UNIVERSITY OF GOTHENBURG

# Backup whenever you're worried

## A study of data-backup practices in an academic environment

**Martin Lundgren**

**Bachelor of Science Thesis**

**Report No. 2012:028**
**ISSN: 1651-4769**

University of Gothenburg
Department of Applied Information Technology
Gothenburg, Sweden, May 2012

**Problem** Data backup is one of many security related topics, and has been the target for many researches as to improve different techniques. However, studies have shown that backup is not a natural behavior for many, and some neglect its importance completely. Some argue that security can only be improved completely if an understanding of what cultural acceptance toward security is as well as what practices is being accepted and used. This paper aims not to improve the culture towards security, but rather to explore the practices and cultural compliance regarding data backup among employees and students at a university.

**Method** A case study was made at an institution of a university. The study consisted of a quantitative study (survey) as well as a qualitative (interview). The survey was designed to extract the practices and cultural compliance to be expressed in a descriptive statistical fashion. The interview was designed as open and was analyzed using a phenomenological approach.

**Findings** The study shows that the respondents recognized themselves mainly at a level of; *Culture*, *Commitment* and *Apathy*. Meaning that the participants performed security related routines as part of, or close to, their natural behavior (*Culture* and *Commitment*), or were unmotivated to proceed with good praxis (*Apathy*). None of the participants recognized themselves at the disobedience level. The overall backup devices used were external hard disks and the use of online backup, dropbox. None of the participants used CD, DVD or Blue-Ray to backup their data. Nearly none of the participants used the universities servers as backup service. It was found that most backups were not protected in any way. The overall respondents found backup to be of importance and none considered it to be of no importance. Most difficult or least motivating among the participants in keeping regular backup was to remember doing so. It was also found that the most common regularity for both students and employees was to backup their data only whenever they felt worried for some particular file and folders.

**Keywords:** Backup practices, Cultural compliance, Academic environment

"*Here we need to remember that what in the end turns out to be feasible will itself be affected by the learning generated by the project itself: human situations are never static*"

(Checkland and Scholes, 1990 see Jackson, 2003, p. 181)

# INDEX

# 1. INTRODUCTION

## 1.1 BACKGROUND

Data backup has been the subject of a significant number of researches, which in turn has led to a lot of solutions (Anderson & Zhang, 2010). However, studies have shown that backup is not a natural behavior for many, and some neglect its importance completely. In a study made by the Ponemon Institute (2008), involving 864 business travelers, showed that there were as much as 42% who did not perform any backup. Consequently we use and trust technical devices to store our information for both personal and job related information. Whether it concerns text reading, editing, movies, music or whatever crosses our mind and interests. This might be more of a concern than you think, as these devices storing our information are technical, which in turn can break, get stolen or defected in some other way. Data on any hard disk drive (HDD) is by its nature able to be overwritten, deleted or lost due to a number of reasons such as power failure, software bugs, viruses or by natural causes such as physical damage; fire or water or simply by human mistakes (Oteng-boateng, 2011). All of these examples may feel a bit off or maybe far from happening you, but consider that 10% of all laptops get lost or stolen during their lifetime (Seagate, 2010), and about 12,000 laptops per week get lost or stolen in U.S airports (Ponemon Institute, 2008). But even if your computer doesn't get stolen, there might be technical faults causing data loss as well. Note that "*in the worst case, latent sector errors affect up to 20% of the disks in 2 years*" (Bairavasudaram, 2008, p. 20), meaning that a block, or a set of blocks in your hard-disk gets corrupt and inaccessible, hence "*a single system cannot be depended upon to reliably store data*" (Bairavasudaram, 2008, p. 20). – As a personal question, how much data on your hard disk is considered important; how much of it can be redone, reproduced… how often do you backup your data?

Even though there is a definite risk of data loss we find that in the most of cases backup routines are not a natural part of our behavior and whenever we do backup our data, the methods we use tends to be rather ad-hoc; for example, manually copying data onto a USB-thumb drive or likewise (Anderson & Zhang, 2010). But no technical solutions will ever really suffice if the user does not accept its practice or importance. According to Leeden (2010), this issue needs to be considered in a non-technical aspect. Not to raise the users awareness to specialism, but rather to introduce and guide the user to accept and master its practices. Furnell and Thomson (2009) agrees with this and states that one must first explore what cultural acceptance/compliance toward security is, as well as accepted practices, before any security can be improved.

## 1.2 PROBLEM DESCRIPTION

Anderson and Zhang (2010) stress the risk of data loss if no backup is performed. However, it is understood by some that security is not only about good technical solutions, but rather the understanding and compliance among the end-users how to protect themselves (Leeden, 2010). Thus both practices and level of security compliance among users are important to pitch the level of security in an organization (Furnell & Thomson, 2009). This study aims to explore the practices and levels of compliance among employees and students at a university. Note however that it is not my intention to recommend or improve any security, but rather to provide an insight of practices an acceptance. This led to the very question of this thesis;

- What backup practices and levels of cultural compliance can be found in an academic environment?

## 1.3 SCOPE AND LIMITATION

The subject of backup was chosen as I believe nearly everyone, at least among the target population, are familiar with it and its concept. Therefore a study concerning backup seemed as a good start in researching security related issues. This study focuses thus only at backup practices, and how participants recognize themselves at cultural compliance. Cultural behavior can, however, be a wide subject but is in this study limited to what Furnell and Thomson (2009) describe to be eight security related behaviors; *culture, commitment, obedience, awareness, ignorance, apathy, resistance* and *disobedience*. I will stress the fact that I do not intend to go into details about culture at an organizational level, nor will I investigate how the culture applies or came to be, but rather to present how participants recognized themselves at the given levels of security culture. The motivation for this was that a complete research towards the subject of organizational culture is all too wide and what I recon would carve a significant qualitative and quantitative study. However, this was not the purpose of this study. This study focuses on personal practice and compliance. The study took place at an IT inspired institution of a university, which I thought would be interesting to investigate as I expected their knowledge of the matter to be fairly high. The limitation of the target population was due to two factors, one; accessibility, as I had access to the buildings and were thus able to meet up with the employees and students in person, as well as the IT-manager for an interview. The second reason was the limit of time. This study could apply for the whole university to expand the results and understanding. However it was the reason of limited time that the focus addressed this particular population. Thus the scope of this paper was to investigate what practices and cultural compliance towards security could be found in an academic environment.

## 1.4 DISPOSITION

Chapter two will discuss the theoretical aspect of the subject, the risks and how to determine security compliance. Chapter three will explain the methods of data gathering and what techniques were used to analyze and present the data. In chapter four the empirical study will be presented in the manner described in the previous chapter. Chapter five is dedicated for a discussion concerning the result, the theory from chapter two and related work, which will lead us to chapter six, where a conclusion regarding the problem description from chapter one will be drawn and propose further extensions.

# 2. THEORY

## 2.1 BACKUP METHODS

Many of the backup solutions used today is according Anderson and Zhang (2010) rather ad-hoc and does often require external device such as 1) a USB thumb drive, writable CD or DVDs, 2) external hard drives or 3) thou rarely used, cloud-based backup (Lenovo-AMD, 2010). According to Anderson and Zhang (2010) new modes of working has put an even greater challenge to uphold good backup, and that existing techniques does not really suffice. They argue that many individuals and organizations have partial or full ad-hoc solutions for backing up data, which in turn can put data at some potential risks, such as:

| Common Backup Risks |
| --- |
| • Backups are often made to a local disk and copies are not stored offsite.<br>• Backups are not encrypted and vulnerable to theft.<br>• Personal (rather than corporate) information is accidentally stored in plaintext on a corporate service where it can be read by other employees.<br>• Backups often just include "user files" in the assumption that "system files" can be easily recovered from elsewhere.<br>• The inconvenience of making backups leads to infrequent and irregular scheduling |

**Table 1 Common Backup Risks (Anderson & Zhang, 2010, p. 1)**

### 2.1.1 LOCAL COPIES

Local backup, such as USB thumb drive, writable CD or DVDs and external hard drives etc. is according to a survey made by Lenovo-AMD (2010), the most common method of backing up data. Devises such as these, including your computers' internal hard disk, might seem secure enough as backup device, and there are quite many recent methods of backing up data locally and automatically. One example is Apple's "Time Machine", which use a technique to backup the data and recover it to any given point (Hoff, 2008). However it, like many other applications which craves a local device to backup data, suffers from the two first problems stated above (Anderson & Zhang, 2010). This can be an issue if 1) the data is sensible and not to be seen by unauthorized persons, 2) as the data is stored locally, there is still the risk of data loss made by any of the fourteen following reasons:

| The 14 most common causes linked to the loss of data | |
| --- | --- |
| • Hard disk drive failure<br>• Component failure (a telltale sign of this is strange noises such as clicking and buzzing emanating from the device).<br>• Electrical failure such as drive not spinning or starting up<br>• Accidental or intentional reformatting or overwriting of disks and partitions<br>• Corrupt or missing critical file system structures and files<br>• Inaccessible drive partitions<br>• Media surface contamination | • Accidental or intentional deletion of data<br>• Virus or worm contamination including adware, spyware, boot sector and file infecting viruses.<br>• Application or operating system crash or boot problems<br>• Damage due to power failure or power surge, lightning strikes<br>• Damage due to water and liquids including floods, rain and accidental spillage<br>• Damage due to smoke or fire,<br>• Failure due to wear/tear and age of drive |

**Table 2 The 14 most common causes linked to the loss of data (Oteng-boateng, 2011, p. 12)**

Anderson and Zhang (2010) agree with this and argue that storing the backup devices in a close range of what is originally backed up might not be such a good idea, as it still exposed to numerous risks such as theft, fire or likewise.

