Application for Incident Response Teams" only contains information on complaints which have been received by the ICTS department and excludes any data by the technical controls. However, the technical controls are preventing incidents. The risks associated with those incidents are already covered. The data on actual incidents, the information in the AIRT system, is expected to be a good source of information to find the risks which currently are not covered by the information security controls and are thus still a risk to the University of Twente.

3.4.2.1 Information gathering process

In order to get a good overview of the incidents that occur at the University of Twente, statistical data is needed over an extended period of time. First of all, daily processing of the incidents by the CERT-UT team has shown the number of incidents fluctuate over time, both in terms of total number of incidents and the type of incident most common at a certain time. Secondly, it is important to look at the recent incidents as these incidents show where current security measures, technical or otherwise, are lacking in effectiveness.

To capture the mentioned fluctuations and the recent developments, a period of a year seemed the minimum. The entire year of 2009 was chosen, extended with the first quarter of 2010. This provided a 15 month period. In some cases a comparison based on a year is used; in those cases the incidents of the 15 month period were normalized to a period of 12 month.

In the period of January 2009 till March 2010, a total of 1606 incident were registered. These incidents were examined in terms of type of incidents, connection type used, and threat agent involved. During this examination, it was found that 3 incidents did not contain any information and 1 incident was indicated as being a test of the incident creation process. These 4 incidents were thus excluded. On the other hand it was found that 2 incidents (concerning successful social engineering attacks) contained information on multiple accounts that were compromised. Based on the incident information, 1 incident was split into 2 separate incidents, and 1 incident into 4 separate incidents. Therefore the total number of incidents included in the analysis is 1606. The following sections, 3.4.2.2 and 3.4.2.3, will first present the factual results (overall and in relation to connection type). In section 0 these results will be discussed.

3.4.2.2 Results

The 1606 incidents collected between January 2009 and March 2010 were grouped by incident type and date when the complaint was processed. Results in Table 4 show the overall distribution of incident as well as the distribution over the different months. In the following section the incidents are discussed based on overall statistics and in relation to connection type and threat agent.

The majority of incidents (1004 of 1606) concern fraud (see Table 4). The class abusive content had 254 complaints and malicious code has 276 complaints. The remaining 72 incidents are spread over the categories of information gathering, intrusion attempts, availability or other.

The summer holiday months at the University of Twente, July and August, contain relatively few complaints: 57 and 45 complaints respectively. The months after these summer holidays saw an increased number of complaints, ranging between 143 and 170. Further analysis shows that the complaints about fraud stand out. Possibly this is caused by the arrival of new users, but this remain speculations as the incidents are not investigated to that level of detail.

Table 4 also shows that there are no registered cases of intrusions or information security. This however does not mean that these cases do not occur, but it means that these categories are either not monitored or not reported currently. As these categories contain no reported incidents, they are excluded from the tables concerning incidents beyond Table 6.

Year	Month	Total	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Intrusions	Availability	Information Security	Fraud	Other
2009	January	71	8	7	0	1	0	0	0	54	1
2009	February	89	8	18	1	2	0	0	0	60	0
2009	March	93	16	21	0	6	0	0	0	50	0
2009	April	93	29	19	0	5	0	0	0	39	1
2009	May	108	14	13	0	1	0	0	0	80	0
2009	June	99	18	8	0	0	0	0	0	73	0
2009	July	57	14	7	2	0	0	0	0	33	1
2009	August	45	9	5	1	1	0	0	0	29	0
2009	September	156	22	11	5	0	0	0	0	118	0
2009	October	170	28	27	0	3	0	0	0	107	5
2009	November	155	10	29	0	2	0	0	0	108	6
2009	December	143	9	38	0	3	0	0	0	89	4
2010	January	116	21	19	0	2	0	1	0	68	5
2010	February	118	29	28	2	1	0	0	0	52	6
2010	March	93	19	26	0	3	0	0	0	44	1
	Total	1606	254	276	11	30	0	1	0	1004	30

Table 4: Overview of incidents per month

	Total	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Intrusions	Availability	Information Security	Fraud	Other
Student	1152	165	173	5	12	0	0	0	778	19
Employee	306	66	69	3	9	0	0	0	151	8
Third-parties	67	5	18	0	0	0	0	0	43	1
Guests	3	0	3	0	0	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0	0	0	0
Saxion	7	0	0	0	0	0	0	0	7	0
Unknown	74	18	16	3	9	0	1	0	25	2
Total	1606	254	276	11	30	0	1	0	1004	30

Table 5: Overview of incidents in relation to threat agents

	Total	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Intrusions	Availability	Information Security	Fraud	Other
WLAN	591	87	63	0	1	0	0	0	440	0
VPN	284	29	31	0	3	0	0	0	221	0
Campusnet	458	74	98	0	10	0	0	0	261	15
Faculties	195	39	68	0	8	0	0	0	69	11
Other	78	25	16	11	8	0	1	0	13	4
Total	1606	254	276	11	30	0	1	0	1004	30

Table 6: Overview of incidents in relation to computer registration

3.4.2.3 Incidents in relation to threat agents

In order to further understand the numbers the incidents were investigated for the threat agent involved and for the connection involved in the incidents. The possible threat agents were classified as: Student, Saxion, Employee, Other or Unknown. This classification is based on the threat agents identified earlier. While most incidents could be positively traced back to a user, given the current tools, in some cases the threat agent remains unknown. In some of these cases, the complaints concerned the faculty ITC which recently joined the university. These connections are registered at the University of Twente, but ICTS currently has no user information. In these and other cases in which the incident could not be traced to an individual user, the threat agent was designated as 'unknown'.

As the figures in Table 5 show, the majority of incidents can be traces back to students as they are involved in 1152 out of the 1606 incidents and an additional 7 caused by Saxion students. Employees were involved in 306 of the reported incidents. The remaining incidents are either caused by third-parties (88 incidents) or could not be traced back to a user (53 incidents).

3.4.2.4 Incidents in relation to computer registration

Besides the threat agent, it also useful to know what kind of computer registration is involved in the incident. This information can give some insight into the question who is responsible for the security on that computer. If university computers are involved, this can mean that people are deliberately circumventing security measures, while if more privately owned computer are involved it may indicate a lack of security due to lack of knowledge on the subject.

The division was made between connections through the wireless network (WLAN): which can concern both private and university notebook-computers, virtual private network (VPN): computers at home, Campusnet: private computers of students and employees registered at the university, the workstations within faculties of the University of Twente or 'other': collection of other connections, e.g. student associations, (e-mail) servers or ADSL connections.

The results of this division can be found in Table 6. The majority of incidents is introduced by computers using a wireless network connection (591 incidents) followed by Campusnet (private computers registered at the university) with 458 incidents. The number of incidents concerning home computers connected via a VPN connection is 283. The workstations within the faculties are involved in 197 incidents, and the group of other connections contains 77 incidents.

3.4.2.5 Discussion of incident statistics

When looking at the tables on the incidents, it can be concluded that:

1. Students are involved in 1152 incidents (71% of total)
2. Employees are involved in 306 incidents (19% of total)
3. There are 1004 ‘Fraud’ related incidents (62% of total), followed by malicious code (17% of total) and Abusive content (16% of total)
4. The majority of incidents is caused by (private) notebooks (591 incidents) and private computers (Campusnet; 458 incidents)

Most incidents occur within the categories of fraud, malicious code and abusive content. These categories, in the eCSIRT framework, are high level incident classes. When examining these incident classes in more detail, the class of fraud can consist of incidents of ‘unauthorized use of resources’, ‘copyright’ or ‘masquerade’. At the University of Twente, the registered incidents only consist of copyright incidents. The class of ‘malicious code’ contain various types of viruses. The incident registration did however not distinguish between different kinds of viruses. During interviews with the employees of the groups of ‘workstation support’ it was discovered that the type of incident was often not investigated and that, even if a virus was successfully identified and cleaned the type of virus is not registered. Therefore, it is not possible to distinguish further between these types.

Lastly, the class of abusive content can contain incidents of ‘spam’, ‘harassment’ or a group ‘Child/Sexual/Violence/...’. At the University of Twente, these incidents only concern ‘spam’ and while investigating these message it was discovered that these messages were not consciously send by the user, but some kind of virus installed on the computer was generating these messages.

As mentioned in section 3.4.2, incident management has produced a number of quarterly reports using the statistics as presented in Table 4, without relation to connection type of user involved. These reports are reported to management to adjust the policies if necessary. When looking solely at the number of incidents, the incident type of fraud (more specifically copyright) would be the largest problem at the University of Twente. Risk, as explained in section 2.2, is a combination of likelihood and impact. Without looking at the impact of these incident, it cannot be stated whether these incidents indicate whether the University of Twente should truly focus on the fraud or on other incidents. Therefore, this thesis will take a look at the impact of incidents at the University of Twente.

3.4.3 Impact of incidents

In section 3.2.3, it was stated that the tangible impact of incidents is currently of most interest to the university. These costs which can be calculated were identified as:

- Cost of repair
- Impairment of business performance.

