UNIVERSITY OF GOTHENBURG

DEPARTMENT OF APPLIED IT

FACULTY REFLECTIONS ON UNIVERSITY INFORMATION SECURITY POLICY

Sofia Dyrendahl

Thesis:	30 hp
Program:	Digital Leadership
Level:	Second Cycle
Year:	2021
Supervisor:	Juho Lindman
Examiner:	Jonas Ivarsson
Report nr:	2021:039

ABSTRACT

Employee noncompliance of information security policy (ISP) is causing organizations more and more money in the battle against cybersecurity threats. Three popular theories within employee compliance and ISP research were used to create a conceptual framework to help explain the employees' reflections, namely: protection motivation theory, deterrence theory and neutralization theory. A case study with faculty members from University of Gothenburg was conducted to see how the faculty members reflect when it comes to the ISP at their workplace and their own protection behavior. Semi-structured interviews were held digitally with six participants. The result indicate that faculty members rarely reflect on their protection behavior, they were unaware what the ISP was and even though they believed the threat of a cyberattack was medium to high, they still engaged in behavior they know could expose the university to unnecessary risk. This research can help the university and other government agencies to structure their Security Education, Training and Awareness (SETA) to match the employees' behavior on IT security and help bring awareness of the knowledge and ideas employees have of information security.

KEYWORDS

Cybersecurity, employee compliance, information security policy, protection motivation theory, deterrence theory, neutralization theory, university.

FOREWORD

Thank you to all participants who helped me make this thesis possible. I also want to thank my professors at the Digital Leadership program who inspired me. Thank you to my family and friends for endless support and thank you to Zeph and Mira for giving me energy and hope. *A special thank you* to Juho for guiding me and helping me stay calm and confident throughout this process!

TABLE OF CONTENT

1 INTRODUCTION 1
2 PREVIOUS RESEARCH 3
2.1 Protection Motivation Theory 3
2.2 Deterrence Theory 5
2.3 Neutralization Theory 7
2.4 Combining the Theories 8
3 CONCEPTUAL FRAMEWORK 9
4 METHODOLOGY 11
4.1 Research Approach 11
4.2 Research Setting 11
4.3 Data Collection 11
4.4 Data Analysis 13
4.5 Covid-19 14
5 RESULTS 16
5.1 Consequences of Cyberattacks 16
5.2 Defense & Role of the Employee 17
5.3 IT Security Systems & Rules 21
6 DISCUSSION 24
6.1 Protection Motivation Theory 24
6.2 Neutralization Theory 27
6.3 Deterrence Theory 29
7 CONCLUSION 31
7.1 Practical Implications 31
7.2 Future Research 32
7.3 Limitations 32
8 REFERENCES 33
9 APPENDIX 37
9.1 Interview Guide 37

1 INTRODUCTION

One of the greatest weaknesses in an organizations' cybersecurity process are the employees (Boss et al., 2009; Luo et al., 2011; Cole, 2015). No matter how extensive an organization's cybersecurity system is, a simple mistake from an ignorant employee can make it all for nothing. Richardson (2008) showed that insider neglect is second highest cause of successful cyberattacks after virus incidents. Cisco (2021) reported that 53 % of cyberattacks result in $500,000 or more in damages. Additionally, Gartner (2021) report that roughly $134 billion was spent on security and risk management worldwide, making it a relevant issue for all organizations.

Due to the increased digitalization of society, risk management of information system security (ISS) is critical for organizational survival (Herath & Rao, 2009). Already in 2004 did Vroom and von Solms bring attention to the issue of how insider negligence caused security breaches and noted that the organizations which pay attention to non-technical factors in their cybersecurity processes are more successful in their efforts. Despite much research being published on the area, organizations have struggled to implement effective information security policies (ISP) (Johnston, Warkentin & Siponen, 2015).

The most common forms of cyberattacks are malware such as viruses, spyware, ransomware and worms; phishing; man-in-the-middle attacks, which steals and filters data, often gained access through unsecure WIFI connections or malware; DDoS attack to exhaust and use up all resources and bandwidth; SQL injection used to get information from webpages by entering malicious code on a webpage's regular input box such as a search field or the fields for login credentials; zero-day exploit which takes advantage of a network vulnerability before it is fixed; DNS tunneling which can be used to bypass IT monitoring or allow remote management of a compromised device. (Cisco, 2021)

Higher education and other government agencies are seen being targeted more frequently by cybercriminals, mostly deploying ransomware attacks (FBI Flash, 2021). The cybercriminals steal sensitive employee data which can be used to extort the individual employee. Furthermore, several big IT scandals involving Swedish government agencies have been reported over the last couple of years (*see:* TT, 2019; Holmberg Karlsson, 2017). A case study will be conducted at University of Gothenburg, which had an IT debacle where faculty members were unable to access or receive email and could not access their calendar, losing important emails and missing meetings (Göteborgs Universitet, 2020). Showing there is a lack of strategic and mindfully implemented cybersecurity at these institutions. Therefore, understanding how faculty members reflect on their protective behavior, along with the ISP of the university where they work, becomes highly relevant and important to protect Swedish citizens.

Lowry, Dinev and Willison (2017) call for research to be done on employees' decision-making process in order to find better solutions for organizations battling with the problem of employee compliance. Therefore, the aim of this study is to help contribute to literature on decision-making and ISS, by exploring faculty members' reflections on the ISP and all official IT security rules at their workplace. ISP and official IT security rules will for the remainder of this thesis only be referred to as ISP. The research question this study aims to answer is:

How do faculty members reflect on university information security policy?

To bring more insight of how to approach the issue of employee compliance at universities, three of the most common ISS theories will be used to interpret the data, protection motivation theory (PMT), deterrence theory (DT) and neutralization theory (NT). A conceptual framework based on these theories was formed to connect the theories and give a new perspective on employee compliance. The conceptual framework is used to structure the discussion of the findings for a more nuanced argument.

The study is limited to a single university setting, with semi-structured interviews being conducted with full-time employees. By doing interviews in single case study the generalizability of the findings is limited. Instead, this study aims to give qualitative data which will provide valuable insight into the thoughts of the employees at a Swedish university. Furthermore, the scope is limited to the reflections of the employees and will not investigate how PMT, DT and NT relate to the actual intention to engage in protective behaviors (for research on this see: Ifinedo, 2012; Herath and Rao, 2009; Aurigemma & Mattson, 2017). Practical implications of the research are a better structure of Security Education, Training and Awareness (SETA) which will engage the employees where they are in their reflections on the cybersecurity, hopefully resulting in higher compliance with ISP and thus, better protection of confidential data.

The structure of the thesis is as follows: in the next section, previous research in the field of ISS is discussed together with the relevant literature within PMT, DT and NT. In the third section the method used to investigate the research question is described. Thereafter, the results from the case study are presented, then a discussion is held to provide more insights to the implications of the results. Lastly, is a conclusion summarizing the findings and answering the research question.

2 PREVIOUS RESEARCH

Dhillon and Backhouse (2000) wrote a paper about the dangers of digitalizing your business without fully understanding the new security threats of cyberspace and planning for these accordingly. The field of information security is still being explored and is ever evolving together with the advancements of technology.

Cram, D'arcy and Proudfoot (2019) made an extensive meta-study in order to optimize the theoretical framing when researching security policy compliance. They found that personal norms, attitude and ethics were the most significant when predicting employee compliance. Further, they found that punishment expectancy, severity and rewards were the least significant. Self-efficacy and response efficacy had average to high effect on compliance. Cram et al. (2019) also found that the variables could have different effects on intended compliance compared to actual compliance. The findings call out for more research on what employees' attitude and norms relating to ISP are and why the effectiveness of variables can differ depending on the circumstances (Cram et al., 2019).

2.1 Protection Motivation Theory

Roger (1975) developed the protection motivation theory (PMT) to understand fear appeal. He wanted to see how fear influence behavior and the changed frequency of behavior in response to fear. Protection motivation is the intention to perform a desired behavior (Norman, Boer & Seydel, 2005). The theory works from the assumption that external or internal stimuli can trigger two appraisal processes: coping appraisal and threat appraisal.

Norman et al. (2005) outlines the main components of PMT:

Adaptive response	A part of coping appraisal. It is the process which push for the desired behavior to be performed. The higher the coping appraisal is, the more likely it is that the employee engage an adaptive response.
Maladaptive responses	The behavior which are aimed to reduce the fear of a threat but does not reduce the threat itself.
Severity	The perceived level of impact of the threat.
Vulnerability	The employee's perception of: "…the probability that an unwanted incident happens if no actions are taken to prevent it" (Vance et al., 2012, p. 191).
Rewards	Benefits of engaging in maladaptive responses which will reduce the employee's threat appraisal.

Response efficacy	"The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others" (Floyd, Prentice-Dunn & Rogers, 2000, p. 411).
Self-efficacy	The employee's belief that they can perform the desired protective behavior.
Response cost	Barriers which hinder the employee's ability to perform the protective behavior/adaptive response.