### 2.1.2 CLOUD BACKUP

Cloud computing is, in short, a delivery system of computer power -or space. Cloud computing can be used to various things such as storage, applications or even full infrastructures (Geambasu, 2011). You might have heard of some storage clouds, or "online backups", such as the SkyDrive, Dropbox or Sugarsync? These services depend upon an infrastructure consisting of a number of servers, called server farms, to provide you with the service you request. This can be highly useful for companies who, for example, don't have to pay for their own servers or technical support, but rather through some service which provides this for them. However in the case of backup, there have been a lot of issues concerning privacy and security. The cloud can in most cases provide you with the storage-capacity you need, but how about privacy? Geambasu (2011) argues that the moment you upload a document to Google Docs or a photo to Facebook you, as the owner of that item, loses control over it. You can't ensure that these services actually delete the items when you want to, nor that they do not replicate on different servers to ensure availability (Geambasu, 2011). Furthermore, if you don't encrypt your information, the cloud backup might suffer from both problem two and three stated in table 1 (Anderson & Zhang, 2010). Anderson and Zhang, (2010) propose another, more local, issue concerning backing up data to the cloud; the need of a decent up -and download speed. One might argue that with the cloud you can simply upload all you content and download it at will later on. Well, as a little theoretical experiment if one has about 1TB (1024GB) of data stored, and an upload speed of 1Mbit/second, then the data would only be fully uploaded about three month later. During that time any given example of data loss might have occurred.

| An example of limited internet connection in the use of cloud backup | |
|---|---|
| 1Mbit/sec = $\frac{1\times10^6}{8} = 125000 byte/sec$<br><br>1TB = $1024^4 = 1099511627776 byte$<br><br>Thus, the speed of transferring 1TB is about;<br><br>$\frac{1099511627776 byte}{125000 byte/sec} \cong 3{,}35 months$ | "*I have a home Internet backup service and about 1TB of data at home. It took me about three months to get all of the data copied off site via my cable connection, which was the bottleneck. If I had a crash before the off-site copy was created, I would have lost data*"<br><br>(Anderson & Zhang, 2010, p. 1) |

**Table 3 An example of limited internet connection in the use of cloud backup**

But except from the issue of time, there are a few others problems as well. The first is that you are dependent on a stable internet connection. In some cases, like mobile 3G connection and likewise, there might be a limit of data traffic. In such case, this can cause some trouble for obvious reasons, i.e. either your connection gets choked thus leading the backup-operation to an even greater time span, or you might have to pay extra to keep the connection at top speed. Another reason why cloud backup might be an issue for some could be companies who must or prefer to keep their data to themselves, only to guarantee that it does not get shared or replicated etc. without their knowledge.

## 2.2 SECURITY COMPLIANCE AND ACCEPTANCE

To address these issues concerning practices as well as security knowledge and acceptance, one must look at the user in a non-technical perspective (Leeden, 2010). To do this one cannot simply express the users compliance to security based on i.e. their historical use of computers, as this would in my opinion not be accurate for obvious reasons, as no concern regarding the users' acceptance would be taken into account. However, Furnell and Thomson (2009) has formed a model which focuses on what security measures are actually accepted and preformed in practice, and how users might relate to it. This model aims to form a security cultural aspect of the user behavior. Using this model we can analyze how individuals relate to the different personalities stated in Furnell and Thomson (2009) scale, see table 4:

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

**Table 4 Levels of security compliance based upon individual behaviours (Furnell & Thomson, 2009, p. 2)**

Furnell and Thomson (2009) argue that in order to help in security related issues, a deeper understanding of the security culture is needed. As in many cases, an organization -or company develops and circulate a security policy, or direct employees to an intranet page describing various security procedures. However, this "*will not be sufficient to foster appropriate understanding and behavior*" (Furnell & Thomson, 2009, p.4). To get a deeper and fuller understanding of the employees' mindset, a good look at the culture found in an organization can help us understand individual behavior. Furnell and Thomson (2009) argues that culture can be like a personality, and that "*it affects in predictable ways how people conduct themselves when no one is instructing them on what to do*" (Furnell & Thomson, 2009, p.1), which is relevant to security as Rezgui and Marks, (2008, p.2) state that "*attitudinal and behavioural features have a socio-cultural and human dimension that need to be analysed and understood to ensure full users' commitment and adherence to IS security regulations*". Furnell and Thomson (2009) table is based on "Schein's Three Levels of Corporate Culture". Schein's model consists of three levels to describe cultural levels, meaning "*the degree to which the cultural phenomenon is visible to the observer*" (Benson, 2005, p.2). 1) *Artifacts*; being described as what we can see, feel and hear. The structures and processes visible to one observing the organization. However, we cannot determine a

corporate culture only by observing this level. 2) *Espoused Values*; is the corporations own stated value, i.e. outlines in their policy, the employees identity, strategies, goals etc. 3) *Basic Underlying Assumptions*; is the shared, unspoken, assumptions which are true and taken for granted by all employed, and have direct impact on individuals behavior (Furnell & Thomson 2009; Benson, 2005). And so Furnell and Thomson (2009) eight levels of compliance derive from Schein's three levels of corporate culture in the following way:

Culture – The topmost secure level is the *culture* level. This means that the user is not only motivated and certain that security is a part of their roll, but that they have the necessary skills to exercise best practices. This level evolves from all three levels of corporate as the shared *basic underlying assumptions*, which directly influences the behavior at the *artifacts* level. These practices will thus be in line of the organizations *espoused values* (Furnell & Thomson 2009).

Commitment – This level evolves from both the *artifacts* and *espoused values*, meaning that security is a process which we accept and relate to as an organizational rule of behavior. Meaning that the user accepts the need of security, feels certain as of how to fulfill the different practices as well as that it is their roll/responsibility to fulfill them. However, the *shared basic assumptions* are note included, and the level lacks the direct influence over user behavior, thus this is not yet part of the users' natural behavior (Furnell & Thomson 2009).

Obedience – At this level the user knows and sees that security is needed throughout the policy of the companies, the *artifacts* level, and the knowledge as of how to do. This according to Ryan (2006) masks *obedience* a bit with the level of *awareness*, as the *awareness* level provides the need and understanding of practices, but lack the compliance to the policy; "*it obliges them to take responsibility but doesn't guarantee that they really accept why they should do so. As such, it would help towards attaining security obedience, but not a genuine security culture*" (Furnell, 2010, p.4).

Awareness – At the *awareness* level, the user has been instructed on correct security practices, but lacks both the stated organizational value stated in policies etc (the *artifacts* level) and so the practices are not fully reflected in their behavior or knowledge. Reaching the level of *awareness* is not done simply by circulating different policies or intranet page presenting security procedures, a program or training to introduce and guide users in security related practices is needed. Note that if this is not done sufficiently the level might slip down from *awareness* to *apathy* (Furnell & Thomson 2009).

Ignorance – At the *ignorance* level, the users' intentions are not to work against security, but lack both the practice and knowledge of security measures.

Apathy/Resistance/Disobedience – All of these possess the correct security knowledge, however of different reasons has chosen to neglect it (Furnell & Thomson 2009). These levels are described as by Rastogi (2011, p. 38) as *"'security fatigue' as one of the main reasons for end-user non-compliance where the fatigue potential of a policy or control is characterized by the levels of effort, difficulty and importance associated with the policy or control*".

