LUNDS UNIVERSITET
Ekonomihögskolan

Department of Informatics

Information Security Cultures and Challenges in Higher Education

A Study from the University Researchers' Perspective

Bachelor's Thesis 15 credits, course SYSK16 in Informatics

Authors: Albin Westermark
Fabrice Lindblom-Levy

Supervisor: Niki Chatzipanagiotou, PhD – Senior Lecturer

Grading teachers: Nicklas Holmberg
Markus Lahtinen

Information security cultures and challenges in higher education: A study from the university researchers' perspective

SWEDISH TITLE: Informationssäkerhetskultur och utmaningar vid universitetet: En studie från universitetsforskares perspektiv

AUTHORS: Albin Westermark and Fabrice Lindblom-Levy

SUPERVISOR: Niki Chatzipanagiotou, PhD - Senior Lecturer

PUBLISHER: Department of Informatics, Lund University School of Economics and Management

EXAMINER: Osama Mansour, PhD

SUBMITTED: May, 2023

DOCUMENT TYPE: Bachelor's Thesis

NUMBER OF PAGES: 79

KEYWORDS: Information Security, Information Security Culture, Information Security Challenges, Researchers, Higher Education

SUMMARY (MAX. 200 WORDS):
This bachelor's thesis research focuses on information security. With the growing use of technology in research, information security has become an increasingly important concern for academic institutions, which face, among other, challenges related to the protection of sensitive data from unauthorised access, theft, and misuse. The research purpose was to explore the current information security cultures and challenges among university researchers with the aim to make suggestions to overcome the information security challenges, if any, and improve the information security culture. For this a study was conducted where the empirical data was collected through semi-structured interviews with purposively selected university researchers. These were analysed thematically and five themes emerged from the analysis of the collected

data that represent the research findings. The findings were explained and discussed supported by the literature review and the protection motivation theory to reach the research outcome. The research outcome highlights the need for tailored information security measures, improved data management practices, and improved communication and documentation of security procedures for the information security practices of university researchers. Thus, the bachelor's thesis research contributes to the informatics research field by improving the understanding of factors that influence researchers' attitudes and behaviours toward information security.

ACKNOWLEDGEMENTS

We would like to thank our supervisor Niki Chatzipanagiotou, PhD - Senior Lecturer for supporting us during the writing of this bachelor's thesis. We would also like to thank Ingegerd Wirehed, the Chief Information Security Officer at Lund University, for giving us inspiration regarding the topic of research and for the support. We would also like to extend our gratitude to every participant for their willingness and enthusiasm to partake in our research.

Table of Contents

Figures

Tables

1 Introduction

This introductory chapter gives an oversight of the scope of this bachelor's thesis. It covers the background of the topic, highlights the identified problem and knowledge gap, outlines the research purpose and questions, and defines limitations related to the bachelor's thesis.

1.1 Background

Information security is of high importance when it comes to organisations. Seeing as organisations contain a lot of information, they can be a target for people looking to profit from malicious activities (Shimeall & Spring, 2014). A survey made in 2010 indicated that the custodial data of an organisation, data on external parties, had a self-evaluated mean value of $750,000 for each organisation (Shimeall & Spring, 2014).

Universities have been increasingly targeted by attacks as they contain vast amounts of information, as well as the fact that universities are open towards the public and possess high amounts of computer power (Bongiovanni, 2019). Universities are a unique form of organisation, as they are open access, decentralised and with many different stakeholders. Bongiovanni (2019) also mentions that information security accidents in higher education have been on the rise in recent years. Information security at universities is a challenge, seeing to the different security practices of the individuals as well as the limited resources of universities (Bongiovanni, 2019).

1.2 Problem Identification

Glaspie (2018) conducted a study to assess the information security culture in higher education, where he stated that information security cultures have a positive impact on the security behaviour of employees. Yerby and Floyd (2018) researched faculty and staff awareness and behaviour of information security at public university in Southeastern United States and found that they in general had a high to moderate level of awareness and behaviour. A conclusion they drew was that the ones that had a higher awareness of information security, also exhibited more secure behaviour. They found that security awareness training is necessary to reduce the risks of information security breaches at a university level. Bongiovanni (2019) argues that research into information security and information security culture at higher education institutions is something that needs to be expanded. Researchers form a large part of the university's staff, including teachers, researchers, doctoral candidates, and administrative staff. These researchers are composed of people from all over the world, and therefore have different approaches to and understandings of information security.

To conclude, previous related studies have shown that information security cultures are an essential part of an organisation in order to be able to protect their information and to foster an environment where protection of data is obvious (Glaspie, 2018). Universities gather vast

amounts of data that might be attractive for hackers to access, and universities are in a unique situation due to them being public and the fact that a lot of different people continuously receive access (Yerby & Floyd, 2018). Universities also tend to have a lacking information security (Bongiovanni, 2019). The characteristics of higher education institutions, researchers' needs and followed information security practices, along with limited research on this topic highlight the importance of expanding the research on information security. Therefore, we identify this knowledge gap as something worth researching further.

1.3 Research Purpose and Research Questions

The purpose of our bachelor's thesis is to explore current information security cultures and challenges among university researchers with the aim to make suggestions to overcoming the information security challenges, if any, and improving the information security cultures. The research questions are the following:

1. How do university researchers perceive information security?
2. What are the information security cultures among university researchers?
3. What are the information security challenges that university researchers identify?

1.4 Limitations

The limitations we impart on our study of information security cultures and challenges revolve around the individuals who are part of the study and the research setting. So, the research involves university researchers who are currently employed at Lund University. The percentage of research that their employment implies were not expected to influence the research outcome and, therefore, was not considered. In addition, university researchers working in other universities, besides Lund University, were not included due to time limitations of the bachelor's thesis research. We are aware that this may affect the outcome of our research as there is considerable variety among university researchers regarding information security practices, depending on the specific university in which they belong. However, we believe that the research results could be applied to universities within a similar context, regulations, and cultural background.

2 Literature Review

This chapter presents the literature review search strategy. The results of the literature review are presented as main concepts to clarify related to the research topic areas, such as *Information Security* and *Information Security Culture*. These concepts along with the Protection Motivation Theory" constitute the theoretical framework of this bachelor's thesis, which is used to explain and discuss the research findings in the discussion chapter.

2.1 Search Strategy

The literature review search was conducted following this search strategy: We selected several scholarly databases of IS, which are accessible via Lund University Library's website. In the databases, we searched by subject "Business and Economics" and then "Information Systems". We searched in several databases, but mainly in ACM Digital Library and EBSCOHost, and complemented our search with Google Scholar. When in each database, we searched by using keywords and combination of keywords such as information security, information security culture, information security challenges, information security history, higher education, which were combined using the Boolean operators AND, OR. We have set some criteria for our literature review search. That is, we aimed at finding peer-reviewed research articles, published in academic journals, and/or academic conferences with a publication date of 2014 and onwards and written in the English language. Research papers written in other languages were excluded. The literature search results were checked by reading the articles' abstracts, the conclusions, and, when considered relevant, the whole article was read.

2.2 Information Security

2.2.1 Defining Information Security

Security is defined as protection according to Whitman and Mattord (2017). It is protection from people that seek to harm. According to the Committee on National Security Systems, an intergovernmental organisation of the United States (CNSS, 2023), and their National Information Assurance (IA) Glossary, they define information security as the following "The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSSI-4009, National Information Assurance (IA) Glossary, 2010, p.37). This is the definition we adhere to in the bachelor's thesis.

2.2.2 History of Information Security

The history of information security can be traced back to the idea of computer security (Whitman & Mattord, 2017). Devices like the Enigma, used in World War II for encrypted communication, had a lot of computer security to protect it from adversaries that wanted access to strategies and plans (Whitman & Mattord, 2017). As the decades continued, so did the complexity as well as the necessity of more involved and complicated measures to protect information (Whitman & Mattord, 2017). With the rise of the ethernet solution ARPANET, Dr. Robert M. Metcalfe saw the need to improve on the lack-lusting information security measures which in 1967 led to the first comprehensive report on how to combat the previously shown security risks (Whitman & Mattord, 2017). Through the 70s and 80s as PCs and microprocessors became more ubiquitous and networking started to show its first beginnings, the US government started to recognise computer security as an integral aspect for federal information systems, and also created a specific response team with the responsibility of handling network security issues (Whitman & Mattord, 2017).

The 90s gave rise to public access to the then newly invented Internet, which brought forth more security issues as they were not prioritised in lieu of other developments (Whitman & Mattord, 2017). Computer security before revolved around physical access to the server, whereas networking made it easier to access a computer without physical access (Whitman & Mattord, 2017). During the 90s and towards the 00s, the first conference on information security, DEFCON, was held in Las Vegas, and organisations began increasingly integrating security into their IT infrastructures, and more antivirus products started being developed (Whitman & Mattord, 2017).

After the 2000s, computer security has become even more relevant as millions upon millions are now inter-connected using computers with varying forms av security (Whitman & Mattord, 2017). At the same time, cyberattacks have increased significantly which has increased the awareness that information security must continue to be a priority, both among nation-states as well as private corporations (Whitman & Mattord, 2017).

2.2.3 Confidentiality, Integrity, and Availability

The term information security is further defined by ISO/IEC 27002 as “the preservation of the confidentiality, integrity and availability of information” (Solms & Niekerk, 2013, p.98). Solms and Niekerk (2013) mention that information security usually includes the CIA triangle, which is composed out of three corners. These are confidentiality, integrity, and availability. They mention that the CIA triangle has been the industry standard for a couple of decades. According to the authors, information security should be seen as a process and something that considers more factors than the technical factor. Solms and Niekerk (2013) conclude with mentioning that the terms information security and information technology security are not the same, since information technology security is purely focused on technological systems, and information security is more all-encompassing.

The CIA triad which has formed the basis of information security thinking the last few decades has at the same time been scrutinised, particularly when it has come to its limitations as perceived by information security researchers (Samonas & Coss, 2014). Samonas and Coss (2014) argue that the CIA triad must be redefined for one to understand why practitioners still see the triad as relevant and will continue to use it in the future as well. According to them, the proposed enhancements to the CIA triad have been authenticity, non-repudiation, correctness,

responsibility, integrity, trust, ethicality as well as identity management. The authors weave these tenets together with the general CIA triad and using a Venn diagram and the intersection of the CIA components, redefines the CIA triad to encompass a larger breadth of perspectives.

2.3 Information Security Culture

2.3.1 *Defining Security Culture*

Information security culture is a component of organisational culture, which determines the perception, thinking, feeling and consequently the behaviour of people working in an organisation related to information security (Malcolmson, 2009).It is therefore part of the informal structure of an organisation and is mainly influenced and ideally even developed by the management of the organisation. Additionally, nine themes of security culture are identified. According to Malcolmson (2009), these are: External influences, human resource activities, impact on business, infrastructure, information security, organisational staff, physical security and working with external parts. This highlights the several factors that define security culture, technological and non-technological, in the context of an organisation that in turn are crucial to maintain adequate information security. This is the definition we adhere to in the bachelor's thesis.

2.3.2 *Compliance with Policies and Guidelines*

According to Amankwa, Loock and Kritzinger (2022) a central aspect of information security culture is the alignment of organisational policies and procedures with the overall information security objectives. This entails the implementation of well-defined guidelines that make enable employees to make informed decisions pertaining to information security. Furthermore Amankwa, Loock and Kritzinger (2022) highlight that information security is influenced by the organisation's leadership and management. This is crucial in creating an environment where employees are engaged and feel confident in the measures they and the leadership take to maintain confidentiality, integrity and availability. This can be achieved through an emphasis on improving communication, actively involving employees in security initiatives and assuring that there are sufficient resources allocated to support these security efforts (Amankwa, Loock & Kritzinger, 2022).

2.3.3 *Information Security Programmes*

Challenges in information security have been listed as a lack of a functioning information security culture which is correlated to lacking information security programmes (Glaspie, 2018). Glaspie (2018) notes that an information security culture leads to positive effects on information security policy adherence and information security behaviour. The conclusion is that human factors are a significant factor when it comes to information security challenges.

2.3.4 *The Human Factor in Relation to Information Security Programmes*

Exploring the domain of information security cultures in the context of higher education institutions Information security programmes take on a discernible role. Glaspie (2018) explores the human factors of an information security programme and their impact on the information security culture. These human factors include the stringency of organisational policies, behaviour deterrence, employee attitudes towards information security, training and awareness as well as how well supported and managed the information security programme is. This study serves to highlight the relevance of social and psychological theories in the context of information security.

2.3.5 *Education, Communication and Awareness of Information Security*

The human factor being important is further reinforced by the fact that information security awareness is a factor relating to the successful implementation of information security measures, and that technological solutions are not enough by themselves (Yerby & Floyd, 2018). Employee behaviours are seen as the greatest challenge for effective security measures (Yerby & Floyd, 2018). This highlights the importance of educating all parts involved in the institution, this is essential to create a consequent implementation of adequate information security.

2.3.6 *Information Security in Relation to Institutions within Higher Education*

Specific to higher education, there are unique information security challenges related to the open nature of universities, the coming and goings of different people, the decentralised infrastructure as well as limited resources which leads to outsourcing (Bongiovanni, 2019). Due to the open nature of universities, according to Yerby and Floyd (2018), it has been specifically mentioned that universities are completely different from other forms of organisations, and therefore possess unique amounts of information security challenges in relation.

Due to the diverse amounts of people that handle information at universities, it makes proper training harder for the universities to accomplish (Bongiovanni, 2019). Faculty and staff at universities might also see the role of information security as being the responsibility of the IT personnel at the university, and not something that they need to involve themselves in (Yerby & Floyd, 2018). Another factor that makes it more challenging to tackle information security breaches in higher education is the fact that universities have access to vast amounts of processing power, which makes them a highly lucrative target for cyber-attacks (Bongiovanni, 2019). There are also large datasets of personal information at universities that make universities attractive for hackers (Yerby & Floyd, 2018).

Furthermore, a challenge is that information security needs to be balanced with access (Whitman & Mattord, 2017). There cannot be perfect information security, and one needs to make sure the individuals can access the system in a comfortable way while still ensuring adequate protective measures are taken (Whitman & Mattord, 2017).

2.4 Information Security in Organisations

2.4.1 *Perceived Experience of Information Security*

The perceived experience of information security within an institution refers to how employees, customers, and stakeholders view the effectiveness of security measures put in place to protect sensitive information (Siponen, Mahmood & Pahnila, 2014). This perception is often influenced by the actual experiences of individuals within the organisation as well as external factors such as media coverage of security breaches (Siponen, Mahmood & Pahnila, 2014).

To improve the perceived experience of information security, Siponen, Mahmood and Pahnila (2014) highlights that organisations can implement regular security training programmes, provide clear guidelines for data handling, and ensure that security protocols are followed consistently. According to the authors, it is also important for organisations to communicate their commitment to information security to all stakeholders, as this can help build trust and confidence in the institution's ability to protect sensitive information.

2.4.2 *The Impact of Leadership on Information Security and Information Security Culture*

Leadership plays a critical role in shaping an institution's information security practices (Hu et al., 2012). Leaders must establish a culture of security within the organisation and ensure that security policies are integrated into all processes (Hu et al., 2012). Some of the vital practices according to Hu et al. (2012) involves setting clear expectations for employees, providing adequate resources to support security initiatives, and holding individuals accountable for compliance with security protocols.

2.4.3 *Education and Training*

Wlosinski (2019) highlights that education is a key component of effective information security practices. According to the author, employees must be trained on security policies, procedures, and best practices to ensure that they are equipped to handle sensitive information appropriately. This includes training on topics such as password hygiene, phishing awareness, and data handling protocols (Wlosinski, 2019).

According to the ISO/IEC 27002 it is crucial to implement information security training and awareness (ISTA) programmes as “all employees of the organization should receive appropriate awareness, education and training and regular update in organizational policies and procedures, as relevant for their job function” (Alshaikh et al., 2018; Solms & Niekerk, 2013). To conclude, investing in effective ISTA programmes i.e. education and training, organisations can improve their overall security posture and reduce the risk of data breaches (Alshaikh et al., 2018; Solms & Niekerk, 2013).

2.5 Protection Motivation Theory

In 1991 the Protection Motivation Theory (PMT) was published, which was originally put forward by Ronald W. Rogers in 1975 (Rogers, 1975). Rogers (1975) proposed a theory of

three components that defined why people respond with protective behaviour. The components as specified by the author are how noxious the event will be, whether it has a high probability of occurring as well as what effect the protective action will have on it. The PMT was further expanded in 1983 to become a more encompassing theory and to include rewards, cost of response and self-efficacy, which were grouped into threat appraisal and coping appraisal (Sommestad, Karlzén & Hallberg, 2015). If an individual sees themselves as vulnerable to a threat and/or they risk large negative consequences when the threat is realised, they will be more motivated to protect themselves. Likewise, if the coping method to handle the threat is simple and has value, it will add to higher protection motivation (Sommestad, Karlzén & Hallberg, 2015). People are therefore influenced by a combination of threat appraisal as well as coping appraisal: a cost-benefit analysis (Sommestad, Karlzén & Hallberg, 2015) as illustrated in figure 1.

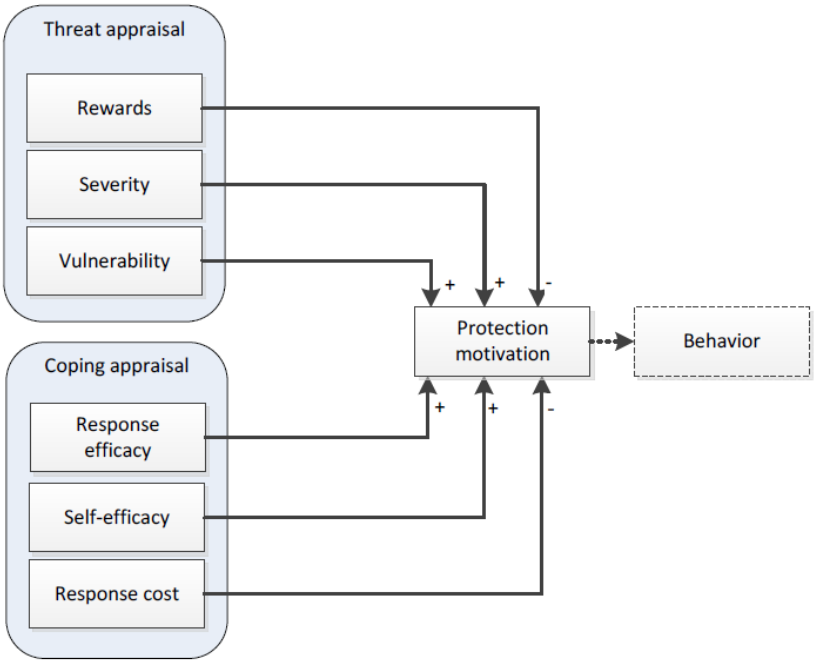

Figure 1. Protection Motivation Theory (Adapted from Sommestad, Karlzén & Hallberg, 2015, p.3)

According to Sommestad, Karlzén and Hallberg (2015) threat appraisal in the PMT consists of the following factors as shown in figure 1:

- Rewards
- Severity
- Vulnerability

They further mention that coping appraisal in the PMT consists of the following factors, illustrated in figure 1:

- Response efficacy
- Self-efficacy
- Response cost

These six factors, i.e. rewards, severity, vulnerability, response efficacy, self-efficacy, and response cost, then culminate in the motivation for protective behaviour as shown in the above figure 1.

The PMT is an established theory that has been shown to have correlation with information security behaviour as well (Sommestad, Karlzén & Hallberg, 2015). At the same time, Sommestad, Karlzén and Hallberg (2015) mention that the PMT was originally developed for health threats against individuals, and that it has not considered organisational threats or mandatory behaviour. In their research they conclude that the PMT is applicable in information security, but that it responds better when the threat is targeted towards the individual, if the threat and coping method is specific, and that it might explain information security behaviour better if that behaviour was voluntarily and not mandated.

The literature review, which includes key concepts of the information systems research field such as information security, information security in organisations, and information security culture create the theoretical basis for the bachelor's thesis study. The aforementioned literature along with the protection motivation theory form the theoretical framework of the bachelor's thesis, which is used to interpret and discuss our research findings. That is, the research findings are discussed in the coming discussion chapter in relation to the research aim, and research questions, and are discussed and explained with the help of the theoretical framework.

3 Method

This chapter presents the research design of the bachelor's thesis. The methodological choices of the research approach and the methods of collecting and analysing the data are presented and justified. The chapter concludes by discussing the validity and reliability of the research, as well as ethical issues that are taken into consideration.