Posey, Roberts and Lowry (2015) emphasize the importance of human behavior and ISP in the effort to ensure the success of a cybersecurity project. Furthermore, their study is one of few which considers both protective intentions and protective behavior. Protective intention is the employee's intention to engage in protective behavior and protective behavior is behaviors performed by the employee in order to protect data or the organization. Posey et al. (2015) have a nuanced discussion about PMT and its literature, pointing out that the use of PMT and the results from the studies have been inconsistent. Nevertheless, they deem it to be an appropriate theory to help explain employee compliance and make two important points. First one, is that employees have a considerable control over the information they have at work and it is their choice to actively protect this information or not. This is an important point because it is an underlying assumption when investigating employee compliance and it highlights the fact that even if there were no policy telling the employee what to do, they still have a choice if they want to protect the information or not. The second point they make, is that some protective behaviors require more energy than other behaviors. This is also an underlying assumption which can help explain why some protective behaviors may be more common among employees than others.

Anderson and Agarwal (2010) state that PMT is one of the most efficient theories in predicting if an individual will engage in protection behavior. Ifinedo (2012) saw that combining PMT with another theory, in this case theory of planned behavior (TPB), better explained ISP compliance and found several correlations between the factors of PMT and ISP compliance. Interestingly, the factor *response cost* did not show a negative correlation to ISP compliance, which was hypothesized. Also worth noting, is that perceived severity did not have a positive influence on ISP compliance. It is common to combine PMT with one of more theories in order to better capture the essence of the results.

Another example of someone who added to PMT to gain more value from the theory is Vance, Siponen and Pahnila (2012). They did a study combining PMT with a habit factor. They investigate if past and automatic behavior influence employees' decision to comply. Vance et al. (2012) applied all the appraisal factors of PMT with the addition of the habit factor. The reason they add habit to the theory is because of the "pervasive effect of habit on human behavior" (Vance et al., 2012, p. 190). They add the habit factor before any PMT factor, thus hypothesizing that habit influence both the threat and coping appraisals. Contrary to Ifinedo

(2012), Vance et al. (2012) found that *vulnerability* instead of *severity* had an insignificant effect on employee compliance. They further found that habit had a strong correlation with all PMT variables.

Warkentin, Johnston, Shropshire and Barnett (2016) use the term 'perceived extraneous circumstances' to capture both rewards and response cost in one term. The study aimed to see how PMT affected protective security behavior continuation, which means performing a protective behavior more than once. However, Warkentin et al. (2016) see the extraneous circumstances as something which affect the behavior directly rather than through the threat and coping appraisals like in the original theory put forward by Rogers (1975). Warkentin et al. (2016) also did not find that response efficacy had a correlation with intention continuation. Similarly did Vance et al. (2012) find that response efficacy had the opposite effect on intention. Therefore, does neither study support that response efficacy have positive influence on protective behavioral intentions. This shows that there are some contingencies in PMT making further research exploring new perspectives highly relevant.

> A lack of a salient threat may lead these individuals to believe that they are no longer susceptible and discontinue the associated behavior. Other research suggests that organizational members must believe in the efficacy of a new security measure before they will use it. (Warkentin et al., 2016, p. 25)

Moody, Siponen and Pahnila (2018) have combined several of the common theories in employee compliance research and formed one more unified ISS model. It draws the main factors from theory of interpersonal behavior, which is quite similar to a combined PMT and deterrence theory (DT). The model becomes a good summary of the various theories and models which are used to try to explain employee (non)compliance. The model also includes a habit factor and put emphasis on fear appeal's relationship with employee compliance. Moody et al. (2018) show that the many of the ISS theories, working from different assumption and backgrounds, can be combined to form an overarching model illustrating the correlation between several factors explaining employee compliance.

2.2 Deterrence Theory

Deterrence theory (DT) work from the assumption that given the choice people will avoid certain action if the sanctions are severe, certain and swift enough (Gibbs, 1968). The theory is based on Beccaria's work from 1764 and is one of the most cited theory in ISS research between 1990-2004 (Siponen, Willison & Baskerville, 2008). Informal sanctions were added by Williams and Hawkins in 1986, such as shame and guilt. Paternoster and Simpson (1996) further developed shame as a component but see this as separate from formal and informal sanctions because it is self-imposed. Current DT discourse suggests that individuals evaluate the perceived costs of both formal and informal sanctions before deciding whether or not to perform an illicit activity (Pratt et al, 2006).

The main components of deterrence theory are the formal sanctions: certainty, severity and swiftness (Beccaria [1764]1963). In order for a formal sanction to be effective it should have high certainty of happening, so likelihood of getting caught and the organization acting on the transgression. It should be severe, if the punishment is too lenient it will not deter from the unwanted behavior and the benefit of the transgression will be perceived as higher than the consequence of the violation. Lastly, the formal sanction should be swift, if it takes too long between the transgression and the punishment then it is likely for the violation to be partly forgotten. In addition to the formal sanctions, does Piquero and Tibbetts (1996) present informal sanctions such as self-approval and social approval. Self-approval refers to how a person views themselves and their actions. Social approval is how people in the person's environment view the person's actions. Both which can influence whether or not a person violates the social norms and rules.

D'arcy and Herath (2011) saw in their literature review of deterrence theory that the effect of sanctions varied depending on the individual. Therefore, the fundamental assumptions that people will avoid certain action if the sanctions are certain, swift and severe enough, is more complex than first assumed. D'arcy and Herath (2011) present several individual and contextual factors which are seen affecting the degree to which the person is deterred by sanction threats. The individual factors are: self-control (individuals with low self-control are more likely to ignore threats of sanctions (Pogarsky & Piquero, 2004)), computer self-efficacy (CSE) (how confident the individual is in their general computer ability and their ability in specific programs and IS tasks (Marakas, Johnson & Clay, 2007)) and moral beliefs (to what extent does the person believe an illicit act to be morally wrong (Paternoster & Simpson, 1996)). The contextual factors are: virtual status (how much of the employee's work is done away from the central workplace (Wiesenfeld, Raghuram & Garud, 1999)) and employee position (is the employee full-time, part-time, manager etc. (Tittle, 1980). Furthermore, D'arcy (2005) showed that as computer literacy increases, IS misuse will increase as well due to employees becoming more confident that they can work around the security systems and avoid security threats. Several of these variables overlap with PMT or other DT variables, most obvious being computer self-efficacy versus PMT's self-efficacy or moral beliefs which are similar to self-approval. Piquero, Paternoster, Pogarsky and Loughran (2011) support D'arcy and Herath's (2011) argument that individual factors carry significance when determining the effectiveness of deterrents.

The research on deterrence theory have evolved not only to include the informal sanctions, but also to focus on individuals' responses to sanctions and threats (c.f. D'arcy & Herath, 2011; Piquero et al, 2011). Therefore, researching not only how the individual differences influence the likelihood of ISP (non)compliance, but also what the individuals themselves think about the ISP becomes highly relevant.

2.3 Neutralization Theory

Siponen and Vance (2010) talks about how neutralization techniques affect employees' intention to violate the ISP. They compared neutralization techniques to deterrence theory and found that neutralization was a strong predictor of intention to violate ISP. Sykes and Matza (1957) presents neutralization theory and claim that both rule-breakers and rule-followers generally believe in the established norms and values of society, indicating that it is not a disbelief in the norms and values which causes people to break the rules. Neutralization theory (NT) presents techniques which people can use to justify their actions (Siponen & Vance, 2010). These techniques allow people to keep their norms and values aligned with society, but still engage in rule breaking (Piquero et al., 2005).

Siponen and Vance (2010) presents a modified version of NT adapted to ISS research. They divided neutralization into six determinants, presented here in order of the highest significance they found: 'metaphor of the ledger', 'defense of necessity', 'denial of injury', 'appeal to higher loyalties', 'condemn the condemners', and 'denial of responsibility' (Siponen & Vance, 2010).

Rogers and Buffalo (1974) explain that denial of responsibility is when a person claim the action is beyond their control. Siponen and Vance (2010) use the example of poachers breaking the law because one did not know hunting was prohibited or programmers blaming the computer when they have made a mistake. Denial of injury is when a person justifies their action by undermining the damage it can cause (Sykes & Matza, 1957). For instance, when hackers explain that their crimes are victimless because they are attacking a computer (Siponen & Vance, 2010). Defense of necessity is the technique of claiming that the violation was necessary therefore one should not feel guilty (Minor 1981). This could be used when an employee breaks the security policy because they felt they had to in order to finish their work. Byers et al. (1999) describe condemnation the condemners as neutralizing one's actions by putting the blame on the target. For example, violating the ISP because they think it is unreasonable or unjust. The technique, appeal to higher loyalties, means using a higher authority to explain one's actions (Piquero, Tibbetts & Blankenship, 2005). For instance, an employee violates the ISP and explain their behavior by appealing to the company values or a memo from management. The metaphor of the ledger, which was the most significant technique in Siponen and Vance's study (2010), means that by doing good you compensate for any wrongdoing. In terms of employees, each time they comply with the ISP, they can then violate it, because they are in the black.