# 3. METHOD

## 3.1 CASE STUDY

This research is based upon a case study, namely the situation of backup routines among students and employees. The choice of a case study is due to the situation I wish to explore, as this was a smaller group of the university. But also be because we are looking for analytical results derived from an empirical research approach, making a case study a good alternative (Sørensen, 2002). The empirical methods used to collect data were done so by *surveys* and *interview*. This is due to that case studies originate from a holistic perspective (Patel & Davidson, 2011). Patel and Davidson, (2011) argues that a case study, due to its holistic perspective, needs to cover as much data as possible. In this case, this is done by using both qualitative and quantitative studies; as it can provide a wider understanding than using only one of them (Patel & Davidson, 2011). The target population of this research was based upon their constant use and need of computers but where knowledge and acceptance of security and safety might vary. The employees and students of a university were selected as a fitting profile.

| | | |
|---|---|---|
| **Theoretical approach** | Literature survey | Theoretically based guidelines, method, framework, taxonomy or model |
| **Empirical approach** | **Case study, questionnaire survey**, experiment | Empirically based guidelines, method, framework, taxonomy or model |
| | **Analytical result** | **Constructive result** |

**Figure 1 Simple characterization of relationship between type of research approaches and type of result (Sørensen, 2002, p. 6)**

Sørensen (2002) argues that what distinguishes research from other activities is that one must be accountable for ones actions. So that any who fancy could, in theory, obtain the same results. To do this one must relate the chosen research approach with other approaches, as to clarify their distinctions (Sørensen, 2002). In figure 1 some general approaches are outlined, creating a simple framework based on the distinctions between theoretical an empirical research. This figure can be used to clarify and map the used research approach. This study, as can be seen in figure 1, is an empirical approach analyzed to display analytical results.

## 3.2 DATA GATHERING

### 3.2.1 SURVEY

The survey (see appendix A) consisted of 13 questions all of which, except for one, where closed-questions. These where distributed manually and over an online service (Google Docs). A total of 62 surveys were answered (100%).

Students – 46 answers was made by students, 18 of which were handed out manually throughout the school, the rest was distributed online, resulting in 28 answered surveys. As the author were, at the time, a student of this very school there were no difficulties in using the different classes Facebook groups as a channel of distribution.

Employees – 16 answers was made by employees, all of these were handed out manually at random. All employed have their own email address, yet emailing all employed would not result in as many answers – I figured.

The questions were made to explore the participants' backup routines and level of compliance (as seen in chapter 2). The survey was signed with a small description of the purpose, as well as contact information should the participant feel to contact the author about results or further questions.

### 3.2.2 PILOT STUDY

A number of 20 surveys where handed out manually to persons at random at the university, 17 of these were answered. The purpose for this pilot study was to get the opinion of the questions by asking the participants, but also see what questions where not answered. This made me rephrase some of the questions and delete one that was pointed out to be of no relevance.

### 3.2.3 INTERVIEW

The focus of the interview was to bring a more technical aspect from the universities point of view. I contacted the institutional IT-manager by email. The email included a short summary of the research purpose. The interview, taking place at the school, took about 35minutes and was designed as open with some additional questions as of how and what measure the university took in preventing data loss among students and employed.

## 3.3 DATA ANALYSIS

All data collected by the surveys and interview was intended to form an understanding of practices, both those used by participants and those offered by the institution. The survey was first summarized into a matrix (see appendix B) in a descriptive statistical fashion, as to give a numerical description to the collected data. The open answers in the survey were summarized, then sorted into categories made from what seemed to be the essence of all the given answers. This whole concept is done in favoring the case studies holistic perspective, rather than using a statistical hypothesis, which are of no concern to this study as its intention were not to prove any theory. Thus the descriptive statistics were used to identify how data in contrast to how the participants, related to the different cultural levels (see chapter 2.2), backed up their data. All described and presented according to an empirical and analytical approach (see table 5).

As for the interview, I took inspiration from the phenomenological approach in analyzing it. Meaning that the interview was first recorded and transcribed. The material was then read and reread as to get familiar with it and trying to categorize what seemed to be the main points. Finally, these categories were used to summarize the content. The analysis of this interview was used to get a deeper understanding of the technical support, as well as the universities point of view regarding backup. Using both quantitative and qualitative studies helped me to get a wider understanding of how routines and adoption among employed and students applied, as well as technical support and opinions offered by the university.

## 3.4 METHOD EVALUATION

This case study focuses not on an entire university, but an institution of one. The limitation is mostly due to time, and the findings are not to be generalizable due to a number of reasons; the institution is a part of a technical/IT university and can thus be expected to have better

understanding of related practices than in many other environments. But also due to that the findings are based upon a number of 62 answered surveys, and one interview, which is not enough to generalizable the findings, but enough to get an insight as of what routines as well as what security compliance where to be found.

It shall also be noted that I participated in a meeting concerning security routines, which to some extent, was relevant to this study. However I was not to take notes or quote the meeting due to its level of classification. It has however given me a better understanding as of the security measures and routines featuring this very institution. And so I consider this study to have fairly high reliability as it present an insight of routines and cultural levels using a quantitative survey, all based upon chapter 2 (which can be seen at appendix A). This survey was undertaken a pilot study (as seen in chapter 3.2.2) so as to provide a higher quality in all its questions. I've tried to design this study so that it can be used as a blue-print or foundation for similar studies; providing both high validity and reliability. However, the qualitative study performed (the interview with the IT-manager) does, obviously, not inflict the same level of reliability found in qualitative studies. I have tried to tackle this fact by looking at the specific *moment*, recording the interview and repeatedly listen to it as to make sure I made nothing slip. This being a good way to reach high reliability (Patel & Davidson, 2011).

# 4. EMPIRICAL RESULTS

In this chapter the result of all gathered data will be presented. I have chosen to present the findings by categorizing the survey answers according to the participants recognized levels of compliance and non-compliance (see appendix A, question 10), and to Furnell and Thomson (2009) model (see chapter 2.2). This will put the different levels of compliance in regard to my research question (as seen in chapter 1.2) *what compliance* as well as *what practices* are being used. A complete list of all the answers can be found in appendix B. Note that there were (as seen in appendix A) open –as well as multiple-choice questions in the survey; hence the answers might exceed 100%. At the end the interview with the IT-management will be presented separately, as to get a contrast of the universities offered support and point of view.

## 4.1 SURVEY

### 4.1.1 COMPLIANCE

**Culture** – The *culture* level had a total of 12 student respondents and 5 employed respondent (see figure 2). 40% of the employees used some sort of software to manage their backup, 20% did it manually (copying files *by hand*), whereas the other 40% said "not to backup their data". However, these 40% who claimed not to backup their data was shown to use the schools servers, creating and using their files directly at these platforms. All of which (40%) had participated in training offered by the school. For the rest of the employed participants (60%) used external hard disks, as well as the online backup service dropbox (66%). Of the participants who used external hard drives, 66% did not keep these together or within range of the computer which was backed up, no other protection was used. For the students in the same category the use of both manually and software were equally used by the participants (66% used software based backup, and 66% did so manually). The most common backup device was the use of online backup dropbox (83%). Other devices used by students was the use of storing the backup at the same computer (8%) which were backed up, using USB-thumb drives (8%) and external hard drives (66%). Note that CD/DVD and Blue-Ray was never used by either students or employees. Among the student respondents, 50% protected their data in some way; 50% did so by encryption, 25% of the user who stored their backup onto USB-thumb drive or onto an external hard drive 22% did not keep these devices together or within range of the computer which was backed up. 16% protected their data in some other way.

The regularity among the employees was divided at a daily (33%), weekly (33%) and hourly/instant (33%) basis. 34% figured backup to be of importance and 66% found backup to be of extreme importance. However, when it came to testing if the backup were fully functional, 66% did so ‘sometimes’, whereas 33% never did. Among the students 50% said that they backed up their data only when worried for some particular file or folder, 25% did so hourly or instant, 16% daily and 8% weekly.

Of all the participants at the *cultural* level 94% had suffered from some sort of technical fault which had lead to data loss. Mostly common among the employed respondents was due to accidental overwriting of data (100%), hard disk failure (75%), accidental deletion of files or folders (75%), loss of data due to application or operating system crash (50%) and that the computer did not start due to loss of critical system files (25%). For students, the reason of hard disk failure (75%), accidental deletion of files (66%), that the computer did not start due to loss of critical system files (41%), application or operating system crash (41%) and power failure (41%).

Among the participants who gave their opinion as of what the most difficult in backing up data was the main reason among the employed participants was ‘hard to remember’ (66%), that it took all too much time (33%) and handling different file versions (33%). The most difficult in backing up data was by the students the reason that it took all too much time (57%), that it required extra work (28%), hard to remember (14%) and handling different file versions (14%).

50% of the student respondents did know about "Rules for IT-security" and 33% of these had read it. As for "Handling portable computer equipment" 41% did know about it, but had never read it, 41% did know about "Your security" but had never read it. Among the employed participants 60% did know about some of the security documents published; "Rules for IT-security" (60%), "Handling portable computer equipment" (40%) and "Your security" (40%). Only one of the employees had read them. The employed participants were asked to answer if they were certain as of how to classify sensitive data according to the universities standards, 80% said to be uncertain. The follow up questions concerned the awareness of security training offered by the university, 80% did know that the university offered such training, whereas 40% had attended one.