3.1 Research Approach

There are primarily three approaches to research. These are the qualitative, quantitative, and mixed methods approach. Qualitative research is appropriate for exploring social phenomena, and it allows for the collection of rich data that can provide insight into our participants' subjective experiences (Oates, Griffiths & McLean, 2022). Qualitative research is based on the collection of qualitative data, which are generated mainly from interviews and observations; not consisting of numerical data (Oates, Griffiths & McLean, 2022). Quantitative research is based on numerical data, which are generated mainly from quantitative surveys and are analysed with statistical methods (Oates, Griffiths & McLean, 2022). The mixed methods approach uses both quantitative and qualitative research practices and, therefore, combines quantitative and qualitative data (Patton, 2014).

We followed the qualitative research approach since our research is based on the participants' thought and perspectives. By conducting qualitative research and collecting our data through interviews, we allowed our participants to express their thoughts about our research topic and us to gain an in-depth understanding of their experiences and perceptions regarding information security challenges and cultures. We also wanted a deeper understanding of the research topic and, thus, deemed the qualitative method as the best method to gain a more nuanced and complex understanding, which Patton (2014) reinforces. We did not see it necessary to combine the qualitative method with a quantitative one due to the limited scope of a bachelor's thesis.

Furthermore, the choice of method was also influenced by our discussions with the Chief Information Security Officer (CISO) at Lund University. We encountered the CISO at a guest lecture that she held. After having some discussions with her, we devised the plan for our research design.

3.2 Method of Data Collection

The qualitative research approach entails several methods of collecting data, among them interviews. We chose to conduct interviews as the purpose of our bachelor's thesis research was to explore current information security cultures and challenges among university researchers. The interviews were semi-structured. Meaning they followed a set pre-determined question template, the interview guide. We have chosen a qualitative approach to gain an in-depth understanding of the experiences and perceptions of researchers at Lund University regarding

information security challenges and cultures. Qualitative research is appropriate for exploring complex social phenomena, and it allows for the collection of rich data that can provide insight into participants' subjective experiences.

Although we conducted our interviews based on our interview guide, the format, semi-structured interviews, allowed follow-up questions which yielded useful information. This supported a more robust and legitimate array of data collected as each interview had its own variances of the same interview guide. When common themes occurred throughout the follow-up questions, we consider this as an indication of relevance. When this was not the case, follow-up questions served to gather additional data.

3.2.1 Research Setting, Sampling Technique, Criteria, Sample Size, Participants and Research Procedure

Our bachelor's thesis research was conducted at Lund University.

We aimed to interview four to six researchers all from different faculties, the number of participants is based on the scope of the bachelor's thesis. Naturally more participants should serve to support the reliability and validity of the data collected. However, due to the scope, we set the initial expected range at four to six as it would give us room to determine whether we had reached saturation continuously throughout the process. Reaching saturation implies that at a certain point the themes of the findings become increasingly repetitive and lose value outside of confirming and validating the previously collected data (Patton, 2014).

The sampling technique used in this bachelor's thesis research is purposive, which means selecting participants who meet specific criteria related to the research question (Patton, 2014). The criteria we set for our participants were the following: the participants should be employed as researchers at the University, they should be working at the University at least two years to have a good knowledge of the university organisation, they should have knowledge on information security. The participants' faculty was not considered when including them in the research. In addition, gender as well as age variables were not expected to influence the research outcome and, therefore, were not considered. However, we did try to maintain a gender balance among the participants.

We found the participants through mutual contacts, the Lund University website and through our network. We thereafter contacted them through e-mail or the social media messaging application. Our primary contact method was through written messages. From the contacted people, we concluded to six participants who met the criteria and accepted to participate in our research. An overview of the participants is shown in the following table.

Table 1. Overview of Participants

Name	Title and Years of Work Experience	Date of Interview	Duration of Interview	Appendix
Participant 1	Associate professor and Researcher, 6	20/3/2023	35:52	4
Participant 2	Researcher, 3	21/3/2023	37:06	5
Participant 3	PhD candidate-Researcher, 3	22/3/2023	19:40	6
Participant 4	PhD candidate-Researcher, 3	24/3/2023	20:58	7
Participant 5	Associate professor and Researcher, >10	17/4/2023	28:03	8
Participant 6	Associate professor and Researcher, >10	18/4/2023	18:47	9

In the above table 1, the real names of the participants were changed to numbers for confidentiality purposes and, therefore, they are presented as Participant 1, Participant 2 etc., which is illustrated in the first column. The second column shows the participants' current title as in academia the researcher's role can coexist with other academic roles, such as senior lecturers, associate professors, professors etc. The third column presents the date that each interview was conducted. The fourth column presents the duration of each interview, and the last column presents the appendix, where each interview transcription can be found.

After deciding on the six participants who met the criteria, we contacted them through e-mail or social media messaging application to provide them more information about our research scope and set available dates and times for the interview. When the interview dates and times were finalised, we sent them the informed consent form via email to read, agree and sign during the interview. The interviews were conducted in March and April 2023 at dates and times convenient for the participants. Three of the interviews were conducted face-to-face at the premises of Lund University and three interviews were held digitally through Zoom to accommodate these participants.

As mentioned earlier, we used an interview guide for our semi-structured interviews. The interview guide was written in accordance with our research purpose and based on our literature review results. We made sure that the interview questions encompassed the topics relevant to our research. The interview guide was translated to Swedish when interviewing Swedish people. We used a semi-structured approach, which meant that the interview questions were sometimes adjusted depending on the answers of the participants. Each interview was recorded with the informed consent of the participants.

3.3 Method for Data Analysis

For the analysis of the transcribed data, we used the 3Cs analysis based on Lichtman (2013). The 3Cs analysis includes the following steps: organising the large amount of transcribed data and make it meaningful in a context, identifying codes, categorising the codes, and finally eliciting concepts (Lichtman, 2013).

Lichtman (2013) further specifies that, one should first start by doing the initial coding through a first careful reading of the text. Codes will appear as you start reading through the text, but some can also be decided on beforehand. The second step is to revisit this initial coding and go through it again to remove unnecessary codes, to clarify as well as to make necessary edits through information that has come up through more recent data. The third step is to categories the codes into relevant categories. The fourth step is to resort or edit the categories. The fifth step is to further revisit the categories and identify whether something is more critical or more important than the other. The final and sixth step is to identify the concepts that makes up the core of what represents the data (Lichtman, 2013).

The entire procedure was the following: We transcribed the data collected through the interviews to be analysed. Transcriptions allow a clear and accurate description of the interview material to be readily available in the appendix for the reader of the bachelor's thesis. It also enables more accurate coding of the data. Additionally, it also serves as a revised, meaning altered for legibility, written source from which one can draw sentiment as well as quotations from. We started by reading again and again the transcribed material to get a full understanding of it and to identify the first codes. The codes were words, or sentences or brief passages of text related to the research purpose and research questions. For example, *challenges, information security breaches, data protection* etc. We moved the initial codes to another document to check for repetitions and redundancies and, therefore, we merged some, while we removed others. We then tried to put the codes into more general categories and therefore some codes were put under same categories. For example, *compliance, data privacy, phishing* was put under the category of information security challenges. We then revisited and checked the categories several times until we concluded to the final ones from which we identified the concepts that presented in the best way our findings.

3.4 Validity and Reliability

According to Oates, Griffiths and McLean (2022), reliability concerns the degree of consistency and dependability of study results, which implies that the study is reliable if its outcomes are consistent and reproducible. Furthermore, according to the authors, methodological choices can make it difficult to ascertain the authenticity of participants' responses, as they may tailor their answers to meet external expectations.

Oates, Griffiths and McLean (2022) further note that constructing a neutral interview guide is crucial in ensuring that questions are not leading, biased, or open to multiple interpretations. This reduces the effect of the researchers' bias on the participant and in turn minimises the risk of drawing erroneous conclusions based on the participants' answers. When formulating the questions for the interviews we avoided language which may have had connotations, implications, or any suggestive language.

According to Oates, Griffiths and McLean (2022) validity can be divided into internal and external validity. They mention that internal validity means that the study should measure what it intends to measure, and that the research must be coherent so that the collected data corresponds to the findings.

Oates, Griffiths and McLean (2022) describe that external validity is related to the research findings and to what extent it can be generalisable to different people or environments. This means that the result should not exclusively be applicable to a specific context. According to the authors, the degree of external validity depends on how representative the research sample is. Due to the scope of the bachelor's thesis and the time restraint associated with this our empirical data is based on six interviews. Based on this, and the fact that the interviews are all conducted at Lund University, one cannot draw generalised conclusions outside of this context. However, it may serve as a potential indication of effective measures and improvements that can be made to information security in the context of higher education. This could in turn be used as insightful information to aid decision makers to make appropriate inquisitions and information security initiatives.

3.5 Ethical Considerations

As the bachelor's thesis covers an important topic, information security, it was vital to consider the ethical aspects of the data collection. We chose to conduct qualitative interviews with active researchers at Lund University using a semi-structured format and have followed more senior researchers' stead in our chosen method of conduct.

To address these ethical qualms, we decided to implement the guidelines presented by Oates, Griffiths and McLean (2022) for conducting ethical research into our process. In these guidelines there are five rights that are highlighted. The right not to participate, to withdraw, to give informed consent, to anonymity and to confidentiality.

These rights were incorporated in the informed consent form they were given prior to the interview. This detailed information about ourselves, the purpose of the bachelor's thesis, how the interview is structured and the extent of it as well as to what end the information will be used. This ensured that participants could provide informed consent for the usage the information they provided through an informed consent form. The recordings were never labelled with labels that can be used to identify anyone and are only shared between ourselves and, on request, our participants.

Additionally, as information security is non-trivial matter, in accordance with Oates, Griffiths and McLean (2022) pseudonyms for individuals and faculty names are redacted, finally we also use gender-neutral-language. This helps us ensure confidentiality, ethicality while serving as a reassuring fact for the participants. This practice ultimately carries over into the rest of the bachelor's thesis as the empirical data is the foundation of which every finding is built upon. This means that it is crucial to ensure the validity as well as the reliability of the data and any derivatives or conclusions that are drawn from it.

4 Analysis and Empirical Findings

The following section presents the themes that emerged from the analysis of the collected data. The themes represent the empirical findings of the bachelor's thesis. The subsequent sections detail the findings, which are supported by quotations from the participants.

4.1 Concept 1: Understandings of Information Security

The understanding of information security varied depending on who was asked. P1 described information security as contextually based and varies on the situation stating:

> *"When you think about information security or security as such, you start understanding it in a way that you target a context. if you don't target the context, you can't really define what security is. If I'm talking about information security in an organisational context, then I must say that information security for an organisation is confidentiality, integrity, and availability."*

Notably they mentioned the triad of Confidentiality, Integrity, and Availability (CIA) which they believed was relevant in the context of an organisation.

P2 set the definition of information security using their own context as the frame for the definition which centred around handling personal information:

> *"If I were to rationalise it in the context of my everyday it would be about how I handle the information, the data, that I receive from my informants."*

P2 found that the central components were how they handle the information they collect ethnographically and that it is handled according to the relevant laws and regulations as well as taking care when working with personal identifiable information.

P3 gave a concise definition revolving around maintaining the integrity of the information one possesses, handling it in an adequate manner:

> *"On a general level? The responsible handling of information so that it is not lost or ends up in the hands of anyone with malicious intent."*

P4 stated that the central question that needed to have a clear answer when defining information security was the following:

> *"Am I the one who has the rights to the data I have collected or is it my supervisor, the institution or the university?"*

P5 expressed they found it to be a hard concept to define, being both broad and complex. For them, the central concepts were the handling of data that is received and produced:

> *"I assume it revolves around obvious things such as patient data where rules are very stringent as it is highly sensitive but also research data. In this context it may revolve around the data being available or unavailable, so to speak."*

The participants also underlined that different forms of data and their nature require different measures and that maintaining control over who has access to this data is a central point.

P6 underlined that the process of collecting and storing data was the key concepts of information security, essentially putting safeguarding the integrity of the data in the forefront:

> *"I would place emphasis on the work we have done with collecting, mostly digital, data and keeping it as safe as possible."*

Concluding, the participants' understanding of information security revolves around integrity, personal information as well as data ownership.

4.2 Concept 2: Communication

The general sentiment found was that the communication from the university regarding information security was often confusing, and at other times lacking. P1, at some level, countered this general sentiment expressing:

> *"One is if you're a full-time researcher, there is a lot of resources telling you what it means to conduct ethical research […]. So, you have all these possibilities to understand what it means to conduct research and really work with this data that you're collecting through your empirical work."*

This statement indicates that there are resources that are readily available for involved parts but does not indicate the level to which their existence is communicated.

P2 mentioned, in relation to the handling of the data, that it was hard to navigate the information security landscape at the university, and how there was not any support given in how to fill out different forms for example. This is mirrored in the following statement:

> *"In my experience it has all been pretty confusing and hard to find the correct answers."*

Furthermore, P2 expressed the lack of discussion between the university and their faculty in particular as they, at times, deal with particularly sensitive data which they exemplified:

> *"An example would be having some kind of critical discussion as to how we are supposed to work with the regulations. To conduct our research do we have to break the rules? We want to be in a situation where we can act according to the rules. This kind of discussion would be good because when it is not, discussions become destructive."*

This same sentiment is brought up in the final question which addresses possible improvements for information security at the university where P2 urges leading information security personnel to act:

> *"Listen to what our challenges are and to actually take them into account when creating the policies."*

All these statements seem to indicate that the discourse between faculty and university is lacking in their context.

P3 described this as one the most lacking aspects of information security at the university. When asked what the university could implement and or improve on, they stated that the university could not provide suitable or approved software alternatives:

> *"The most challenging aspect for us has been when we, in not so critical security contexts use services that are then classified as unreliable by the university."*

The context for this is when their main form of communication software was disallowed which is an essential piece of information as it is relevant to a lot of individuals at the faculty:

> *"When Slack was banned there was no alternative recommended service and when there is a lack of approved alternatives for any purpose people will end up being less cautious."*.

P3 stated that the lack of communication and clarity around what software is allowed results in confusion. This in turn, they surmise, potentially increased the risk for further breach of the information security guidelines due to a lessened sense of caution.

P4 mentioned that more information and transparency was needed in regard to the university's work with information security:

> *"It doesn't feel very transparent, neither what the university is doing nor what I am supposed to do.."*

Furthermore, P4 mentioned that it would be good if the university would continuously inform the research community what was expected of them and what kind of policies and solutions that were in place but also in the works. The lack of communication as well as specific things like a lacking e-mail spam filter led to a worry that university did not have proper control of their information security. This sentiment aligns with P4's closing statement when describing how they felt about the information security at the university:

> *"It feels like there is a general feeling amongst my colleagues that the university doesn't really know what is going on."*

In the same vein P5 expressed that there is a complete absence of useful information related to security procedures:

> *"In general there is nothing official, absolutely nothing formal. Like, now that you are a postgraduate student, this is how you conduct yourself with concern to data. It should be stored here. these are the security procedures when sending emails. I don't have a clue about any of that."*

This statement indicates that the perception is that there is a lack of communication when it comes to the procedures and rules in place at the university. P5 also described having to ask colleagues about the right code of conduct in various security matters.

At the same time, P6 felt that the university raised awareness about and communicated information security well. The individual also said that the university has made good strides in improving the communication around information security policies over the years, and in clarifying what is acceptable and what is not.

Concluding, the participants' opinions on the university's communication varied but a majority described it as either unclear, confusing, or nonexistent.

4.3 Concept 3: Information Security Behaviours

The participants were varied in their responses regarding the information security culture. There was an even division between researchers who believed the information security culture was well-developed and underdeveloped.

P1 praised their department and their focus on information security, but also mentioned that these concerns were considered important all over the university. P6 also thought that the information security culture at the university was good from their point of view as well as stating that there have been marked improvements over the years. When asked if they believed that the university was reliable in this context they said:

> *"Absolutely, and I am able to say this because our IT personnel do a superb job and I feel very safe."*

P2 highlighted that certain faculties, theirs included, seemed reluctant to conform to the present rules set forth by the university. Citing a lack of discussion and accommodation for the high variance of required measures for information security at the different faculties as the main concern. However, their perception of information security culture has changed over time:

> *"In my opinion we have seen a change the past, 5-7 years and because of this it has become more stringent in regard to what you're allowed to do. There is another level of conciseness as to what must be done."*

The lack of willingness to adhere to rules at times was attributed to the frustration at the faculty due to the lack of inclusiveness:

> *"There is an idea that all the rules we need to abide to are drafted without our subject area in mind but rather other subjects that make them incompatible."*

P3 mentioned that there are a few people that take the information security culture very seriously at the university, which might be needed due to what they saw as lacking adherence to information security policies. This is reflected in the following statement:

> *"I feel like these people that take it seriously and are strict produce good results. I believe that we are at least slightly more thorough than we were previously with not using any service on an any American server."*

The people who deemed information security highly important contributed to the information security culture being better but P3still described the culture as laidback and slightly confused.

P4 mentioned that they thought the information security culture at the university was messy, referencing the fact that people they knew did not have backups of their data. This was coupled with what they saw as a general culture of mistrust regarding information security handling at the university:

> *"It feels like people do not put enough emphasis on the matter. I feel like there is a lack of trust that the university can support us in the matter."*

P5 echoed P4's sentiment with an emphasis on the information security culture in general, stating that:

> *"In general the culture is relaxed. I believe that reflects how we all handle it and think of it and that this is the consequence of us not having any information about it. There is no, 'this is how it is done.'."*

Concluding, the participants' perception of information security culture and behaviour is that it is messy, laidback, and confused. Notably there was praise for the IT personnel who were brought up as notable attributers to upholding a better information security culture at the university.

4.4 Concept 4: Handling of Data

Handling of the data was in most cases addressed differently as each field of research collect different forms of data. The only exception was the printing of physical documents. This is because all printers at the university require you to input your physical university access card in order to print.

P1 underlined that sensitive data was never to be shared over e-mail, there were simply other ways of communicating this data:

> *"Let's say I'm running a research project and there is an empirical context where I am going to invite a couple of researchers that have to have access to that very confidential data. I would never share it over e-mail, so as simple as that."*

P1 referred to the data management plan at the university that they were going to follow when handling their research data:

> *"I must make sure that I'm following the data management plan at Lund University, which allows me to store data in a very local repository, so not on cloud services."*

This practice avoids unnecessary risk, they would then inform and give specific access to the researchers that needed access.

One question posed was how to store data long term, where P2 mentioned that there was a lot back and forth regarding how to store their data, but where they eventually reached the conclusion that they would need an external hard drive and store it in a safe, saying:

> *"At the end I was informed that I should buy an external hard drive and lock it into a safe. I thought it was very odd but that is how I begun with my current project so I assume I will have to solve it some other way before the next project."*

P2 was also careful in handling personal identifiable data, and only used Canvas for communicating student names and grades for students. P2 stated that when it came to their informants only their e-mail was used or other digital channels of communication to set up meeting points. This was to avoid the need to extract and store information that could be used by external parties to potentially endanger them.

Physical access to workplaces and eventual physical data was handled differently by the participants. The question posed was how they would have handled a situation where they were going to enter through a door requiring Lund University (LU) card access. In this hypothetical scenario a person was following behind them and wished to enter as well. We asked the participants what their behaviour would be in this scenario and whether they knew of any guidelines regarding this.

P3 would let the person in if it seemed like it was a student and was not aware of any policies regarding this. P3 mentioned that they did not consider this aspect very important stating:

> *"I know I have seen a guideline. Although, as I only enter rooms where research is conducted or teaching rooms, I don't see physical access as such a grave matter."*

P1 would let people in if they recognised the person as being a colleague for example, and if there was someone that the person did not know, would ask them whether they were looking

for someone. P5 mentioned a cultural aspect of being Swedish as relevant in this scenario, that people are afraid of confronting someone else which might be a factor, but that the person still tried to see if the person had a LU card. They could also try to close the door without being seen as unpolite, e.g., keeping enough distance from the person behind them. P5 otherwise tended to ask who they were going to see, but that it was a difficult social situation to handle.

Concluding, the participants' expressed their mindfulness when handling personal information or other sensitive data, especially in regard to email. Dealing with this data, the participants generally favoured local repositories over cloud services. In regard to physical security when put in a hypothetical scenario where this was in question, most would act on their own intuition. Most participants did not know what concrete guidelines related to physical security were put in place by the university or where to find them.