Gwebu, Wang and Hu (2016) found that neutralization was a more effective explanation for noncompliance than other variables, such as social culture. They also found that neutralization increase the effect of perceived response cost by encouraging noncompliance. Thus, concluding that neutralization may be a stronger predictor when it comes to employee compliance than other variables from PMT and DT. Therefore, making NT an interesting addition to the other theories on order to gain a better understanding of employees' reflections on protection behavior and ISP.

2.4 Combining the Theories

DT and NT are often researched together, examples being: Silic, Barlow and Back (2017), Willison and Warkentin (2013) and Cheng, Li, Zhai and Smyth (2014). Vance and Siponen (2010) combine DT and NT by studying how both influences the intention to violate the ISP. Furthermore, DT and PMT is also researched together in several instances, examples being: Moody et al. (2018), Kinnunen (2016) and Johnston et al. (2015). Herath and Rao (2009) combine DT and PMT similarly to how DT and NT was combined, by seeing how the variables from both theories affect ISP compliance intention. Thus, showing that the theories work from assumptions which are possible to combine to get a wider perspective on employee (non)compliance.

However, PMT and NT are rarely researched together, this thesis will help filling the gap to see how well these theories work together when combined. PMT's maladaptive response is not to be confused with maladaptive behavior. Where maladaptive response aims to reduce the fear (Posey et al., 2015) and maladaptive behavior is e.g., violating the ISP. Maladaptive response could be seen overlapping with the neutralization techniques presented by Siponen and Vance (2010). High threat appraisal increases the likelihood of maladaptive responses such as wishful thinking and avoidance, which is similar to neutralization techniques such as denial of responsibility. However, the difference being that maladaptive responses aim to reduce fear while neutralization techniques aim to justify maladaptive behavior. Moody et al. (2018) makes an attempt at combining these theories and does so by introducing the factor: *reactance*. Reactance means denying that there is an ISS problem altogether. This is in addition to current choices of compliance and noncompliance, giving the individual three possible ways to react, comply, violate, or ignore. Reactance, is in their theory, influenced by both the fear appeal from PMT and neutralization techniques from NT. So, like with the other studies combining two or more theories, they investigate how the theories influence a third variable when combined.

Combining all three theories will give a wider understanding of how the faculty members reflect on ISP. The study is not looking to find a correlation between faculty reflections and intention to comply to ISP, but provide in-depth knowledge about individual reflection by analyzing the data with the help of PMT, DT and NT. Therefore, providing a foundation to build further research on where these theories are combined to help explain and increase employee compliance.

3 CONCEPTUAL FRAMEWORK

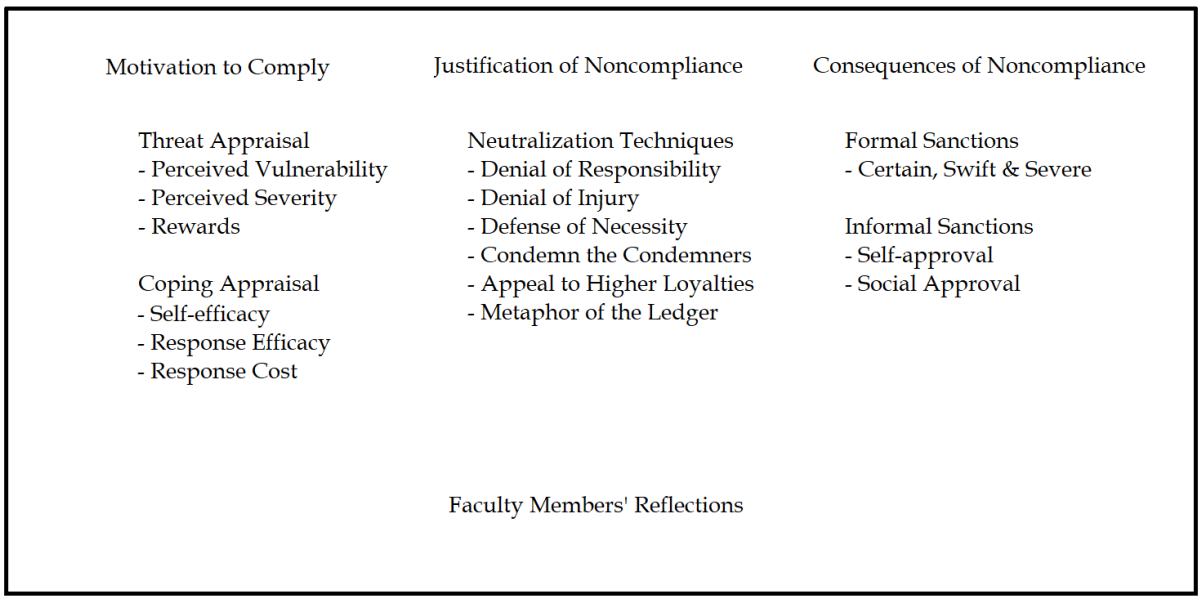
A conceptual framework was formed based on the previous research presented above. The framework combines the three theories: protection motivation theory (PMT), deterrence theory (DT) and neutralization theory (NT), into a simple model. The framework presents the different variables which will be used from each theory in the remainder of the thesis.

Both PMT and DT build on an individual's level of fear of a threat (Rogers, 1975; Gibbs, 1968). PMT fear appeal is based on threats external to the organization, while DT builds on threats from internal factors, such as the organization where they work, their colleagues and their moral compass. Therefore, the theories complement each other and give a more holistic view, covering more situations and factors an employee may reflect on. NT on the other hand, discuss more the coping mechanisms when not complying with the rules. PMT have two coping factors which increase likelihood of compliance, response efficacy and self-efficacy (Rogers, 1975). However, these work to affect the behavior in direct response to the threat. NT does therefore bring a new way to understand how the employees think by explaining noncompliance. In previous studies all three theories have been used to bring light as to why employees comply or do not comply with ISP. When they are combined they cover employees' reasoning of the external threat of a cyberattack (PMT), the believed effectiveness and capability of their protective behavior (PMT), the consequences they face if they violate the rules, both formal and informal (DT), and lastly, how they justify their noncompliance behavior (NT). Each theory help bring understanding to a different aspect of security compliance and by using all theories together, this thesis aim shed light on faculty members' reflections on the security situation, their behavior, the consequences and their internal dialogue.

To bring further understanding on how these theories are connected and complement each other, a conceptual framework has been formed, see figure 1. The codes presented under each theory are later used when analyzing the data from the interviews to form relevant themes which will help answer: *How do faculty members reflect on university information security policy?* In the spirit of previous studies combining these theories, they are joined to see how they together help broaden the understanding of the faculty members' reflections. The study assumes that combining all three when analyzing and discussing the research data will result in the most in-depth knowledge.

This study is not looking at actual compliance with ISP, but rather how the faculty members reflect on ISP and will use the three theories to shape the perspective and understanding of those reflections to be able to contribute to the literature on employee compliance and ISP. Therefore, as you can see in figure 1, most theories study to see how the theories affect Intention to Comply, this study aim to understand how the faculty members' reflections can be understood with the help of the theories.

Figure 1. Framework for Structuring Faculty Members' Reflections.



4 METHODOLOGY

4.1 Research Approach

The aim of the thesis is to evaluate how faculty members reflect on the organization's information security policies (ISP) along with their protection behavior. Therefore, the empirical data was collected in a single case study through semi-structured interviews because it is appropriate when aiming to provide an "in-depth understanding of a single or small number of cases; set in their real-world contexts" (Yin, 2011, p. 4). Additionally, inductive reasoning was used to explore the research question: *How do faculty members reflect on university information security policy?* Inductive reasoning is used to be able to generate meaning from the empirical data collected through the interviews to be able to identify patterns and answer the research question (Bell & Bryman, 2018). Furthermore, by using an exploratory research design the study will better capture the *How* of the research question and provide insight into the phenomenon of employee compliance with the focus of faculty members' reflections (Denscombe, 2014).

4.2 Research Setting

The case study was conducted at the department of Applied IT at the University of Gothenburg. The department conduct research in informatics; cognition and communication; learning, communication and IT; and human-computer interaction (University of Gothenburg, 2021). There is a significant amount of international and English-speaking professors and lecturers. It's a medium-sized department with five divisions and a total of 90 staff members. There were no information security researchers working for the department at the time the study took place.

The university was chosen for this study because the professors have access to sensitive student data, such as personal information, potential candidates, existing students and previous student, through large government databases and handle confidential research data. Because of this, it could make them a potential victim of e.g., ransomware attacks or DDoS attacks. Furthermore, the University of Gothenburg had a great IT incident in September 2020 where faculty members lost access to their email and calendar for several weeks. Emails from several years back were lost and never recovered. Therefore, it is highly relevant to research how the faculty members at a department at University of Gothenburg think regarding their information security.