It was stated in section 3.2.3 that the main factor determining these costs is 'time'. When an incident need to be resolved, the CERT-UT team and possibly the workstation support group come into action and depending on the actions necessary to resolve the incident, the user involved in the incident might be impair in performing their normal duties. The time of impairment would in that case be equal to the time needed by workstation support to resolve the incident. The impact could thus be further defined as:

Financial costs of repair

- Time spent on incident processing by CERT-UT
- Time spent on incident resolution by 'Workstation Support'

Impairment of business performance by the users

- Time spend on incident resolution by 'Workstation Support'

To quantify the costs, information is needed on the incident processing and the resolution of the incident. The CERT-UT team had documented procedures on the incident processing, which allows for identification of the steps involved. Detailed information regarding time spend on the steps involved was gathered by questioning the CERT-UT team members.

No such documents were available regarding the incident resolution. To gather information on the activities involved and their costs, interviews were held with the four 'workstation support' groups. In addition, the two helpdesks at the University of Twente (ICTS Service desk and Notebook service centre) were questioned regarding their involvement in the incidents that are occurring. The ICTS service desk stated that they receive numerous questions about phishing e-mail, almost every day, but these usually go unregistered. Other than the question about phishing e-mails, they are not significantly involved in the resolution process. Every once in a while, the notebook service centre might receive a request of a student to install a new image on their notebook, but usually students re-install their notebook themselves. The notebooks service centre is thus not significantly involved in resolving incidents.

The complete impact analysis can be found in Appendix B. During this impact analysis is was found that the time needed by the CERT-UT depends on the connection type involved rather that the type of users, while with the time needed by workstation support this was the other way around. The resulting tables

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
WLAN	5	5	7	5	9	4	4
VPN	4	4	6	4	8	3	3
Campusnet	3	3	5	3	7	2	2
Faculties	3	3	5	3	7	2	2

Table 7: Time needed (in minutes) by CERT-UT per incident

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Students	0	0	0	0	0	0	0
Employees	240	240	10	240	10	10	10
Third-parties	0	0	0	0	0	0	0
Guests	0	0	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0
Saxion	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

Table 8: Resolution time (in minutes) of workstation support in relation to incident type and type of user

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Students	0	0	0	0	0	0	0
Employees	240	240	10	240	0	0	0
Third-parties	0	0	0	0	0	0	0
Guests	0	0	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0
Saxion	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

Table 9: Impairment of business performance for a user (in minutes)

As Table 7 depends on the type of connection (in relation to incident type) and Table 8 and Table 9 depend on the type of user (in relation to incident type) a combined table would be a three-dimensional table.

With the use of Microsoft Excel, one table was generated per type of user and within these tables the type of connection was related to the type on incident. These resulting 7 tables could each be combined with the correct value in Table 7, Table 8 or Table 9 and subsequently recombined into a single table giving the total impact of incidents in relation to the user group over a period of 15 month. To show the impact of incident over a year these results were normalised to the period of a year. The results are shown in Table 10 below

	Total	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Student	6285,6	529,6	524,8	20	54,4	0	5126,4	30,4
Employee	46928	19389,6	23596,8	60	2728,8	0	1076	76,8
Third-party	295,2	13,6	36	0	0	0	244	1,6
Guest	12	0	12	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0	0
Saxion	47,2	0	0	0	0	0	47,2	0
Unknown	228,8	47,2	42,4	12	48	2,4	73,6	3,2
Total	53796,8	19980	24212	92	2831,2	2,4	6567,2	112

Table 10: Total time lost due to information security incidents at the University of Twente per year

3.4.4 Benefits of the impact analysis

While the impact analysis was, due to lack of an overall risk analysis, limited to the resolution process, the previous section shows the importance of this risk analysis. By combining the incident statistics with the impact, section 0 shows that the incident causing the most impact at the University of Twente are the virus incidents of employees and the incidents concerning abusive content of employees which, as mentioned in section 0, also concern viruses. The reason for the high impact is because these incidents require an employee of workstation support to re-install the computer; during which time the user is likely unable to perform his or her duties. The hours of both the user and the employee of workstation support are paid by the university.

With students, the hours needed to re-install their computer are not paid by the university and because a student is usually more flexible regarding 'working hours', the impact of the virus related incidents is likely minimal. The amount of time needed to resolve incidents of the type of 'fraud' of students not necessarily negligible, but compared to an overall impact of nearly 54.000 minutes, these incidents should not be the first priority of the University of Twente.

3.5 Analyse and adjust

The fourth phase of the model in section 2.1, concerns analysing the incidents and adjusting the controls or risk management process is necessary. While the incidents are not investigated thoroughly in regards of impact, vulnerability or threat involved, it can be said that a start has been made to report the frequency of the incidents. With the security policy having being officially accepted, and the implementation and enforcement just starting, it is too early to see whether the feedback process will result in changes in the policies. The feedback process has however been implemented.

Although the causes are not investigated per incident, the groups of workstation support do see a general trend. That trend is that users awareness, especially regarding phishing e-mail, e-mail containing viruses and (un)safe browsing on the internet, as perceived as low and a major cause contributing to the incidents. The support of 'Ravelijn' and 'Horst' both mentioned that a rather large portion of users write down password which can be found under their keyboard or even as a post-it attached to their monitor. They also mentioned that a lot of users do not lock their workstation while away from the computer and they regard this as a potential security hazard.

Most interesting regarding awareness however is that they stated that 'they expected better from users at a university'. While there are a lot of users at the university, with different computer background, the low-skilled (and lower educated) administrative staff is not regarded as a severe problem. Should they receive an e-mail asking for their account or contained a dubious attachment, they often 'panic and ask for help'. It is perceived that the higher-educated do not ask for this help and are more prone to fall victim to such e-mail, viruses and such.

3.6 Summary

Information security can, as shown in chapter 0, understood in terms of a cyclical process including risk management, information security controls, information security incidents management, and analysing and adjusting to the incidents. In this chapter, chapter 0, these various processes were described in relation to the University of Twente and it was found that the extent to which these processes are incorporated in the University of Twente is limited.

The first process, Risk management, includes the assessment of risks and deciding upon the treatment of these risks. As the risk management process is described in the information security policy, the University of Twente recognizes the need for risk management. However, the process has not yet been performed and therefore is can be concluded that this process is absent.

When looking at Information security controls, it was found that there should be organisational, technical and human controls and that one important organisational control is the information security policy. Overall, is can be said that, at the University of Twente, all these elements are present. The only negative point might be that the information security should the linking pin between organisational goals and the (other) information security controls. These controls should be aimed at reducing risks to the organisation goals and without a risk analysis it seems like a crucial role of the information security policy cannot be fulfilled. In defence of the information security policy and information security controls, it must be said that there are many best practices in the area of information security. While the information security policy or controls have not been compared to the best practices available on these areas, the lack of a risk analysis does not necessarily mean these controls wrong. Should the risk management process be executed at the University of Twente, the information security policies and controls may need to be revised.

Information security incident management should, besides incident resolution, include investigating the incidents in terms of impact, vulnerability and threat and make sure the impact and frequency are reported in order to check these against the expected risks. While the frequency of incidents is currently being reported, this chapter showed that the impact of these incidents can show a very different overview and is thus very important in order to make accurate decision on these incidents. Calculating the impact of incidents is a process which is currently not yet performed at the University of Twente. In addition, it was found that the incidents are not investigated in terms of vulnerability or threat. Even if the impact or frequency would show that additional controls might be requires; without information on the vulnerabilities or threat the controls cannot be adjusted.

The fourth phase in the cycle was 'analyse and adjust'. While there is a periodical feedback between information security incident management and management of the University of Twente, currently only the frequency of incident can be reported. As shown in section 3.4.4 this information alone is not enough to make accurate decision to revise the policies. In addition, the vulnerabilities and threat are not investigated at the University of Twente and therefore cannot be analysed or acted upon.

The extent to which processes are present at the University of Twente can also be visually represented. Figure 5 below represent this in the same way the conceptual model was represented in chapter 2.1.

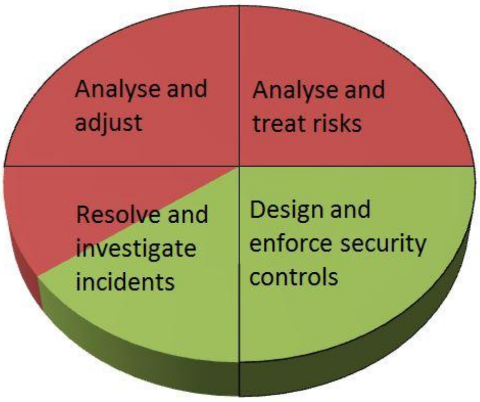

Analyse and adjust
Analyse and treat risks
Resolve and investigate incidents
Design and enforce security controls

Figure 5: Information security processes at the University of Twente

The green areas represent (parts of) the processes which are present, while the red areas represent processes which are not present. It clearly shows that, while more operational sides like security controls and incidents resolution are present, more can be done in the areas of planning (risk management) and feedback (analyse and adjust). However, before drawing further conclusions, this thesis will first look at these aspects at other universities in the Netherlands.