4.5 Concept 5: Information Security Challenges

Regarding information security challenges, a majority related to the deletion of their data or backups. Some of the cited reasons were the risk of ransomware, flooding of server rooms, theft, or other accidents. The risk of data breaches was most detrimental for researchers dealing with confidential information regarding individuals or groups. In these cases, it was very important for the researchers to be able to guarantee that there would be no way for the data to be leaked and or tracked back to the source. This was a point where there seemed to be a conflict of interest in terms of information security practices and conducting research in the field.

P1 described that challenges vary in nature and frequency depending on the individual involved:

> *"Perhaps, it depends on the grade of role you have, so you might deal with certain contexts where you actually deal with information security challenges on a very daily basis. But that's not my context."*

For P1 the information security challenges revolved around conducting research and assuring the safety of data. These challenges pertained to answering questions such as the ones described in the following statement:

> *"So that will be with when you're actually conducting research, how do you make sure that when you're holding interviews, when you're collecting data from surveys. What does it mean for all these people involved? How can you guarantee? Because you're giving them a personal information sheet about your project that you're also giving them a consent form. And so how do you actually stand by that?"*

P2 stated that there was a lack of understanding from the higher-ups of the university regarding their IS policies and how they may impact research conducted abroad. This was described in the following statement:

> *"There are examples of rules that we follow that were obviously put in place in different socio-political context compared to other countries in the world, and the reality there. So, when you are working you have to adjust accordingly."*

As a contrasting opinion P2 also shared an external researcher's perspective on the university's policies and practices:

> *"As we are dealing with external recruitment at the moment it is clear that there are very different ideas of what needs to be done in different countries. It is very, very apparent that many react to it being very strict here."*

P3 stated that in their field of study there was no abundance of information security challenges relating to actual data or sensitive information. However, they highlighted, as previously brought up, that their biggest challenge was communication:

> *"The most challenging aspect for us has been when we, in not so critical security contexts use services that are then classified as unreliable by the university."*

This could serve as a general challenge amongst researchers at the university as there was, at least, a lack of communication in relation to which software solutions were supposed to be used. The stated reason for P3 was that there was a lack of recommended and approved services. To combat this P3 proposed that the university should broaden their catalogue of allowed software:

> *"Make sure that there is an approved alternative for every purpose. This makes it so that people are a lot more willing to abide to the set limitations."*

P4 described a daily information security being avoiding phishing through emails:

> *"I believe that the challenge I face most frequently, unrelated to my research but in my every day is emails. At times it is very hard to determine what is spam or emails that could potentially hack my computer. It feels like spam has become very sophisticated."*

This was followed by the description of P4 having received emails that mimic their supervisor's identity, asking them to enter a Zoom meeting using a link. In addition to this P4 described their experience at another organisation where they received fake phishing emails from the organisation to spread awareness.

P4 highlighted that experience and described it as a fruitful exercise:

> *"It was really good because it taught me to read emails thoroughly. I have yet to receive this during my many years at Lund University, but I would appreciate it. I believe it would be very beneficial."*

Concluding, the participants' listed a variety of challenges mostly centred around communicating clear guidelines, security initiatives and policies. It was also stated that researchers were not involved enough in the decision making and the impact this could have on certain fields of study.

5 Discussion

This chapter constitutes a discussion of the empirical findings of the bachelor's thesis. The findings are discussed with the help of the literature and the Protection Motivation Theory (PMT). The discussion is structured under the research questions. The implications of the research are then discussed in the final section of the chapter.

Table 2. Research questions and correlating concepts

Research Question	Concepts
How do university researchers perceive information security?	1. Understandings of Information security
What are the information security cultures among university researchers?	2. Communication 3. Perceived Information Security Cultures
What are the information security challenges that university researchers identify?	4. Handling of data 5. Information security challenges

5.1 How Do University Researchers Perceive Information Security?

The understanding of information security had variations depending on who was asked, which shows that there is no uniform understanding of the concept. Relating to the CIA (Confidentiality, Integrity, and Availability triad) as defined by ISO/IEC 27002 from Solms and Niekerk (2013), no person mentioned it directly except P1, which meant that the concept forming the basis of information security has not been clearly defined or communicated by the university. Nonetheless, the findings showed that a reference to the CIA triad was made to some degree, i.e., the availability of information and the safeguarding of information. They also related to the general understanding of protection as a concept, as defined by Whitman and Mattord (2017). Thus, the findings showed that there is no common understanding among university researchers regarding what information security constitutes.

5.2 What Are the Information Security Cultures Among University Researchers?

To explore the different cultures among the university researchers and how they perceive it we paraphrased Malcolmson (2009) to give them a baseline for the concept. The definition we used was that information security culture is a component of organisational culture, which determines the perception, thinking, feeling and consequently the behaviour of people working in an organisation related to information security (Malcolmson, 2009).

With this as a foundation the findings of the bachelor's thesis indicate that there are issues related to communication and support of information security. The findings showed that university researchers experience some confusion and a lack of support from their university regarding information security policies and solutions. These observations encompassed various complications related to how to handle sensitive data, as well as a general lack of transparency and communication on the side of the university. Based on the findings the university researchers engaged in different behaviours to resolve the issues, varying from asking colleagues, not taking it into consideration or finding workarounds or circumventions to the policies. These findings align with the Protection Motivation Theory (PMT), which suggests that individuals engage in protective behaviour when they perceive a threat and when they believe that the recommended protective action will be effective (Sommestad, Karlzén & Hallberg, 2015). The findings, in other words, indicate that although there is a clear perception of potential threat of information security breaches there is a lack of trust in or awareness of the recommended protective actions.

Amankwa, Loock and Kritzinger (2022) highlight that a central part of information security is the alignment of policies and procedures with overall information security objectives. According to the authors, this is accomplished by communicating and documenting well-defined guidelines that aid employees in making informed decisions regarding information security. However, our findings showed that the university researchers, when asked about rules, neither could relate them to any guidelines communicated by the university organisation, nor define or pinpoint any form of documentation of the implemented guidelines, procedures, and measures.

Further, the findings showed that some university researchers observed improvements made over the last years regarding communication concerning information security policies by the university. While this is encouraging, it is important to ensure that all members of the university community have access to clear and effective communication and support related to information security.

Concluding, based on the findings, the issues of communication and support of information security can be addressed by providing clearer guidelines and support for handling sensitive data, as well as providing suitable and approved software alternatives. This could potentially be addressed through security programmes. Glaspie (2018) outlined the correlation between information security challenges and information security cultures which, by definition, is directly related to information security programmes. The author also highlighted the importance of information security culture in promoting security policy adherence and in turn adequate information security behaviour. So, in our case, by implementing this, the university can increase university researchers' perception of the effectiveness of recommended protective actions. This in turn should lead to an increase of perceived protective behaviours, which is in

line with the PMT (Sommestad, Karlzén & Hallberg, 2015). Moreover, this suggestion is also supported by Siponen et. al.(2014) who highlight the importance of the perceived experience of information security from the individuals within an organisation. Further they highlight the importance to communicate their continued commitment to information security to help build trust and inspire confidence in their ability to safeguard sensitive information which is aligned with our findings.

5.3 What Are the Information Security Challenges That University Researchers Identify?

Regarding the identified information security challenges by the university researchers, the findings showed that there are many and they vary. Yerby and Floyd (2018) stated that due to the open nature of universities there are unique challenges that come associated with information security in higher education. This is confirmed by our findings. In addition, the university researchers agreed that there is a need for proper training on information security procedures. However, based on our findings, determining who would receive the training, when the training should be offered and who would be responsible for offering the training is difficult. This aligns with Bongiovanni (2019) who attributed this difficulty to the diverse amounts of people that handle information at universities. Thus, this makes proper training harder for the universities to accomplish.

Yerby and Floyd (2018) also describe the potential lack of involvement from faculty and staff at universities as they may see information security as being the responsibility of the IT personnel at the university. This comes in contrast with our findings, which showed that resignation of responsibility does not apply as most of the university researchers seem to either be, or want to be, active in following the progression of information security at the university. Further, our findings showed that the involvement of university researchers in the decision making about information security was supported by the researchers themselves. In addition, the findings showed that there was a willingness related to discourse between the university researchers and their respective IT personnel.

The findings also highlighted the importance of perceived threat and efficacy which in turn affects protective behaviours. This was shown in the finding regarding physical access to workplaces and eventual physical data. Some university researchers were aware of policies being in place regarding physical access, while others were not or were unsure about them. Further, our findings showed that the university researchers were able to recall serious physical breaches that have happened in the past. However, most of them seemed to default to their own judgement as there was no single comprehensive guideline identified by the university researchers. This could be interpreted as lack of confidence in the existing protective actions.

For university researchers dealing with confidential information, the perceived severity construct of PMT is particularly relevant (Sommestad, Karlzén & Hallberg, 2015). Our findings showed that ensuring the security of such information is crucial to prevent potential data breaches that can have severe consequences. However, the conflicting interests between information security practices and research in the field can pose a challenge, as highlighted in our findings. This is an area for university leaders, university decision makers and policy makers to look beyond immediate problems and threats, and proactively work on staying up to date Hu et al. (2012). The findings also showed that there is a lack of understanding from higher-

ups in the university regarding the impact of information security policies on research conducted abroad, something that can exacerbate the already challenging context.

Regarding the challenges of data handling that the university researchers face the findings highlighted a wide variety such as data deletion or loss due to potential threats such as ransomware, server room flooding, theft, or accidents. Apart from printing physical documents which was done in a uniform manner due to the university's printer access policy, a variety of issues was found that centred around storage. The perceived vulnerability construct of PMT here is relevant (Sommestad, Karlzén & Hallberg, 2015). The perceived vulnerability of information assets can be minimised by implementing adequate backup and storage solutions and educating individuals on proper data management as this would increase researchers' confidence. However, in our findings we found a variety of official and unofficial storage processes. These varied from storing hard drives in a safe to having everything backed up in a server room. What should be noted is that university researchers had been reminded to always create backups of their data by IT personnel. The presence and activeness of IT managers seemed to vary between the faculties.

The conflict between information security practices and usability in the context of the strengthening of information security policies is another important aspect that was raised in our findings. Our findings showed that there is a trade-off between security and usability. Furthermore, a challenge is that information security needs to be balanced with access, as also supported by Whitman and Mattord (2017). The perceived self-efficacy construct of the PMT is relevant here as university researchers must have confidence in their own ability to use the system effectively, while also ensuring the security of their data (Sommestad, Karlzén & Hallberg, 2015). This also ties back to the previous paragraph where alternatives for storage were in question. Presenting useable alternative storage solutions for different purposes would allow for more confident university researchers who are willing and able to adhere to information security policies. Our findings also highlighted the lack of approved software alternatives as a challenge pertaining to information security, and the associated difficulty with identifying what is acceptable by the university. The responsibility here lies with the leaders according to Hu et al. (2012), who make a point of setting clear expectations, providing adequate resources and holding individuals accountable for compliance with security protocols. This comes in contrast with our findings as there were cases when the university researchers were informed of unacceptable conduct well after the fact.

Our findings showed that the challenges related to information security illustrate the complex interplay between information security practices and other factors, such as research needs, usability, education, training, communication, and awareness. Additionally, the protection motivation theory (PMT) suggests that individuals' decision to adopt protective behaviours is influenced by their perception of the threat, perceived vulnerability and severity, and their perception of the efficacy of the protective measures, response efficacy and self-efficacy (Sommestad, Karlzén & Hallberg, 2015). Applying this theory to our findings, we can see that most university researchers who view information security as important, take proactive measures to protect their data and devices, and have a higher perceived vulnerability and severity of information security threats. This is especially crucial in the context of large organisations with sensitive data, such as universities. The variance in perceived vulnerability and severity in this case could be seen to directly correlate to the amount of sensitive data handled by the university researchers. This in turn affected their thoroughness when following implemented measures and guidelines. Therefore, PMT provided a useful lens to interpret and

explain the findings of the study, particularly in understanding the factors that influence university researchers' attitudes and behaviours towards information security.

5.4 Suggested Improvements and Measures

Following are suggestions for improvements regarding information security culture and challenges based on our findings. The suggestions varied in nature but often related to either communication or direct actionable measures from the university's side. These are listed below grouped by the nature of the suggestion:

Information security exercises

1 The first suggestion is to introduce exercise phishing mails, where the university sends out fake phishing mails to enlighten people on the importance of being wary what enters one's inbox.

2 The second suggestion is to ensure that there are actual storage solutions to assure long-term safety of data for multiple purposes. In addition to this, in the same vein, allocate resources so that the university can teach one how to manage their data in an official and structured manner.

Communication and documentation

3 The third suggestion is to improve communication frequency for the university researchers to remain updated regarding information security, and to continuously send out reminders regarding this.

4 The fourth suggestion is to improve the accessibility of the university documentation regarding information security. This can be done by informing verbally and/or in writing what these documents constitute and where one can find them. Thus, the awareness about information security is improved.

5 The fifth suggestion is to have a list of approved software and another list of software that is not allowed. In addition, when software is not approved, approved alternatives should be clearly suggested to avoid functional voids.

Miscellaneous

6 The sixth suggestion is to consider the physical security of e.g., paper documents, which currently is prioritised to a lesser extent when compared to the comprehensiveness of digital security.

The participants provided valuable insights into their views on the university's information security (IS) measures and offered several suggestions for improvements. Using the PMT framework, we can analyse the perceived effectiveness of these suggestions in mitigating the potential threats and risks to the university's information assets (Sommestad, Karlzén & Hallberg, 2015).

The first suggestion was to introduce exercise phishing emails to educate individuals on the importance of being cautious of suspicious emails. This suggestion aligns with the PMT's perceived severity construct, which emphasises the importance of understanding the severity of potential threats (Sommestad, Karlzén & Hallberg, 2015). By exposing individuals to fake phishing emails, the university can illustrate the severity of the risks associated with phishing and encourage individuals to be more cautious when handling emails. Phishing awareness is also brought up by Wlosinski (2019) who also describes the importance of educating individuals of password hygiene and data handling protocols.

The second suggestion made was to ensure that there were adequate storage solutions to ensure the long-term safety of data, and to teach students and staff how to properly manage their data. This suggestion is in line with the PMT's perceived vulnerability construct, which emphasises the importance of minimising the vulnerability of information assets to potential threats (Sommestad, Karlzén & Hallberg, 2015). By providing adequate storage solutions and educating individuals on how to manage their data, the university can reduce the likelihood of data loss or theft due to user error. This practice of educating stakeholders is also described as a key component by Wlosinski (2019). This entails education and training on security policies, procedures, and best practices, and ensures that the university researchers are capable of handling sensitive information in an appropriate manner.

The third suggestion was to improve communication about the information security measures in place and send out reminders regularly. This suggestion aligns with the PMT's perceived response efficacy construct, which emphasises the importance of awareness and involvement in mitigating potential threats (Sommestad, Karlzén & Hallberg, 2015). By keeping people informed and reminded about the latest information security measures, the university can increase involvement and reduce the likelihood of potential security breaches due to individual negligence.

The fourth suggestion was to improve documentation on information security measures and to educate everyone of their importance verbally and in writing. This suggestion aligns with the PMT's perceived self-efficacy construct, which emphasises the importance of confidence in their ability to mitigate potential threats (Sommestad, Karlzén & Hallberg, 2015). By providing clear and accessible documentation and verbally educating people on information security measures, the university can increase confidence in their ability to mitigate potential security risks. This, along with the suggestion two and three is also in line with what Wlosinski (2019) describes as effective information security practices.

The fifth suggestion was to provide a list of approved software and alternatives to prohibited software. This suggestion aligns with the PMT's perceived costs construct, which emphasises the importance of understanding the costs associated with potential threats (Sommestad, Karlzén & Hallberg, 2015). By providing approved software and alternatives to prohibited software, the university can reduce the likelihood of potential security breaches due to the use of unauthorised or vulnerable software. This is an actionable suggestion that the leaders need to address as setting expectations for employees, providing backing for security initiatives, and holding individuals responsible for their adherence to protocols is vital, as also supported by Hu et al. (2012).

The sixth suggestion was to consider the physical security of paper documents in addition to digital security. This suggestion aligns with the PMT's perceived susceptibility construct (Sommestad, Karlzén & Hallberg, 2015), which emphasises the importance of understanding

the potential vulnerabilities of information assets. By acknowledging the vulnerability of physical documents and taking appropriate measures to secure them, the university can reduce the likelihood of data loss or theft due to physical breaches.

Overall, the suggestions provided by the university researchers through our findings offer valuable insights and improvements on information security. By using the PMT to interpret and discuss these suggestions, one can better understand how they can contribute to mitigating potential threats and risks to the university's information assets.

6 Conclusion

6.1 Practical Conclusions

This bachelor's thesis research focused on information security. With the growing use of technology in research, information security has become an increasingly important concern for academic institutions, which face, among other, challenges related to the protection of sensitive data from unauthorised access, theft, and misuse. The research purpose was to explore the current information security cultures and challenges among university researchers with the aim to make suggestions to overcoming the information security challenges, if any, and improving the information security culture. To achieve the aim of the research, we posed the following research questions:

How do university researchers perceive information security?

What are the information security cultures among university researchers?

What are the information security challenges that university researchers identify?

For this a study was conducted where the empirical data were collected through semi-structured interviews with six purposively selected university researchers at Lund University and were analysed thematically. Five themes emerged from the analysis of the collected data that represent the research findings. The findings were then explained and discussed with the help of the literature review and the protection motivation theory to conclude to the research outcome.

The findings showed that university researchers have different perceptions of information security, which are influenced by their individual and, at times, by their colleagues' experiences in their research area. Some researchers view information security as a critical component of their work and take proactive measures to protect their data and devices. Others view information security policies as a hindrance to their work as they must be circumvented to allow them to work smoothly. Overall, there is a need for more awareness, training, and support to help researchers better understand the importance of information security and how to implement effective security measures and precautions. This should be tailored for their area of research and involve them actively partaking in the decision making. The findings showed that improving information security requires a multifaceted approach that includes education, communication, documentation, physical security measures, and software regulation. By implementing these recommendations, the university can ensure that its staff and students are better equipped to protect themselves against cyber threats and maintain the security of its sensitive data.

In addition, the findings showed that there are different information security cultures among university researchers. A minority of the researchers believed there is a general culture of responsibility and accountability amongst their colleagues, while the majority felt that it was either too relaxed or messy. The findings showed that information security culture is influenced by various factors, such as personal experiences especially in relation to the policies in place at

the university. Some university researchers expressed lack of trust in the university's ability to support when it comes to information security matters. Others expressed lack of willingness to adapt to information security policies set by the university. This was due to absence of discourse between faculty and the people in charge of information security at the university.

Concluding, university researchers face various information security challenges, such as the lack of secure storage solutions for sensitive data, the difficulty of keeping up with constantly evolving threats and technologies, i.e. ransomware or phishing attempts, and the limited resources and support for information security. Other challenges include the lack of clarity on institutional policies and guidelines, the difficulty of balancing convenience with security and the lack of alternatives for what was deemed as unapproved software services.

Thus, the bachelor's thesis research contributes to the information systems research field by improving the understanding of factors that influence university researchers' attitudes and behaviours towards information security in higher education. It also contributes to university decision makers and policy makers, university staff and other interested stakeholders regarding measures and practices that can be taken to overcome information security challenges and improve the information security culture.

6.2 Suggestions for Future Research

Information security among university researchers in higher education requires further research as universities constitute a vital foundation in society, and, at the same time, represents a unique environment.

An interesting future study could replicate our research with a more extended number of university researchers to strengthen the research results. Another suggestion is to conduct similar research by including more than one university from the same or other Swedish regions and make a comparison. In addition, future research among university researchers from universities in different countries would be of interest. Finally, a suggestion is to repeat a similar study complemented with quantitative data.

Appendix 1 – Informed Consent Form

Informed Consent Form for Bachelor's Thesis

Date: March 2023

Title of the Research: Information security challenges and cultures among researchers at Lund University

Researchers: Albin Westermark, Fabrice Lindblom-Levy, Bachelor's Programme in Information Systems, Lund University, mail@student.lu.se, +46 70 000 0000, mail@student.lu.se, +46 70 000 0000

Purpose of the Research:

The purpose of our bachelor's thesis is to research the current information security cultures and challenges at Lund University among researchers. We also aim to explore how to overcome the challenges if there are any and see whether an improvement to the information security cultures is relevant.

What you will be asked to do in the Research: You will be asked to participate in an interview not more than 45 minutes for us to receive an understanding of the information security cultures and information security challenges at Lund University. By later analysing the answers, it will help us understand the current state of information security at Lund University, as well as potential areas for improvement.

Risks and Discomforts: We do not foresee any risks or discomforts from your participation in the research.