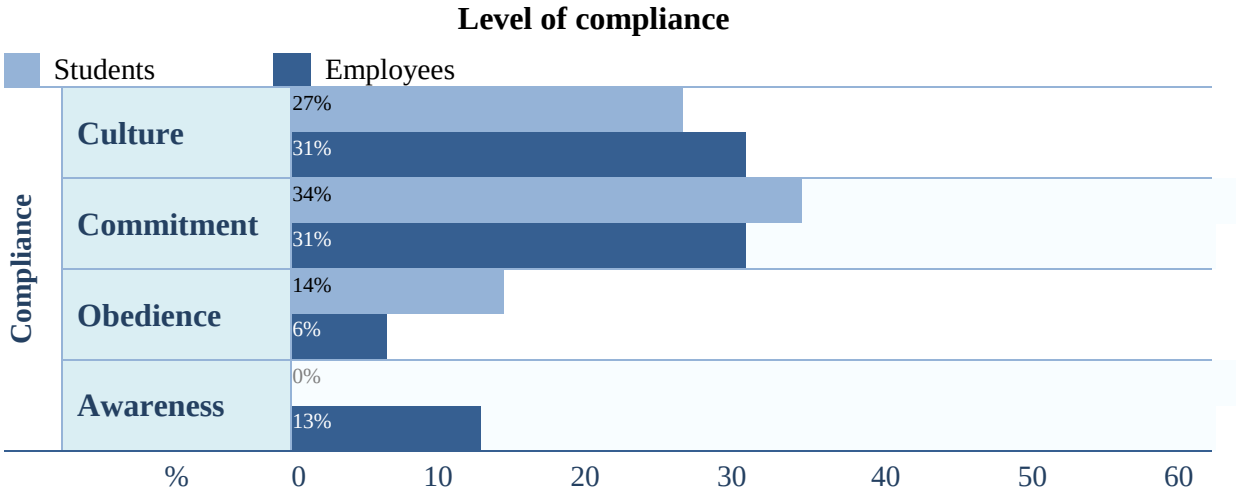


Figure 2 Level of participants’ recognition regarding their compliance

Figure 2 shows how the participants answered at what level of compliance they recognized themselves at (according to Furnell and Thomson (2009) model as seen in chapter 2).

**Commitment** – Among the employed respondents at the *commitment* level, all except one (83%), managed their backup using both manually and software. None of the participants, either student or employed, did not backup their data nor was any unsure as of how to do so. 81% of the students did backup manually whereas 50% did so by using some software. The most common way to backup data, both by students and employed, was by using external hard drives (60% employed; 75% students). Other devices used by the employed to backup data were the use of USB-thumb drives (40%) and online backup (40%). For students, the use of USB-thumb drives (37%) was used, as well as backing up data at the same computer which had been backed up (31%) and the use of online based backup (75%); dropbox (83%), mail (8%) and some other service (25%).

80% of the employed participants who used USB-thumb drive or external hard disks to backup their data did not keep the devices together or within range of the computer which was backed up. For students, 56% did protect their data in some way; 11% by encryption, 44% of

the student participants which used USB-thumb drive or external hard disks did not keep these devices together or within close range of the computer which had been backed up, and 11% of the students protected their data in some other way.

Among the employed participants, the regularity of backup was evenly spread, 20% did backup their data daily, 20% did so weekly, 20% monthly, 20% only whenever they felt worried for a particular file or folder, and 20% did so hourly or instant. Among the student participants, 73% backed up their data only whenever they did feel worried for some particular file or folder, 20% backed up their data daily and 6% did so at a weekly basis. None of the participants found backup to be of either no importance, or somewhat important. 60% of the employed participants found backup to be of extreme importance and 40% found it to be of importance. Among the student participants 75% found backup to be of importance, and the rest (25%) to be of extreme importance. However, 60% of the employed participants did 'sometimes' test if their backup actually worked, 20% did so rarely and 20% never tested their backup. By the student respondents, 25% did test their backup at every time, 37% did so sometimes, 31% did rarely do so and 6% never tested their backup.

50% of the answers given by the employed concerning what they found to be most difficult in backing up their data was due to that it was hard to remember and 50% that it took all too much time. Among the students 42% found that it was hard to remember, and that it took all too much time (42%), 7% said that the most difficult was due to file-version handling and 7% that it involved to much extra work.

All of the participants, both students and employed, had suffered from some technical faults which had led to data loss. By the employees 80% had suffered from hard disk failure, 60% have had some application or operating system crashed, 40% had due to loss of critical system files not been able to start their computer, 40% had accidentally deleted some data, 20% had suffered data loss due to viruses and 20% due to power failure. Among the students, the most common fault was due to accidental overwritten files (75%), hard disk failure (62%), accidental deletion of data (62%), data loss due to some application or operating system crashed (56%), unable to start their computer due to loss of critical system files (43%), data loss due to viruses (43%) and due to power failure or likewise (43%).

Among the employed respondents 40% did know about, but had not read, all three security documents, namely; "Rules for IT-Security", "Handling portable computer equipment" and "Your security". None of the employed participants was certain how to classify sensitive data according to the universities guidelines, 40% did know that the university offered security training and 20% of the participants had been to one. Among the students, 50% did know about "Rules for IT-Security", 37% of these had read it, 31% did know about "Handling portable computer equipment" whereas 40% of them had read it, and 37% did know about "Your Security" 16% had read it.

**Obedience** – The *obedience* level had a total of 6 student respondents and one employed respondent. The employed respondent backed up all data manually and did sometimes test to see if the backup was accurate. The employed found backup to be of importance. Among the students, 66% backed up their data manually and 33% did not backup their data at all. The backup device used by the employed respondent was by using a USB-thumb drive as well as online backup using dropbox. By the student respondents 50% used external hard disks, and 75% used online backup; dropbox (66%), FTP (33%), Google Drive (66%) and by some other service (33%). The employed respondent protected the used USB-thumb drive by not keeping it together or within range of the computer which was backed up. Among the students, 50% of

those who stored their data onto external hard disks did not keep the device together or within close range of the computer which had been backed up. As for the importance of backup, 50% of the students thought backup to be of importance, the rest of the student respondents found backup to be of either extreme importance (25%) or somewhat important (25%). Furthermore, 50% of the students never did test if their backup was fully functional, 25% did so rarely, and 25% did so sometimes.

The most difficult to backup data was according to the employed respondent the reason of extra work and the amount of time it took. For the student respondents, 60% found it hard to remember, 20% to consist of extra work and 60% found backup to be difficult and hard do learn.

The employed respondent had lost data due to loss of critical system files not been able to start the computer, among the students, the following had all been reasons of data loss; hard disk failure (80%), accidental overwritten files (60%), accidental deletion of files (80%), unable to start the computer due to loss of critical system files (80%), data loss due to viruses (60%), data loss due to an application or operating system crash (80%), data loss due to power failure (60%).

The employed participant did not know of any of the security documents. As for the awareness of data classification the employed respondent was not certain how to do so nor did the participant know about any offered security trainings. Among the students 40% did know about "Rules for IT-security", and 20% did know about "Your security", however, none of the respondents had read any of the documents.

**Awareness** – This level had but two employed participants and no students. Neither of these participants did backup their data. However, both had suffered from some technical faults where data had been lost, these includes; viruses, and accidental overwriting of data (50%) as well as an application or operating crashed (50%). Only one of the two did know about "Rules for IT-security", "Handling computer equipment" and "Your security". None of the participants where certain about how to classify sensible information according to the university standards, and neither of them did know about any offered security training.

### 4.1.2 NON-COMPLIANCE

**Ignorance** – At the *ignorance* level there were but only one student participating who did not backup, the reason given was that the student figured that the data was not of importance. The participant had not suffered from any technical faults, nor did the student know about any of the security documents published by the university.

**Apathy** – A number of two employed and eight students had recognized themselves at the level of *apathy* (see figure 3). The employees' copied their data manually, 62% of the students did so as well, and 37% of the students did not backup their data at all. The employees used online backup; one of which used dropbox at a monthly basis, and the other used an FTP to backup data, only whenever feeling worried for some particular file or folder. Neither of them protected their data in any given way. Among the students, all of which used dropbox as backup solution, 50% used their email, 25% stored their data onto the very same computer which had been backed up, 50% used USB-thumb drives, and 75% external hard disks. 50% of the students using USB/external hard disks protected it by not keeping the device together or in close range to the computer which had been backed up, 20% locked it away. No other types of protection were applied. As for the importance of backup, none of the participants,

either student or employed, found backup to be of extreme importance, however, 50% of the employees and 80% of the students found backup to be of importance and the remaining 50% of the employed and 20% of the students considered backup to be somewhat important.