4 Information security at four universities in the Netherlands

When investigating the status of information security at the University, it quickly became clear that, when compared to literature, improvements are possible at the University of Twente. Information security is however a 'problem' facing many organisation. SURFnet, the federation providing the internet connections to educational institutions in the Netherlands, regularly organises meetings for participating institution on the subject of information security. Other universities in the Netherlands are thus facing the same problems as the University of Twente. The question is then how are they dealing with these problems and have they found solutions which the University of Twente, as a comparable institution, could adopt. Therefore the status of information security at a number of other universities in the Netherlands will be investigated in this chapter. To this end, four Dutch universities were chosen: Technical University Eindhoven, Technical University Delft, the Open University and Wageningen University & Research.

The goal for this chapter is to investigate the status of information security at these institutions. Therefore this chapter will first describe these universities and their population, followed by the setup of the interview. The results of the interviews will be presented in the categories as the conceptual model (Risk management, information security controls, information security incident management and analyse and adjust) to facilitate comparison. The next chapter will investigate how the University of Twente can improve its information security processes.

4.1 The universities

The universities of Eindhoven and Delft are technical universities while Wageningen and the Open University are not considered technical universities. The technical universities were chosen because their situation is comparable to the University of Twente and might thus experience similar events regarding information security. The two other universities were deliberately chosen to be less comparable to the University of Twente to look beyond the technical universities. The University of Twente used to be a technical university and while many technical studies are still given at the University of Twente, there are also several non-technical studies at the University of Twente. The focus of Wageningen is more in the agricultural and environmental studies. The Open University is an institution for remote learning. Their student population consist mainly of student following smaller courses. The students participate part-time in these courses besides e.g. their daily work. Because of the 'remote' learning part, which places more emphasis on information being available everywhere all the time, is expected to have a great influence on information security.

Within all of these institutions, the information security manager was interviewed. They all had a coordinating role regarding information security with internal and external parties and a role a policy advisor in the area of information security.

To gain understanding of the specific situation at each university, the human factors at these institutions have been examined. Besides students and employees, all institutions have facilities for guests to access or use the network. Within all institutions, a distinction is made between short term and longer term guests. The exact during of short or long term guests stay varies between institutions, but the underlying idea of the different user accounts is similar to the University of Twente: a short term account should be active immediately and only last a short time (a number of days). The longer term accounts require registration of the user but can also be active over a longer period. An overview of active accounts is shown in Table 11 below. While the University of Twente has already been discussed in the previous chapter, for reference purposes the University of Twente has been included in the tables throughout this chapter.

	Type of studies	Number of student accounts	Number of employee accounts	Other accounts
University of Twente	Varied	10356	4239	1038 third-party accounts, 62 guest accounts
TU Eindhoven	Technical	7000	3000	Short and long term accounts
Wageningen U&R	Varied	8500	5000**	6500 guest accounts
TU Delft	Technical	16000	6000	Short and long term accounts
Open University	Varied	26000*	750*	Guests, federation members

* The Open University is an institution for remote learning at which student are usually participating part-time in short courses. Therefore they have a large student base which they can still maintain with very few employees.

** Wageningen U&R has a relatively high number of employees due to large research branch at Wageningen

Table 11: Users and studies at the interviewed universities

The open university, in addition to guests, make special note in their information security policy of ‘federation members’; a group of users which is allowed to user certain facilities as member of a cooperating institution. In additional, all universities provide the Eduroam wireless network whereby users of cooperating educational institutions can easily access the wireless network at all connected institutions. In terms of this research, both the federation members and the Eduroam users can be considered external insiders.

4.2 Interview setup

Based on the fact that there were regular meetings regarding information security among universities in the Netherlands, the interviews were created with the idea in mind that all universities would be experiencing information security incidents. There was also the expectation that not all universities might have accurate reports on the number of incidents or might be able to generate those for the interview. The goal of the interview was to assess whether the universities were experiencing incidents, which types of incidents they experienced and in which environment (e.g. users, connections and controls) these incidents took place.

The areas of attention as given in the conceptual model (section 2.1) were used a base for the interviews. The contents of the interview can be divided over 7 subjects:

- The university
- The types of connections within the network
- The (managed) workstations within the university
- The incidents
- Incident management
- Policies

- Risk analysis

From these subjects a checklist was generated with key topics to discuss. These key topics ensured on the one hand that the same topics were discussed among all interviews, while not being restricted to specific questions. The interview thus followed a semi-structured setup and while the interview on high level are comparable, there was a large deal of flexibility regarding the exact detail in which certain topic were discussed. The results of the interviews will be discussed in the following sections.

4.3 Risk management

While at the University of Twente no risk analysis has been performed, there were aspects which could be described. These were the connections from which the threats originate and the possible impact analysis. For the interviewed universities these same subjects will be discussed.

4.3.1 Risk analysis

The University of Twente has not yet performed a risk analysis. In the interview the subject was (supposed) to receive additional attention to investigate the practices at the other universities and learn from those practices. The conclusion of this subject of the interview is that none of the interviewed universities performed a (periodical) risk analysis.

With regards to the servers of the various institutions it can be said that at time of installation the risks for the system were examined, these were however not collected centrally or updated throughout the lifecycle of the system. The Open University reported that they used to investigate the threats to the systems in use by means of the Secunia service for organization. This is a commercial service which collects information on vulnerabilities in applications and filters out the relevant messages for the customers. This service was provided collectively through the SURFnet federation, but this federation ceased providing this service.

Regarding an overview of the information presents within the universities, they all report that there is no real overview. Usually there is however partial knowledge in the heads of the administrators, but this knowledge is mainly focused on the servers these administrators manage than possible information the end-users have.

4.3.2 Types of connections within the network

The types of computers connection to the network at the University of Twente were determined to constitute of:

- WLAN
- VPN
- Campusnet
- Faculties

The computers within the faculties were mainly managed computers for employees, but there were several managed workstations for students as well. These connections can all be found at the interviewed universities with 2 exceptions:

The TU Eindhoven does not have managed workstations for students. This is possible because they have been very active in the notebook project, providing notebooks to the students are a reduced price. This practice and its implications will be discussed further in the section on information security controls (section 0).

The other exception is the Open University. As an institution for remote learning they do not have private computers of students connected directly to the network. The other universities, while not having student homes in a campus setting, do have student homes directly connected to the network of the university.

4.3.3 Impact of risks

As with the risks, and similarly to the University of Twente, all interviewed universities reported that the impact of risks nor of incidents is being not quantified at the universities.

4.4 Information security controls

As information security is a subject all universities are dealing with, all universities have various technical controls in place like firewalls or virus scanners. Without a risk analysis, the controls can be seen as best practice methods of dealing with risks. While the information security policy will be discussed in the next section, all universities reported that they are addressing awareness by means of campaigns; either by using the material provided by SURFnet or with material developed by the university itself.

4.4.1 Information security policy

In section 2.3, the information security policy was given as an important control for information security. As Table 12 however shows, not all universities have such a policy.

	Information security policy	**Goal of information security**	**Objects subject to the policy**
University of Twente	Available	Confidentiality, Integrity, Availability	Information in digital form
TU Eindhoven	Not available	-	-
Wageningen U&R	Not available	-	-
TU Delft	Available	Confidentiality, Integrity, Availability Priority: Ensure business continuity	Information in digital form Physical security of servers Clear desk policy
Open University	Available	Confidentiality, Integrity, Availability Priority: Ensure Availability	Information in all forms, but primarily information in digital form as this is the main source

Table 12: Policies at the interviewed universities

The universities that do have an information security policy, the Open University and the TU Delft, focus on the information security attributes of confidentiality, integrity and availability. This is not surprising at these attributes are considered the basic security attributes and the policies state that they are based on the ISO/IEC 27000 standards.

While the goal of the information security policy at Delft is to ensure information security of digital information, the security is extended beyond the digital borders and includes the physical security of servers as well as policies regarding the desks of employees. The Open University recognizes that there are many forms in which information can exist, although their main focus is on digital information as this is usually the primary form.

While the TU Eindhoven does not have an information security policy, they have a contingency plan and a continuity plan in case of emergencies. In addition, a yearly (external) audit is performed on the available ICT and the procedures.

Wageningen U&R has network rules (user guidelines), and ICT security plan and an ICT calamity plan. The TU Delft, besides the information security policy, has an ICT calamity plan.

While some universities might thus not have an explicit information security policy, there are plans to cope with emergencies and ensure availability.

4.4.2 Approach to information security

While the TU Delft did not mention any special way they treat incidents or a special focus for point of control, Wageningen U&R explained that they have a ‘zero tolerance’ method for dealing with incidents. Even incidents that, at the University of Twente, are regarded as relatively minor, the copyright incidents, they treat with disconnecting the internet connection. The goal is that the user in the future will think twice before exhibiting the same behaviour. The rationale behind this is to ensure availability to the users. Incidents like copyright complaints are reported by American institutions representing the owners of the content involved. They regard the behaviour of downloading copyrighted material as illegal, while the Dutch government is more lenient is that regards. As they however regard it as illegal, it would be possible for American institution to start erecting block-lists preventing access to American website. Should this occur and Wageningen be put on this list, the university and its large staff of researchers would be unable to cooperate with American counterparts.