4.3 Data Collection

Tittle (1980) pointed out that employee position can be a contextual factor affecting employee engagement. Therefore, it is controlled for by only asking full-time professors and senior

lecturers to participate. Since there were no active information security research taking place, everyone with the titles professor or senior lecturer were asked to participate. The interviews were conducted in either Swedish or English depending on the participants' preference. All professors and senior lecturers who were available and wanted to participate were interviewed.

The department of Applied IT was chosen because all professors and lecturers are assumed to have basic IT knowledge as well as an extended understanding of cyberspace, however theoretical. Furthermore, they educate students in digitalization and publish information system research which makes their knowledge, interest and general attitude towards information security influential beyond their actions.

4.3.1 Interviews

Conducting interviews is an effective method to get primary data to give a deeper understanding of a topic (Bell & Bryman, 2018). The aim of the study is to bring more understanding of faculty members' internal reflections. Therefore, semi-structured interviews were chosen to allow the participants to talk more freely about their reflections and allow follow-up questions for interesting and relevant thoughts. Semi-structured interviews also give some basic structure ensuring that the topics important to this study is covered in each interview (*see:* Appendix). This will help to get an accurate picture of how the participants think about the information security policy (ISP).

The interviews were held digitally on the platform Zoom. Cameras were on during the whole interview to establish a rapport. The participants answered both general questions about ISP and questions related to each theory/model. They were also asked what they think about their employer's ISP and information security in general.

Table 1. *Participant, position and month they were interviewed.*

Participant	Position	Month 2021
P1	Senior Lecturer	March
P2	Senior Lecturer	March
P3	Senior Lecturer	April
P4	Senior Lecturer	April
P5	Professor	April
P6	Senior Lecturer	May

4.3.2 Documents

The documents were collected from the university's website (*see:* Medarbetarportalen, 2021). The documents collected were:

Table 2. *Documents for Secondary Data.*

Document Name	Retrieved	Description
Policy for IT security	15 March 2021	Overarching IT security policy
Regulations for IT security	15 March 2021	The IT security rules for everyone at the university
Policy for security work	15 March 2021	More general policy on university's security
Din Säkerhet	15 May 2021	Short employee guide for online and fire safety

They were used in the interviews to provide necessary information to the participants and make sure I know what the university's official ISP is. Additionally, the documents provided information about what the faculty members are expected to know and comply with.

The information security policy (ISP) in this thesis includes all rules and guidelines in the documents above. Such as, changing password every 6 months and not use Box for data which is confidential or containing personal details (Din Säkerhet, p. 2). Also, when employees use a cloud service they "must, before usage, consider the risks in relation to the information/material … based on GU's regulations for information classification." (Regulations for IT security, p.5).

4.3.3 Ethical considerations

Participants were asked questions about their knowledge about their employer's information security policy and what they think about their employer's ISP. This could have internal consequences for the individual participant. Therefore, all participants are anonymous.

Participants were kept anonymous by limiting the information about each individual. They are only referred to as participant 1, participant 2, etc. Furthermore, since the division they worked in had no significant effect on the findings, all information which could be linked to a specific division is also removed to further secure the anonymity of the individual.

4.4 Data Analysis

The interviews were transcribed continually shortly after they were conducted. The text was mindfully read to find quotes which highlighted the relevant subjects from each interview (Denscombe, 2014). Thematic analysis was used to sort the emergent themes. A thematic analysis helped find the general themes from the data and see how these themes were communicated by the participants. The selected quotes from the interviews were coded based

on the variables from the theories used in the conceptual framework from section three. These codes were then organized into relevant themes presented in the result section. An example of the coding is showed in Table 3.

Table 3. *Thematic analysis of interview data.*

Quotes	Codes	Themes
I'm not sure about the policy actually. (P4)	Denial of Responsibility (NT)	
We know very little about the policy and maybe it's not really our fault, in my opinion. (P5)	Condemn the Condemners (NT)	Lack of Knowledge
I wouldn't be fooled into, sort of stereotypical phishing emails and stuff like this. (P3)	Self-efficacy (PMT)	
But I can't say I'm technically knowledgeable. (P6)	Self-efficacy (PMT)	Employee Capability
I would kind of say that probably in terms of like a vulnerability, which is sort of an intensity of being targeted, it's probably somewhere medium to high, I would say. (P2)	Vulnerability (PMT)	
No, judging by this disaster with the emails it takes the University an incredibly long time to respond to any [IT disturbance]. They don't have the capacity. (P1)	Severity (PMT)	Consequences of a Cyberattack

4.5 Covid-19

The study was conducted in Gothenburg, Sweden during the spring of 2021 in the middle of the covid-19 pandemic. Sweden had at this time several restrictions in place and the university

recommended that all teaching and research to be done digitally. Due to this, the interviews were not considered to be done in any other way other than digitally. However, other criteria such as camera on during the interview were in place, see more above under, *interviews*. A few considerations were done due to covid-19 however none are considered to have affected the findings.

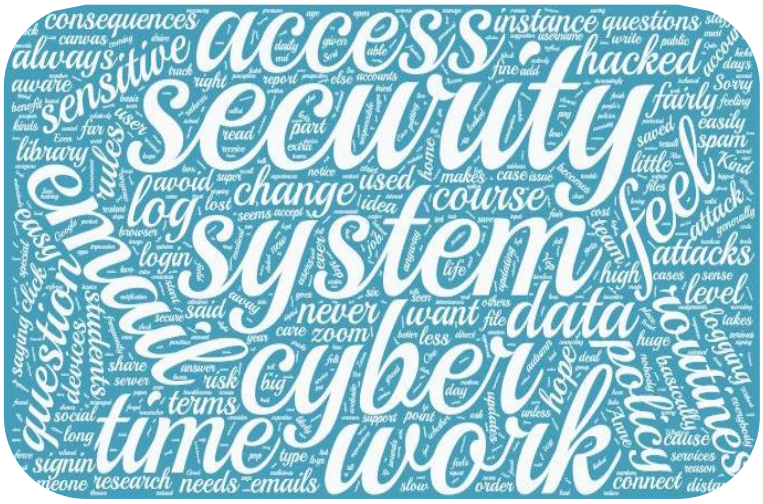
5 RESULTS

The results from the interviews are presented below under the themes found from the analysis. The interviews showed that there is a clear commitment and understanding that cybersecurity is important both professionally and personally.

> *The importance of keeping information that is personal, safe and so forth, is extremely important in the day and age that we live in where so much of what we do is digital in one form or another. (P3)*

An interesting finding is that most of the participants' reflections on ISP were similar with the lack of knowledge of the ISP being the most prevalent issue.

Figure 2. The most common words used in the interviews.



5.1 Consequences of Cyberattacks

All participants agreed that there is always a risk of the university being the victim of a cyberattack. However, some deemed it to be a lower or average risk, wondering why anyone would target a university, while others saw a higher risk and an increased interest in government agencies such as universities. Some shared similar opinions on the university's vulnerability and believed the risk to be medium to high, participant 4 pointed out that there is a growing understanding that government organizations, including universities, can be targeted and vulnerable to cyberattacks. The others saw the risk as average or low. The ones who believed in a lower risk tended to be more skeptical towards ISP in general and had more demands on it being invisible. The ones who believed in a higher vulnerability were more open to adding more security but did not show any further engagement in cybersecurity or any difference in

reflections other than more willingness to learn about the ISP. There was also the idea that there is not much to protect. With participant 1 wondering why anyone would target a university employee, seeing the risk as low. In the same spirit did participant 5 point out that often they were not handling anything sensitive.

When it comes to the consequences and severity of an attack, the belief in the university's capability to respond was low. Participant 6 pointed out that there is a general idea that the university would be slow to act and be very by the book, doing things in the right order and therefore having a less effective response. Overall, the participants were hesitant to respond and often they refer to in the IT incident which happened in September 2020. In some cases, this incident effected the participants' belief in the IT system at large. They argued that this incident showed the lack capacity from the university, where participant 5 wonders how the employees can be expected to know things when the university themselves does not, "*you have to know what you're doing and the university doesn't always know themselves"*. The employees suffered professional damage and it was also something which caused a lot of frustration and was met with a level of disbelief on how badly handled the whole situation was.

> *No, judging by this disaster with the emails it takes the University an incredibly long time to respond to any [IT disturbance]. They don't have the capacity; they don't have the strategic kind of thinking to deal with many of these issues. (P1)*

Additionally, they often mentioned their lack of technical knowledge on the area before answering, pointing out that they are not aware of the status of the university's IT infrastructure.