Neither of the groups, student or employed, tested at a regular basis if their backed up data was accurate. 60% of the students did sometimes do so, 40% did so rarely. Among the employees 50% tested the backup rarely and 50% never did. The most difficult in keeping backups was according to 50% of the employed, that it was hard to remember, and 50% found the lack of training and knowledge about backup to be an issue. The reasons given by students where; that their data was of no importance (42%), extra work (28%), that it was hard to remember (28%), and that it took all too much time (14%).

All of the participants had suffered from some technical faults, most common among the students was due to accidental overwritten data (87%), loss of data due to viruses (75%), loss of data due to crash of an application or operating system (62%), accidental deletion of files (50%), unable to start the computer due to loss of critical system files (50%), hard disk failure (37%) and loss of data due to a power failure (37%). Among the employed participants the following faults had been reasons for data loss; accidental overwritten data (50%), accidental permanent deletion of data (50%), loss of data due to viruses (50%) and loss of data due to an application or operating system crash (50%).

None of the employed knew about any of the security document published by the university, nor did they know how to classify sensible data according to the university standards, one out of the two did know that the university offered security training, but had never participated in any. All of the students did know about the "Rules for IT-security", 66% knew about "Handling portable computer equipment" as well as 66% knew about "Your security". Only one student had read "Rules for IT-security".

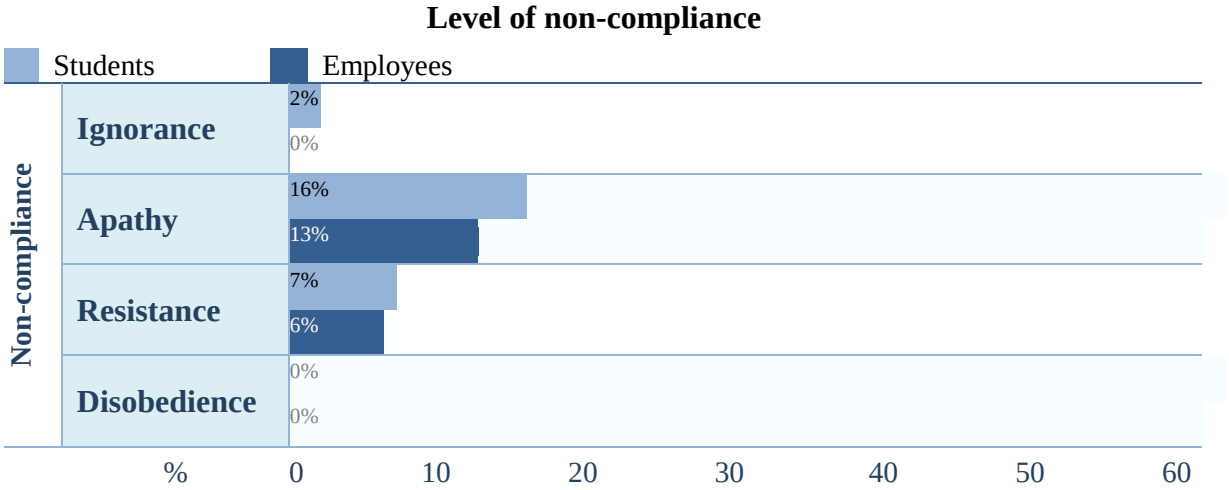


Figure 3 Level of participants' recognition regarding their non-compliance

Figure 3 shows how the participants answered at what level of non-compliance (according to Furnell and Thomson (2009) model as seen in chapter 2) they recognized themselves at.

**Resistance** – The *resistance* level consisted of one employed and three students. The employed participant used some software to backup data onto the very same computer which were backed up, as well as onto an eternal hard disk and the online service dropbox. This was done at a monthly basis and regarded as extremely important. The external hard drive was protected by not keeping it together with -or at close range to the computer which had been

backed up. One of the students used some software to backup data (33%) and the other two copied it manually (66%). All of the students participating used some online backup; 66% used dropbox, 66% used some other service and 33% used their mail. One of the students also used a USB-thumb drive (33%), which was protected by not keeping it together with –or at close range to the computer which had been backed up. No other protection was used by any of the students. The regularity of backing up data was among the students divided at; daily (33%), weekly (33%) and only whenever feeling worried over a particular file or folder (33%). The students found backup to be of importance (66%) and somewhat important (33%). However, none of the participants tested at a regular basis if their backup was accurate, but the employed participant together with one of the student (33%) did so sometime, another of the students (33%) did so rarely.

All respondents had experienced some technical faults. The employees had suffered a hard disk failure and viruses which had led to data loss or damage. All of the students had suffered a hard disk failure, accidental overwritten information (66%), accidental deletion of data (66%), loss of data due to viruses (66%), loss of data due to application or operating system crash (66%) and unable to start the computer due to loss of critical system files (33%).

None of the participants had read any of the security documents published, however, one of the students did know about "Rules for IT-security" and the employed knew about all of them but did not know how to classify information according to the university standards or about any offered security training.

**Disobedience** – No student or employed recognized themselves at this level.

## 4.2 INTERVIEW

**"People tend to think it involves a lot of work"**

Today the university provides network storage up to 20 gigabyte worth of space, for students as well as employees. This system has an automatic backup routine which provides both high reliability and availability, storing all changed files for as long as 30 days. If anything gets lost or you need your data from yesterday or last week, you can just contact the support and have them restore that date for you. For windows users, this is a very easy-made solution, as you can map-up this storage as a regular hard disk and work directly to it. All of these instructions as of how to setup this network storage are described at the universities homepage. All students and employees have direct and automatic access to this private network storage the moment they are registered at the school. However, these network storages are only reachable within the universities network, if you are outside this boundary, you could connect to it using a VPN (virtual private network), which "people tend to think it involves a lot of work". "These systems have been the same for maybe 20 years or so, it's just that we've been a bit unclear in informing about it". All university computers throughout the school are directly mapped to your network storage, if the storage does not work, so doesn't the computers, and so "the uptime would definitely be about 99.95% or something close to it".

**"Save it to the home catalog… but they don't really listen until something actually happened to them"**

I moved the discussion further by telling the interviewed that a number of employees and students where using i.e. USB thumb drives and external hard disks for their backup, the reply was that it is a problem that they are working on. I asked how the universities network storage

services were advertised, “for newly employed I try to be clear about where to store important files, however, depending on peoples background, they have different expectations of the backup system”. According to the interviewed what might be a reason for some not to use the school servers is that Mac computer uses a different type of wireless network technique which makes it harder to get working properly with the network storages, unless you plug-in your computer to the network by cable, the same goes for iPads etc. For this reason an experiment for Mac, based upon the inbuilt Apple TimeMachine, is currently under development, enabling your Apple products to directly sync onto a server. For Windows however, we say “save it to the home catalog… it’s nothing to fuss about… but they don’t really listen until something actually happened to them”. However these network storages are private, and thus difficulties in sharing documents and folders between workgroups etc. arises. Another issue is that Mac computers tend to be more “unsorted” when trying to use these network storages and file/folder mapping takes longer to load than for Windows computer, which the interviewed figures to be a factor why people don’t like using it. –To fix all these problems a new set of cloud service called Box.net, much like dropbox, is at a pilot stage at this very moment. For this reason the university has no real plan of putting too much effort in developing new “ad-hoc” solutions to compensate for Mac and Windows problems. However, the current systems will still exist and be used even after the launch of this new cloud service as it might provide every user with about 20-40gigabyte of storage space, which would simply not be enough for some of the employees work.

I asked whether services, such as dropbox for example, were prohibited by the university. The answer was that it all came down to what type of information we were talking about, and what classification should apply to it. Some of the personal for example handles sensitive data, like video interviews, and you have to ask yourself; where is it okay to backup these files? Can they be traced back to the person or persons in this film? Is it encrypted etc…? “It is really all about how employed and students takes into account what is really stored and on what device… The files in your home catalog is safe, not your computer”.

# 5. DISCUSSION

This discussion is categorized according to what I found to be the most noteworthy findings; importance of backup, device and protection, regularity and most difficult or least motivating. About 76% of the respondents recognized themselves above the non-compliance level; culture ~27%, commitment ~33%, obedience ~11%, awareness ~3%. Whereas 24% found themselves to be below the level of compliance; ignorance ~1%, apathy ~16%, resistance ~6%. Making the *cultural*, *commitment* and *apathy* target levels of discussion as these where recognized by the majority of the respondents.