Confidentiality: Your identity will not be revealed in the thesis. Additionally, your full name will not be exposed during and after the research. The results of our meeting will be used solely for the purpose of the research. Your contribution will only be shared with us and our bachelor's thesis supervisor. Confidentiality will be provided to the fullest extent possible by law.

Benefits of the research and benefits to you: As the researchers, we will acquire knowledge and understanding about the existing situation regarding your perceptions of the current information security culture and challenges at Lund University. As a researcher at Lund University, you could benefit by learning of other researchers' perspective on the matter. It also brings potential points of interest to the forefront which may contribute to a higher level of information security.

Voluntary Participation and Withdrawal: Your participation in the research study is voluntary. You may refuse to answer any question that makes you feel uncomfortable, or you

may choose to withdraw your participation at any time or any reason. Your decision not to volunteer or stop participating will not influence the nature of your relationship with the researcher or Lund University either now, or in the future. In the event you withdraw from the research study, all associated data collected will be immediately destroyed.

Questions about the research: If you have questions about the research or about your role in the research study, please do not hesitate to contact Albin Westermark or Fabrice Lindblom-Levy either by telephone or by e-mail.

Legal Rights and Signatures: I consent to participate in the research study "**Information security challenges and cultures among researchers at Lund University**" conducted by Albin Westermark & Fabrice Lindblom-Levy. I have understood the nature of this research study and I wish to participate and allow the recording of the discussion. I am not resigning any of my legal rights by signing this form. My signature below indicates my consent.

Signature:

Participant: X

Date: X

Signature:

Researchers: Albin Westermark & Fabrice Lindblom-Levy

Date: X

Appendix 2 – Interview Guide

Introduction
For the sake of the interview, could you please state your name and your role at Lund University?
Based on your role as a researcher, what is your area of research (or research field)?
How long have you been a researcher at Lund University?
Do you have previous experience as a researcher at other universities? If so, for how long and which universities?
Main Questions
How would you define information security based on your understanding of the term?
What training or education on information security measures or policies at Lund University have you received? What training on information security measures or policies have you received at other universities?
How would you describe information security at Lund University (do you think that information security is taken into adequate consideration at Lund University)? Why?
Main Questions: Information Security Cases
How do you handle confidential data when exchanged via email? Could you give us an example?
How do you handle confidential data when printing out physical documents? Could you give us an example?
How do you handle confidential data when sharing data with others, both digitally and physically? Could you give us an example?
When accessing rooms that require a LU card and there is another person present that also wants to enter, how would you handle that situation? Are you aware of any rules regarding this scenario?
Please share an information security breach or incident/scenario that would have the most devastating impact on your current research.
Main Questions: Information Security Challenges
What would be some information security challenges you encounter in your daily research at Lund University?
Main Questions: Information Security Culture

Would you say that there is an information security culture at Lund University?
Do you have any thoughts on how the information security culture at Lund University could be improved? Please share concrete steps and activities if possible.
Closing Part
To conclude, do you have any additional thoughts or comments related to information security?

Appendix 3 – Interview Request

Hi x,

We are two students studying Information Systems. Our bachelor thesis will focus on information security at Lund University, and more specifically on researchers' experiences of the information security culture and any perceived challenges with information security. We will conduct interviews with five researchers at Lund University during the month of March.

First and foremost, are you conducting any active research at the moment at Lund University? If so, we would be very grateful if you could take the time to participate in an interview in relation to our thesis. The interview will take about 30-45 minutes. We are very flexible when it comes to time and place and have the opportunity to come to wherever you are. We also have the possibility to conduct the interview on Zoom but prefer to do it in person.

The interview data will be treated confidentially and only in the context of our bachelor's thesis. Your name will not be included in the bachelor thesis.

At the time of the interview, you will be asked to sign a consent form. The consent form further clarifies, among other things, the purpose of our research project, what you will be asked, the integrity aspect and other clarifications. If you are interested in participating, we will email the consent form to you before the interview so that you have the opportunity to read it in advance.

If you are conducting active research, would you be interested in participating? If so, what days and times (e.g. morning/afternoon) would suit you? If you are not able to participate, that is of course no problem.

Thanks in advance for your help,
Albin Westermark & Fabrice Lindblom-Levy

Appendix 4 – Interview 1

AW

My name is Albin, and this is Fabrice. As stated, we're conducting a study on information security challenges and cultures at Lund University.

AW

For the sake of the interview, please state your name and your role at Lund University.

P1

Yes, thank you for very much for inviting me for this interview, Albin and Fabrice.

P1

My name is [redacted].

P1

I work as an associate professor at [redacted] Lund University.

FLL

Based on your role as a researcher, what area of research are you conducting?

P1

So my research area focuses on [redacted] And I do tackle different [redacted] So my most recent work [redacted]

AW

Right. And how long have you been a researcher at Lund University?

P1

Right, so I started at Lund University since 2015 and 2016 versus January basically, I had a full contract where I started to conduct research activities directly. Before that I was so in 2015 when I started, it was more about educational activities, but at the same time I was, uh, employed at [redacted] as a full time researcher and so and then 2015 was a year when I kind of distributed my percentage to work as a researcher at [redacted],

while as an educational teacher and then moved slowly or gradually to Lund University fully. So now I conduct research only here.

FLL

I believe that ties into our other question that do you have any previous experience as a researcher at other universities and if so how long?

P1

Right, so my research experience actually spends beyond just Lund and [redacted]. I started my PhD studies full time PhD studies at [redacted]. So five years at [redacted] and actually after that I also stayed for post research activities at [redacted] again for another two years. In 2012, I also had the chance to stay for half a year at the [redacted] where I went solely for research purposes. So I do have a couple of experiences across four different universities and of course not to forget that I have been to many conferences and other visiting universities and I have visited other universities around the world for research purposes, mostly on a short stays.

AW

Right. So now we're getting into the main questions. So let's start off by how would you define information security based on your understanding of the term?

P1

Well, so, uh, when you think about information security or security as such, you start understanding it in a way that you target a context. If you don't target the context, you can't really define what security is. If I'm talking about information security in an organisational context, then I must say that information security for an organisation is confidentiality, integrity and availability. So organisations have to be very wary that they have to couple in for security as such by understanding technological and information security, but then also other dimensions that pop up with security. You have only cyber security. You can have only physical security. And how do you view that? So I would say information security has multiple dimensions. It is does not really provide a clear definition unless you have a context to actually define it. So that was the organisational context, and that mostly pertains to my early research work.

Then if I start talking about information security from a more individual perspective and again individual, it can be an employee perspective, but I'm moving a little bit away from that and I'm saying individual, as you know, a typical citizen. If you think of information security as a citizen, then the first thing that comes to your mind is to say, oh, I want to keep my data secure. That's what information security would be. But then you see we are already using different terminology here. We're seeing data, we're seeing information, information that's kind of an evolutionary perspective. People think first. Oh I want my data or information. They use this interchangeably and not necessarily that is interchangeable. Well, from an individual perspective, information security would mean that you want to protect the right of the individual of and their information that they actually share online and information can be interpreted in many ways.

You can submit a picture on a social media network as an individual, and then that picture might have a meaning, right? So as long as it has a meaning, then it is information and so if you want to put information security on that type of posting then that individual feels like I have shared it into a closed network and this is where it should stay. That's the belief that individual might hold. But in fact, if that service that allows you to actually share that information is not that protective, the individual might not be able to comprehend it that way and still believe that they have information security. But they might not, and again sometimes that protection is leaked and then maybe partial information is shared, which means that it is bits and pieces of your data so because as we know data can be anything, data can be just an address of mine, but nothing else pointing at me. Yeah, but data can also mean just my surname. Without again pumping it more than just that, as long as we start combining an address, a surname, and maybe you start realising that there is also a name related to it, then here it is. We've got information about a specific person.

FLL

What training or education on information security measures or policies at Lund University have you received? And I can highlight that we wanted to contrast this with potentially what training or measures you've received at other universities.

P1

Right. Well, so all of the universities that I mentioned have not really given me any particular type of training or particular type of measures that I must comply with.

When I conduct research, that means that at the current state, universities are often recognised as some of the most vulnerable institutions out there, mostly because you see they are a bit reactive rather than proactive.

I understand now that my university is very cautious about these matters. And at the same time, depending on the type of research that you conduct, you are actually introduced to different measures that must be taken to make sure that the data that you produce as a researcher must be protected. So in our university, we do have different. I would call it a platform that contains different services on how we make sure that there is a potential to actually safeguard the data that we produce through our research, but that there is a particular training about information security and its measures. That's not the case. Maybe that's in development, but how do you actually collect data, store data, keep data or all the longevity of data after you've stored it, and how you also dispose data. That is in place.

Actually Lund University have a system called data management plan. And the system allows you to make sure that any kind of research that you're conducting, whether you're a doctoral student or a full professor, so all the range in between, you must use the data management system.

And that data management system allows you to actually develop and really unfold the way of how you're gonna from data collection to data disposal. If that's the case because you know you can keep the data for so long and maybe at some point you want to dispose it. So how does that even happen?

Data storage is also very critical. I know that at Lund University also, the IT department offers a lot of explanations on what it means to store data. Because we know, as researchers,

we often tend to use easy services such as cloud services so you and these cloud services can also be available through your university, through my university, but at the same time we have to be cautious on what kind of data you can store there because a lot of that data that is stored, if it's a cloud service, the actual repository that is holding it's not in Sweden at all. It might be elsewhere so that all starts to jeopardise the safety of that data. So we have to be cautious about that. So there is a lot of information, there is a lot of ways to find out how you can make sure that you conduct research in the most ethical way, but also how do you make it possible that this research progresses without jeopardising the safety of the data.

AW

Right, OK. This ties into our next question, which is how would you describe information security at Lund University in relation to whether information security is taken into adequate consideration at Lund University?

P1

That's a very good question and I would see this as two levels. One is if you're a full-time researcher, there is a lot of resources telling you what it means to conduct ethical research and there is all these services in place and that's why earlier I said all these services call it the platform because they're all kind of interconnected with one another. So, you have all these possibilities to understand what it means to conduct research and really work with this data that you're collecting through your empirical work. And at the same time at Lund University, you can also be, you know, just typical student or a typical employee that not necessarily collects data for research. So what does it mean if you're using services that are not connected to the university, but you have a computer? That is the property of the university. Do we have the right training in place or the awareness in place? I think this is not true at the moment, but this is developing. I know for a fact that Lund University is very serious about what it means to train and raise awareness for information security practice practices at Lund University. And so that is evolving very rapidly I would say.

FLL

The next questions are in pertaining to information security cases, this is in particular handling of data and this is your data that is in question and we're just asking how do you handle confidential data when exchanged via e-mail? Could you give us an example?

P1

Right. So that's another very, very good question. Let's say I'm running a research project and there is an empirical context where I am going to invite a couple of researchers that have to have access to that very confidential data. I would never share it over e-mail, so as simple as that. It can be that I'm conducting interviews and these interviews are going to hold a lot of private data of that interviewee. I must make sure that I'm following the data management plan at Lund University, which allows me to store data in a very local repository, so not on cloud services. and then give access to these colleagues that have to access the data direct at the storage and maybe mention that this is the data that is in the storage rather than using the e-mail to share that.

AW

OK. And how do you handle confidential data when it comes to something you have to print out as a physical document? And could you give you an example here as well?

P1

That's another very good question and I'm not sure it fits very well with me because I basically do not print, also for the environmental reasons, I just do not print unless it is of utmost importance, but sometimes again, sometimes I might need to print a paper. What I can say is that at my department, we do have a printing office. And all the facilities there are actually making it possible that any data that you print that are confidential can actually be destroyed completely, such as we have a shredding machine. So or we have a box where you can put the put the paper in and then it will be shredded by a responsible staff. So in that regard, again, I barely print, so any confidential data that I would have to be printing I'm hoping I don't need to because I don't really like printing. Mostly, as I said, for environmental reasons. But if I do and I know that it holds very confidential data. I would try to manage it as best as I can. Sometimes you have to mail it and I put it in the mailbox which is protected by an office where only people with the right access can enter it. So this is how I view it. Printed data and its movement. Right? Because you have to mail it, let's say. I would be dependent on a lot of services that are actually working with that data, such as I have to also trust the organisation that offers the service of transportation. So postal services for us.

The whole chain of events, it's not about only me holding that data, but what happened with that data when it actually leaves my hands. Goes through that protected office and then from that office, who takes it? And how does the whole transport work? So I have to rely on trust and trust that organisation, that takes care of that data, knows that it must be kept confidential.

FLL

How do you handle confidential data when sharing it with others? Through discussions in physical person or through Zoom?

P1

Right. So data as in research, right? Data as in research, we would have a service. Let's say we're using interview data and there is a service for us available through a software called NVivo. We'll put all the data on NVivo. Holding that locally in your computer. I wouldn't go through zoom and share that and say here here's what I've done. I'd rather anonymise, produce the 1st results, send it over to a colleague in a complete anonymous way, right? So if I induce some meanings out of that data from interviewees I haven't already recognised their names or. Jeopardised their identity, but rather used what I have identified in an anonymous way and share it. That's what I will do. But not directly and not directly. And if we would meet again, it's from a local perspective, I would open my computer and show it. And again, a lot of the transcribed data, we don't put the name on it. So it's not that someone is going to identify a particular person who said what if I have to? I have to do that, but then this is again this is a specific type of empirical data collection. I'm talking about interviews. You can have other types of data collection as research such as you can have quantitative data through surveys. You can have quantitative data through specifically very rigorous design experiments as well. And again, as a type of researcher, I am, I don't deal with data that some of my colleagues let's say the medical faculty would deal. Right. So in my interest, I don't work with very delicate data where patients'information are put to test of confidentiality. It's more about right, talking about privacy is still a very, very delicate matter, but it's not in my interest to identify any

person in that regard. It's more about. Understanding how people view privacy and what does privacy mean for them. So that kind of data is still I want to safeguard it in every way possible because I don't want the data to be leaked for the reason of being stolen, right? I don't want that data to be stolen. It's my research independent of what it holds, whether it is based on information or not. It's still my data, my research data.

AW

Next question is when accessing rooms that require a LU card and there's another person present behind you, to those wants to enter. How would you handle that situation? And also, if you're aware of any rules regarding this scenario?

P1

So you're talking about that other person and you always think who is that other person? If it's my next door colleague, of course you don't even question it. It's very natural. But if it's a very new stranger. I have noticed not this behaviour not only myself, but also. My colleagues like. Are you looking for someone? Right. So you wouldn't act before you actually question the stranger, right? That's the typical behaviour that I've, again, I've seen it across most of my colleagues, including myself, because that's I think very natural to do as well.

FLL

Are there any rules in regard to this or is it just the natural behaviour on your part?

P1

Well, so of course there are rules. For instance, at our department, our department is closed from 12 to 1 and now if and only people with access are able to get in. Now if you find someone that you just saw a very new face, right? I'm not talking about students because sometimes the teacher might have something with students, you know, seminar at the lunch time. So you would all open the door for them, but if you find someone just, you know, lurking around without understanding what they're doing, that they're not accompanied by someone at the department. Then of course. We don't take it very lightly. It's like we are told that we must be cautious about these things.

So first thing you do, we have a safety representative. It's best if you actually go to the safety representative. Then you have the head of department. Then you have the school itself which has different resources to report strange events. If that's the case, so of course we have a line of orders, so to say, to actually report strange sightings, misbehaviour and all that.

AW

And also if you could share an information security breach or incidental scenario that would have the most devastating impact on your current research?

P1

Yeah, I think I touched a little bit up on this earlier on, but it would be if the data that I've stored from an empirical setting, it could be hours of Research work right, because as a researcher, you go out in the field and collect the data. Yeah, it could also be very costly because sometimes as a researcher, you might pay for secondary data, and if that is stolen,

then it becomes a huge problem, right? That is very critical because. Not only are you losing as an institution, you're also putting the safety of these people involved in that research. Putting their safety into the hands of an intruder.

FLL

Yes, we have one question regarding information security challenges specifically and that is what would be some information security challenges you encounter in your daily research at Lund University.

P1

I wouldn't say that you would have daily challenges. But challenges that are more spontaneous at time to time rather than daily, because once you're in a routine on how you work at an institution, be it at Lund University or elsewhere. Perhaps, it depends with the grade of role you have, so you might deal with certain contexts where you actually deal with information security challenges on a very daily basis. But that's not my context. So I wouldn't say it is daily, but rather more spontaneous. So that will be with when you're actually conducting research, how do you make sure that when you're holding interviews, when you're collecting data from surveys. What does it mean for all these people involved? How can you guarantee? Because you're giving them a personal information sheet about your project that you're also giving them a consent form. And so how do you actually stand by that? Because again, your role is to protect that. But what if that is stolen? What if a repository that you feel it has been very safe has been actually compromised? What happens then? So that is the challenge. That it is at the back of your head. What if this happens. That's what I would say.

AW

And going forward, we're going to ask a question regarding the information security culture. According to Malcolmson, 2009 security culture is defined as assumptions, values, attitudes, beliefs and behaviours of members of an organisation that could impact the security of that organisation. And would you say, how would you describe the information security culture at Lund University? And would you say that there is a culture of information security at Lund University?

P1

Right. So if I talk from my very own perspective, which is representing my department rather than the whole university. I would say that we have a strength as a department because we focus on information systems and that means that security takes a central role in that kind of field. As opposed to other departments that might not have this edgy focus, I would say so as, so influenced by that by, by my own context, where I work at Lund University, I would say that we do definitely have a culture and information security culture because I know how rigorously all of my colleagues would speak of what it means. To be ethical with all the data that you collect. But whether that's the case or that holds true for everybody else at university at large, it is very difficult to say. But what I know is that when you are a researcher at Lund University, you know very well that you have been trained on ethical matters. Right. So that kind of training as a researcher is definitely a must. And it is always put into practice and into place at Lund University for all researchers, and that everybody talks about these ethical matters quite openly. I just started to have some discussions with colleagues at the Faculty of Social Sciences. And I have realised that in that conversation, they are as wary and as careful

about these matters as we are, right. So even though I feel that my perspective really drives me to think more and my colleagues as well, about information security and create that culture where the ethical perspective is really key, right? So what does it mean to hold data that is not yours? That is private, that it belongs to someone else? How do you deal with that? And I realise that the colleagues you know down at the centre from us, they work with us just as well as we do, so I believe that there is an information security culture. Across all the researchers at Lund University on what they do, how they work ethically with all the data that they collect for their research.

AW

And do you have any further thoughts on how the culture could be improved and whether you have any concrete steps or examples that you can think of as of right now?

P1

Exactly. What I would recommend, and I see that lacking, is to be a bit more vocal about this matter, reminders, right? So I would say that Lund University has to has have... a way on reminding all of their employees, not just employees that conduct research. Because, as I said, those are that might be more wary about information security practices and have that culture because they deal with something very delicate. But at the same time, employees who are teaching, they also deal with very, very delicate data when it comes to their students. So across all the employees, but also across all the students. I would say that Lund University would need to have a practice in how they send reminders, right? So be very, very pointy at that. It's about information security and the practices at our university wall equally. And then if you want to target certain groups. Of course, these reminders will work just as well. But it feels like reminders are not as important. And again, if you create a culture, maybe you don't need the reminders. But what if a system is changing or a small practice has changed. You've got new employees and I think it takes a lot of courage to actually bring in everybody into the culture, so instead of... Letting it flow more slowly, perhaps you can speed it up by being very concrete and very specific with how you send out reminders, what it means to conduct research, to work with student data and grades, because it's all very, very detailed profiles on the grading system such as Ladok, but also students themselves. What it means for the students. Because all of our students are writing research work at the end of the day which asks them to produce data. How, where are they? Right? So do we have everything in practice?

FLL

Additionally on that one, do you have any? Is there anything you've experienced that other universities that you've been a researcher at do better like [redacted] or?

P1

I don’t know, I don't necessarily see any huge difference in that regard. Well, so I'm talking about the times when I was at [redacted] almost 10 years ago, and then at [redacted] is a couple of years old as well. I don't know what they're up to in today's context, but I believe that everybody is rapidly progressing towards more concrete ways. So all of these institutions are becoming more aware of what it means to do information security, especially in in a world where the physical and the digital are intertwined and that the digital in many ways is taking over and then the digital as we know it as well. Offers more room for insecurity. So just

having that fact upfront. Everybody is stepping up and trying to be more wary of what it means to. To educate, to train. To raise awareness, but as well as to keep a culture developing in this regard because the information security is not uhm that it stays in a position. That it sustains itself, but rather it evolves all the time. So we have to evolve with that as well.