5.2 Defense & Role of the Employee

5.2.1 Effectiveness

Many express that they do not know, but they *hope* that the security systems and routines will work. They have more of a hands-off approach, most likely because of a general lack of knowledge of the ISP they choose to believe that the systems will be effective, even though there is an underlying lack of faith. Many no longer report spam email to the IT department because they get so many. Nevertheless, most participants praised the IT department for being competent and helpful.

Participant 1 and 3 points out that people have their passwords saved so some security systems which logs the person out, forcing them to log in again for added security, becomes useless since they just click log in again since the password is already filled in. Moreover, the main system they use logs them after about 10min of inactivation, participant 1 saying, "*like if your computer goes to sleep or whatever, then it logs you out again and then you have to type in everything all over again, which is super annoying"*. This shows the lack of thought put into the security system and leaves the employees wondering why the system is there. It disturbs their workflow and thus having systems which eats up their time and energy becomes a great cost. Participant 1 also noted that some security measures can decrease the effectiveness of the

overall security process, an example is being forced to have multiple login which results in people having their login credentials on a post-it next to their computer.

Furthermore, employees show that maybe not all of the policy is appreciated or something they agree with. Participant 6 stating, "*I mean, I think you have to know the policy, because maybe there are around three things which are important",* and participant 1 even more boldly saying, "*a lot of those are ridiculous. I wouldn't follow them anyway",* showing that the lack of effort by the university directly affect the faculty members' willingness to follow all of the ISP. This is also interesting because they are unfamiliar with the ISP but already have some doubt whether it is effective or not. In both quotes above there is however the space for a few good ISP, which they can agree with and hopefully then follow. Nevertheless, participant 6 says there might be three important ones and participant 1 says a lot are ridiculous, showing that the majority of ISP are seen as less useful and ineffective.

5.2.2 Employee Capability

The participants thought themselves to be fairly educated on the most common cyberthreats. Participant 4 stating, "*if I just say for myself, whether I have some competence, I would say yes".* However, the only cyberattack mentioned and which they elaborate on is phishing emails. In regard to these phishing emails did several participants express an expectation that they would, and should, not fall victim to them, because that it would be embarrassing.

> *I wouldn't be fooled into, sort of stereotypical phishing emails and stuff like this, but if it were to happen, of course it would be you sort of feel a bit foolish or disappointed to fall for of something like that. So, I think it would be the level of embarrassment. I suppose we all are supposed to be relatively tech savvy. (P3)*

Several participants freely listed the different protective behaviors they engage in. Often they also listed other protective behaviors which they do not engage in but is often talked about. Additionally, they also talk about some of the common cyberthreats and cybersecurity recommendations such as, avoiding suspicious websites, password recommendations, protecting your transaction data, be careful with what you download, the problems of having many different and international suppliers and not mixing your professional and personal devices and logins. However, it is also pointed out that they often do not comply with these, as many put it, common sense rules.

It was also brought up that the workload will affect the employees' possibility to learn new routines and programs, as participant 6 said, "*when you are overburden you don't have the energy learn new things"*. Since they already have a heavy workload, having to learn new security programs and routines will take away from their actual work. Therefore, the educational support they get, along with a helpful IT department, was much appreciated. But the barriers to contact IT support can sometimes be too high and the fact that they sit in a different location limits the possibility for IT to actually show the employee how to do something properly so they know it for next time. Because of this, a lot of time is spent on

employees trying to figure out the systems themselves, which may be less than ideal. Participant 2 capturing the problem, "*I assume all of those have been audited and are approved equally for storage. But, also, I don't know for sure."* Showing that the participants make assumptions of the systems and try to figure it out but they do not know what the best course of action is. The solutions the employees find may not be the correct and secure way. Furthermore, participant 6 brought up that technical problems during lecture will reduce time spent teaching students. Whenever they spend a lot of time trying to fix any IT problem it takes away time and energy from their primary tasks. Participant 6 confessing that, "*I can't say I'm technically knowledgeable"*, highlighting why employees having to figure things out IT problems for themselves is an issue, simply because the IT department is too far away, even though they are very helpful when contacted.

5.2.3 Moral of the Self and Others

The participants have clear differences in how they judge their actions. Most agreed that keeping their personal information safe was important and something they engaged actively in. When it comes to the workplace they believe they should follow the university's restrictions because they are in place for a reason. Some participants were more relaxed and not very bothered about the ISP, while others were more concerned and interested in finding out what the policy is and what they do not know. Most agreed that keeping track of updates and such is their own responsibility as long as the IT department support and remind them. Participant 6 believed that management should play a role and take responsibility to mention it and highlight the importance of these updates and security measures. Participant 3 on the other hand, pointed out that each individual need to take responsibility because they all have different needs and expectations on these systems.

Participant 4 did not focus much on the ISP or security in general instead they said, "*I think for me I focus more on my research and on my teaching"* showing that security is not a priority because that is not what they are hired to do. However, the participant further state, "*as an employee of the University, I think okay, if they have certain rules then as an employee I should probably follow it"* so even though they may not actively engage in the security work, they are willing to follow the ISP, as long as it is reasonable and does not stand in the way of their research and teaching.

Furthermore, cybersecurity is rarely, if ever, talked about at the workplace. It is not something mentioned by the management nor brought up by the employees. It could be mentioned if someone get a weird email or something have happened to someone. Nothing preventative. Nevertheless, there is a social culture surrounding shadow IT. Other programs and software which has not been approved by the university is used and since these sites are quite common and convenient, people who reflect on the safety of these sites does not speak up because they do not want to be annoying or cause problems in the group, especially if they are not the one leading the project.

It is the social aspect. You have to share certain things and then we do it in boxes, e.g. in, what's it called? Google docs. They say, now we're going to share! And I think, is that good? Because it is a private company you share with and it's interview data. (P5)

Participant 4 and 6 both say that they do not discuss cybersecurity at the workplace or in their work group. Participant 3, when reflecting on the social aspect, do not think that there is pressure from the group to behave securely but rather obvious to everyone that digital information needs to be handled seriously, further stating, "*it's important to all of us because we take it quite seriously and professionally".* There is a consensus that a dialogue about cybersecurity is lacking. The participants do not feel like it is their fault, but they also expressed little need for it and it was not something they were actively missing.

5.2.4 Lack of Knowledge of ISP

The lack of knowledge of the ISP was brought up several times during each interview. This is what the participants considered the biggest problem. Some pointed out they go with the easiest option, doing what they usually do or the same way they deal with a problem in private. It is also clear they feel that it is the university's responsibility to educate them if it is important, that this is not something which should be the employees' responsibility. As participant 5 put it, "*we know very little about the policy and maybe it's not really our fault, in my opinion".*

On the other hand, along with various GDPR pop-ups and license agreements, did participant 1 point out that at some point there was probably a screen with a lot of text, they just clicked accept and does not have any clue what was written there and what they have agreed to. Furthermore, the document *Din Säkerhet*, presents a short summary of the most important security policies the faculty members need to consider, which no one had read. Showing little engagement from the employees' side even though there are efforts being made from the university.

Participant 4, among others, clearly stated, "*I'm not sure about the policy actually",* not a single participant could mention one thing in the ISP, but some could guess or assumed certain rules were written. They do not know the ISP and expressed that they do not mean to break it if they do. But even so, they expect themselves to have the common sense to engage in a certain level of protective behavior. Also, even though they claim not to intentionally violate the ISP, they admit to engaging in unsafe behavior online.

Participant 5 called out for more information about the routines, the security systems and what they need to do for it to function. The reason being that they are unaware of what system exist and what to do in different situations. All participants agreed that there is a lack of knowledge and participant 2 developed on this explaining that even though they sometimes do the easiest thing, such as google drive or similar, they do not know if that is the best thing to do. There is little choice because they are unsure what the correct system and correct routines are. As participant 2 puts it, "*it's not written down in the big red letters with what you need to do",* showing that it needs to be very clear what they are supposed to do. A long, tedious text before

they can access their account is not the right way if they university want their employees to be aware of what the ISP is.

Furthermore, there is an understanding that the university does not take responsibility for the security capability among the employees but instead depend on them being intelligent about it. Participant 6 showing how the norm is relying on employees' common sense and the lack of engagement from the employee themselves, "*I mean no, I guess it's more that you use your common sense and don't think about the fact that there might be a policy"*. Thus, showing how the lack of knowledge stems from both the employee and the employer.

5.3 IT Security Systems & Rules

5.3.1 Ease of Use

A majority of the participants expressed that there are several systems which are time-consuming, inefficient or bulky. Participant 3 are here describing two of the systems the faculty members have to use, "*the programs is awfully clunky and seems very archaic and not very functional, so those two systems come to mind"*. Participant 2 pointed out that some systems cause quite a disturbance when used and that they therefore avoid those systems. There was also a difference in how much this bothered the participants, with some being very disturbed and others not being able to really think of any system which bothers them. However, all participants agreed that the systems are easy to use and see no real trouble managing any security related task. So, the problem is not that it is difficult, but rather that it is inefficient and can be in the way of the faculty members doing their work by taking up time and performance.