In sheer contrast with this approach of immediately blocking off every incident, the TU Eindhoven tries to contact the owner of the computer in question first and schedule a time for resolution. While they try to resolve the incidents as soon as possible, their rationale is that an employee could be finishing a paper for a conference or a student busy making an exam. An while incidents need to be resolved quickly, it can often wait an hour or two.

Another difference that may be observed is the focus of the point of control. The TU Eindhoven reported that they focus on end-point security. The rationale is that if every node in the network is secure, then so is the network. While this can easily be achieved for the computer that are managed by the university, this is more difficult to achieve for private computers; especially as the TU Eindhoven expects students to have a notebook and does not provide managed workstations for students. More on how they deal with this will be discussed in the next section on notebooks.

In contrast to this way of protecting the network is the Open University. They focus they protection on the middle layer: the network. As they do not have any form of control over many of the endpoints and every connection needs to pass through the network layer, this is a logical choice.

4.4.3 Notable practices

When investigating information security practices among the universities, several practices were found when stood out. One such practice is how the TU Eindhoven approaches information security regarding notebooks. In two other cases practices were found in which different universities try to deal with security in opposing ways. These concern administrator rights and authentication methods for wireless LAN or VPN.

4.4.3.1 Notebooks

As seen with the incidents at the University of Twente, many of the incidents concern notebooks. As the TU Eindhoven expects every student to have a notebooks, the way they dealt with this security was of special interest to this thesis and the interview showed that there was indeed special attention to notebooks.

Since 1997, the TU Eindhoven has been an active participant of the 'notebook project' which facilitates affordable notebooks for students. They even participated to the extent that every student should have a notebook for the studies. The University of Twente became active later in the project and the same trend is showing there.

The difference is in how the universities try to deal with security. 'Try to' because their influence is limited as the notebooks bought by the students are of course the legal property of the students. Notebooks bought through the University of Twente are delivered straight to the students. The University of Twente has a website from which students can download licensed security software and study-specific software. Students can access introduce the notebooks on the university network by means of their ICT account without any intervention of the University of Twente. In summary, the University of Twente enables the possibility for students to purchase an affordable notebook but does not (have to) intervene in the rest of the process.

At the TU Eindhoven, this is organised differently. The notebooks are not delivered to the students, but to the university. The university (re)installs the notebooks with an installation image containing the most recent operating system, security software and study-specific software. They can also set the software to update automatically. As the notebooks are the legal property of the students, the students can change all of this later on. The main difference is that, when the student receives the notebook the installation is security while at the University of Twente the installation is insecure.

As notebooks are, by now, quite affordable at your local store, the TU Eindhoven also needs to deal with privately purchased notebooks. Here, the TU Eindhoven can exert influence because the notebooks cannot be used automatically within the university network but has to be registered first by the ICT Service Desk. When a student comes in with such a notebook, the ICT service desk check some basic requirements, like whether the operating system is up-to-date and a virus scanner is installed. In addition to checking basic requirements, this moment of contact have other benefits:

- Advice can be given on how to improve information security for the user
- It is known who owns which notebooks
- The moment of contact can be used to improve user awareness

While the TU Eindhoven is still in control of the notebooks connections at the university, they are detecting a trend that, due to decreasing prices, more notebooks are bought at local stores rather than through the notebook project. This means that they can exert less control over the notebooks, which is a trend they describe as ‘worrying’.

4.4.3.2 Client for VPN and wireless connections

All universities have VPN facilities and allow wireless connections to the network, although the TU Delft reports that the VPN facilities are used quite little. To allow access to the VPN facilities, the Open University requires users to authenticate via a special client. While this works fine on the windows operating system, the clients ceases to function every time the Mac operating system is updated. To facilitate ease of use, a project has been started to remove the need for a special client.

In contrast, at Wageningen U&R a project has been started to investigate the possibility to introduce a special client for VPN connections and possible the wireless connections. This client should, in addition to authenticating the client, check basic security settings.

This shows that the various universities are still searching which practices work for their institution.

4.4.3.3 Workstations within the universities

All universities provide, and manage, the workstations or notebooks for employees. With the exception of de TU Eindhoven also have managed workstations available for students. On the computers for students, the Windows operating system is installed and the user does not have administrator right. The universities in the area of administrator right to employees:

- TU Eindhoven grants every employee administrator right as certain printers, software, hardware or network facilities refuse to function properly without administrator rights.
- At the TU Delft, users are not given administrator rights as a standard, although these rights may be requested.
- Wageningen U&R does not grant administrator rights on workstations, but grants those right on notebooks. Notebooks need to function outside of the university and outside of the normal boundaries of control.
- At the Open University, employees are not given administrator rights. The Open University has an application catalogue, accessible via the web browser, which contains the application for which the Open University has bought licenses. The applications available to the user depend on the specific user (e.g. to which faculty the user belongs) and via this web interface the user can install the software.

This shows that, while all universities are looking at the exact same problem, they all solve it in a different way.

4.5 Incident management

The practices regarding incident handling are rather similar: all universities have an information security team (cert-team) which contains members from various parts of the IT department. In addition, there are often one or two additional people are involved with the day to day handling of the incidents. The resolution of the actual incident may usually include members of the IT support group.

4.5.1 Incidents

Every university is experiencing information security incidents and they commonly see copyright, phishing attempts or virus infections. In some cases more severe incidents are mentioned to occur once or twice a year. The incidents, the user groups involved and the connection types involved at the various universities are shown in Table 13 below.

	Type of incidents	Impact of incidents	User groups involved	Connection types involved
University of Twente	In order of frequency: 1) Copyright 2) Infected computers 3) Spam 4) Intrusion attempts 5) Phishing	Not quantified	Mostly students	Mostly wireless connections
TU Eindhoven	Mostly Phishing attempts	Not quantified	Mostly students	60% wireless, VPN or home computers 40% workstations
Wageningen U&R	Daily (multiple): Copyright Daily: Phishing attempts Weekly: Viruses Quarterly: Serious incidents like fraud	Not quantified	Mostly students	Mostly notebooks, followed by VPN and workstations at home
TU Delft	Mostly: 1) Copyright 2) Viruses	Not quantified	Mostly students	Not known
Open University	Overall, very little incidents. The incidents that occurred were mostly viruses	Not quantified	Employees	Workstation of the university or server of the university

Table 13: Incidents and the users involved

The tables show that phishing attempts, copyright complaints and viruses are seen at the universities and the majority of incidents involve students and wireless or other external connections. The exception is the Open University which has no student connections (directly) to the network. This user groups and types of connections are based on frequency of incidents. The impact of those incidents is not quantified at any university.

While the table above shown a rather comparable situation, there are some differences in how the incidents are registered and reported, as can be seen in Table 14.

	Incident information registered	**Incident information reported**	**Complaining party**	**(perceived) cause**
University of Twente	Incident, User information	Quarterly statistical: type of incidents that occurred	Mostly external	Human behaviour
TU Eindhoven	Incidents, User information, Forensic data, Underlying cause, Remedy	Periodical reports including underlying cause. Reports are used for policy adjustment	Mostly external	Human behaviour
Wageningen U&R	Unknown	Unknown	Mostly external	Human behaviour, people should be aware of what they are doing
TU Delft	Unknown	Periodical reports: incidents, password resets and other special cases	Mostly external	Human naivety, computer not up to date, visiting 'wrong' web sites.
Open University	Incident, User information, Resolution time, Cause (if known), Remedy	Yearly reports about the incidents and how they were solved.	Mostly internal	Improper management by administrators

Table 14: Incident registration and reporting

Regarding the information recorded, the TU Eindhoven stands out especially. Besides basic information about the incident and the user information necessary to resolve the incident, they also investigate the incident forensically as to how this incident occurred (technically), what the underlying cause was and how the incident was resolved. The University of Twente, by comparison, only registers incident information and user information. The Open University registers the resolution time and the cause, if known, in addition to incident and user information. At Wageningen U&R and TU Delft, incident and user information will certainly be registered. It is however unknown whether additional information is registered.

The TU Eindhoven also reported generating (detailed) reports based on the incident information and that these reports are an important input for the policies. For example, based on the incident information they found that the Windows 2000 operating system was involved in high number of incidents. It was therefore decided to speed up the process of replacing this operating system. Other universities also report periodically on the incidents that occur, also at Wageningen U&R. At Wageningen U&R it however unknown whether the report additional information besides the incidents that have occurred.

4.5.2 Awareness

As shown in Table 14, incidents are usually received from external parties and human behaviour is usually perceived the cause. Reponses were given that the users, being member of a university, are expected to know what they are doing and that the users are well aware that distributing copyrighted material is illegal. Viruses, in part, come from websites that users should not have to visit. In general it was stated that there is a good chance users known that they are performing dubious or illegal actions. Or at least that they *should* know.