FLL

This is the final question, the closing part. To conclude do you have any additional thoughts or comments related to information security or perhaps the interview questions or anything a like?

P1

Yeah, what I would like to close this with is that if we look at information security from a societal perspective, I think that that there is a huge discrepancy on what it means to understand your own safety online. Nowadays you have all these children online, right? And the whole dependency on what it means for them to share their private lives as a child depends on their parents. And to me, this is very critical because not every parent views privacy equally. And if we don't view privacy equally then, we are leading a digital world out there that can be extremely dangerous for the safety of a child. So in my perspective, what I see is lacking is that in this country, in all the countries in the world. The web is really developing exponentially, and with that their dependency on our data is increasing even more. The danger that it represents to the younger generations is substantial, and we must take action. We must be more vocal. In knowing how do we actually raise a child nowadays, right? Raising a child is not only about teaching them how to save. We climb a tree and jump from that because we know that that could cause physical harm if they don't know how to jump or how to climb down. I think we should treat the, their data privacy online as same as that right. It is so fundamental that we should start acting rather than ignoring it. So that's what I would like to end this with.

AW

OK. Thank you for participating in the interview. It's really appreciated.

P1

Thank you very much. It was a pleasure to be here. I do hope that some of what I have said today will be useful for your work.

Appendix 5 – Interview 2

AW

Så som sagt [redacted] välkommen till intervjun så för intervjun skull kan du uppge ditt namn och din roll vid Lunds universitet.

P2

Ja, [redacted] är mitt namn och jag just nu så är jag forskare i [redacted]. Jag undervisar också i [redacted] och [redacted]

AW

hur länge har du varit forskare vid Lunds universitet?

P2

Jag har ju varit forskare lite av och till för att jag är anställd som forskare varje gång jag får externa medel, men just nu den senaste gången så är jag på Jag 3 år. Jag är på ett fyraårigt projekt finansierade av ”vetenskapsrådet”. Så ja, nu är jag på typ år 3/4 4,5.

FLL

Har du någon tidigare erfarenhet som forskar vi andra universitet?

P2

Det har jag inte. Jag, nej, jag diskuterar det här och har bara. Forskat på Lunds universitet.

AW

Hur skulle du definiera informationssäkerhet utifrån din förståelse av begreppet?

P2

Nej det, det känns nästan som en kuggfråga nej. Om jag liksom bara det rent operationaliserar den ner i min vardag så handlar det om hur jag hanterar den information, den datan jag får in från mina informanter. Jag jobbar etnografiskt. Jag har väldigt mycket intervjumaterial. Det är väl det, för mig, som det handlar om. Att jag hantera detta tillräckligt säkert enligt lag och regler och jag arkiverar ordentligt och så. Sen kan man ju kan jag också se att det handlar lite om hur man sprider personuppgifter runt i systemet. Ja, om man till exempel väljer att man har någon lite mer ledande position och man väljer att skriva namn på folk eller e-post och den typen av personuppgifter, det är nog informationssäkerhet för mig.

FLL

Har du fått någon utbildning eller träning om information säkerhet? Riktlinjer eller policy vid Lunds universitet?

P2

Nej det har jag inte men jag har ju gått igenom en etikprövning av mitt projekt och innan jag skrev den etikprövning ansökan till den här etikprövningsmyndigheten då. Då var jag med på någon sådan workshop som hölls om just det och det är mycket av det som ju inte handlar om informationssäkerhet, men en del av det gör det ju alltså. Så det är nog det enda som jag har.

AW

Utifrån din definition av informationssäkerhet och hur skulle du beskriva informationssäkerheten vid Lunds universitet?

P2

Förvirrad skulle jag vilja säga. Nu har vi liksom varit med några år och har kontakt med bibliotek och IT enhet och sådär. Jag kan inte riktigt bedöma vad som är Lunds universitet och vad som återfallit i alla frågor här. Men från mitt perspektiv så har det ju varit väldigt många frågor kring när den här till exempel och den här etikprövningsregeln kom och att alla projekt skulle prövas. När vi alla behövde implementera det så var det väldigt förvirrande med data, hanteringsplaner och särskilt var saker ska lagras. Arkiveras säkert. Det har varit så mycket fram och tillbaka och nu har jag förstått att det nog finns någon säker krypterad tjänst någonstans. Men när jag började mitt projekt så var allt bara uppe i luften. Det gjorde att jag fick liksom köpa in en extra hårddisk som jag låst in i en safe på ett kontor liksom. Det var det är det gamla sättet för att det var ingen som visste bättre. Så min erfarenhet är att det mesta har varit ganska förvirrat och det har varit svårt att få raka svar. Sen inbillar jag mig att det har blivit bättre sedan att jag startade upp. Eller att mitt projekt startade i en period när alla skulle få saker på plats så jag hoppas och tror att det har blivit bättre.

FLL

Har du någon reflektion om varför den här förvirringen kan uppstå eller varför det är otydlig kommunikation kring riktlinjerna?

P2

Nej, jag kände väl att det var typiskt Lunds på vissa frågor att det när väl typiskt Lunds universitet, det är en jättestor trög organisation så jag bara tänker att man började för sent och sen liksom skulle allt fixas på en samma gång. Sen gick det inte för att man inte har haft ordentliga digtaliserings- och lagringsmöjligheter förräns typ nu tror jag. Ni vet säkert det bättre än jag, men bara det är ju helt absurt tycker jag det borde man ha börjat jobba med för 15 år sedan liksom, jag tror att det är lite så att man är lite sen på bollen. Vi behöver det nu inte liksom inte om 3 år och så vidare och sen blev de bara förvirrat av det. Sen tror jag också att det är många kockar. Det är helt enkelt för mångas som fördelats ansvaret och på många olika nivåer. Då flyter inte informationen lika bra. Så ja, det blir sådana saker tror jag rent organisatoriska. Sen är det möjligt att det finns eller att det har funnits utmaningar från annat

håll av annan karaktär som jag inte känner till, som har gjort att det försenats liksom. Men på någon tidpunkt var det jättesvårt att få information. Man sökte överallt och alla sa liksom sa att ja, men den här personen vet. Så skickas man runt. Ingen visste någonting.

AW

Då hoppar vi in på huvudfrågorna då om informationssäkerhet och specifikt och hantering av uppgifter. Hur hanterar du konfidentiella uppgifter när de utbyts via epost kan du ge ett exempel.

P2

Ja, det skulle till exempel vara när man skickar studenters betyg. Att jag ser till och aldrig koppla namn eller personnummer med betyget i det jag skickar. Det var en sak. Ja personnummer skriver jag aldrig ner om jag behöver få information om någon, till exempel en student och jag ska registrera direkt. Så frågar jag om jag liksom kan ringa upp dig och få det, till exempel. Jag tror att vi kanske alla är olika känsliga för olika delar, men just det positivt liten, inte jättemycket bara så där, där är jag försiktig. Sen har man ju när det gäller studenter så har man ju Canvas. Så där kan man kommunicera. Där har vi fått besked om att där får man kommunicera. Sen vet jag ju inte om det är mer säkert eller inte. Man gör väl som högre hönsen säger. Där är ju kanske inte personnummer synliga, men namnen är ju det och där får man ju skriva liksom i kommentarsfält, vilket betyg de fått så där har man ju mer direkt. Kontakt liksom på det sättet. När hanterar jag personuppgifter eller något liknande annars? Nej, jag vet inte, det måste vara när jag har till exempel kontakt med mina informanter via email. Då skickar jag liksom aldrig frågor som kan generera material från dem via mail. Det enda jag gör är att jag har liksom en och ibland som att jag har ju informant [redacted], liksom whatsapp som vi använder alla de andra eller Messenger eller så. Det använder jag aldrig till något annat än att bara bestämma tid för att träffa så den typen så att jag är tydlig att de inte ska liksom skriva sina livshistorier där och skicka dem till mig så blev det mitt material liksom.

AW

Men då är det främst personuppgifter som du ser som konfidentiell data. Jag tänker, finns det annan forskningsdata som du får fram som kan tänka sig vara känsligt?

P2

Inte hos mig inte i mitt forskningsprojekt. Allt är kopplat till personer så det är personuppgifter i och med att jag håller på med [redacted] så håller jag på med känsliga personuppgifter hela tiden och känslig information och det liksom underlagen är det per definition är ju att vi pratar om människors religion eller personer. Så mitt första hela mitt fokus är att man ska liksom inte enkelt kunna spåra mitt material till personen.

FLL

Och när du skriver ut fysiska dokument, hur hanterar du eventuella personuppgifter eller andra konfidentiella uppgifter. Och ifall du kan ge ett exempel?

P2

När det gäller forskningen, till exempel när jag transkriberat mina intervjuar. De märker jag aldrig med namn eller sådant så där det som finns där är bara det som har sagts. Annars arbetar jag ju digitalt med det. Om man tänker studenter och så jag vet inte om det är liksom på något sätt känsligt, men uppsats och så skriver jag bara ut som vanligt liksom. Där är ju ofta både namn och personer man kopplar till texten. Men betyget skrevs inte på det men. Ja när det gäller, liksom det som jag ja, men jag tror det bara det är och självklart då utkast av det jag skriver och som ska till publicering så där. Men då är det ju redan liksom. Kanske inte helt anonymiserat, men i alla fall pseudonymiserat. Sen har jag liksom ingen riktig kodnyckel heller till mina informanter. Jag tror enligt lag ska jag ha en kodnyckel, men jag tycker det är ännu säkrare om man inte har en kodnyckel men ja, jag skulle nog komma i trubbel om någon vill leta fram de här informanterna i efterhand, för då behöver man kodnyckel, eller hur? Jag sätter random namn på de som kopplar det till deras riktiga namn och personuppgifter. Men det detta handlar ju om att jag studerar en [redacted] i [redacted] och att det är av ytterst liksom vikt att det inte de kopplas till mina forskningsprojekt så att det går på. För mig går det framför liksom om det nu är skulle finnas en regel i Sverige som. Säger att jag måste ha en kodning. Ja, ja, det är väldigt bra att jag är anonym här ni får fram allt om hur vi inte följer regler och lagar.

AW

Hur hanterar du delningen av konfidentiella uppgifter när du diskuterar högt med andra i verkligheten?

P2

Ja just det och nu det projektet som jag har nu är ju. Det är ju ett individuellt projekt, så jag delar inte de uppgifterna med andra. Delningen kommer sen och det är pseudonymiserat och det finns liksom inga andra som skulle vara intresserad av att ha de här personuppgifterna. Däremot så sätter vi igång med ett projekt nu med forskare från tre andra länder och då ska vi ha det gemensamt och det är tanken att det ska sätta igång nästa år. Frågan är hur och där har vi nu inte riktigt klurat ut det, kanske vi inte måste dela just personuppgifter. Kanske varje forskare kan sitta på dem i sina länder och sen kan vi dela det pseudonymiserade materialet så. Men inom min typ av forskning så är det liksom inte den kopplingen som är så intressant. Nej, det är bara den existerar för vi har med riktiga människor att göra liksom, men jag samlar ju inte in mycket information om dem heller, men jag bandar ju allt och alla intervjuer och det i sig själv är ju liksom möjligt att spåra personen utifrån det. Men för det här nästa projektet, då får vi ju faktiskt ha etikprövning av datahantering planer i 4 länder för att kunna genomföra det här projektet så det tänker jag att hade ni frågat mig efter den processen så hade jag säkert haft andra idéer om det svenska systemet när det kommer jämföras med tyska och brittiska och det nya zeeländska.

FLL
Lite om fysisk säkerhet, när det går in i ett rum som kräver ett LU kortet och det finns en annan person närvarande som också vill gå in. Hur skulle du hantera den situationen?

P2
Ja det här händer ju ofta här. Och ja, där beror det ju på hur övertygande den personen är. Liksom ”Jag student och jag har glömt mitt kort får jag följa med in?” Det beror också på vilket rum det är. om det liksom är huvudingången så släpper jag nog in dem. Om jag får

känslan av att de faktiskt är studenter, ja då kan jag fråga ”Vad pluggar du?” liksom eller någonting sådant. Men om jag inte känner dem och när det gäller liksom undervisningslokaler eller in i korridorer och så då har jag nog aldrig. Nej, då skulle jag vara mycket mer försiktig. Om det är någon jag aldrig har sett förut som inte kan liksom förklara vem den skall till så skulle jag inte släppa in dem. Nej, vi har ju alltså det där är ju någonting som vi har drillats ganska mycket i. På SOL har, språk och litteraturcentrum, då var det en period där det var jättemånga inbrott och datorer försvann. Så vi har verkligen fått höra det, att man inte får släppa eller man och ska man släppa in dem så ska man gå med dem till dit de säger. Men jag tror inte jag skulle få sätta mig i den situationen jag skulle nog bara säga nej. Särskilt om det var skumma typer. Tyvärr så fungerar vi ju lite så om folk ser skumma ut så blir vi mer skeptiska.

AW
Nästa fråga berätta om ett informationssäkerhetsintrång eller en incident, ett scenario, som skulle vara det mest förödande för din nuvarande forskning?

P2
Men det är ju om det är ju om det skulle. Om [redacted]staten skulle få uppgifter om mina informanter. Det är absolut det som. Nästan all min, så då tar säkerhet handlar om alltså, det ska inte hända. För då kan de komma i trubbel. Ja, det är det och där kan jag berätta om någonting. Enligt [redacted]. Den ska underskrivas, så det ska finnas information och så där. Det är ju ytterligare ett dokument som kan komma att [redacted]staten i händerna med en signatur på att jag är med på detta projektet. Och det är jätteproblematisk [redacted]. Till exempel [redacted]. [redacted]Om jag hade skrivit [redacted]. Men jag har gjort min consent form jag har gjort allt det som man ska göra och har presenterat det för [redacted]. Det finns ju liksom ett exempel på att reglerna som vi förhåller oss till är ju helt uppenbart, liksom är framtaget i andra sociala politiska kontexter än vad vissa länder i världen, liksom vad som är realiteten där. När man då jobbar så måste man liksom anpassa det. [redacted], det är att skydda informanterna. Så det är en sån typisk grej som är problematisk.

FLL
Det var intressant. Och du var inne på det lite innan vi pratade om informationssäkerhet eller informationssäkerhet vid Lunds universitet. Men vilka informationssäkerhetsutmaningar ska du säga att du stöter på i ditt dagliga forskningsarbete här vid Lunds universitet?

P2
Det är att anpassa, operationalisera det jag måste göra till det jag kan göra i fält. Det var just ett exempel på det. Det är den absolut största utmaningen sen och där finns många sådana utmaningar. Där finns till exempel att man inte ska spela in på mobil för att tanka vara kopplad. Så och men där när man intervjuar människor som är lite rädda för vad som ska hända om man kommer med en sån inspelningsmakapär och sätter den på bordet så tystnar liksom människor. Men har man en telefon säger att jag spelar in, men det är telefonen så ligger där så är folk mycket mer avslappnad. Ska man ha in sitt material så är det inte alltid säkert att man kan göra som man har lovat. Så det finns en del sådana? Sen hur ska jag nu långtids lagra data? Men det tror jag har löst nu. Jag tror det finns en sådan tjänst, men när jag startade upp mitt projekt så var det mycket diskussion om hur jag ska göra det. Till slut så fick

jag veta att jag skulle köpa en extern hårddisk och låsa in den i ett safe. Jag tycker det är mycket märkligt men nu har jag börjat med det så jag gör det på detta projektet och så får jag nog ta något annat på nästa liksom. Vilka andra? Alltså, jag tycker mer att det är liksom att navigera i vad det är man måste göra och var man hittar informationen och hur man ska liksom fylla i en datahanterings plan och allt det där. Det har varit jätteförvirrat. Sen hoppas och tror jag att det är bättre nu som sagt. Men ja, och vara liksom lite säker på att nu gör jag det jag ska och där var ju faktiskt den här etik. Prövningen bra för där när man fick ett godkänt då hade jag beskrivit allt vad jag hade tänkt att göra. Och får man då ett godkänt så utgår jag bara från OK men. Gör detta så. Gör jag rätt, och sen är i alla fall medveten om vilka var. Hur jag liksom går från det jag har sagt och det som är rätt så då vet jag vilka delar som jag kanske inte gör helt rätt.

AW
Nu går vi vidare till informationssäkerhetkultur. Informationssäkehetskultur definieras bland annat som: Åsikter, tankar, värderingar och beteenden av medlemmar av en organisation som skulle kunna påverka säkerheten av organisationen. Hur skulle du då beskriva informationssäkerhetkulturen vid Lunds universitet?

P2
Min reflektion är att vi har skett en förändring, kanske de senaste 5, 6, 7 åren och att i och med att det här liksom stramats upp lite och vad man får göra och inte får göra. Det har liksom det har blivit en annan medvetenhet om vad vi faktiskt behöver göra. Så det har skett en förändring, men om jag liksom utgår ifrån den omedelbar omgivningen, vad alltså institutionen och ”HM” som jag fungerar i så har ju den varit ganska så motvillig skulle jag vilja säga. Det finns ju en idé om att alla de regler förordningar vi behöver förhålla oss till vad vi behöver göra är utarbetat inte efter våra ämnen, mer men efter medicin och så att det inte passar det inte går. Det går att uppfylla alla krav när man jobbar som med människor och när man jobbar etnografiskt, till exempel alla som åker på fältarbeten och så där finns ett jättemotstånd mot att liksom etikpröva och ens tänka strukturerat över sitt material insamlande och förvarande av material så där. Sen så är det flera särskilt bland yngre forskare, doktorander som går igenom och gör det någorlunda korrekt så blir det fler och fler som inser att det är viktigt och att det inte är så jobbigt som man tror att det är. Jag tror att vi är liksom på väg mot att det integreras mer. Men sen har ju vi en del extern rekryteringar nu och där finns ju väldigt olika idéer om vad som behöver göras i olika länder. Det är ju väldigt, väldigt tydligt liksom och många reagerar ju på att det är väldigt strikt här. Det är väldigt mycket man ska göra. Det är väldigt mycket regler kring hur man får hantera data. Särskilt för dem som kommer utanför GDPR området och så. Den kulturen är liksom lite i gungning och utveckling från att vi typ har haft någon alltså att få tycker att vi har haft någon forskningsetisk hederskodex. Liksom när det är så här vi forskar etiskt men inte liksom kopplat den till någon till lagstiftning eller regelverk och inte liksom kopplat den till administrativa grejer. Så ja, så skulle jag vilja beskriva det. Och jag inbillar mig att liksom ”HT” fakulteterna och vi är liksom lite, Ja, men vi kanske är liksom bland de sista bastionerna som har stretat emot. Jag vet inte om det är så, men jag har lite känslan på att det att vissa av de här processerna har funnits över mycket längre tid och varit mycket enklare att implementera på andra fakulteter. Här har vi också en mycket starkare tradition av att jobba i enskilda individuella stora projekt. Och jag tror att det är också lite ”kom inte här och kom trånga inte in här i min domän och säger vad jag ska göra med mitt material”, att det finns den här typen av idéer. I och med att man skickar data hit och dit så att man har det gemensamt så tänker jag att det blir en större självklarhet att man liksom tar höjd för säkerheten kring det.

FLL

Ja i samma bana då har du några tankar om hur information säkerhetskulturen vid Lunds universitet skulle kunna förbättras? Och om du skulle komma kunna komma på någon konkret åtgärd eller aktivitet?

P2

Jag vet inte om jag har något konkret förslag, men det vore ju väldigt väldigt bra och om allt var väldigt tydligt vid Lunds universitet och om man visste vem man skulle prata med. Se till att de faktiskt hade svar på frågor om det faktiskt fanns lagringlösningar. Men sen tror jag att man måste ge det lite tid bara sen kommer det. Men det finns ju också den här att jag tror att våra ämnen hade tjänat på haft lite mer kritiska diskussioner kring kring inte bara så att det blir så här, men det där passar inte oss och vårt material, men lite mer kritiska diskussioner kring. Till exempel om hur man kan få det att passa? Vad kan man göra? Vad är det som är viktigt? Och så ja, allt det här, alla som jobbar med känsliga teman i till exempel auktoritära stater har en typ av utmaning som inte liksom tas hänsyn till alls i regelverket här. Till exempel har någon form av kritiska diskussioner kring hur ska vi förhålla oss till detta? För att skydda våra informanter måste vi alltid vara regel brytarna? Måste vi hela tiden välja? Vi vill komma någonstans där även vi kan få göra rätt. Ja den typ av diskussioner tror jag hade varit bra för när de inte är på plats då blir diskussionen mycket mer destruktiva. Det funkar inte ändå alltså. Ni vet det blir så här destruktivt diskurs kring det.