The participants were also willing to sacrifice a certain level of convenience for more security if they understood why it was necessary and depended a lot on what they are protecting. However, if a system is significantly reducing the performance of their devices then the reflection is that they will not use the system unless it is necessary, regardless of the safety benefits. Both participant 1 and 4 state that they only use certain security systems in order to access resources. Thereof, not using it in other situations in order to keep the university and sensitive data safe.

Furthermore, the participants did not really see any benefits of not using the IT security systems, they pointed out some flaws of the systems and how it can be improved but were overall satisfied with their interaction with the systems. Showing that having easy to use systems is beneficial to make the system blend in and become invisible.

5.3.2 Signs of breaking or violating the ISP

All participants talked about ways they break the ISP, either by not using the recommended systems, using their own devices, using external software for e.g., storage, using their professional email for personal business or by not changing their password every six to eight months. However, as discussed above, none of them knew what the ISP contains. Some stating if they knew they would follow it, while others were more skeptical. An example of this being

that the ISP does specifically say that GU Box should not be used for confidential data (*Din Säkerhet)* but several participants view GU Box as the place to share that kind of information. Showing a large inconsistency of storage. The participants often mentioned storage as a big problem, either in terms of violating the ISP or by not knowing how to approach that problem. Participant 6 said that they store data from research interviews on their computer and use dropbox even though they are aware that management does not want them to use dropbox. Participant 6 says that they are supposed to use GU Box instead for the sensitive data. Something which is mentioned by several other participants as well.

> *You might not always be so aware about the risks. If you think in terms of shadow IT, that maybe you sometimes want to use different software to make your work easier, like transcribing and things like that, and maybe you then try to download something without really thinking of the consequences. (P6)*

Many have used their email for private purposes, they use google drive to collaborate, dropbox for storage, other external software for transcribing, download software without really making sure it is completely safe and connecting their professional devices towards unprotected networks such as a public network at a café. As one can see, there are no great transgressions of the policy, the faculty members seem to use their professional devices in a similar fashion as their private ones, with small variations. It is not clear if they are more careful and mindful of cyberthreats with their private devices or their professional ones. They avoid mixing their personal and professional errands on the devices, however, they all explained that cybersecurity is important to them generally in life. They use similar security practices in professional settings as they do in private settings, showing that habit place a large part in how they approach security. Additionally, many participants bring with them security habits from previous workplaces, where ISP have been stricter and better communicated.

5.3.3 Formal Sanctions

No participant had any knowledge about formal sanctions from the university in cases where employees violated the ISP. Participant 3 mentioning, "*without having tried to break it, it's not something that I worry too much about"*. The formal sanctions from the university is not something which worry the participants, even though they do not know what they are.

The participants did however have opinions on what they thought the sanctions and the procedure following a possible violation should be. Suggestions from the participants stemmed from the assumption that the violation was not ill-intended, so they advocated having an educational approach to help people do the right thing before using sanctions.

> *For the first instance [of violation] they would sort of take an educational approach and then if it was clear that somebody was being, yeah not taking their job seriously, even after a warning and a support, then things might be more serious. (P3)*

Also, making sure that the ISP are not too strict so you set up barriers for the faculty members to do their job. Participant 1 explaining, "*If you try to enforce ISP too tightly, you actually*

prevent people from doing their work and the tendency would then be for people just not to do their work."

There was a significant number of participants who asked about the formal sanctions when asked about the consequences of violating the policy, showing that there is an interest in how the university handles a violation.

6 DISCUSSION

The discussion section aim answer the research question: *How do faculty members reflect on university information security policy?* Finding that faculty members rarely reflect on their protection behavior, they were unaware what the ISP was and they believed the university's vulnerability is medium to high. To justify their violations of ISP and maladaptive behavior they used e.g., denial of responsibility and metaphor of the ledger. Furthermore, formal sanctions seem to play a small role on determining compliance. Thus, showing there is a width to the faculty members' reflections and even though they have limited knowledge of both IT and the ISP, they still express valuable reflections which are important to understanding employee compliance.

6.1 Protection Motivation Theory

6.1.1 Perceived vulnerability

The participants expressed an overall understanding of the threat the university faces. The perceived vulnerability makes the participant expect a certain degree of ISP and also expressed the possibility for more security, due to the risk the university face and the lack of engagement from the university. However, since the faculty have not engaged in learning the ISP, reading the information available, it does not seem like the perceived vulnerability motivates them to comply with ISP. This finding supports the findings from Vance et al. (2012) that perceived vulnerability did not have a significant effect on intention to comply with ISP. The perceived vulnerability does however increase the motivation to learn the ISP and try to understand what they should do. Thus, showing that perceived vulnerability might still be a relevant factor in employee compliance, even though it is not directly related to the intention to engage in protective behavior.

6.1.2 Perceived Severity

The participants often referred to lack of knowledge of the technicality of the IT systems. However, the problem is the lack of knowledge of the possible attacks and the consequences of those attacks, not their technical knowledge of how the cybersecurity systems work.

Many referred to the big email debacle the previous year which damaged their faith in the IT capability of the university. Thus, increasing the perceived severity because members of the faculty now believe that the impact of a cyberattack would be higher than before the email debacle. However, no one seem to have previously reflected on the fact that poor management of the email incident could mean poor management in the case of a cyberattack and that they as employees should therefore help prevent that from happening. Thereof, showing that experiences of low capability from the university in IT areas other than cybersecurity did not

affect their reflections on their protective behavior. Ifinedo (2012) also found that perceived severity did not affect intention to comply with ISP and this could help to better understand his findings.

6.1.3 Rewards

The rewards of not complying with ISP should reduce the perceived vulnerability and severity of the threats. The reason no real benefit was noted by the participants can be explained by the ease of use of the systems and also that there are not that many security systems. Furthermore, the fact that the systems are mandatory can make the system more invisible, it becomes an unavoidable "truth". Since there is no other way to enter the system other than entering your password and the system logs you out after 10 minutes of inactivity, they just comply. In the beginning it might be annoying, when asked to reflect upon it their attention might once again be brought to it. But during a regular workday, it is not something which they reflect on or which bothers them.

Nevertheless, participant admitted to not using systems which reduced the performance or cause a disturbance. Showing that there is a reward in engaging in the maladaptive behavior, not using these systems. Furthermore, participants mixed their professional and personal email for both work-related and private errands. This study cannot say anything on how rewards may affect perceived vulnerability and severity. However, there are clear rewards in engaging in maladaptive behavior, thus giving a possible explanation why, despite seeing the university's vulnerability and the severity a cyberattack can have, the participants do not reflect more on their protective behavior or have increase motivation to comply with ISP.

6.1.4 Self-efficacy

Self-efficacy is the belief in oneself that you can perform all the tasks necessary to follow the ISP. The participants had quite high self-efficacy, seeing themselves as quite capable to both handle the task necessary to complete a security response and also, avoid a possible cyberthreat. The belief of their ability to avoid a possible cyberthreat could stem from the high computer literacy (D'arcy, 2005). The high self-efficacy was even though they did not know the ISP or had gotten any guidance from the university. Therefore, the belief of their cybersecurity capability comes from other sources. However, since they see themselves as fairly computer-savvy, the confidence from other digital areas might result in their high self-efficacy concerning cybersecurity as well. Moreover, since only one form of cyberattack was mentioned, phishing emails, the lack of consideration for other forms of attack and the understanding of what these attacks entail may result in a higher self-efficacy.

Due to feeling overburden by work, the self-efficacy regarding learning new things might be lower. Here, it shows that low self-efficacy might decrease the engagement in protective behavior, such as feeling they can take the time to learn the ISP and doing that would be meaningful. Furthermore, they expressed that common sense is what is expected and the norm. It is likely that since they do not know the ISP they instead their so-called common sense. Common sense seems to be their general knowledge about protective behavior and habits from

personal usage and previous workplaces. Additionally, the lack of discussion about cybersecurity at the university is interpreted by the participants as leaving it up to the faculty members to use their general knowledge of online security to keep themselves and the data safe.

A higher self-efficacy should result in an increased coping appraisal (Floyd et al., 2000). The reflections about their self-efficacy showed reflections about engaging in protective behavior and an awareness of various protective behavior such as avoiding suspicious websites and emails. Therefore, indicating that self-efficacy might play a role in overall employee compliance.

6.1.5 Response efficacy

The response efficacy is the belief that if you follow the security systems and routines, this will be effective in protecting the organization and yourself. The results showed that employees have a low belief in that their behavior will make a significant change in protecting the university. This is expected since the university does not engage the faculty making sure they know the ISP and understand the security environment the university exist in. Raising the response efficacy could be necessary if other IT security routines are implemented or if the university wants to increase the usage of security systems which are not mandatory.