**The importance of backup** – To start with the *cultural* level, two out of three employed found backup to be of extreme importance but only two out of twelve students as well. However, among the student eight out of twelve (66%) thought it to be important and only one considered it somewhat important. At the level of *commitment*, three out of five employees found backup to be of extreme importance as well as four out of sixteen students, this being the same as what we've seen in the *cultural* level (both reaching 33%), however the *commitment* has a higher level of participants who figures backup to be of importance. Moving down Furnell and Thomson (2009) model of compliance (see chapter 2.2) we find that at the *obedience* level, only one student find backup to be of extreme importance, and the majority of the participants finds backup to be of importance. This seems to be a common understanding, even for the majority of *non-compliance* participants, as we can see that the most common consideration was that backup were of importance. What differs non-compliance (the *ignorance, apathy, resistance* and *disobedience* levels) from the compliance level (the *cultural, commitment, obedience* and *awareness* levels) in this matter is that the number of participants finding backup to be of importance or extreme importance is higher at the levels of *compliance*. I figure this is, to some extent, the reflection of different levels of acceptance toward security. For example, only one of the participants at the levels of *non-compliance* found backup to be of extreme importance. It shall be noted that none of the participants found backup to be of no importance.

**Device and protection** – As mentioned above, the *compliance* level had among its employed participants a somewhat higher consideration as of backup importance than at the level of *non-compliance*. This is arguably somewhat reflected in the behavior at the *cultural* level, as the two employees of this level had probably had the most secure backup routines of all, that is; creating and working directly against the universities servers. Note that both employees stated that no backups where performed, this is true to some extent (as *they* do not perform any backups themselves) and might look remarkable if only looking at the matrix shown in appendix B. The matter is however explained in chapter 4.1.1. What shall be noted is that there were but no other participants who used the universities servers as backup device, and that both employees had been to some security training offered by the school. This is interesting, as this might be the very reason as of why they perform this type of backup in the first place, and why no one else does. The fact that the university offers network backup services shall be noted here as well. As seen in chapter 4.2 the school provides each employee and student this service, which not only offers a reasonable storage space but also 30 days of any changes made; which makes, as can be seen in the topic of "It is hard to remember", the reason of i.e. "hard to remember" less significant. However, based on the routines found in the survey, not many seem to know about this. I myself as a student at this school did not know about it, as well as the interviewees' statement that "these systems have been the same for maybe 20 years or so, it's just that we've been a bit unclear in informing about it".

Instead, the survey showed that the most common methods of backing up data were the use of online backup dropbox or by using an external hard disk. Note that CD/DVD or Blue-Ray disc where never used by any of the surveys participant. Interestingly about dropbox is that among all the participants 78% backed up their data using some online backup solution; dropbox being 75% of these solutions. However, online backup was not the most used device found in this survey, in fact external hard disks stands for 31% and dropbox 29% of all backup devices used. Other devices were somewhat evenly spread. However, online backups such as dropbox might, as mentioned in chapter 2.1 as well as in the interview, not be suitable for storing all type of data and information. If not stored correctly and protected sufficiently that is. The same goes for external hard disks, USB-thumb drives and every other backup device as well. It is however important to note that any backup containing sensitive information should, according to the interviewed (seen in chapter 4.2), follow the appropriate classification rules. However, only 6% of all the employees are today certain as of how to classify their information. By encrypting the information or locking the local devices into a safe, the problem of sensible data would not be as significant, however, none of the employed participants encrypted their data nor did any of them lock their devices into a safe or likewise. However, other physical protection was exerted; 80% of all the employees' local devices were not placed in close range to the computer that had been backed up. Among the students we find that 40% of them protected their local devices in the same way, but only one student (recognized at the apathy level) locked the device into a safe. Overall 72% of all backups (local or online) were not protected in any way.

**Backup whenever you're worried** – What differs in the aspect for backup regularity between the *cultural* and *commitment* level is that among the cultural level 33% of the employed and 25% of the students backup their data hourly or instant. This is actually (as can easily be seen in the matrix located in appendix B) not done by any other than at these two (*cultural* and *commitment*) levels. However, at the *commitment* level, there where but one employee out of five who backed up data at an hourly or instant basis, none of the students did. Interesting to notice is that most common among all students (66%) and employed (25%) in the whole survey was to backup their data only whenever they felt worried for some particular file and folders (total 58% of all backups). This can be the product of the two main reasons found in "It is hard to remember" (see below), that it is *hard to remember* and that *it takes too long time*. Only backing up whenever feeling worried for it could implies that the file is either too important not to backup, no matter the time consumption and/or in some direct consequence if not backed up that it is done instantly or at least remembered. Furthermore we find that this behavior is not based strictly to the experience of data loss due to technical faults which might seems as an explanation "they don't really listen until something actually happened to them". Nor was this, as one might think, directly reflected in the participants recognized level of compliance. This is shown for example in the commitment level as 73% of the students and 20% of the employed did in fact backup their data only whenever feeling worried, which is the second greatest procental level for this type of "regularity". Meaning that even if the backup is quite well protected (as seen in "Device and protection"), the routine of backing up data is less so. For example, take the level of apathy which had the richest number of respondents only backing up files whenever they felt worried (100% among the students, and 50% among the employed). This lack of regularity at the non-compliance levels might be explained as Rastogi (2011) put it; "security fatigue" (see chapter 2.2).

Another interesting point of backup regularity (which on the other hand seems to have everything to do with acceptance) is the usage of either backing up data using a software or

manually. As in the example of "The importance of backup", the same way the level of compliance reflected the considered backup importance among participants, the same contrast can be found in backup routines as well as method of backing up. The closer we get the level of disobedience, backing up data using a software declines and the number of "non-backup takers" increases (44% of the participants at the compliance level used a software to backup their data and 13% at the non-compliance). To some extent the same goes for the backup regularity. In both culture and commitment level, backups was performed instantly/hourly, daily or weekly. Only one participant at the non-compliance did so daily or weekly. However, this is not close to be generalized, but it sure is an interesting pattern which might mean that different routines might be expected based upon the users' security acceptance.

As for the non-backup takes at the *compliance* level, one might argue that the number of non-backup takers is the same at both *compliance* and *non-compliance*. This is true so some extent. I, on the other hand, argue that the employee at the level of *awareness* as well as those at the level of *obedience* does in fact not *belong* there. For example, the case of *obedience*, the two students who did not backup their data said that the most difficult in doing so was that they don't know how. This is interesting as Ryan (2006) argues (see chapter 2.2) that you might be at the level of *obedience*, in theory, as you may accept the need of security routines. But you must really have been thoroughly instructed at the level of *awareness* first; as it is the level of *awareness* which provides the understanding for practices. And so there is a gap between these levels, as Ryan (2006) already pointed out (see chapter 2.2). This "awareness problem" could maybe have been solved if, for example, the university had stressed the matter of technical support; "These systems have been the same for maybe 20 years or so, it's just that we've been a bit unclear in informing about it", and that instructions are given at the universities homepage. However only by circulating policies or direct each and every user to an intranet page describing how to proceed won't, according to Furnell and Thomson (2009), even get users from *ignorance* to *awareness*, and even more so, might even let slip users down to the level of *apathy*. This can be seen in the case of *awareness*, consisting of only two employed, both of which did not backup their data and neither of them had read any of the security documents, nor did they know about any security trainings. This might be a product of why backup is not performed. I argue that even if the employed recognized themselves at the level of *awareness*, the lack of enforcement concerning both policy and training might have caused them to actually slip down to the level of *apathy*.

**It is hard to remember** – Looking at what the participants said to be most difficult or the least motivating reasons to keep up with regular backups it shows that two out of three employed at the *cultural* level considered backup to be "hard to remember" and by 57% of the students found "that it took all too much time". The reason of time as well as that of being hard to remember is common at the *commitment* level as well, both reaching 38% of all the student answers and 50% by all the employees. Looking at the whole survey we find that the reason of time (that took all too much time) resulted in 28% of all answers, while the reason as of hard to remember reached 32%. Corresponding to the quote "people tend to think involves a lot of work". One interesting reason why some choose not to backup their data was to be found at the *non-compliance* level (namely at *ignorance* and *apathy*) which were the only levels featuring the reason "my data is not important enough" (7% of all the students surveys answers), which only more so reflects the lack of motivation recognized at these levels.

# 6. CONCLUSION

Based on the findings, the following conclusion were made; the compliance was among the participants found to be mostly motivated towards performing security related tasks, however, a smaller group was found to be unmotivated to do so. The backup practices found among the participants were mainly by using external hard disks or dropbox, generally whenever feeling worried for some particular file. Only a small amount of all backups where protected in any way. It was also found that backup were considered important by a majority of all participants and that negligence towards it did not reflect in their experience in data loss or level of compliance, but rather due to the reason that it was hard to remember. Furthermore, these findings might provide a useful insight of security as well as backup routines at this institution. This might serve as a foundation or at least tip on how to improve general practices, development of support, methods and/or guidelines as well as adapting these towards the different groups of compliance. Contributing to a better understanding and support regarding backup practices and protection. However I believe this is not enough to actually raise the very culture of security (described and discusses in chapter 2.2 and 5.1). This is however recommended as an area of further research; a more thorough exploration of the cultural security acceptance and what could be done to improve it. This might be done by manually analyze and categorize what cultural level seems to fit different participants best. All based upon their behavior, routines and compliance. Rather than (as in this case) letting the participants recognize themselves at the levels of compliance. This might lead to a more accurate categorization. In this study I managed to present the participants practices and level of compliance based upon their own recognition. But a significant qualitative, as well as quantitative, study of an environment might however lead to recommendations as of how to improve the very culture of security.