FLL
Ta er lite mer att de tar er i beaktning alltså?

P2
Ja, men lyssna på vad det som är utmaningen och på något sätt kanske ta det på allvar när man utformar regler. Många hos oss också bara agerar gnällspiken för att vara gnällspikar, men man kan ju få lite känsla av att det är så vi bemöts. Liksom sluta gnälla, gå tillbaka och gör ert jobb.

AW
Just det och då avslutningsvis om du har några ytterligare tankar eller kommentarer som du har informationssäkerhet?

P2
Nej, men jag sitter här och tänker på att jag gärna skulle vilja att ni ger mig definitionen på informationssäkerhet för att jag inbillar mig att jag har har liksom pratat om en så här liten del av vad det kan vara medan det nog säkert kan vara så fruktansvärt mycket mer som jag inte tänker på.

AW
Det är också en definition som det diskuteras kring, liksom vad exakt det innebär, lite som tänker religions begreppet också men. Klassiskt sett så har det väl setts som en triad som heter CIA, alltså Confidentiality, Integrity and Availability av datan som man hanterar och informationssäkerhet sträcker sig då utöver de tekniska aspekterna till också att beröra till exempel fysisk säkerhet eller till och med när man diskuterar någonting med en annan kollega eller vad den information man delar med sig då är. Ja sen ser det ut olika för alla individer som beroende på vad man hanterar för data och exakt vilket sammanhang

informationssäkerheten och sen så är det också sammanhang som alla är med på, som till exempel fysisk säkerhet med salar och kontor. Ja printa ut papper och dela med sig av information och så.

P2

Ja, det finns ju en sådan sak jag skrev nog gick någon forskarutbildningskurs någon gång som vi måste gå för att kunna handleda doktorander, och då gjorde jag någon lite som en uppsats där jag intervjuar är lite seniora, handledare från lite olika, inte bara ”HT” också ”s fack”. Där frågade jag, bland annat, i vilka sammanhang de pratar om sina doktorander och doktorandernas liksom kvalitéer eller resultat. Där var det ju ganska många som sa så här. OK om det är någonting negativt med doktoranden då pratar jag bara med de allra närstående kollegorna och jag pratar bara för att få råd eller om det är någonting och vi pratar liksom alltid med stängd dörr inne på kontoret. Men när det gäller positiva saker då säger det gärna i lunchrummet och kaffeautomaten och så där och det tyckte jag var väldigt intressant. Min analys på det var ju att ja, men det är väl bra att man tar de utmanande och negativa saker där liksom konfidentiellt på något sätt, men när man består av kaffeautomaten och pratar om sina briljanta doktorander, då skapar man någonting i kulturen att man att både bland handledare men också doktoranderna själva skapar någon form av hierarki och med vem som är mer och mindre briljant. Det påverkar miljön och det påverkar doktoranderna. Det behöver inte ha någonting med hur briljanta de är. Det kan ha någonting att göra med att man har en handledare som pratar mycket liksom det. Det tyckte jag var intressant och det nu tänker jag det kan man ju koppla till det här med informationssäkerhet. Så ja nej, men jag tror det finns liksom en sådan kultur att man gör det, säger positiva saker om sina doktorander och studenter. Man brukar inte prata så mycket om när man har hela klasser liksom men där kanske vi borde tänka ett steg till nu.

Appendix 6 – Interview 3

AW

Så och ja, tack igen för att du väljer att delta för intervjun kan du uppge ditt namn och din roll vid Lunds universitet.

P3

Jag heter [redacted], jag är doktorand i [redacted] på Institutionen för [redacted] vid [redacted] fakulteten.

FLL

Baserat på din roll som forskare, vad är ditt forskningsområde?

P3

Så jag forskar i området [redacted], det vill säga, de mest [redacted]. Vi gör detta på det teoretiska planet, men till skillnad från vissa teoretiker så forskar jag på partiklar som är kända att de existerar och vill bara utlösa dess beteende i större detalj.

AW

Och hur länge har du varit forskare vid Lunds Universitet?

P3

Det här är mitt fjärde år som doktorand, jag började doktorera hösten 19. Innan dess så skrev jag mitt mastersarbete inom i stort sett samma sak.

AW

Hur skulle du definiera informationssäkerhet utifrån din förståelse av begreppet?

P3

Ja så på ett allmänt plan? Den ansvarsfulla hanteringen av ja information så att den inte går förlorad eller hamnar i händer som kan missbruka den.

FLL

Vilken utbildning eller träning om informationssäkerhets åtgärder eller policies vid Lunds universitet har du fått?

P3

Väldigt lite. Som var genomgående tema så hanterar vi ingen information som klassas som känslig, så bortsett från lite common sense och en och annan datahantering datapolicy som vi har fått givet. Så har jag inte gått någon formell utbildning i det. Det har inte varit några större tonvikt vid det.

AW

Och hur skulle du beskriva informationssäkerheten här vid Lunds universitet?

P3

Så jag har ju då funnit hela min utbildning på just den institution, så. Jag kan inte tala för hela universitetet. Det är i alla fall en sak som uppenbarligen folk tänker på, även om hanteringen kanske inte är perfekt så är det fortfarande att från uppifrån så kommer det fler policies än vad just vi egentligen behöver. Vilket är förståeligt eftersom det finns gott om folkgrupper som hanterar faktiskt känslig information och då är det bättre att ha ett gemensamt ramverk. Från vårt perspektiv så hade vi sett det som överdrivet.

AW

Jag tänker också ni hanterar inga personuppgifter eller annat. Jag tänker också att informationsäkerhet kan komma i beaktande när typ betydelse betygssättning av studenter.

P3

Ja, såklart. Vi har människor här. Det finns personer. Efter både de anställda och Studenternas och i det avseendet. Dock just vi, vi har typiskt väldigt små studentgrupper. Så vi finner det inte praktiskt att ha helt anonymiserade tentor just för att det är så få studenter läraren kommer att känna alla dem vid namn och handstil innan kursen är över. Så, vi tar liksom den informella vägen där, men såklart alla personuppgifter hanteras enligt konstens alla regler i systemet, Canvas, inte slänga ut folks mail på gatan. Common sense.

FLL

Hur hanterar du konfidentiella uppgifter när de utbyts via i email om du kan ge något exempel? Du sa innan att ni inte hanterar så mycket konfidentiella uppgifter, men du kan också tänka utifrån ett teoretiskt plan alltså skulle hanteras.

P3

Det mest konfidentiella vi hanterar är väl just i undervisningssammanhang när studenter säger saker som är mer känsliga som exempelvis ”kan jag få uppskov på tentan för jag har drabbats av det här personliga problemet”. Då är det självklart att det får aldrig bli mer publikt än den mejltråden där det startade, helst mindre, helst prata personligen eller personliga samtal med säg, studierektor eller liknande personer som är mer kapabel att hantera sådana svåra situationer. I forskningssammanhang som sagt mer av det jag sa om min förståelse av vår datasäkerhet är att datan inte ska gå förlorad finns ju klart hos oss, men att den inte ska hamna i orätta händer. Det är, väsentligen omöjligt. Vi hade varit väldigt lyckliga ifall någon kunde använda vad resultatet för ondskefulla ändamål, för det skulle också innebära att någon äntligen har hittat en tillämpning. Alltså det värsta som skulle kunna hända med våra resultat är att någon oseriös forskare plagierade, men det är inte heller, i vårt fält, så förekommer det inte så mycket hets och panik kring att man kring publish and perish. På andra delar av fysik finns det ju betydligt mer tillämpbar forskning. Man måste inte gå längre än till den andra änden för att saker ska tillämpningsbart, bara på kärnvapenutveckling och det var ju uppmärksammat häromsistens hur någon som hade doktorerat på en annan avdelning fysik numera utveckla missiler och Kinas militär. Det är å andra sidan är det kanske inte fråga om datasäkerhet just för att den här personen var doktorand. Om de nu skulle vara doktorand så är det ju helt klart absolut inte ska ha tillgång till allting, men det är ingenting till att fysik behöver hänga upp sig på just för att om, 50 år kanske någon finner nyttan med det här. Men det är inga ondskefulla ändamålen än så länge. Det är fortfarande så att man inte ska vara dum och slänga ut emailadresser till höger och vänster, det leder bara till spam och phishing och

liknande. När det gäller vår data så är vårt fokus då på ordentliga backups och praktisk tillgänglighet för alla som jobbar med det. Vi använder Overleaf för internationella samarbeten om vi skriver och så vidare. Och även om det innebär att saker lagras på deras servrar så finner vi att säkerhetsaspekterna är så liten att praktikalitets aspekten vinner över.

AW

Information informationssäkerhet är ju också fysisk säkerhet och ifall det skulle gå in i ett rum som kräver ett LU-kort och det finns en annan person närvarande som också vill gå in just bakom dig. Hur skulle du hantera den situationen och också ifall du känner till några regler för det här scenariot?

P3

Ja helt ärligt, skulle jag, ifall den här personen ser ut att vara en student, så skulle jag lita på det och släppa in personen. Skulle den personen inte sett ut som en student så jag skulle vara fördomsfull så kanske jag skulle fråga lite vänligt vart de ska. Jag vet att jag har sett en riktlinje. Men eftersom de enda lokaler jag går in i är sådana där det bedrivs den här sortens forskning eller undervisningslokaler så tar jag inte extremt hårt på just fysisk tillgångssäkerhet. Jag tror också jag råkade lämna kontorsdörren öppen när jag gick ut för att släppa in er.

FLL

Men ni har inte någon datorsal eller något sådant som är i byggnaden?

P3

Det finns en datasal i byggnaden. Men den ägs och används av [redacted] och den tar vi inte i med tång det finns en annan datorsal på astronomihuset som vi använder när vi behöver en datorsal.

FLL

Berätta om ett informationssäkerhet intrång eller ett scenario som skulle ha den mest förödande effekten på din forskning. Och ifall det inte finns, så är det också ett svar.

P3

Alltså det som skulle vara förödande skulle ju vara en total dataförlust och jag kan säga det är den enda punkten som var IT-ansvarige verkligen driver hårt. Ta ordentliga backups för helvete. Vi har våra alltså de flesta datorerna här är sammanlänkade i ett kluster som används dels för att det ska gå att komma åt allting och dels för att man ska kunna låna beräkningskraft av varandra. Den som har en privat laptop ska en gång i veckan backa upp till den stationära datorn här och varje natt så backas allting här upp på en server som jag står i en skrubb någonstans och då backas det också upp. Det som skulle vara katastrofalt då är ju om jag tappa min laptop i en vattenpöl och ignorerat allt vår IT-ansvarige har sagt de senaste åren och plötsligt så har all min data försvunnit. Ordet intrång kom ju inte med någonstans där. Vi skulle kunna utsättas för någon bara bred ransomware attack som bara låser allas datorer utan att de bryr sig om vad som finns där. Det är såklart en möjlighet. Där är det återigen bara att tillämpa common sense när man hantera datorer.

AW

Nej, men det behöver inte gälla intrång heller. Som en av pelarna för informationssäkerhet är, som det är klassiskt sätt definierats, är just dataintegritet också att också se till att datan finns tillgänglig. Vilka informationssäkerhets utmaningar skulle du stöta på i din dagliga forskning på Lunds universitet.

P3

Jag kommer att svara lite bakvänt på den här att det som har varit mest utmanande för oss är just när vi för våra inte särskilt säkerhetskritiska ändamål använder tjänster som sedan klassas som icke tillförlitliga av Lunds universitet. Så som att under covid så skaffade hela vår avdelning en stor slackkanal för bara våra vardagliga kafferums-konversationen och lite så här bara för att slippa ha 1000 mejltrådar. Detta får vi icke göra. Så nu efter att centrala folk satte ner foten rörande Slacks informationssäkerhet så är vi just nu utan en meddelandetjänst just för att även för jobbrelaterade sociala ändamål så är det fortfarande lite för nära gränsen för bekvämligheten tydligen. Liksom efterlevnad av universitetets allmänna informationssäkerhets riktlinjer gör att vi faktiskt måste bry oss lite mer om informationssäkerheten än vad vi egentligen skulle göra bara för vår egen skull.

FLL

Om vi går in på mer om informationssäkerhet, kultur och informationssäkerhet. Informationssäkerhetskultur definieras då som: Värderingar, tankar, åsikter och beteenden av medlemmar av en organisation som skulle kunna påverka säkerheten av den organisationen. Så hur skulle du beskriva informationssäkerhets kulturen vid Lunds universitet?

P3

Så forskare är ju en flock höns det är verkligen så, särskilt vi som tycker ”men vi har ju ingen känslig information”. Det finns ett fåtal personer mer eller mindre centralt som tar det väldigt seriöst och som är inhyrda just för att man måste ta det seriöst. Och sen är folk väldigt lulliga med det och behöver piskas runt som höns. Skulle inte säga att vi är någorlunda duktiga för att vara sådana som skulle kunna komma undan med att lulla runt. Exempelvis så har vi fortfarande problem med att Lunds universitets mail-domän är svartlistad i diverse mail-sammanhang för att någon professor, jag har hört att det var humaniora, råkade sälja sin mail till ett spammnätverk. Så även sådana enkla saker som egentligen inte är forskning specifika utan drabbade befolkningen det har ju konsekvenser som man får leva med. Jag känner att dessa personer som tar det seriöst och är stränga, de ger ändå resultat. Vi är ändå lite noggrannare än vi var när jag började med att inte använda vilken tjänst på en amerikansk server som helst. På avdelningen har vi också fjärrinloggning så jag kan sitta hemma och gå in. Nu är jag inuti min dator att jag kan köra på tunga beräkningar eller komma åt mina eller min handledares fil. Det har vi fortfarande, men nu har vi faktiskt specifika inkörsportar för det där så att den IT-ansvarige kan ha lite koll snarare än att man loggar in genom en central server, vilket är mycket praktiskt för det märks ingen skillnad för användaren. Men tydligen så finns det nu liksom ett hål snarare än 1000. Men ja, tillbakalutad och lite virrig och några ansvariga som tar ansvar är väl min uppfattning av kulturen.

AW

Har du några tankar på om hur informationssäkerhetskulturen vid Lunds universitet skulle kunna förbättras? Om du har någon konkret åtgärd du skulle kunna tänka dig?

P3
Ja, återigen att när slack förbjöds så finns det ingen rekommenderad tjänst och när det inte finns ett godkänt alternativ för något ändamål så leder det ju till att folk slarvar. Så att se till

att för alla ändamål att det finns ett godkänt alternativ gör ju att folk kommer vara mycket villiga att efterleva begränsningarna. Eftersom vi sätter ju ofta praktikalitet i första rummet och då för att säkerhet inte ska komma i andra rummet så är det bra om det går att kombinera sömlöst, så sömlöst som möjligt.

FLL

Avslutningsvis har du några ytterligare tankar eller kommentarer som rör informationssäkerhet eller det vi har diskuterat?

P3

Jag tror inte det. Ja, nu har ni er kontrollgrupp!

Appendix 7 – Interview 4

AW

För intervjuns skull, skulle du kunna uppge ditt namn och din roll vid Lunds universitet.

P4

Jag heter [redacted] [redacted] och jag är doktorand vid Lunds universitet vid avdelningen för astrofysik vid institutionen för [redacted].

FLL

Utifrån din roll som forskare, Vad är ditt forskningsområde / fält?

P4

Så jag, som sagt inom [redacted], men mer specifikt så studerar jag hur [redacted] vår [redacted] har bildats och hur den ser ut genom att samla in data [redacted] världen över och analysera den datan.

FLL

Och hur länge har du forskat vid Lunds universitet?

P4

Det här med forska och forska, ja, jag har gjort all min utbildning på Lunds universitet, så jag började med en kandidat. 2014 började jag en masterutbildning och så började jag disputera 2019. Så om man ska forskningsaktivt är väl sedan 19 i sådana fall, så 4 år.

AW

Absolut, och då har du ingen tidigare erfarenhet som forskare vid andra universitet?

P4

Inte så gammal i gemet än.

FLL

Ja, och hur skulle du definiera informationssäkerhet utifrån din förståelse av begreppet?

P4

Utifrån min förståelse, utifrån min erfarenhet också från liksom specifikt från min forskning, eller?

FLL

Ja alltså, generellt hur du skulle förstå begreppet informationssäkerhet.

P4

Alltså exakt informationssäkerhet för mig tänker jag på vem som har rätten till information. Som sagt är det jag som äger rätten till min data som jag samlat in eller är det min handledare eller institutionen eller universitetet. Vem äger rätten till den liksom faktiska fysiska datan? Den datan som jag har på min dator. Är det jag som äger den, det är sånt som jag inte heller har koll på och likaväl mina vetenskapliga artiklar innan de är publicerade. Vem är det som äger rätten till det materialet där det tänker jag är informationssäkerhet framförallt för mig då min forskning vem äger den? Sen finns såklart informationssäkerhet också som, jag är rätt så aktiv inom studentkårslivet och där finns det ju också information som kanske inte alltid ska komma att bli publik och där får vi ju lära oss att all mejl vi skickar som anställda i och med att vi är en statlig myndighet kan begäras ut av journalister så man får tänka på hur man, vad man, skriver i mejl som sagt för det kan begäras ut av vem som helst, så det är väl de två aspekterna jag tänker.

AW

Har du fått någon utbildning eller träning om informationssäkerhet, åtgärder eller policies på Lunds universitet?

P4

När man börjar som doktorand har man liksom en introduktionskurs i att vara doktorand liksom vid Lunds universitet och då har de exakt lite där informationen om att din mail är en del av en statlig myndighets mail så det kan begäras ut. Men annars inte riktigt skulle jag säga, man får väl ha det så här: du ska backa upp din data liksom, men jag skulle inte säga att jag har som sagt fått så mycket kunskap om informationssäkerhet annat än så. Det var väldigt sparsamt.

FLL

Hur skulle du beskriva informationssäkerheten vid Lunds universitet, kanske i relation till hur du anser informationssäkerheten beaktas och om du anser att det är i tillräcklig utsträckning eller liknande?

P4

Jag vet inte. Jag känner att det kanske är svar i termer av att jag känner att jag har väldigt dålig insikt och transparens i hur universitetet behandlar informationssäkerhet, vad som förväntas av mig som forskare eller doktorand i det här fallet. Exakt, det känns inte så transparent, varken vad de gör eller vad jag ska göra. Det känns också som att det finns en allmän känsla bland mig och mina kollegor att universitetet inte har riktigt koll. Generellt så fungerar inte spamfilter så bra, till exempel på mailen och, ja, men det är väl en allmän oroskänsla över att det inte finns en bra koll på informationssäkerhet skulle jag säga. Det är min uppfattning. Exakt att jag kanske inte vet bättre eller inte vet så mycket då kanske säger mer, liksom än om jag vet saker.

AW

Hur om du hanterar konfidentiella uppgifter hur hanterar du dem då när de utbyts via epost? Om du hade något exempel på det?

P4

Ja det är väldigt sällan jag känner att jag behöver ha att göra med konfidentiella uppgifter inom min forskning. Tack och lov. Mm men exakt det känns ju som att det är något som är väldigt svårt att hantera när det handlar om diskussioner som man inte vill ska bli publika och det är snarare så att jag undviker att ta diskussioner via mejl. För att jag inte vet hur det kan spridas eller vad det kan hamna. Om det är ett bra svar nog?

AW

Absolut, såklart. Och hur skulle du hantera eventuella uppgifter ifall du hade behövt skriva ut dem på fysiskt papper?

P4

Som vi har nu är med som att skriva ut saker här så dels så skrivs dokumentet ut först när man är vid skrivaren och jag blippar mitt accesskort så ingenting skrivs ut så att det liksom hamnar i skrivaren och sen får jag gå och hämta det så det känns ju ändå tryggt tycker jag, framförallt om jag ska behöva skriva ut saker som är relevant till mig själv. Alltså typ biljetter eller jag menar mitt CV och liknande där personnummer kan stå, det är ju för mig själv, men sen också hur man ska hantera de papperna. Det är ju en helt annan grej som sagt, jag har ju mitt kontor där jag har papper, men det är ett kontor jag delar med en annan person. Det är inte som att vi alltid låser det. kontoret, men korridoren är ju låst. Men det är absolut ingenting jag känner att jag blivit tränad i hur jag ska, till exempel jag undervisar, vilket innebär att jag rättar tentor eller inlämningsuppgifter och jag försöker ju ha allting i största möjliga mån på min dator för att det inte har papper som ligger omkring som eventuellt kan hamna någonstans. Så att så undviker jag att skriva ut om jag kan egentligen.