Furthermore, the reflections about the university's capability did seem to affect the faculty members' reflections about the importance of following the ISP. Along with if the ISP seemed necessary and actually protected something the faculty members believed to be worth protecting. There were also reflections on response efficacy where the participants seemed to be more willing to endure a more annoying security process if there is high response efficacy.

Vance et al. (2012) found that response efficacy had the negative effect on intention to comply. Meanwhile, Warkentin et al. (2016) found that response efficacy did not correlate to intention to continuation of protective behavior. So, one explanation for the inconsistent findings could be that response efficacy can increase the acceptance of security system, even though it is annoying, but not increase the intention to comply. However, if response efficacy is paired with a high usefulness of the system, perhaps this could affect intentions to comply as well.

6.1.6 Response cost

Response cost is anything which makes it more difficult or inconvenient for the faculty members to follow the ISP. The findings showed that there are several security systems which the participants find to be unnecessary and time-consuming. These systems raise the response cost and decreases the likelihood of continued use. However, since several systems are mandatory and difficult to work around they are used anyway. The participants did not indicate that the response costs affect their decision to follow the ISP but rather the necessity of the system. Therefore, the lack of knowledge of ISP and cyberthreat becomes an issue since the faculty members do not fully understand the importance of the IT security systems.

Posey et al. (2015) pointed out that some protective behaviors require more effort than others to perform, which can be one explanation why some of these systems are seen as more in the way than others. Logging in and out is not seen as overly annoying, probably because it requires little effort from the employee, it is just a mild nuisance.

Overall, the participants do not reflect on cybersecurity a lot, but rather use the basic knowledge they have and use the systems they have to in order to complete a task. When asked to reflect on security, all think it is important and something worth looking into and even increase. However, there is a fear of awkwardly installed programs which will increase their workload and take up too much of their time. Nevertheless, the willingness to engage is there as well as the basic understanding of how important cybersecurity is.

6.2 Neutralization Theory

6.2.1 Denial of Responsibility

The lack of knowledge was the most common explanation for lack of an answer and explanation for why they do not follow the ISP. The lack of knowledge was used as an explanation for any violation of the ISP, why they were unable to answer what possible risk the university could be facing and what the consequences of a possible cyberattack could be. Denying any responsibility makes it easier for the member of faculty to justify their ignorance and lack of knowledge of the ISP. Posey et al. (2015) explained that each employee has the choice of whether or not to actively engage in protecting the information they have access to. Denial of responsibility enables the faculty members to choose to not actively engage in protecting the information and instead leave that responsibility to someone else.

6.2.2 Denial of Injury

The perceived vulnerability of the university was by some seen as average. Not all shared this opinion, instead viewing the vulnerability as high. Nevertheless, the ones rating the perceived vulnerability as low might be using denial of injury to help justify their possible violation of ISP or engagement in maladaptive behavior. By downplaying the risks, they also lower their perceived risk of their behavior causing damage to the university. Furthermore, by saying that there might not be any information worth protecting or wondering why anyone would target a university, they also deny the injury of their maladaptive behavior.

6.2.3 Defense of Necessity

There is little in the result showing that defense of necessity is a justification technique used by the participants. No participant raised a situation where they felt the need to violate the security system in order to get something done or due to a moral dilemma. Therefore, the participants raise that there is little cybersecurity in place and that more could be done. Perhaps because there are so few systems and they are all fairly easy to use, there are few situations which present a moral dilemma. Also, because a lot of the systems are mandatory and difficult to work around, few dilemmas occur.

However, the bulkiness and inefficiency of some of the university systems can justify not using them. It becomes necessary for the faculty members to use other sharing platforms which are not approved by management. It could be seen as unreasonable or too inefficient to use the university's software and all security programs. Therefore, putting the faculty members in the moral dilemma of either doing their work easy and efficiently or spend a lot of time handling bulky systems.

6.2.4 Condemn the Condemners

P1 "*a lot of those are ridiculous. I wouldn't follow them anyway*". Siponen and Vance (2010) gave an example of condemn the condemners as breaking the rule because it is unreasonable, which is exactly what participant 1 is saying, thus, justifying breaking part of the ISP. There were a significant number of participants who questioned part of the ISP, even if they did not know it. However, some expressed that they have a responsibility to follow the ISP. Showing clearly there are varied used of the neutralization techniques. There are those who justify their actions through condemnation and those who does not, instead they see it as their responsibility to follow all rules even though they might be ridiculous in someone else's eyes.

6.2.5 Appeal to higher loyalties

Appeals to higher loyalties was used when the participants choose to use external software for sensitive information sharing by saying they were not the project leader and there was a social factor to using those services. This is a way to justify the usage of these external websites which, when asked about it, they are unsure about using due to security reasons. This shows that some of the protection behavior trickles down, making it more important that management and people in leadership positions understand the importance of using secure sharing platforms. Furthermore, the participants express that as an employee it is their responsibility to follow the ISP and the rules the university sets. This again is an appeal to higher loyalties but instead justifying why they might use inefficient or awkward systems. Thus, concluding that appeal to higher loyalties does occur in the participants reflection and is a relevant aspect when trying to understand employee compliance.

6.2.6 Metaphor of the Ledger

The participant listed all the protective behaviors they engage in, they also listed other protective behaviors whether they engaged in them or not. This could be explained by the metaphor of the ledger. By listing situations where they engage in protective behavior could be interpreted as them trying to justify all the times they violate the ISP or engage in maladaptive behavior. Furthermore, by listing other protective behavior, showing that they know of them, can also be an indication of a way to justify their violations. They violate the ISP because they do know a lot of protective behaviors and just knowing these behaviors can count as an action in favor or protecting the university. The conclusion being that the faculty members count their knowledge as a good act compensating for the violations.

The participants show that their reflection coincide with the justification techniques presented in neutralization theory. No participant showed any evidence that they used all justification

techniques. Therefore, the techniques might be applied differently by each individual. Furthermore, each individual has different moral dilemmas and face unique situations, thus presenting a varied need for each of the techniques.

6.3 Deterrence Theory

6.3.1 Formal Sanctions

Formal sanctions are any sanctions from the university. These are supposed to be certain, swift and severe if they are to be efficient (Gibbs, 1968). The main issue here being, no participant had any knowledge about any formal sanctions and they did not have any reflections about what the certainty, swiftness and severity could be. The results showed that the participants do not want strict punishments but they were encouraging a system which helps them understand and better follow the current ISP. Therefore, if a deterrence system is in place, having an educational approach could be greatly appreciated by the faculty members. The participants did not believe that people were breaking the ISP will ill-intentions but rather out of ignorance. Showing good faith in their fellow faculty members. Therefore, the perceived vulnerability to internal threat might affect the reflections about the formal sanctions. If there is no perceived internal threat, the faculty member might feel there is little justification to have certain, strict and severe punishments.

6.3.2 Informal Sanctions

The self-approval played a substantial role for the participants in their reflection to comply with the ISP. However, based on the results even though some participants had higher expectations on themselves and were more committed to learning the ISP, there was no difference in knowledge about the ISP nor any difference on their perception of usage of voluntary security systems. Therefore, just because someone feels it is more important did not seem to affect their perception of other aspect of cybersecurity, such as vulnerability or severity. The only difference was a more of a willingness and openness to learn the ISP in order to follow it. The others were also willing to learn and follow the ISP. However, several were still more critical and required more thought and purpose behind it and would not willingly sacrifice their time and convenience just because someone said so. This could mean that if other security measures are implemented, possible critique should not be seen as an unwillingness or resistance to the change but rather as a lack of communication of the necessity of the change or, possibly, as a critique on the effectiveness and necessity of the change.

Furthermore, social approval was believed to directly affect the participants ability to speak up against ISP violation, such as using external sharing services. Thus, indicating that social approval does not necessarily increase employees' intention to comply but it depends on the social norms at that workplace. Therefore, managing the social culture and actively engaging the faculty members becomes important to foster an environment where it is easy to follow the ISP.

Additionally, there is no security culture at the university. It is barely talked about and could be one reason why there is little knowledge and no one feels any real pressure to follow the ISP or know it. But interestingly, Paternoster and Simpson (1996) introduced shame as factor in DT and shame would be a good explanation for the statements about why the faculty members would feel "foolish" if they fell for a phishing email. Thus, providing motivation to be aware of phishing emails, because the shame if they were to fall victim of a phishing email is deterring enough.

7 CONCLUSION

The purpose of this thesis was to bring more understanding to employee compliance by researching how faculty members reflect on university information security policy. To answer the question the theories protection motivation theory (PMT), deterrence theory (DT) and neutralization theory (NT) were used to help explain and give a deeper understanding on why faculty members reflect the way they do and how this can be interpreted. The results show that the university faculty members lack knowledge of the information security policy (ISP), they know information security is important and engage in an ad hoc collection of protective behaviors. However, they also admit engaging in behavior they know can put the university at risk, even though most view the university's vulnerability to be average to high and expect the severity of a possible cyberattack to be high. Furthermore, they did not have any reflections on formal sanctions as they were unaware if there were any. Nevertheless, the informal sanctions provided interesting insight with social approval being something the faculty members deemed relevant in whether or not they violate the ISP. Neutralization techniques such as denial of responsibility and condemnation was used to undermine the consequences of their actions and justify why they violate the ISP. Therefore, PMT, DT and NT were effective in deepening the understanding of how the faculty members reflect on university information security policy.