As awareness is mentioned as an important factor in the incidents among the interviewed universities, chapter 0 will take more detailed look at user awareness at the University of Twente.

4.6 Analyse & adjust

While none of the interviewed universities are performing a risk analysis, the TU Eindhoven and the Open University reported that they investigated the incidents and recorded information security could be retrieved. The TU Eindhoven records the most information, identifying not only the vulnerability and threat involved, but also the underlying cause of which human related actions lead to the incident. The Open University does this for the most part, but did not report searching for the underlying cause. This information is used for decision to improve information security and prevent future incidents. It can thus be said that the TU Eindhoven and Open University are analysing incidents and adjusting information security based on the findings. At the TU Delft and Wageningen U&R these practices were not reported.

4.7 Summary

The four universities in the Netherlands were interviewed with the expectation in mind that they would experiencing information security incidents and that they would be performing information security to reduce the incidents or their impact. While this was found to be true, there were also remarkable conclusions:

- None of the interviewed universities is performing risk management (regarding information security).
- None of the interviewed universities is quantifying the impact of incidents.
- 2 out of 4 interviewed universities have an information security policy; all have various other information security controls.
- 2 out of 4 interviewed universities investigate the incidents in terms of vulnerability an threats and report using this information to adjust information security processes.
- 2 out of 4 interviewed universities adjust the information security process based on the investigation of incidents.
- All universities report that low awareness is a major contributing or causing factor on incidents and that the users of a university should know better.

When comparing and charting the universities to the aspects covered in literature, the following figures can be observed:

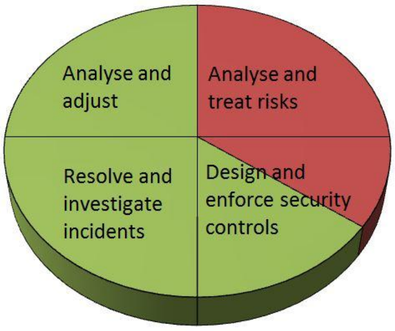


Figure 6: TU Eindhoven

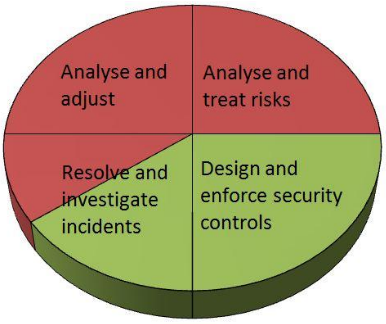


Figure 7: TU Delft

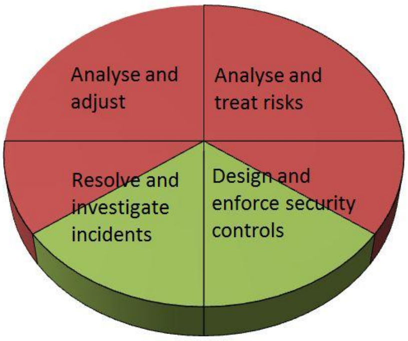


Figure 8: Wageningen U&R

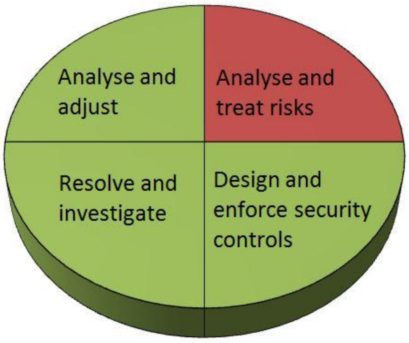


Figure 9: Open University

Figure 10: overview of information security practices at the interviewed universities

When looking at this overview is can be concluded that the Open University is the most advanced regarding information security followed by the TU Eindhoven. This is due to fact that at these universities the incidents are investigated in terms of vulnerabilities and threats and that this information is used to adjust the information security processes.

Before comparing these finding to the University of Twente, the next chapter will first look at the user awareness at the University of Twente

5 User awareness at the University of Twente

During this research, the human factors to be of great importance to information security. During the investigation, it was found that the *insiders*, the students and employees, are involved in 1458 out 1606 incidents; this constitutes the majority of incidents. While exact figures on the interviewed universities are not present, they all reported that students are involved in the most incidents.

When the interviewed universities were asked about the causes of this many incidents by insiders, they consistently reported human factors as a problem. While copyright incidents are perceived to be on purpose, the virus related incidents are perceived to be unintentional. The universities perceive (information security) unaware or naïve users to be the cause of the problem. They consistently reported that they expected better of users at a university; many of which will have an above normal level of education.

With these observations in mind, the employees of workstation support were interviewed again to find out how they perceived this situation in general and more specifically related to virus incidents; as these appear generate the most impact currently.

Their observations are similar to those of the other universities and they stated that users are imprudent with passwords and physical access to the work stations. Passwords are written down on notes and some users even have lists of passwords posted on their bookcase and when support employees ask the user to log into the work station the user often refers them to these notes or lists for the password. In addition, they report cases of the sharing of personal credentials between employees '*to be able access each other's workstation is necessary*'. This is not necessary as users can log into each workstation using their own credentials. This fact has been communicated to them many times, but they *'refuse'* to understand it.

The fact that user are easy to give away their account data is also apparent from phishing e-mail. One support employee reported he was asked by a user to '*check an e-mail whether the correct data was entered in the e-mail*'. The user was apparently just about to reply to a phishing e-mail. According to the support staff, this behaviour is due to the fact that users are not aware and refuse to think about the possible damage that can be done when someone else can access their account, their files or their e-mail.

The virus incidents are in a way related to the phishing e-mail. According to workstation support, while incidents are not investigated in terms of vulnerabilities and threat, many virus incidents seem to be related to e-mail containing hyperlinks linking to viruses. Another observation is that these viruses are able to infect computers which have a virus scanner where the user does not has administrator rights. In addition, the workstations are kept up-to-date automatically.

Viruses that can be installed on a workstation with virus scanner and limited user accounts are the worst kind of virus to protect against. However, these viruses do not install themselves; user interaction in addition to some vulnerability is required. Therefore, this does not absolve the user from causing the incident. In terms of levels of security compliance of Furnell & Thomson (2009) this behaviour may be classified as 'ignorance'. While the user does have a basic (technical) security, the user apparently does not have enough knowledge to recognize e-mails as a threat and might be unaware of threat being able to bypass the protection of a virus scanner.

The low user awareness may another consequence at the University of Twente; users may not know that their computer is infected. Workstation support reports that user reports come in regarding *bad performance* for workstations, which can later be identified as virus incidents. One group of workstation support mentioned that they currently try to report these cases to the CERT-UT team for registration; other groups do not report this. As long as these incidents are not reported, these incidents will remain invisible to information security as a) the support request are registered is a separate IT systems and b) the incidents are not recorded as a virus incident but as bad performance or as a request to re-install the computer.

6 Improving information security at the University of Twente

When comparing the practices at the University of Twente (presented again in Figure 11) with the interviewed universities, it can be concluded that the information security practices are equal to the TU Delft, falling behind the Open University and the TU Eindhoven

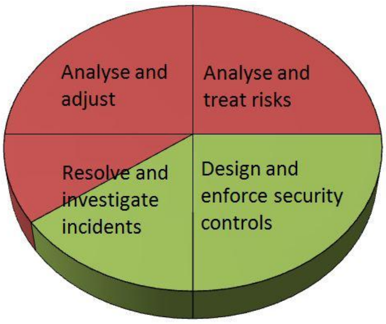


Figure 11: Information security practices at the University of Twente

The main difference is can be found in the area of information security incident management' and 'Analysis and Adjust'. The Open University and TU Eindhoven are more in control of information management in these areas because they look beyond resolving the incidents, investigating the causes and adjusting security control to prevent future incidents. While regular feedback meetings are organised regarding information security incidents at the University of Twente, only the type and frequency are being reported during those meetings. As the impact analysis has shown, this information is not enough to make accurate decisions to adjust the information security process.

The impact analysis performed in the context of this research shows that there are significant costs involved in resolving the virus-related incidents of employees, improving security controls should not be the first priority for the University of Twente. Information on the vulnerabilities and threats involved in the incidents, the cause (and therefore solution) of these incidents remains guesswork and without a proper risk analysis this process will remain reactive instead of proactive.

The focus should thus be on these two aspects:

- Investigating vulnerabilities, threat and impact of incidents during information security incident management at the University of Twente
- Performing risk management in the area of information security at the University of Twente.

As the current processes already incorporate the feedback process to management in an attempt to adjust the information security processes, the analysis and adjust phase should only require a minor change in the processes to include the vulnerability, threat and impact information.

7 Conclusion

In this research the status of information security at the University of Twente and four Universities in the Netherlands was investigated. During the investigation, several remarkable findings were discovered. This section will first present the general conclusions and after that revisit the research questions as presented at the beginning of this thesis.