FLL

Den här är väl lite i samma veva, men hur hanterar du konfidentiella uppgifter när du delar uppgifter med andra, både digitalt och fysiskt?

P4

Alltså generellt så ser ju till att det bara är folk som ska ta del av den diskussionen som kan höra diskussionen, men också så se till, hur ser jag till det? Det är inte som att jag ser till att allas telefoner är avstängda eller liknande, utan det är mer att det sker bakom stängda dörrar. Men var det också frågor kring hur det sker online?

FLL

Ja, precis, digitalt. Jag tänker till exempel Zoom-möten eller annat.

P4

Ja, det är ju liksom. Jag har ju varit med om typ informationsmöten från prefekter och liknande där vi har bett att få saker i skrift. Och prefekten inte velat ge saker i skrift för att då finns det ett rekord och personen vill bara prata över zoom då eller på plats. Men jag tänkte,

du har ingen garanti för att ingen sitter och smyginspelar det, vilket jag har fått mig att tänka kring: hur vet jag att ingen annan sitter och smyginspelar någonting och jag vet inte hur man ska hantera det liksom hur? Hur checkar man sådant? Som ett svar, jag vet inte verkligen. Det är ju mycket enklare när man sitter så här liksom, men såklart. Nu vet jag att du spelar in där, men jag vet ju inte vad ni har uppe på era datorer liksom.

AW

Och lite om fysisk säkerhet också. När du går in i ett rum som kräver LU-kortsaccess och det finns en annan person närvarande som också vill komma in och som följer bakom dig, hur skulle du hantera den situationen?

P4

Ofta så brukar jag försöka vara väldigt trevligt i termer av att vi är en rätt så liten avdelning här om det är någon som kommer in så brukar jag vara ”åh, vem ska du träffa eller vart ska du?” för då kan jag liksom visa den personen till om den ska träffa någon utav de andra forskarna. För att dels för att det känns trevligt, men också för att checka lite vem är den här personen. Så jag försöker, men jag menar det är inte som att jag skulle så hysa ut någon. Men jag tycker det känns om jag tycker känns rimligt att fråga liksom vad. Oftast har ju personen ett ärende liksom. Jag har aldrig varit med om ett fall där en person aldrig haft något ärende någonstans. Men nu hur jag skulle hantera om personen bara. Nej, jag vill kolla omkring. Då hade jag ju sagt nej, det får du inte liksom när det bara är för de som forskar här.

AW

Absolut och känner du till några policys kring det här?

P4

Det gör jag inte.

FLL

Ja, då går vi vidare till nästa fråga. Berätta om ett informationssäkerhetsintrång eller en incident eller ett scenario som skulle ha den mest förödande effekten på din nuvarande forskning?

P4

Oj. Det är ju om någon. Alltså jag vet inte. Jag vill säga om någon skulle sno min dator, men det stämmer inte riktigt för mycket utav min data ligger inte på min faktiska laptop utan på en server här i källaren, men min analys ligger ju på min dator men. Så jag vet inte om det hade varit den största. Nej men jag tror det om någon hade tagit min dator, så.

FLL

Fysisk stöld?

P4

Exakt. Eller ja, alltså. Nu när du säger det, men de kan ju säkert hacka min dator också, vilket skulle ha samma effekt. Så men ja, intrång på min dator, antingen att den blir tagen fysiskt eller tagen digitalt.

FLL

Absolut och er forskningsdata och annat är alltså lagrat i en server i källaren här?

P4

Jag tror olika forskare har olika metoder. Faktiskt, för att lagra sin data så att jag har det på en server nere i liksom källan bakom en låst dörr som inte är jätte… jag har inte ens access till den datorn, liksom det är typ två personer här som har access till det rummet där servrarna står. Men sen också vårt alltså astronomi är ett, det är bara svengelska överallt här nu, men det är ett väldigt open access fält generellt eller så är det så att man har liksom 2, 3 år på att säga publicera sin data innan den blir publik och andra får take their shot at it. Som sagt i mitt fall så är min data inte publik utan det är min data i typ ett år till. Så, oftast är den liksom inte. Så här, om man har jobbat igenom sin data snabbt så är det. Vad är det jag vill säga? Efter ett tag så kommer alla kunna se status oavsett så det handlar mer liksom om att man vill vara ute snabbt och först med sin forskning för att kunna ge mest genomslag och det är därför det hade varit rätt så katastrofalt om någon liksom tar min dator och ser analysen jag har gjort med min dator och kan kopiera det rakt av. Men som sagt alla gör olika, men jag tror de flesta har det liksom antingen på sin egna laptop, på en hårddisk eller på en server här liksom. Jag hoppas folk har backups, men det vet jag inte alltid om folk har.

AW

Absolut. Och vilka informationssäkerhetutmaningar skulle säga att du möter på i din dagliga forskning?

P4

Jag tror det jag möter absolut mest, kanske inte i min forskning, men i min vardag, är som sagt väldigt mycket mejl som jag inte alltid kan bedöma om det är spam, eller inte, vilket jag antar mejl som eventuellt kan hacka min dator eller liknande. Det känns som att spammejl har blivit väldigt sofistikerade. Ibland får vi liksom, kan jag få mejl som ser ut att komma från min handledare som jag så bara hej, kan du ba ringa mig snabbt eller liksom kan du gå in på den här zoom-länken snabbt, så, vi behöver bara prata och det ser verkligen ut som något som min handledare hade kunnat skicka, även om det ibland är någonting som känns lite funky med det. Så det är väl det jag ser som det största, liksom att kunna bedöma sånt. Ehm, för man får rätt så mycket och det är väldigt sofistikerat.

AW

Jag är nyfiken om Lunds universitet har, alltså vissa organisationer har ju så att de skickar ut fake phishingmejl för att testa, jag vet inte om Lund…

P4

Just det. Alltså, jag har varit på en organisation som hade det och jag tyckte det var väldigt bra för det var redan min för jag var på, skit samma, men jag var borta härifrån ett halvår för att göra en annan tjänst och då liksom min andra dag så fick jag sånt där det stod liksom bara

”ditt lösenord har blivit breached” och jag bara herregud det är min andra dag på jobbet I fucked up och då trycker jag liksom recover password eller vad det nu var och då var det en sådan phishing som de hade som test. Det var ju superbra för jag lärde mig verkligen att liksom kolla igenom, men jag har inte fått något sådant från mina många år på Lunds universitet. Men jag, jag hade uppskattat det tror jag. Jag tror det hade varit väldigt nyttigt.

FLL

Och nu kommer vi in på informationssäkerhetskulturen och det kan väl beskrivas som attityder värderingar, tankar och beteenden av personer i en organisation som kan påverka säkerheten av den organisationen. Och hur skulle du beskriva informationssäkerhetskulturen här vid Lunds universitet?

P4

Jag känner generellt att det finns ett. Ja, men som sagt ett slarv kring det, delvis för att. Jag tror att de flesta typ inte har en backup på sin information och sin data och tänk man är ju lite så här ba, men det kommer inte hända att min dator kraschar eller blir hijackad av någon eller blir stulen. Det känns som man kanske inte har liksom en sådan grav vikt vid det som det skulle kunna behövas ha. Jag tycker att det känns som att det finns en kultur av, att man inte litar på att universitetet kan stötta en i det. Och jag vet inte om det är något kulturellt, men det känns som att jag kanske inte om jag sagt inte en misstro, men. Jag tror en misstro till universitetet som liksom stödorgan i att upprätthålla informationssäkerhet.

AW

Ja, har du några tankar om hur informationssäkerhetskulturen hade kunnat förbättras på Lunds universitet, någon åtgärd eller aktivitet?

P4

Ja alltså dels sådana här övnings-spammail. Tror jag hade varit jättebra, dels också alltså regelbundet informera anställda om hur man jobbar med informationssäkerhet, alltså va transparenta liksom i vad universitetet gör och i liksom det forumet vilket forum det skulle kunna vara liksom också påminna anställda vad som förväntas av anställda. Jag tror generellt när man börjar som anställd så får man jättemycket information och ni frågar liksom finns det någon policy? Att jag, jag vet inte, det kanske finns jag kanske fått höra om det någon gång för 4 år sedan när jag också fick massa massa massa information slängd på mig så jag tror liksom regelbundet påminna folk, som sagt vad universitet att jag vad som förväntas av mig vad för olika policy som finns. Hur jag bör tänka kring min data. Som sagt också hade det varit trevligt få höra hur universitetet liksom, för det är en värld som ändras väldigt, väldigt snabbt och hur de försöker vara en del av den förändringen. Sen som sagt nu, det blir tydligt, men nu tror inte jag att de är en del av den förändringen, men det hade varit bra om de var det. Men, vad vet jag? Ja transparens som sagt, det kommer också att påminna folk tror jag att tänka på det. Så absolut.

FLL

Och då avslutningsvis om du har några ytterligare tankar eller kommentarer kring det vi diskuterat, informationssäkerhet eller vad som helst?

P4

Haha. Förlåt. Nej, jag har nog inga fler kommentarer. Vi har inte alls hållit på i 45 minuter, men det kanske är för att jag är kort och koncis.

Appendix 8 – Interview 5

FLL
För intervjuns skull kan du uppge ditt namn och din roll på Lunds universitet?

P5

Mitt namn är [redacted] och jag är [redacted] och docent vid [redacted] fakulteten.

AW

Och utifrån din roll som forskare. Vad skulle säga att ditt forskningsområde är?

P5

Jag forskar på [redacted] och framför allt en viss typ av [redacted] och som uppstår redan under [redacted]. Alltså, det vill säga när [redacted] är i [redacted] och vi försöker förstå varför det kan bli en tumör redan så tidigt.

FLL

Hur länge har du forskat vid Lunds universitet?

P5

Jag började 2008 men sen har jag varit iväg en liten stund i [redacted], men sen är jag tillbaka så att till och från fast större delen här sedan 2008.

FLL

Har du någon tidigare erfarenhet som forskar vid andra universitet?

P5

Ja nej, jag var bara i [redacted], men inte annars.

FLL

Hur skulle du definiera informationssäkerhet utifrån din förståelse?

P5

Ja, det är en jättebra fråga för jag vet inte riktigt. Jag tänker att det är hur vi hanterar data både som vi genererar och då antar jag att det är både liksom sådana uppenbara saker som patientdata som är så här som verkligen är stora restriktioner kring som är superkänsligt. Men

sen är det ju även forskningsdata som både ska vara tillgänglig och inte vara tillgänglig så att säga och typ det vi skickar, hur det skickas och hur känsligt material hanteras. Det tänker jag att det är.

AW

Vilken utbildning eller träning om informationssäkerhet, åtgärder eller policys eller liknande vid universitetet har du fått?

P5

Äh ingen.

FLL

Hur skulle du beskriva informationssäkerheten vid Lunds universitet? Anser du att det beaktas till tillräckligt stor utsträckning?

P5

Nej alltså kanske helt självklart efter att jag svarade ingen på förra frågan så tycker jag verkligen inte att det är bra. Jag har typ fått höra, så jag vet ju lite grann. Jag vet lite grann om så här patientdata. Nu jobbar inte jag så mycket med det och jag gissar ju att om man jobbar med det så har man väl alltså, då är man mycket mer insatt i det men i övrigt liksom. Men bara vad jag har hört från när jag typ doktorerat så där, ja, hur länge man måste spara labböcker och den här typen av öppen forskningsdata. Men det är bara sånt jag har lärt mig av folk runt om i labbet så egentligen alltså. De kunde ju ha lurat mig. Det har de inte, men alltså så. Men i övrigt så är ju inget officiellt, absolut ingenting formellt. Typ nu har du en doktorand, så här ska det gå eller liksom någonting att så här ska det fungera med data. Det ska finnas här. Det är den här säkerheten om du skickar mejl. Jag har ingen aning om det. Förutom att jag vet att alla våra mail är officiella och det har ju till exempel fått liksom ändå ganska nyligen beskrivet lite mer hur det funkar. Det har inte varit beskrivit alls innan. Nu har jag fått det för att jag har fått mediaträning liksom. Men i övrigt typ. Hur funkar det när vi skickar mail? Vem har tillgång, ingen aning? Hur länge är det? Vad händer när mailen stängs av, om jag lagrar där eller där, vad händer då? Får jag ha saker på min dator ingen aning. Du får aldrig lämna datorn obevakad. Det är typ sådant som jag har hört också. Det hade man ju uppskattat om man hade vetat allt det där? Nu kanske jag borde tagit reda på det själv, men det är i alla fall ingenting formellt man får. Så att det tycker jag att det borde verkligen vara.

P5

Hur skulle du hantera konfidentiella uppgifter när de utbyts via e-post och ifall du kan ge ett exempel här också?

P5

Jag är framför allt ska jag säga ganska dålig på det att tänka efter med sånt. Så att jag mejlar ju ofta. Jag skulle aldrig skriva “så den här patienten eller det här är embryot som kom från humana embryon” till exempel. Sånt skulle jag aldrig ha i text och jag vet lite grann med förvaring, men inte sådär jättemycket egentligen. Inte heller hur man förvarar utan det är

kodnycklar och sånt med patienter. Det har ju inte jag behövt ha liksom, men i övrigt så är det generellt. Jag skickar ofta mail för att det är så enkelt liksom att ja men nu. Hade jag tid. Nu när man skickar ett mail och så kommer man liksom på sen att ja just det. Det där kanske egentligen inte borde stå någonstans. Men jag är ju lite så här om det är någonting som är halvt känsligt, alltid ringa liksom. Till exempel, jag börjar försöka tänka på det. Det är ingenting som jag har tänkt på innan. Så förvaring generellt att jag försöker ha koll. Men om det egentligen är så att jag har dokument som inte ska vara här så vet inte jag det och jag mejlar nog alldeles för ofta skulle jag säga, men jag försöker börja tänka på det lite mer. Men samma sak med förvaring. Jag använder ju bara universitetets egna servrar och vi har ju cloud tjänster och sånt som är beställda genom universitetet så där ligger ju allting. Men i övrigt samma sak. Där har jag bara litat på att det är.

FLL

I samma bana då, om du hade skrivit ut ett fysiskt dokument som bra konfidentiella uppgifter eller känsliga information hade du? Hur hade du hanterat det och har du något exempel som du kan berätta om?

P5

Alltså, jag har, halv-känsliga dokument för olika tumörer, material som vi har samlat in och då har vi även uppgifter men vi har inte namn på patienten, men vi har ju uppgifter för att kunna följa och den har ju jag. För att jag inte vet och inte har fått information utan det jag har fått höra ja, det här ska du ha. Men det är känsligt och liksom så. Men igen alltså. Det är ju det exemplet på vad jag har, men. Om det egentligen borde förvaras någon annanstans, om det egentligen borde finnas någonstans som var lite mera säkert än på mitt kontor gör jag inte det i alla fall?

AW

Hur skulle du hantera när du delar uppgifter med andra, både i person men också kanske via zoom?

P5

Om det verkligen skulle vara känsliga uppgifter så skulle jag inte mejla. Så långt har jag i alla fall kommit, men på telefon eller så här som vi pratar eller om man skulle prata direkt tror jag inte jag skulle tänka på det så mycket. Men jag menar om det var att jag diskuterar något känsligt material med en annan forskare skulle jag nog inte tänka på kontexten? Inte maila liksom, men så tror jag inte jag tänker så mycket på restriktioner heller och definitivt inte om vi ses och pratar. Men mejl är nog den enda där man tänker sig för om det är riktigt känsligt. Det är nog sådana här gränsfall som man har lätt att inte tänka på.

FLL

När du går in i ett rum som kräver ett LU-kort och det finns en annan person närvarande som också vill bli insläppt, hur skulle du hantera den situationen?

P5

Ja den är jättejobbig tycker jag alltså på riktigt. Det har jag också fått höra av en administrativ personal innan som var så här aldrig släppa in en, det tycker jag generellt att det kanske kunde vara lite bättre information om också. Men det har väl de flesta kanske hört bara i liksom rumor höll jag på att säga men som går runt, men det är ju jättesvårt för det är ju superotrevligt att smälla igen dörrar. Vi är ju svenskar liksom, man stänger inte igen dörren för någon, men oftast försöker jag se om personen själv har ett LU-kort för oftast om man kommer så har ju båda LU korten uppe. Och då ser man ju. Eller så försöker jag liksom att man har tillräckligt med avstånd så att den hinner slå igen utan att det verkar alltför otrevligt eller som när man går in på BMC där jag sitter så kommer man ju bara in första steget. Sen kommer de ju ingen annanstans utan att ha LU-kortet. Det är ju egentligen fortfarande fel, jag vet det, men där tänker jag ibland OK. Men det är ändå en säkerhet. Jag skulle inte släppa in honom om det inte är helt uppenbart liksom, men om det kommer någon som vill in så brukar jag ju fråga vem de ska till liksom. Eller om man vet vem det är, men jag tycker verkligen att den är jobbig.

FLL

Och du hade som sagt hört regler då i samband med detta från andra?

P5

Ja och det var verkligen inte sen jag började alltså. Det var ändå ganska sent jag fick höra "Nä just det får ni ju absolut inte göra det här". Det låter ju rimligt ungefär men. Men absolut nej, jag tror aldrig hört eller jag har absolut inte hört något officiellt.

AW

Och då, om du skulle kunna berätta om ett informationssäkerhet intrång eller incidenter, ett scenario som skulle ha den mest förödande effekten på din nuvarande forskning?

P5

Ja, men det skulle nog vara. Alltså, på ett sätt tänker jag direkt, ja, men det är ju om min dator skulle försvinna och jag känner mig inte jätteorolig för det för jag har verkligen alltid med mig den. Men det är klart jag lämnar den på kontoret om jag bara ska gå här eller på något annat möte Men vi försöker låsa dörren om vi verkligen ska iväg. Men det känner jag så här direkt att det vore egentligen alltså det värsta för då skulle ju data försvinna. Men å andra sidan har jag ju ingen forskningsdata på min dator så egentligen kanske inte det vore det värsta, men det känns ju som det. För datorn känns ju som det man har. Nu måste jag liksom titta här vad jag har. Annars är det väl egentligen också, det här tänker jag att ingen intresserad av, men jag har ju här under mitt skrivbord två stora kartonger med labböcker från folk som har varit på min labb och de måste vi förvara i 10 år. Det som sagt har jag lärt mig. Så om de skulle försvinna så vore det ju egentligen jätteilla. Sannolikheten att någon någonsin kommer vilja ha dem är dock så liten. Det finns utrustning här, men det är ju egentligen det är liksom ingenting känsligt. Jag vet inte riktigt alltså. Det är ju sånt som skulle vara så här förödande för oss för att om det skulle försvinna en stor maskin som kostar jättemycket pengar. Det vore ju förödande. Men nu är det informationssäkerhet synpunkt så är inte det någon fara.

FLL

Men då går vi vidare till utmaningar i samband med informationssäkerhet. Då är frågan vilka informationssäkerhet utmaningar skulle du stöta på i din dagliga forskning vid Lunds universitet?

P5

Ja, men jag är ju så här generellt som person lite naiv. Jag vill att världen ska vara bättre än vad den är så att jag är så. Jag tänker att man inte ska behöva tänka så himla mycket på det här. Men det har ju faktiskt hänt en del vid universitetet som gör att man har tänkt efter mycket. Mer och på min förra arbetsplats. Jag var ute på [redacted] förut och då fick vi ju höra i efterhand, men då var det en forskare som hade fått sparken alltså, personen skulle lämna universitetet. Det hade liksom varit någon incident men personen hade kvar sitt kort eller på något sätt kom in i byggnaden och ställde det. Det var ju ingenting som jag upplevde personligen, men det var ju huset bredvid mig. Jag vet fortfarande inte vem det är så det sköter de ganska bra men att det hände och ungefär vilken miljö det var i och så där. Där jag är nu faktiskt så skedde ju forskningsfusk för ett par år sedan där de fälldes och det har ju varit en jättestor historia på universitet. Där var det ju massa hot och grejer sen som vi kan diskutera i mångt och mycket. Men det var ju vakter här liksom och sånt så att jag menar det har ju funnits incidenter. Jag har hört om någon mer liksom som gör att man ändå fattar allvaret. Alltså, och det finns ju personer som man aldrig alltså, det kan ju vara någon som man tror är en jättebra människa som det kan vara någonting med. Jag känner ju egentligen att det skulle behövas liksom vilket utsvävande svar det här blev, men alltså att man ändå har hört att det har varit incidenter. Dessa har med säkerhet att göra på så sätt att det kanske är personer som inte ska vara här eller hotbrev som kommer till jobbet eller folk som blir fysiskt hotade och sånt. Det ska liksom inte få förekomma. Sen har man ju hört om det har varit inbrott och stölder. Det har det inte varit i närheten av mig, men det är också sånt man har hört i korridoren. Då borde man egentligen alltid låsa om sig överallt, liksom när man inte är på plats och det gör vi ju inte, men vi låser ju alltid våra dörren när vi går härifrån och sånt har vi ju blivit liksom bättre på. Att alltid se till att den som är sist låser allting och så där. Men med det skulle jag nog säga att jag ändå är medveten om sen går jag inte runt och känner något dagligt men ändå.