# REFERENCES


Anderson, P. & Zhang, L., (2010) *Fast and Secure Laptop Backups with Encrypted De-duplication*. In LISA'10 Proceedings of the 24th international conference on Large installation system administration, 7-12 November, 2010, San Jose, USA

Bairavasudaram, L.N. (2008) *Characteristics, impact, and tolerance of partial disk failures*. Diss. The University of Wisconsin, USA. Madison: ProQuest, UMI Dissertations Publishing

Benson, A.S, (2005) *The Role of Organizational Culture in Creating Secure and Resilient Supply Chains*. Civil and Environmental Engineering, Massachusetts Institute of Technology

Chervenak, A., Vellanki, V. & Kurmas, Z., (1998) *Protecting File Systems: A Survey of Backup Techniques*. In Joint NASA and IEEE Mass Storage Conference, 23-26 March, 1998, Maryland, USA

Furnell, S. (2010) Jumping security hurdles. *Computer Fraud & Security*, vol. 2010, issue 6, p. 10-14.

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

Geambasu, R., (2011) *Regaining Control over Cloud and Mobile Data*. Diss. University of Washington, USA. Washington: ProQuest, UMI Dissertations Publishing

Hoff, D.C, (2008) *Cryptic Backup: a framework for automated compression, encryption, and backup of data*. Diss. Iowa State University, USA. Iowa: ProQuest, UMI Dissertations Publishing

Jackson, M.C. (2003) *Systems Thinking: Creative Holism for Managers*. John Wiley & Sons

Leeden, K. (2010) *Security without risk? Investigating information security among Dutch Universities* Business Information Technology, University of Twente

Lenovo-AMD (2010) *Survey Finds SMBs Overworked, Cutting Corners & Engaging in Risky Technology Behavior*. Research Triangle Park, NC, 2 December

Oteng-boateng, M.L, (2011) *DATA BACKUP SECURITY: BEST PRACTICES FOR K-12 INTERNATIONAL SCHOOLS IN SOUTH KOREA*. Information Security, Lewis University

Ponemon Institute (2008) *Airport Insecurity: The Case of Missing & Lost Laptops*. Ponemon Institute LLC, 29 July

Rezgui, Y. & Marks, A., (2008) Information security awareness in higher education: An exploratory study. *Computer Fraud & Security*, vol. 27, issues 7-8, pages 241-253

Ryan, J.E (2006) *A comparison of information security trends between formal and informal environments*. Diss. Auburn University, USA

Seagate (2010) *FIPS 140-2 Standard and Self- Encrypting Drive Technology.* Seagate Technology LLC, 29 July

Sørensen, C. (2002) *This is Not an Article - Just Some Food for Thoughts on How to Write One.* Department of Information Systems, The London School of Economics and Political Science

# APPENDIX A – SURVEY

This is a survey which will form the foundation of my bachelor thesis and its research regarding backup routines at the institution of this university. I'm most grateful for your answers.

Martin Lundgren xxxxxxxx@xxxxx.xxxx.xx

**I'm currently**

O Studying my first year O Studying my second year
O Studying my third year O Employed

**1) How do you backup your files and folders?**

[ ] I'm using software to do that for me
[ ] I do this manually, that is, I copy the files myself
[ ] I don't backup (please, jump to question 7)
[ ] I don't know how to! (please, jump to question 8)

**2) What do you backup your files to?**

[ ] Onto the very computer which was backed up
[ ] Onto a USB-thumb drive
[ ] Onto an external hard drive
[ ] Onto a CD, DVD or Blue-Ray disc
[ ] By uploading it to the internet (i.e. cloud, dropbox, ftp etc.), please specify: ……
[ ] Other, please specify: ……

**3) How do you protect your backup?**

[ ] By encrypting the information
[ ] I do not keep my USB-thumb drive/external hard disk/CD, DVD or Blue-Ray discs together or in close range to the computer which was backed up
[ ] I lock my USB-thumb drive/external hard disk/CD, DVD or Blue-Ray discs into a safe or likewise
[ ] I protect it in some other way: ……..

**4) How often do you backup your data?**

O Daily
O Weekly
O Monthly
O Only whenever I feel worried for some particular file or folder
O None of these, please specify: ……

**5) How important do you consider backup to be?**

O Extremely important O Important
O Somewhat important O Not important

**6) Do you test if the data you backed up is fully functional and accurate?**

O Always O Sometimes
O Rarely O Never

**7) What do you find most difficult or least motivating to keep up with regular backups?**

……..
……..
……..
……..

**8) Have you ever lost any data due to any of the following reasons?**

[ ] Hard disk failure
[ ] Accidentally overwriting files
[ ] Accidentally permanently deleted a file or files
[ ] The computer won't start due to loss of some critical system files
[ ] By viruses or likewise
[ ] Due to an application or operating system crashed
[ ] Due to a power failure or likewise

**9) The university has published some security documents, which of these do you know about/have read:**

| | **I have read** | **I know about** |
|---|---|---|
| Rules for IT-security | O | O |
| Handling portable computer equipment | O | O |
| Your security | O | O |

**10) Which of these personalities do you recognize yourself the most?**

O Security is an implicitly part of your natural behavior and you do it regularly

O Security is not a natural part of your behavior, but you accept the need and make associated efforts

O Security routines is something you do first when provided with appropriate authorities

O You're not completely sure as of *how* and *why* you need to perform some of the security routines

O You don't know *how* or *what* to do in securing your data/information

O You know how to protect your data, but you are not motivated to follow good praxis

O You work passively against security, and does not proceed with the routines you don't agree with

O You work actively against security, breaking the rules and circumventing controls

**<u>(If you are employed at the university, please proceed to question 11, 12 and 13)</u>**

**11) Are you certain as of how to classify sensible information according to the university standards?**

O Yes
O No

**12) Have you ever participated in any of the offered security trainings by the university?**

O Yes
O No (please proceed to question 12)