7.1 General conclusions

No risk management

When looking at the universities as presented in section 3.6, section 4.7 and chapter 0, the first and foremost conclusion must be that none of the universities are performing Risk Management regarding information security.

Risk Management is the organisation task of determining the 'what and why' of information security by looking at the risks to the organisational goals. In addition, risk management should determine the impact of the risks in order to appropriate treatment.

Without risk analysis, Risks can be treated but it will be unknown whether the right risks are being treated and investments cannot be justified is terms of risks they reduce. Without risk analysis, information security is performed blindly.

Best practice approach to information security controls

Information security controls should be aimed at the goals of information security. These goals should be linked to the risks the organisation aims to reduce. The information security policy is the document to make this link. The information security policy is only available 3 out of the 5 investigated universities. However, even when the information security policy is available, without a risk analysis it is impossible for this document to provide the link between controls and the risks to be treated.

Many information security controls are described in best practices and information security can be performed based on these best practices. At the universities due to a lack of risk management, the controls to information security can be seen as following a best practice approach.

Best practice for the universities not yet discovered

Information security is a trade-off. In one part a trade-off between the costs of protection versus the impact of the incidents, but also between the need for protection and the need to the user to be able to work. This can be seen in the case where one university is removing the need for VPN client and another is introducing it, but also where some take a 'zero-tolerance' approach while another is very lenient to the user.

While all institutions are rather similar; all universities, comparable user base, comparable incidents, they are all still searching which practices fit their institution.

Information security incidents management equals incident resolution

In order to adjust the information security process, feedback is needed on the incidents which have occurred. This feedback consists of the frequency, impact, vulnerabilities and threat of the incidents and this information should be investigated during the handling of incidents. However, only the Open University and the TU Eindhoven report investigating and recording the aspects of vulnerability and threat in addition to resolving the incidents. None of the universities quantify the impact of incidents.

Without a quantified impact of incidents, it may still be possible to subjectively judge which incidents should be prevented in the future and adjust the information security process accordingly. The process of investigating incidents and using the feedback to make adjustments to the process was only reported by the Open University and the TU Eindhoven, therefore these are the only universities which have covered the 'analysis and adjust' part of information security.

Low user awareness

While user awareness is a difficult aspect to measure or to improve, the universities consistently report that they regard the user awareness as low and as a major contributing cause of incidents. Examples of a member of the support staff being asked to check whether the account information inserted in a phishing email is correct, users making entire passwords lists and leaving them on the desk, or visiting dubious website are reported as all too common practices. Low user awareness in combination with viruses that can disregard virus scanner are a serious threat.

Information security incidents at the universities are mainly caused by *insiders*

With the exception of the Open University, the recorded incidents are caused by *insiders*. Incidents concern the computers of student or employees. Complaints about copyright infringement and viruses are common among these users and user interaction is usually required for these problems to occur. The incidents in which an outsider tries to break into a system or make the system unavailable are rare. At the University of Twente these incidents were not recorded within the measured period.

7.2 Conclusions regarding information security at the University of Twente

Reporting of incidents partially limited by the registration application

The reporting on information security incidents should be more than reporting only the frequency. The application, used to register the incidents, records the incidents based on type and connection used. User information cannot be added in such a way that is can be used for reporting purposes. Nor are there proper facilities to add additional information regarding vulnerabilities, threat, causes or solutions.

Investigating frequency of incidents is not enough

The analysis of incident at the University of Twente showed that the incidents, in order of frequency, are:

1. Fraud (copyright infringement)
2. Malicious code
3. Abusive content (spam)

When only looking at the frequency of incidents the most incidents are caused by students and regarding connection type most incidents concern notebooks.

According to the impact analysis, focusing information security on students and their notebooks would be a mistake. Based on resolution time and impairment of business performance, the incidents concerning employees using computers within the faculties have the most impact.

Invisible incidents

During this research it was found that complaints about possible information security incidents are not the only way incidents are detected and resolved. Users themselves may contact workstation support because their computer is showing bad performance. These incidents are registered in a separate system as a support request, rather than an incident, among the normal support requests.

It was stated by workstation support the incidents, reported by information security incidents management, may account for 50% to 70% of the actual incidents. Therefore between 30% and 50% may yet be unknown to information security incident management.

7.3 Reflection on research problem and research questions

This research set out to investigate the status in information security at the University of Twente and similar institutions in the Netherlands and examine how information security practices, mainly at the University of Twente, can be improved. In section 1.1 this goal was translated into the following research problem:

What is the status of information security at the University of Twente and other universities in the Netherlands and how can information security practices at the University of Twente be improved?

Before any investigation into the status of information security or possible improvements could start, it was necessary to gain understanding of the subject of information security. The first research question was thus formulated as:

1. **What is information security?**

In chapter 0, it was shown that information security is about ensuring that security attributes of information, like confidentiality, integrity and availability, are met to a level desired by an organisation. In order to ensure that these attributes are met, an organisation will often implement information security controls. Information security, however, is much more that implementing possible protection mechanisms. Information security should also include the process of risk management in order to analyse what the expected risks are to information and decide (with a cost-benefit trade-off) which risks to treat. Treating risks can be done by reducing it (through the use of information security controls) but also by transferring it to third-parties, avoiding it or by accepting it.

When information security incidents occur, they should not only be resolved but they also need to be investigated in terms of impact, vulnerability and threat. The impact can be used to check whether the actual impact of incidents is in accordance with the expected risk; if not, perhaps a risk which was previously accepted should now be addressed. The information on vulnerabilities and threat is necessary, when the impact of incidents show that adjustment to the processes are necessary, to investigate how the processes should be adjusted. All of these processes were identified in chapter 0 and described as the practices of Performing r*isk management, Designing and enforcing information security controls, resolving and checking information security incidents and analysing and acting upon incidents.*

In order to investigate the status of information security at the University of Twente and other universities in the Netherlands two research questions were formulated:

2. **How is information security being performed at the University of Twente?**
3. **What is the status of information security at other universities in the Netherlands?**

It was found that of the practices identified in literature, none of the universities was performing the complete cycle. Risk management regarding information security was the one practice missing at all of the investigated universities. While all of the universities have information security controls and all universities are resolving incidents, the practice of analysis the incidents and using that knowledge to adjust the information security process was only performed at two universities.

During the investigation it was found that the specific approaches to information security among the universities varied; some were very strict in the resolution of incident while other were very lenient to the user. While the approaches differed, the incidents which can be seen at the universities were quite similar. One question was how user awareness was involved in these incidents, therefore the fourth research question was:

4. **How is user awareness involved in the information security incident at the University of Twente and the interviewed universities in the Netherlands?**

While there is no definitive proof, user awareness is perceived by all universities as low and as a major contributing cause of incidents. These incidents, at the University of Twente, consist mainly of cases of *Fraud* (complaints about copyright infringement) and mainly of students. An impact analysis, based on the costs of resolving incidents, however show that, while these incidents occur most, that most costs are involved with viruses on the computers of employees and that in these cases user awareness may play a crucial role. The question then is:

5. **How can information security be improved at the University of Twente?**

Based on the research, it can be stated that the University of Twente is performing information security *blindly*. The frequency of incidents is being reported to management, but the impact analysis shows that the frequency of incidents does not necessary show the main problem. However, even if other incidents, like virus, are accepted as a problem which needs to be addressed; it is not known how. If it is true that, as reported by workstation support, that some of these viruses can be installed on an up-to-date workstation with up-to-date virus scanner without administrator rights, then there is another vulnerability that allows these viruses to be installed. The question is which?

The incidents, however, should only be accepted as a problem if they are in conflict with the expectation of risk management. This is because reducing risk will likely require investments. The costs of these investments need to be weighed against the benefits gained when these incidents are prevented.

Therefore the recommendations to improve information security at the University of Twente are twofold and are to:

- investigate the vulnerabilities, threats and impact of incidents during information security incident management at the University of Twente
- perform risk management in the area of information security at the University of Twente

In addition, the recommendation of investigating the vulnerabilities and threats of incidents also hold for the TU Delft and Wageningen U&R; the recommendation to investigate the risks and the impact of incidents hold for all of the investigated universities.

8 Recommendations

8.1 Information and risk analysis

The desire to perform a risk analysis is already described in the information security policy of the University of Twente (UT, 2010). With the amount of IT at the University of Twente and the lack of an overview of information present at the University of Twente or a more extensive calculation of possible impact of risk, this process can be time consuming. As, according to the information security, the risk analysis is to be performed by ICTS, the ICTS department should assign one or more people to perform risk analysis on information security at the University of Twente.

8.2 Investigating incidents

In order to prevent future incidents, knowledge on the causes of current incidents is required. This would need to be performed by those in direct contact with the incidents during resolution: the employees of Workstation Support.

Investigating the incidents and the causes, in addition to resolving them, takes time; especially with viruses the investigation into the exact sequence of events can be difficult; although crucial in order to prevent future incidents. Therefore additional time and money will need to be freed to allow Workstation Support to investigate these incidents.

As the TU Eindhoven already investigates each incident, their knowledge on this subject may help with the design of this process.