7.1 Practical Implications

Security Education, Training and Awareness (SETA) is needed at the university. It highlights the importance of following the ISP and bring understanding of the threat the university is facing. This does not need to be a large investment but just having a more interactive and easily digested ISP could help, such as a workshop or short presentation. However, SETA does not automatically result in compliance with ISP, but it can increase the success rate of the cybersecurity process. Also, engaging each department and not putting the responsibility on the faculty members, unintentionally relying on their common sense, habits and computer knowledge in regard to cybersecurity .

The thesis shows that having ISP which are not too complicated, is mandatory to complete certain tasks and serves a purpose, are the ones faculty accept the most and does not mind following. This can be implemented by the university to instead have an ISP which they work actively with rather than one passively sitting on their webpage because they have to have one. Engaging the faculty members to increase security and ensure the safety of university resources.

7.2 Future Research

Suggestions for future research is deterrence theory's variable virtual status, which means how much of the work is done away from the central workplace. Because of Covid-19 more of the work is done at home, if not all of it, including meetings and lectures. Therefore, it would be interesting to see how this have affected the overall understanding of deterrence theory and efficiency of sanctions.

Conducting research where the theories PMT, DT and NT are combined in order to better explain employee compliance overall can be meaningful and would be the next step to see how well these theories work together to help understand employee compliance.

Reflections from other settings, such as other departments, other government agencies and also private organizations, and from other positions is needed to expand the understanding of how employees reflect on ISP. Complementing this study, would be investigating the reflections of the employees at the IT department at University of Gothenburg. Thus, enabling a comparison between the faculty members and members of the IT department. Lastly, research connecting employee reflections to employee compliance can be interesting and help connect the different fields of research within employee compliance research to bring a deeper understanding and help find important factors in how to translate employee reflections into employee compliance.

7.3 Limitations

The study's generalizability is limited to a university setting. Furthermore, can the other reflections and a more complete view of faculty members' reflection be achieved if interviews were not only conducted with full-time employees. Interviews can be time-consuming and complementing with a survey, gathering data from more departments and participants would increase the generalizability within the university. Moreover, the scope is limited to how the reflections of the faculty members can be explained by PMT, DT and NT and will not investigate how these theories relates to the actual intention to engage in protective behaviors. Other conclusions and insights could be reached if other theories were used to analyze the data.

8 REFERENCES

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, 613-643.

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security*.

Beccaria, C. (1963). On crimes and punishments (H. Paolucci, Trans.). *Indianapolis, IN: Bobbs-Merrill.(Original work published 1764)*.

Bell, E., Bryman, A., & Harley, B. (2018). *Business research methods*. Oxford university press.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Byers, B., Crider, B. W., & Biggers, G. K. (1999). Bias crime motivation: A study of hate crime and offender neutralization techniques used against the Amish. *Journal of Contemporary Criminal Justice*, *15*(1), 78-96.

Cheng, L., Li, W., Zhai, Q., and Smyth, R. 2014. "Understanding Personal Use of the Internet at Work: An Integrated Model of Neutralization Techniques and General Deterrence Theory," Computers in Human Behavior (38), pp. 220-228.

Cisco (n.d.). What Are the Most Common Cyber Attacks?. Cisco. Retrieved 15 May 2021 from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work

Cole, E. (2015), Insider Threats and the Need for Fast and Directed Response, SANS Institute.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

D'arcy, J. P. (2005). *Security countermeasures and their impact on information systems misuse: A deterrence perspective*. Temple University.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

Denscombe, M. (2014). *The good research guide: for small-scale social research projects*. McGraw-Hill Education (UK).

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

FBI Flash (2021, March 16). *Increase in PYSA Ransomware Targeting Education Institutions.* Federal Bureau of Investigation (FBI), Cyber Division. https://www.ic3.gov/Media/News/2021/210316.pdf

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly*, 515-530.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, *30*(2), 220-269.

Göteborgs Universitet (2020, October 14). *Serverkraschen orsakar fortfarande problem.* https://www.gu.se/nyheter/serverkraschen-orsakar-fortfarande-problem

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Holmberg Karlsson, M. (2017, July 24). *Skandalen växer kring Transportstyrelsen: Detta vet vi*. Göteborgs-Posten. http://www.gp.se/1.4472760

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework. *MIS quarterly*, *39*(1), 113-134.

Kinnunen, S. (2016). Exploring determinants of different information security behaviors.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. European Journal of Information Systems, 26(6), 546-563.Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), 1-8.

Marakas, G., Johnson, R., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, *8*(1), 2.

Matza, D., & Sykes, G. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664-670.

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of research in crime and delinquency*, *18*(2), 295-318.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1).

Moore, S. (2017, May 17). *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021*. Gartner. Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting health behaviour*, *81*, 126. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549-583.

Piquero, A. R., Paternoster, R., Pogarsky, G., & Loughran, T. (2011). Elaborating the individual difference component in deterrence theory. *Annual Review of Law and Social Science*, *7*, 335-360.

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice quarterly*, *13*(3), 481-510.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime.

Pogarsky, G., & Piquero, A. R. (2004). Studying the reach of deterrence: Can deterrence theory help explain police misconduct?. *Journal of criminal justice*, *32*(4), 371-386.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2017). The empirical status of deterrence theory: A meta-analysis. In *Taking stock* (pp. 367-395). Routledge.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Rogers, J. W., & Buffalo, M. D. (1974). Neutralization techniques: toward a simplified measurement scale. *Pacific Sociological Review*, *17*(3), 313-331.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management, 54(8), 1023-1037.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Tittle, C. R. (1980). Sanctions and social deviance: The question of deterrence.

TT (2019, March 4). *Datainspektionen granskar efter 1177-skandal.* Göteborgs-Posten. http://www.gp.se/1.13816064

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, *23*(3), 191-198.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25-35.

Warkentin, M., Malimage, N., & Malimage, K. (2012, December). Impact of protection motivation and deterrence on is security policy compliance: a multi-cultural view. In Pre-ICIS Workshop on Information Security and Privacy (SIGSEC).

Wiesenfeld, B. M., Raghuram, S., & Garud, R. (1999). Communication patterns as determinants of organizational identification in a virtual organization. *Organization science*, *10*(6), 777-790.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*, 545-572.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly, 1-20.

Yin, R. K. (2011). Applications of case study research. sage.

9 APPENDIX

9.1 Interview Guide

These are the questions used during the interviews. The questions were asked in an ad hoc manner so the order below is not related to how they were asked during the interviews. Due to the interviews being semi-structured, all questions were not asked to all participants . Furthermore, other follow-up questions, not listed here, were asked when appropriate.

- Do you know about the university's cybersecurity policy?
- What are your thoughts on the university's cybersecurity policy and routines?
- When working on distance do you use Cisco VPN AnyConnect?
- Do you have access to sensitive, confidential, or personal data?
- Do you use your own computer or one from GU?
- Have you experience any hacking attempt?
- Would you be willing to sacrifice convenience for guaranteed security?
- Any security system which is annoying?
- Do you think it is important in your role as a researcher, teacher, and employee to follow the cybersecurity policy?
- Are there situations where you believe it is justified not to follow the cybersecurity policy?
- Do you think it is necessary to follow all cybersecurity routines or is it enough to just follow some?
- Is it okay to break the cybersecurity rules if you feel it was necessary?
- Is it okay to break the cybersecurity rules if it is preventing you to get your job done?
- Is cybersecurity important to you in generally in life?
- What is the security culture like in your work group?
- Do you think the consequences from the university of breaking the cybersecurity routines are severe and just?
    - *Changed to*: do you know of any consequences from the university if you violate the cybersecurity policy?

- Is it likely to get caught breaking the security policy?
- Is the university quick to notice someone breaking the security policy?
- Do you have the technical know-how and all necessary information to follow the ISP?
- Do you feel like you have to technical know-how to avoid cyberthreats more efficiently than others?
- Does the university care about security?
- What are your thoughts on the usefulness of the university's cybersecurity systems and routines against cyberattacks?
- Do you feel that the cybersecurity systems and routines easy to use?
- How often do you use or come across security systems in a day? Like entering your password etc.
- If a system needs updating is that something you can do or is it IT support's responsibility to keep track of it?
- What are the benefits of not using the security systems? Social, time, efficiency?
- What are the costs of not using it?
- If the university were attacked, do you think it would be easily resolved?
- What do you think is the risk of the university being the victim of a cyberattacks?
- Are the security routines enough to reduce the cyberthreats the university are facing?
- How do you respond to a cybersecurity threat?