**13) Are you aware that the university offered such training?**

O Yes
O No

# APPNDIX B – SURVEY RESULTS

## COMPLIANCE LEVEL

| | Culture | | Commitment | | Obedience | | Awareness | |
|---|---|---|---|---|---|---|---|---|
| | Employed | Student | Employed | Student | Employed | Student | Employed | Student |
| **Backup practices** | *Tot.5* | *Tot. 12* | *Tot.5* | *Tot. 16* | *Tot. 1* | *Tot. 6* | *Tot. 2* | *Tot. 0* |
| Uses Software | 2 | 8 | 3 | 8 | | | | |
| Copies Manually | 1 | 8 | 3 | 13 | 1 | 4 | | |
| Does not backup | 2 | | | | | 2 | 2 | |
| Don't know how | | | | | | | | |
| **Backup Devices** | *Tot. 3* | *Tot. 12* | *Tot. 5* | *Tot. 16* | *Tot. 1* | *Tot. 4* | *Tot. 0* | *Tot. 0* |
| On the computer | | 1 | | 5 | | | | |
| USB-thumb drive | | 1 | 2 | 6 | 1 | | | |
| External HDD | 3 | 8 | 3 | 12 | | 2 | | |
| CD/DVD/Blue-Ray | | | | | | | | |
| **Online Backup** | *Tot. 2* | *Tot. 10* | *Tot. 2* | *Tot. 12* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| Dropbox | 2 | 7 | | 10 | 1 | 2 | | |
| School Server | | | | | | | | |
| FTP | | | | | | 1 | | |
| Mail | | | | 1 | | | | |
| Google Drive | | 1 | | | | 2 | | |
| SkyDrive | | 1 | | | | | | |
| Other | | 2 | 2 | 3 | | 1 | | |
| **Backup Protection** | *Tot. 2* | *Tot. 6* | *Tot. 4* | *Tot. 9* | *Tot. 1* | *Tot. 1* | *Tot. 0* | *Tot. 0* |
| Encryption | | 3 | | 1 | | | | |
| Local medium not nearby computer | 2 | 2 | 4 | 8 | 1 | 1 | | |
| Local medium locked away | | | | | | | | |
| Other | | 1 | | 1 | | | | |
| **Backup Regularity** | *Tot. 3* | *Tot. 12* | *Tot. 5* | *Tot. 15* | *Tot. 1* | *Tot. 4* | *Tot. 0* | *Tot. 0* |
| Daily | 1 | 2 | 1 | 3 | | | | |
| Weekly | 1 | 1 | 1 | 1 | | | | |
| Monthly | | | 1 | | | 1 | | |
| Only when worried | | 6 | 1 | 11 | 1 | 3 | | |
| Hourly or instant | 1 | 3 | 1 | | | | | |
| **Importance** | *Tot. 3* | *Tot.12* | *Tot. 5* | *Tot. 16* | *Tot. 1* | *Tot. 4* | *Tot. 0* | *Tot. 0* |
| Extremely Important | 2 | 3 | 3 | 4 | | 1 | | |
| Important | 1 | 8 | 2 | 12 | 1 | 2 | | |
| Somewhat important | | 1 | | | | 1 | | |
| Not important | | | | | | | | |
| **Tests backup** | *Tot. 3* | *Tot. 11* | *Tot. 5* | *Tot. 16* | *Tot. 1* | *Tot. 4* | *Tot. 0* | *Tot. 0* |
| Always | | 4 | | 4 | | | | |
| Sometimes | 2 | 5 | 3 | 6 | 1 | 1 | | |
| Rarely | | 1 | 1 | 5 | | 1 | | |
| Never | 1 | 1 | 1 | 1 | | 2 | | |
| **Most difficult** | *Tot. 3* | *Tot. 7* | *Tot. 2* | *Tot. 14* | *Tot. 1* | *Tot. 5* | *Tot. 0* | *Tot. 0* |
| Version handling | 1 | 1 | | 1 | | | | |
| Hard to remember | 2 | 1 | 1 | 6 | | 3 | | |
| Extra work | | 2 | | 1 | 1 | 1 | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Hard to learn/bad training | | | | | | 3 | | |
| Takes a lot of time | 1 | 4 | 1 | 6 | 1 | | | |
| My data isn't important | | | | | | | | |
| **Technical faults** | *Tot. 4* | *Tot. 12* | *Tot. 5* | *Tot.16* | *Tot. 1* | *Tot. 5* | *Tot. 2* | *Tot. 0* |
| HDD failure | 3 | 9 | 4 | 10 | | 4 | | |
| Accidental overwrite | 4 | 9 | 1 | 12 | | 3 | 1 | |
| Accidental deletion | 3 | 8 | 2 | 10 | | 4 | | |
| Missing critical files | 1 | 5 | 2 | 7 | 1 | 4 | | |
| Viruses etc. | | 3 | 1 | 7 | | 3 | 2 | |
| Application/OS crash | 2 | 5 | 3 | 9 | | 4 | 1 | |
| Power failure etc. | | 5 | 1 | 7 | | 3 | | |
| **Sec. Cultivation** | | | | | | | | |
| ***Knows about:*** | *Tot. 3* | *Tot. 6* | *Tot. 2* | *Tot.8* | *Tot. 0* | *Tot. 2* | *Tot. 1* | *Tot. 0* |
| Rules for IT-Sec. | 3 | 6 | 2 | 8 | | 2 | 1 | |
| Handling portable computer equipment | 2 | 5 | 2 | 5 | | | 1 | |
| Your Security | 2 | 5 | 2 | 6 | | 1 | 1 | |
| ***Has read:*** | | | | | | | | |
| Rules for IT-Sec. | 1 | 2 | | 3 | | | | |
| Handling portable computer equipment | 1 | | | 2 | | | | |
| Your Security | 1 | | | 1 | | | | |
| **Certain of data classification awareness** | *Tot. 5* | | *Tot. 5* | | *Tot. 1* | | *Tot. 2* | |
| Yes | 1 | | | | | | | |
| No | 4 | | 5 | | 1 | | 2 | |
| **Knows about offered Security training** | | | | | | | | |
| Yes | 4 | | 2 | | | | | |
| No | 1 | | 3 | | 1 | | 2 | |
| **Has been to any security trainings** | | | | | | | | |
| Yes | 2 | | 1 | | | | | |
| No | 3 | | 4 | | 1 | | 2 | |

## NON-COMPLIANCE LEVEL

| | **Ignorance** | | **Apathy** | | **Resistance** | | **Disobedience** | |
|---|---|---|---|---|---|---|---|---|
| | Employed | Student | Employed | Student | Employed | Student | Employed | Student |
| **Backup practices** | *Tot.0* | *Tot. 1* | *Tot.2* | *Tot. 8* | *Tot. 1* | *Tot.3* | *Tot. 0* | *Tot. 0* |
| Uses Software | | | | | 1 | 1 | | |
| Copies Manually | | | 2 | 5 | | 2 | | |
| Does not backup | | 1 | | 3 | | | | |
| Don't know how to | | | | | | | | |
| **Backup Devices** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot. 4* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| On the computer | | | | 1 | 1 | | | |
| USB-thumb drive | | | | 2 | | 1 | | |
| External HDD | | | | 3 | 1 | | | |
| CD/DVD/Blue-Ray | | | | | | | | |
| **Online Backup** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot. 4* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Dropbox | | | 1 | 4 | 1 | 2 | | |
| School Server | | | | | | | | |
| FTP | | | 1 | | | | | |
| Mail | | | | 2 | | 1 | | |
| Google Drive | | | | | | | | |
| SkyDrive | | | | | | | | |
| Other | | | | | | 2 | | |
| **Backup Protection** | *Tot. 0* | *Tot. 0* | *Tot. 0* | *Tot. 3* | *Tot. 1* | *Tot. 1* | *Tot. 0* | *Tot. 0* |
| Encryption | | | | | | | | |
| Local medium not nearby computer | | | | 2 | 1 | 1 | | |
| Local medium locked away | | | | 1 | | | | |
| Other | | | | | | | | |
| **Backup Regularity** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot. 5* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| Daily | | | | | | 1 | | |
| Weekly | | | | | | 1 | | |
| Monthly | | | 1 | | 1 | | | |
| Only when worried | | | 1 | 5 | | 1 | | |
| Hourly or instant | | | | | | | | |
| **Importance** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot. 5* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| Extremely Important | | | | | 1 | | | |
| Important | | | 1 | 4 | | 2 | | |
| Somewhat important | | | 1 | 1 | | 1 | | |
| Not important | | | | | | | | |
| **Tests backup** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot. 5* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| Always | | | | | | | | |
| Sometimes | | | | 3 | 1 | 1 | | |
| Rarely | | | 1 | 2 | | 1 | | |
| Never | | | 1 | | | 1 | | |
| **Most difficult** | *Tot. 0* | *Tot. 1* | *Tot. 2* | *Tot. 7* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| Version handling | | | | | | | | |
| Hard to remember | | | 1 | 2 | 1 | | | |
| Extra work | | | | 2 | | 2 | | |
| Hard to learn/bad training | | | 1 | | | 1 | | |
| Takes a lot of time | | | | 1 | | 1 | | |
| My data isn't important | | 1 | | 3 | | | | |
| **Technical faults** | *Tot. 0* | *Tot. 0* | *Tot. 2* | *Tot.8* | *Tot. 1* | *Tot. 3* | *Tot. 0* | *Tot. 0* |
| HDD failure | | | | 3 | 1 | 3 | | |
| Accidental overwrite | | | 1 | 7 | | 2 | | |
| Accidental deletion | | | 1 | 4 | | 2 | | |
| Missing critical files | | | | 4 | | 1 | | |
| Viruses etc. | | | 1 | 6 | 1 | 2 | | |
| Application/OS crash | | | 1 | 5 | | 2 | | |
| Power failure etc. | | | | 3 | | | | |
| **Sec. Cultivation** ***Knows about:*** | *Tot. 0* | *Tot. 0* | *Tot. 0* | *Tot.3* | *Tot. 1* | *Tot. 2* | *Tot. 0* | *Tot. 0* |
| Rules for IT-Sec. | | | | 3 | 1 | 2 | | |
| Handling portable computer equipment | | | | 2 | 1 | 1 | | |
| Your Security | | | | 2 | 1 | 1 | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ***Has read:*** | | | | | | | | |
| Rules for IT-Sec. | | | | 1 | | | | |
| Handling portable computer equipment | | | | | | | | |
| Your Security | | | | | | | | |
| **Certain of data classification awareness** | *Tot. 0* | | *Tot. 2* | | *Tot. 1* | | *Tot. 0* | |
| Yes | | | | | | | | |
| No | | | 2 | | 1 | | | |
| **Knows about offered Security training** | | | | | | | | |
| Yes | | | 1 | | | | | |
| No | | | 1 | | 1 | | | |
| **Has been to any security trainings** | | | | | | | | |
| Yes | | | | | | | | |
| No | | | 2 | | 1 | | | |