8.3 Change registration application

To make accurate decisions on the incidents, it is not only important do have detailed information on the incidents but also have the correct number of incidents. While all incidents received by information security is forwarded to workstation support for resolution, the incidents received by workstation support are often not reported to information security.

As the incidents received by workstation support are registered in a separate system and not marked as information security incidents; these incidents are not traceable by information security.

Taking into account that the University of Twente is in the process of streamlining the organisation using ITIL to design the processes, it is recommended to abandon the two-system approach and register incident in a single system. The recommendation would be to abandon the current AIRT application and use the service desk application for a number of reasons:

- **Incident registration**: The Servicedesk application is aimed at incident registration. Information security incidents are (special kind of) incidents.
- **Dual registration**: The AIRT application forwards the complaints to the service desk, which registers the incidents in the service desk application anyway.
- **Hidden incidents**: In case of resolution, should any additional information be recorded, is recorded in the service desk application. This information is used by information security, thus policy adjustment are not possible (with this information as input).

- **User registration**: In order to calculate the impact, information on the user is necessary. This feature is already build into the service desk application.
- **Standardized work**: The service desk application supports (or is aimed at) standardized work processes. Incident registration and resolution is completely standardized).
- **Multiple input channels**: information security incident are not always reported to information security as an incident, but may also be reported to work station support are a computer with reduced performance.
- **Better user support:** When a user, disconnected from the network, calls the service desk for support the service desk may not know the current status of the incident (although this is improved as the incidents are currently forwarded to them for registration). By using the service desk application for the complete registration process the service desk and the user may be better informed of the actual status of incidents.

There is, however, one major question before migrating the incident registration to the service desk application and that is security. Currently (as far as known) all support requests are visible to all ICTS employees. This means this information is semi-public, which may not be entirely desirable for information security incident.

References

Albrechtsen, E. (2008). Friend or foe? Information security management of employees. *PhD Thesis* .

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report , 14* (4), 195-201.

Beautement, A., Sasse, M., & Wonham, M. (2008). The Compliance Budget: Managing Security Behaviour in Organisations. *New Security Paradigms Workshop*, (pp. 47-58). Lake Tahoe, California, USA.

Cooper, M. (2009). Information Security Training - What will you Communicate? *SIGUCCS'09 - Proceedings of the 2009 ACM SIGUCCS Fall Conference*, (pp. 217-219). St Louis, Missouri.

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computer and Security , 25*, 55-63.

Furnell, S., & Thomson, K. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security , 2009* (2), 5-10.

Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by User. *Proceedings of the 2009 workshop on New security paradigms workshop* , 133-144.

ISO/IEC. (2008). *Information technology - Security techniques - Information security risk management.* Delft: NEN.

ISO/IEC. (2005). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.* International Organization for Standardization.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathsways to vulnerabilities. *Computers & Security , 28*, 509-520.

Kritzinger, E., & Smith, E. (2008). Information Security Management: an information security retrieval and awareness model for industry. *Computer & Security , 27*, 224-231.

Kruger, H., & Kearney, W. (2006). A Prototype for assessing information security awareness. *Computers & Security , 25*, 289-296.

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture? *International Carnahan Conference on Security Technology*, (pp. 361-366). Zurich.

Marks, A., & Rezgui, Y. (2009). A comparative study of information security awareness in higher education based on the concept of design theorizing. *International Conference on Management and Service Science*, (pp. 1-7). Wuhan, China.

NIST. (2002). *sp 800-30: Risk Management Guide for Information Technology Systems.* National Institute for Standards and Technology.

Nunes Leal Franqueira, V. (2009). Finding Multi-Step Attacks in Computer Networks using Heuristic Search and Mobile Ambients. *PhD Thesis* .

Nunes Leal Franqueira, V., Cleeff, A. v., Eck, P. v., & Wieringa, R. (2010). External Insider Threat: a Real Security Challenge in Enterprise Value Webs. *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES'2010)* (pp. 446-453). Krakow, Poland: IEEE Computer Society Press.

Oliver, M. (2002). Database privacy: balancing confidentiality, integrity and availability. *ACM SIGKDD Explorations Newsletter , 4* (2), 20-27.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security , 8* (1), 31-41.

Siponen, M., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contribution. *The DATA BASE for Advances in Information Systems , 38* (1), 60-80.

Stefanek, G. (2002). *Information security best practices - 205 basic rules.* http://www.sciencedirect.com/science/book/9781878707963: Elsevier Inc.

UT. (2010). *Informatie Beveiligingsbeleid 2010.* Opgeroepen op 6 1, 2010, van Informatie Management: http://www.utwente.nl/secr/im/security/Informatiebeveiligingsbeleid%20Universiteit%20Twente%202010/

UT. (2008). *Informatieplan UT 2008-2010.* Opgeroepen op 6 1, 2010, van Informatie Management: http://www.utwente.nl/secr/im/Informatie-%20en%20ICT-plan%20UT%202008-2010/Informatieplan%20UT%202008-2010/

Ward, J., & Peppard, J. (2002). *Strategic Planning for Information Systems* (3rd ed.). Chichester, West Sussex, England: John Wiley & Sons Ltd.

Willison, R., & Siponen, M. (2009, 09). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Cumminication of the ACM , 52* (9), pp. 133-137.

Yin, R. (1997). Case study evaluations: a decade of progress? *New Directions for Evaluation , 76*, 69-78.

Yin, R. (1981). The Case Study Crisis: Some Answers. *Administrative Science Quarterly , 26* (1), 58-65.

List of interviewees

Assistant information manager of the University of Twente	Wim Koolhoven
Workstation support 'Ravelijn'	Barry van der Hulst Richard Hanekamp Rob Bouhuis Wilco Jansen
Workstation support 'Carré'	Marc Berenschot Henk van de Zandschulp
Workstation support 'Horst'	Martijn Elferink Clement Nijkamp
Workstation support 'ICT'	Martin Blankestijn
TU Delft	Alf Moens
TU Eindhoven	Erik te Nijenhuis
Wageningen U&R	Jaap Booij
Open Universiteit	Peter Timmermans

List of figures

List of tables

Appendix A: eCSIRT framework for incident reporting

Source: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html

This classification scheme is used for the collection of statistical data - Type 2 Incident Information.

Each Incident has one primary type (so the numbers given for primary type add up to the number of all incidents). However, additional or secondary incident types can happen in the context of an incident. But these aren't taken into account here.

Example: After a successful intrusion the attacker gains root privileges on a system. As a result of it he gets access to sensitive information. The primary type of this incident is an "intrusion" (incident class) with a "privileged account compromise" (incident type). All further events which are based on this intrusion should be not registered.

Note: The number of incident types is not fixed and should be enlarged any time if it seems necessary.

The following table shows the current used eCSIRT.net incident classes and types and gives some additional descriptions or examples:

Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a

		non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoors, cross side scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS- a. PING- flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Appendix B: Impact analysis at the University of Twente

This appendix will look at the impact of information security incidents at the University of Twente. The impact was determined in section 3.2.3 to include:

- Financial cost of report
- Impairment of business performance

This appendix will look at these factors in more detail.

Financial cost of repair

Incident processing

The processing of the incident is done by the CERT-UT team of the University of Twente, which receives notification of potential incidents. If the notification is a valid incident, the incident is traced back to a computer and/or user. Based on this information, the correct support department is notified if additional actions to resolve the incident are required. If there is a risk of continued abusive behaviour or there is a risk of the incident spreading (e.g. a computer virus), the cert team can also take additional action like adding e-mail addresses to a block list or blocking a computer from the university network.

In general the steps involved with incident processing consist of:

1. Receiving and registering the complaint.
2. Trace the user information
3. Perform measures to prevent further incidents
4. Forward the complaint to a support department for resolution

The cost involved with this processing by the CERT-UT consists of the time they spend processing the incidents. Steps 1 and 4 in the list above are mostly automated via the AIRT application. The time it takes to retrieve the user information depends on the type of connection the user is using rather that the type of incident or the type of user. The connection types at the University of Twente can be categorized as:

- Faculty: a computer belonging to the University of Twente which is connected to the wired network
- Campusnet: a private computer which is connected to the wired network
- Wireless LAN: a private or university notebook using the wireless network at the university
- Virtual Private Network: a private computer using VPN to connect to the university network

The user information and connection information is collected into a database. Depending on the type of connection used different tables may be needed and some of the database tables involved, particularly those involved with wireless connections, are rather slow. The costs, in terms of time consumed for processing the incidents, is therefore composed of three parts:

1. The time consumed by registering (step 1) and forwarding (step 4) the incident, which is equal for all incidents.
2. The time consumed by tracing the user information, dependant on the connection type used by the user
3. The time consumed by executing 'preventative' actions, dependant on the incident type.

Registering and forwarding the incident

Every incident is registered. In some cases, an incident may be imported automatically in the registration application, while in most cases they need to be registered manually. On average the steps of registering an incident and forwarding it take about 1 minute (combined).