AW

Då går vi in på informationssäkerhetskultur och det definieras bland annat som åsikter, tankar, värderingar och beteenden av personer i organisationen som skulle kunna påverka säkerheten av den organisationen. Och hur skulle du då beskriva informationssäkerhetskulturen vid universitetet?

P5

Alltså, nu tar jag ju då den miljö som jag befinner mig, det vill säga i den här omgivningen där jag var förut och så där. Ja, alltså, jag skulle säga att det jag har sagt idag avspeglar allt, alltså generellt. Om vi generaliserar skulle jag tro att det avspeglar hur vi tänker på det här. Nu återkommer jag till det med patientsäkerhet med liksom personnummer och den typen. Den sköts. Nu finns det såklart exempel på att den inte alltid sköts. Men den sköts nog. Vi har ju varit med patologer och så där och den skulle jag säga ändå är betydligt bättre för att där är det ju jättetydliga riktlinjer så där är det ju lättare att följa dem. Samma sak på datorn då ska det ju vara kodlås och det ska liksom finnas en kodnyckel som bara en person har och det tror jag funkar ganska bra. Men i övrigt runt sånt en sådan där grej som att släppa in någon som

kommer samtidigt. Alltså folk gör ju det. Alltså, jag har kanske sett något fall där någon inte gör det men oftast. Det är samma sak om jag kommer alltså folk släpper ju in en. Jag går ju in samtidigt som någon annan. Så att generellt så är kulturen alltså slapp. Jag upplever som att det avspeglar hur vi alla hanterar det och tänker på det och att det faktiskt är en konsekvens av att vi inte har någon information om det. Eftersom vi inte har ett ”så här ska det funka”. Hade man haft det så hade man ju både varit tvungen och känt mycket mer att man skulle ha det. När ni skickade mail så var jag så här ”ja just det.” liksom för att man tänker ju inte på det nästan alls.

FLL

Jag har en liten bonusfråga då till dig eftersom du är på [redacted]fakulteten. Vi har ju haft intervjuer på ett antal andra fakulteter, det är 4 stycken nu och 2 av de fakulteterna har kommenterat och påpekat att de tror att informationssäkerhetsreglerna och policysen är väldigt inriktade mot just eran fakultet faktiskt. Vi är bara nyfikna om hur du känner dig kring det?

P5

Ja nej alltså. Jag kan tänka mig att de tänker det för att det är har också med sjukvård att göra. Det är min gissning att folk tänker att det är inriktat på [redacted] för att de tänker så här. ”Ja, men det är patienter”. Om jag liksom ska gissa varför de har sagt det och att så här man tänker att medicinsk forskning är mycket känsligare. Vi har djurförsök, vi har ju många saker som kanske är mycket mer känsligt för samhället än vad kanske annan forskning har så jag förstår att folk tänker så. Jag skulle kanske inte säga att jag tror att någon annan har mer för att det tror jag kanske inte och jag har ingen aning. Jag som håller på med grundforskning som är ute på universitetet, upplever ju inte det som så, nej. Det är möjligtvis på läkarsidan som insatserna sitter i sådana fall. Det är möjligt. Men inte forskning.

FLL

Har du några tankar om hur informationssäkerhetskulturen vid Lunds universitet skulle kunna förbättras och om du kan föreställa dig någon konkret åtgärd som du känner hade kunnat åtgärda detta?

P5

Jo, men absolut och framför allt det har vi varit inne på, men alltså officiella riktlinjer som borde kommuniceras muntligt men också ska de ju självklart finnas skrivna som alla ska ha tillgång till. Men även muntligt och där är det egentligen ganska svårt. Ska det vara den dagen man blir anställd på universitetet ska det vara till exempel mitt ansvar som [redacted]att se till att alla i min [redacted]vet eller? Ska man från första dagen som student veta då man gör ett masterarbete? Vem har i sådana fall ansvar för det? Så att det är ganska svårt. Det är lätt att säga att ja, men det ska finnas officiella dokument men det är ju inte jättelätt. När, vem exakt, vilka ska ha de här dokumenten och vilka ska man gå igenom med? För jag menar, det är ju egentligen jätteomfattande, jag som [redacted]där känner jag att jag borde ju verkligen ha mycket mer information. Att bli [redacted]på universitet här i Sverige är ju mycket mer flytande alltså. I andra länder är det ju mycket ”från den här dagen är du [redacted]innan var du inte det” så är det inte i Sverige. Så om jag då som [redacted]skulle ha fått träningen, när skulle jag ha fått det till exempel? Jag har väldigt svårt att säga exakt hur man skulle

implementera det för när, var och för vilka liksom. Men det skulle ju behövas mycket mer och det skulle man ju säkert kunna hitta något bra sätt på? Egentligen borde det vara om man blir anställd universitet för egentligen skulle vi få en introduktion när man anställs och det händer ju typ inte heller. De har ibland så introduktionsdag för nyanställda och då samlar de upp typ så här de som kommit det senaste halvåret. Men den är ju väldigt generell och det är ju ingenting man måste gå på. Det är inte alltid det är och så där. Men om man skulle ha någonting där om du anställs av universitet så här har du material eller någonting. Egentligen ska man ju få information om allt som försäkring, friskvård osv. Alltså då rätt så basic saker, men om man inte vet dem så är det ju egentligen alltså universitets skyldighet och vad man har för rättigheter och skyldigheter på universitetet, men det får man ju inte heller. Det är ju nästan ingen som får. Och där tänker jag att man skulle kunna det. Det är ju en del av det, fast kanske ännu viktigare. Så att definitivt både muntligt någon slags träning eller att man verkligen får förklarat för sig. Och att det sen ska finnas dokument som man alltid kan gå tillbaka till och det kanske det gör men då måste man ju kommunicera att de finns.

AW

Avslutningsvis, har du några ytterligare tankar eller kommentarer som rör informationssäkerhet och det vi just har diskuterat?

P5

Nej, men det jag tror ju som sagt när ni skickar mailet så var det verkligen så här. Ja, just det alltså. Det här är ju verkligen en viktig fråga. Jag har ju tänkt på det innan kan jag ju säga. Men sen så släpper man den tanken liksom så att jag tänker att det att det är jättebra. Jag tror också att ni kommer få fram lite oroande data. Nej, men så att jag hoppas att det här som ni gör kan användas till nåt. Att det ni gör och kan sammanställa att det kan nå någon som behöver förstå att folk, det kanske bara är jag och alla andra kanske är jätte informerade och då är det ju lugnt, liksom. Det måste ju finnas på universitetet, folk som verkligen jobbar med bara de här frågorna och där måste man göra en insats och där hoppas jag verkligen att det kan nå fram till personer som måste höra det här och att man verkligen kan göra en insats. En satsning och sedan implementera ett system som kan fungera framöver för jag tycker att det är jätteviktigt, det är ju det och det är ju synd att vi inte vet mer. Jag tror verkligen inte alla vet att alla våra mail är offentliga handlingar, till exempel. Man skriver ju ändå mycket ja, men om djurförsök alltså allting liksom. Som för oss är självklart, men det kan uppröra ganska många känslor till exempel och det är ju många som skriver väldigt känsliga material, så bara att få veta det tror jag skulle vara en chock för väldigt många. Så jag hoppas verkligen att det kan leda till någonting att det kommer upp till folk som skulle behöva höra det.

Appendix 9 – Interview 6

FLL

Så, för intervjuns skull skulle du kunna uppge ditt namn och din roll vid Lunds universitet?

P6

[redacted] och jag är [redacted] för en [redacted], Lunds Universitet, fakultet, [redacted] fakulteten.

AW

Och utifrån din roll som forskare. Vad skulle du säga att ditt forskningsområde är?

P6

Mitt forskningsområde handlar om att försöka ta reda på varför [redacted] utvecklar typ [redacted] eller [redacted].

FLL

Hur länge har du varit forskare vid Lunds universitet?

P6

Det har jag varit sedan. Vad ska vi säga, HT2013 kan man väl säga? I så fall när jag började min doktorandutbildning.

AW

Och har du då någon tidigare erfarenhet vid som forskare vid andra universitet?

P6

Nej, det är bara i Lund.

FLL

Ja då hoppar vi till lite mer informationssäkerhetsrelaterade frågor och då vill vi fråga dig hur du skulle definiera informationssäkerhet utifrån din egen förståelse?

P6

Informationssäkerhet.. men jag tänker, ehhh är det fokus framför allt på digital informationssäkerhet eller är det liksom generellt?

FLL

Ja, det är hur du tolkar det.

P6

Haha hur jag tolkar det.

FLL

Vill inte ställa ledande frågor.

P6

Nej, precis. Nej, men jag. Jag tänker väl mycket på det arbetet som vi har gjort här med. Nej, men det är väl liksom i och med att man samlar in data det mesta är ju digitalt och då och då är det ju att försöka hålla det så säkert som möjligt. Och det har väl liksom gått upp för oss lite mer de senaste åren? Det ja, men det krävs en hel del. För att hålla koll på all data som vi har.

AW

Och vilken utbildning eller träning om informationssäkerhetspolicy, åtgärder eller policys eller liknande vid Lunds Universitet, har du fått?

P6

Ingen? Jag har väl gått. Nej, jag har inte fått någon träning mer än informationsmöte när det gäller saker som GDPR och framför allt någon typ av information när det gäller, ja men spara digital data. Men mer på informationsnivå liksom.

FLL

Hur skulle du beskriva informationssäkerheten vid Lunds universitet, anser du att informationssäkerheten beaktas i tillräcklig utsträckning?

P6

Om jag tänker från min egen verksamhet och dagliga, så svar ja.

AW

Varför, eller skulle du kunna expandera på det?

P6

Nej, men just informationssäkerhet. Hm ja men just det här när man ska logga in i olika system. Det är ju såna här 2 stegs inloggningar. Jo men litegrann, vi har ju också gått igenom vad vi får lov att lagra på våra olika kataloger. Så det har vi också gjort, liksom en stor genomgång och så vidare. Vi använder ju det här LUSEC till exempel för långtidsförvaring och så att en sådan genomgång har vi ju gjort.

AW

Nu kommer vi in på hantering av uppgifter, alltså hur skulle du hantera konfidentiella uppgifter när de utbyts via e post och ifall du har möjlighet till att ge exempel också?

P6

Jag skulle just som i min roll som chef vi håller på med anställningsunderlag och sånt där så använder jag ju säker epost när det gäller våra forskningsdeltagare. Vi har ju flera olika studier som vi gör, men där när vi utbyter information så är det ju aldrig personliga uppgifter utan det är pseudonymiserade så vi har ju typ local code, subject id och allt sånt där som vi skickar aldrig personnummer eller någonting sådant.

FLL

Samma bana, hur hanterar du konfidentiella uppgifter när ni skriver ut fysiska dokument om du har ett exempel där också?

P6

Där tycker jag, nu har vi fått närmare liksom kopierar innan så kunde man ju printa och så låg det öppet i kopieringsapparatsrummet, men det gör det ju inte nu längre och nu har vi ju liksom typ ID kort som man måste trycka på så att det är ingen obehörig som kan se när man printar. Så det är väl en sak som jag har lagt märke till.

AW

Och hur hanterar du konfidentiella uppgifter när du delar uppgifter med andra, alltså i person eller via zoom till exempel? Och ifall du också har något exempel att ge?

P6

Nej, alltså. Jag tänker om vi har våra möten och man, alltså pratar vi specifikt om våra studiedeltagare och vi skrivna i de för olika antikroppar för de här olika sjukdomarna och då har vi ju liksom inom forskargruppen har vi ju månadsmöten, men då pratar vi ju bara fortfarande i form utav alltså de här local code och subject ids, så vi har ju liksom aldrig något namn eller någonting sådant utan. Och det kan jag också se, på de kanske sista ska vi se 5-10 åren, så har det skett en förändring just hur man pratar om studiedeltagare i forskargruppen, att det är mer anonymt nu utan det är mer bara liksom rakare kurs.

FLL

När du går in i ett rum som kräver ett l kort och det finns annan person närvarande som också vill gå in. Hur skulle du hantera den situationen? Och har du fått ta del av någon regel angående det eller någon policy?

P6

Nej nej det nej det har jag inte en tanke på. Det var mer, här går jag in på udda tider när huset generellt är låst. Det är klart att jag har blivit tillsagd att jag inte ska släppa in någon annan i huset eh om de inte själva har ID kort. Det är väl egentligen den enda regeln.

AW

Och berätta om ett informationssäkerhetaintrång eller en incident, ett scenario som skulle ha den mest förödande effekten på just din forskning.

P6

Ja, men det är det skulle ju vara om någon kan hacka sig in eller ta sig in i de olika systemen som vi använder. Vi har ju, dels använder vi ju RedCap där vi, liksom alla våra studier, det som samlas in, informationen läggs i det systemet. Vi samlar in mycket kostdata på barnen i några studier så har vi ju ett elektroniskt inmatningsprogram där all kostdata ligger ifrån över 3 olika studier nu, jag menar, skulle någon ta sig in där och förstöra sig klart att då försvinner ju all forskning som vi gör.

FLL

Vilka informationssäkerhetsutmaningar skulle du stöta på i din dagliga forskning?

P6

Utmaningar.. ja, men det är väl, men vi hade ju, det var ju. Jag tänker speciellt med den här näringsberäkningsprogrammet som vi har där vet jag att våra datakillar här, vid något tillfälle, sagt att de kunde uppleva att det var liksom en svaghet med säkerheten just med det här programmet och där har vi ju fått lov att alla vi som använder programmet fått ange våra datorers IP adresser. Så att de är liksom? OK. Så skulle man logga in på det här programmet från någon annan data med annan IP så är det oklart om man ändå har åtkomst.

AW

Och då går vi vidare till informationssäkerhetskultur och det definieras då bland annat som åsikter, tankar, värderingar och beteenden av medlemmar av en organisation som skulle kunna påverka säkerheten vid organisationen. Så utifrån det hur skulle du beskriva informationssäkerhetskulturen vid Lunds universitet?

P6

Men den uppfattar jag som god, det är min känsla generellt att när man att man har blivit mer medveten om vilka hot som finns, så att man skärper upp. Men jag kan väl också känna det vi, vi är ju en verksamhet som är står med ett ben in i universitetet och ett ben vid Skånes universitetssjukhus och innan har det varit ganska lätt att röra sig mellan de här två organisationerna. Man märker mer att organisationerna vill, liksom alltså? Det är det inte den här flytande linjen mellan de här två olika organisationer utan nu är det lite mer krångel när det gäller liksom allt digitalt utbyte. Alltså både på ekonomisidan, ja allt. Och det kan väl vara liksom just att man stärker sitt skalskydd så att säga.

AW

Vad skulle du säga föranlett den här förändringen som det har sett över åren?

P6

Men jag tror att det är det är väl regelverk som har föranlett det, men man om det är i och med GDPR eller vad det är. Att man i varje organisation försöker stärka liksom sina egen verksamhet och skydda sig.

FLL

Jag har också en fråga som specifikt till dig då som är på [redacted] fakulteten, som vi har haft, vi har haft lite intervjuer med 4 andra fakulteterna också och 2 av dem har påpekat att de tror att policyn och hur de upplever att policyn och riktlinjerna är mer inriktade mot [redacted] fakulteten när det gäller informationssäkerhet och att dom tror att ni har mer av en öppen dialog med universitet när det kommer till det. Hur känner du kring det?

P6

Jo, men det kan jag nog hålla med om och vad det beror på varför skulle, varför skulle vara skillnaden vet jag inte, men. Men ja vi håller väl på med forskning oavsett vilken fakultet man tillhör, men det är väl mer att vi den [redacted] forskningen, det är väl mycket alltså just att det är särskilt känslig data som vi håller på med. Och kanske också kan det vara det i och med att många är kanske läkare och jobbar med sekretessfrågor inom sjukvården, så det är ju naturligt på ett annat sätt?

AW

Och har du några tankar om hur informationssäkerhetskulturen vid Lunds universitet skulle kunna förbättras? Och då ifall du också har någon konkret åtgärd eller aktivitet som du har valt tanke.

P6

Nej alltså nej, inga direkta tankar kan jag inte säga att ja det. Det enda som är funderar på det är ja, men det är just att det varit så mycket om just den elektroniska säkerheten och så men sen samtidigt. Å andra sidan går man in i mitt kontor. Jag har ju väldigt mycket papper här. Och där känner jag att det här har man inte riktigt fokuserat lika mycket på den. Ja, men lite grann vi, vi försöker ju ändå när man lämnar dagen så ska det inte ligga pärmar framme på skrivbordet med känslig information, utan det ska ju låsas in. Men det är väl ungefär på den nivån.

FLL

Avslutningsvis har du några ytterligare kommentarer eller tanke som rör informationssäkerhet eller det vi snackat om nu?

P6

Det är väl liksom än så länge allting går bra så känner man sig trygg men jag men jag kan ju tänka mig om man någon gång skulle bli utsatt för någonting. Så är det bra att vi har riktlinjer och, ja, hade inte varit roligt att bli utsatt att man helt plötsligt komma till jobbet och sen så är ens konto kapat på något sätt, men.

FLL

Men du har förtroende i att Lunds universitet kan förebygga det?

P6

Men absolut och de vågar jag säga då våra IT killar gör ett superbra jobb och jag är ju väldigt liksom trygg. Ja man försöker hålla liksom koll och allt sånt där så att jag känner mig definitivt trygg.

References

Alshaikh, M., Maynard, S., Ahmad, A. & Chang, S. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations, Proceedings of the 51st Hawaii International Conference on System Sciences, 1 January 2018

Amankwa, E., Loock, M. & Kritzinger, E. (2022). The Determinants of an Information Security Policy Compliance Culture in Organisations: The Combined Effects of Organisational and Behavioural Factors, *Information and Computer Security*, vol. 30, no. 4, pp.583–614

Bongiovanni, I. (2019). The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education. Computers and Security, *Computers and Security*, vol. 86, pp.350–357

CNSS. (2023). *About CNSS*, Available Online: https://www.cnss.gov/CNSS/about/about.cfm [Accessed 4 March 2023]

CNSSI-4009, National Information Assurance (IA) Glossary. (2010). , Available Online: https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

Glaspie, H. (2018). Assessment of Information Security Culture in Higher Education, *Electronic Theses and Dissertations*, no. 6009

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, *Decision Sciences*, vol. 43, no. 4, pp.615–660

Lichtman, M. (2013). Making Meaning From Your Data, in *Qualitative Research in Education: A User's Guide*, 3rd edn, Thousand Oaks: SAGE Publications, pp.241–268

Malcolmson, J. (2009). What Is Security Culture? Does It Differ in Content from General Organisational Culture?, 43rd Annual 2009 International Carnahan Conference on Security Technology, Zurich, Switzerland, 2009, Zurich, Switzerland, pp.361–366

Oates, B. J., Griffiths, M. & McLean, R. (2022). Researching Information Systems and Computing, SAGE Publications

Patton, M. Q. (2014). Qualitative Research & Evaluation Methods: Integrating Theory and Practice, 4th edn, SAGE Publications

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change, *The Journal of Psychology*, vol. 91, no. 1, pp.93–114

Samonas, S. & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security, *Journal of Information System Security*, vol. 10, no. 3, pp.21–45

Shimeall, T. J. & Spring, J. M. (2014). Introduction to Information Security: A Strategic-Based Approach, Syngress

Siponen, M., Mahmood, A. & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study, *Information & Management*, vol. 51, no. 2, pp.217–224

Solms, R. von & Niekerk, J. van. (2013). From Information Security to Cyber Security, *Computers & Security*, no. 38, pp.97–102

Sommestad, T., Karlzén, H. & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour, *International Journal of Information Security and Privacy*, vol. 9, no. 1

Whitman, M. E. & Mattord, H. J. (2017). Principles of Information Security, Cengage Learning

Wlosinski, L. (2019). The Benefits of Information Security and Privacy Awareness Training Programs, *ISACA*, vol. 1, no. 2019

Yerby, J. & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behavior, *Journal of The Colloquium for Information System Security Education*, vol. 6, no. 1