Tracing the user information

Tracing the computer connection and/or user information depends on the type of connection used. The normal, wired, connections are very easily traced, the VPN and wireless connections take addition time as the database containing these connections are much larger and more slow, combined with the fact that more database tables are required to trace a wireless connection to a user when compared to wired connections. Based on observation of the cert team, the times required in order to trace the incident to a computer and/or a user is shown in Table 15 below.

	WLAN	VPN	Campusnet	Faculties
Time	3	2	1	1

Table 15: Time required (in minutes) to trace the computer and/or user information

Measures to prevent further incidents

The time it takes to take additional actions to prevent further abuse depends on 1) the incident and 2) the specific actions taken.

In case of:

- Abusive content the internet access of the computer is blocked or account the account is locked to prevent more spam from being sent.
- Malicious code or intrusion attempts the internet access of the computer blocked
- Information gathering, thus far cases of phishing e-mail, the source address is registered in the block lists of the University of Twente. In addition, it is investigated whether e-mails have been sent to the reply address of the phishing e-mail and those accounts are then locked until the user changes his or her password.

When analysing the incidents it will be shown that there was a single incident concerning ‘availability’. After notification of reduced performance, it was quickly found that the gateway for the e-mail facilities was the target of a distributed denial of service attack. Due to lack of time of the administrators (the incident was outside of normal office hours), the service was shut down. The next day the service was restarted and reconfigured to better cope with future incidents of this type. In this case, the actions taken to prevent possibilities of damage took only 5 minutes. Future occurrences concerning availability will have to be investigated to give a better indication of the time it takes to resolve this type of incidents. An overall table of the time it take to implement measure to prevent an incident from escalating is show in Table 16.

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Time	1	1	3	1	5	-	-

Table 16: Time (in minutes) to implement measure in order to prevent further abusive behaviour

Incident resolution

The University of Twente is divided into six different faculties. Within the ICTS departments there are four ‘workstation support’ groups servicing these faculties as well as the additional administrative or service departments.

The incidents identified in the AIRT system are forwarded to the different departments, so it is known which incidents the support groups need to resolve. The process of how they resolved those incidents and how much time and effort it takes to resolve those incidents was unknown. In order to gain insight into these processes, interviews were held with the 4 ‘workstation support’ groups as well as the helpdesks (ICTS Service desk and Notebook service centre) at the University of Twente.

The goal of the interview was to determine the costs (for the University of Twente) given the different incident types. Within the interview of each department, it was important to touch upon 1) the methods their used to deal with the incidents their receive, 2) what costs they perceive for the University of Twente (and what those cost are in the different cases), 3) what the situation is within the department(s) they service, both in terms of technical facilities and user awareness regarding those issues. While these 3 questions were to be answered in each interview, it was important to be flexible in the interview as the situation might differ completely. While it is changing, in the past there was very little communication between the different groups of the IT departments as they each fell under the responsibility of the faculties they services (instead of one single IT service department as is now the case) To cope with possible exceptions and differences between groups, the form of a semi-structured interview was chosen with the questions and the incident types as guidelines.

The goal of the interviews was to identify the impact for the University of Twente. Questions were asked on the costs (‘only’ man hours or also material costs), how incidents were resolved and how much time it takes (on average) to resolve the incidents. As this thesis is also interested in the human factors behind the incidents, a question was also asked on their perception on user awareness.

Earlier the incidents were classified by means of the ECSIRT framework and it was stated that the goal of the framework was to register the primary incident (the root cause of the incident). The support groups did not distinguish between these incident to the same level, as ‘abusive content’, ‘malicious code’ and ‘intrusion attempts’ all mean that the computer is infected with some kind of malicious software and it needs to be either cleaned or reformatted.

Infected computers

The way the different groups handle infected computers differs between departments. The group ‘Ravelijn’ does not take any chances with infected machines and gives the machine a complete format and re-install. The ‘Horst’ and ‘Carré’ groups first try to clean the system. ‘Horst’ reports that they do this because they have to deal with fairly complex research systems (which makes re-installing them also more troublesome). They, however, also note that they find it difficult to decide when to switch from trying to clean the system to re-installing the system. The ‘Carré’ reports little trouble with the workstations within the faculty, as they are all managed by the IT department, have virus scanners installed and the users do not have administrator rights. They do however have some old service level agreements which state that, in some cases, that also support the private computers at home of some employees. These systems might have more personal data (like photo’s) which justify an initial attempt to clean it. If the cleaning attempt was unsuccessful for about 30 minutes the decision was usually made, in discussing with the owner, to re-install the computer.

The faculty of ITC is a recent addition to the University of Twente. It therefore still has its own measures and procedures in place. While the network at the rest of the university is very open, they have been very strict in their management of workstations, firewall setting and virus scanners. They report that it virtually never occurs that a workstation is infected. They do however see infections of private computers, like notebooks, but these are not supported by the group of ‘workstation support’. Should it occur that a managed workstation is infected, it is to be formatted and re-installed; taking about 3 to 4 hours. The time is takes to re-install a computer thus varies between groups, depending on the complexity of the system to be re-installed. The times given by the groups are shown in Table 17 below.

Group	Action	Time
Ravelijn	Format and re-install, in all cases	About 4 hours
Horst	Try to clean first, format and re-install if unsuccessful	30 minutes to 6 hours
Carré	Try to clean first (+- 30 minutes), else proceed to format and re-install	30 minutes to 3 hours.
ITC	Does not really occur, but format and re-install should it occur	3 to 4 hours

Table 17: Time needed to re-install a workstation and its applications

Phishing

If the user has given away his or her account information in a phishing attempt, the first step is to block the account. The user is also called, or a support employee walks by the office of the employee, to notify the person of the fact that this incident occurred and that the employee needs to change his or her password through the service desk.

In the best case scenario, the CERT-UT team gets notified by (other) recipients of the phishing e-mail that this has occurred. E-mail messages to and from e-mail addresses related to the phishing attempt are blocked to prevent users from sending their data and preventing further phishing mail from this address. It is also check in the logs whether people have replied to this message. While the contents of the message cannot be seen, the worst is presumed; that the user has in fact submitted their account information.

When a phishing e-mail targets a select group of accounts and should those users not report the incident, the phishing attempt may go undetected for the CERT-UT team. Should a user give away his or her account information, we cannot prevent the account to be misused. When this occurs, the CERT-UT team will usually receive notifications of spam being sent from that account and process it then.

Fraud and other cases

These cases are handled with little effort involved In cases of fraud, the user is e-mailed on a first offence. On a repeated offence, the supervisor of the users is notified. The group of 'other' cases is also handled and solved by one or more e-mail message or phone calls. All in all, these cases can be resolved within five to ten minutes.

Awareness

All departments regard the user awareness regarding information security, especially regarding phishing e-mail, e-mail containing viruses and (un)safe browsing on the internet, as low. The support of 'Ravelijn' and 'Horst' both mentioned that a rather large portion of users write down password which can be found under their keyboard or even as a post-it attached to their monitor. They also mentioned that a lot of users do not lock their workstation while away from the computer and they regard this as a potential security hazard.

Most interesting regarding awareness however is that they stated that 'they expected better from users at a university'. While there are a lot of users at the university, with different computer background, the low-skilled (and lower educated) administrative staff is not regarded as a severe problem. Should they receive an e-mail asking for their account or contained a dubious attachment, they often 'panic and ask for help'. It is perceived that the higher-educated do not ask for this help and are more prone to fall victim to such e-mail, viruses and such.

Resolution time of 'workstation support'

The group 'workstation support' only supports employees. Based on the interview, resolution times of various incident types were gathered. In cases of infected computer these time varied somewhat between groups, as shown in Table 17. Based on this table, an average a resolution time of 4 hours seems reasonable. While there may certainly be cases which can be resolved quickly, these may be compensated by cases in which cleaning the computer fails and the overall resolution time take up to 6 hours. Combining all the resolution times with the incidents, the time spend by workstation support on a certain type of incident is given in Table 18.

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Students	0	0	0	0	0	0	0
Employees	240	240	10	240	10	10	10
Third-parties	0	0	0	0	0	0	0
Guests	0	0	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0
Saxion	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

Table 18: Resolution time (in minutes) of workstation support in relation to incident type and type of user

Impairment of business performance

During the resolution process of some incidents, there may be cases of impaired business performance. This occurs when personnel of the workstation support group need to perform action which inhibits the user from performing normal day-to-day tasks, like taking the computer away to be re-installed. Table 19 below shows impairment with the three incident types which are currently resolved by re-installing the computer, but also impairment in cases of information gathering. When a case of information gathering is found, the e-mail account of the user is locked. Unlocking this account involved calling the service desk for a password reset, during which time the user may be impaired.

	Abusive Content	Malicious code	Information Gathering	Intrusion Attempts	Availability	Fraud	Other
Students	0	0	0	0	0	0	0
Employees	240	240	10	240	0	0	0
Third-parties	0	0	0	0	0	0	0
Guests	0	0	0	0	0	0	0
Eduroam	0	0	0	0	0	0	0
Saxion	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

Table 19: Impairment of business performance (in minutes)