UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

Adequacy of Computer Backup Strategies
Final Year Project

Student
David Leen – 12040193
Supervisor
Prof. Brian Fitzgerald

LM113
B.Sc. Digital Media Design
Department of Computer Science and Information Systems
University of Limerick
2016

Acknowledgements

I wish to acknowledge the help provided to me by my supervisor Prof. Brian Fitzgerald, whose advice and guidance helped me through this project. I would also like to thank my classmates in DMD and the good friends I've made over the last few years.

I'd like to thank my friends and housemates for their help and putting up with my ramblings and endless giving out over the year. I'd also like to thank my family for their encouragement and support. Their help was invaluable and I greatly appreciate it.

Finally, a thank you to everyone who participated in the research and helped me with this project in any way.

Declaration

I, David Leen, hereby declare that this Final Year Project is entirely my own work and all sources used are fully acknowledged and appropriately referenced. I understand and have adhered to the ethical implications associated with this project and I have secured ethical approval from the Science and Engineering Research Ethics Committee.

This project is presented in part fulfilment of the requirements for the degree of Bachelor of Digital Media Design and has not been submitted to any other University or higher education institution, or for any other academic award in this University.

This work was conducted under the supervision of Prof. Brian Fitzgerald at the University of Limerick.

David Leen	14/04/2016

Table of Contents

1. Project Summary

This research project aims to investigate the adequacy of people's backup strategies in today's technologically influenced world. The intent of the project is to gain an understanding of the available backup options, look at how they are perceived and used and how they inform people's strategies. It proposes to aid those who lack an understanding of the importance of a good backup strategy and those who are less technologically minded.

Research will be conducted through a review of the relevant literature and state of the art. This research will look to convey some of the issues and insights that have been established around backup strategies and practises.

Nowadays almost everyone depends to an increasing extent on the information and data stored on a computer device. However, in many cases, there is probably no coherent or sensible backup strategy in place. While understandable in the case of 'lay people' using technology, is the situation any better for those who are computer savvy? The situation might appear straightforward given the endless possibilities of storage that exist today. It may be that the plethora of options available complicates the issue.

This project, undertakes a study of available backup options and conducts a survey into the extent of actual use of these options, by the technologically literate and those less so. It also evaluates the adequacy of the various strategies being used.

This project aspires to understand the relevant issues, and hopes to contribute some insight regarding these issues and highlight the need for good backup practises. Overall it hopes to convey what an adequate backup strategy is and the need for a sound strategy no matter how technological an individual is.

2. Introduction

2.1 Project Overview

Jack Schofield, the Guardian newspapers computer editor, came up with three laws of computing. The second law "states that data doesn't really exist unless there is at least two copies of it." (Schofield, 2014) This research builds on that notion and the need for a sound backup strategy when it comes to one's data. Updated copies of data should be made for protection against data loss. This is because of the prevalent nature of data and how it often can be of a great importance to the owner or other individuals. Data can vary from being work or professional related, to personal items such as pictures and videos. Therefore, it becomes immensely important to have a good data backup strategy in place. In the event of data loss, important content can be retrieved without much hassle and considerable damage to the individual. If such strategies are inadequate, valuable data can be lost forever, much to the dismay of the individual.

Obviously, in today's digital-age, technology has become an integral part of everyday life. People are in constant contact with technology. From smart phones to tablets to laptops, it is easy to see that the world today relies heavily on such items. Often however, people do not consider their devices reliability. The modern life is lived at a fast pace, with information and resources just the touch of a button away. There is a huge dependency on the information and data stored on people's devices. Large amounts of data can be found on these technological items. How much of this data is important or could be done without? Could this data be retrieved and restored if it was lost? This research project aims to investigate further, by examining the adequacy of computer backup strategies and some of the intricacies that encompasses such work.

Admittedly, there is of course a plethora of backup options available today. It is important for this research is to gain an understanding of these backup options. For this reason, the project will examine the different services and features available and how they inform people's strategies. It seeks to understand why some have no coherent plan in place with so many options at their disposal. Existing research and backup solutions will aid this project's investigation.

Furthermore, this research also proposes to find the obstacles for good backup practices. It may be somewhat understandable in the case of an average person using technology, that they do not have an adequate plan in place. However, is the situation any better for those who are computer savvy or those who keep up to date with technology? The situation at first glance might appear straightforward. As mentioned, there exist many possibilities for storage today. Could it be, that these vast amount of options, only further complicate the issue?

The basis for this research will be through the reviewing and examining of any relevant research in the area. This along with the study of available backup options, will aid in the creation of a survey. This survey will establish what the strategies of different individuals are (the technologically minded and those not so). It will find out the extent to which people use the options available to them today. It will also ask evaluate the adequacy of the various strategies being used and if any are deemed to be adequate.

Overall the project aspires to understand the relevant factors and seeks to unearth the issues faced by people when it comes to backing-up important data. It hopes to contribute some insight regarding these issues and thus improve people's data backup strategies. Finally, it aims to provide some type of future direction in the form of practical support. The results of the survey informed by the research may highlight certain needs for individuals. Some form of practical support or service design could be implemented in the future. This could be done through the development and design of a prototyped application. An example of this may be an application that would assist anyone with backup needs and especially those people who have inadequate backup strategies or those who are less knowledgeable in the area and require help.

2.2 Motivation

As discussed the people who use computer devices, of some sort, is plentiful. This project interested me in many ways. How and why do people fail to have a backup of important data and files in this day and age. From the point of view of someone who is technologically minded, it may seem nonsensical to be without a backup plan. Therefore, is it a problem

for only people who lack computer skills or those not so technologically advanced? I surmised that this was an issue for a lot of individuals, including those with good technological knowledge and skills. Also being a technologically minded person, it interests me as to why people would not have some form of an adequate backup plan for their important data. After all data loss is something that can be quite common no matter the individual.

The Digital Media Design course afforded students the opportunity to work with many forms of media and create important content and data. Despite having many technological people, data loss and the subsequent inability to retrieve important files befell students every year. It ranged from important coursework to personal data on broken phones to failed hard drives and memory sticks. On most occasions data was lost forever and people had not thought about a backup plan until it was too late. Individuals didn't learn from each others mistakes and files and data continued to be lost. It may be something associated with people with little computer skills, but is it also indicative of a technologically savvy people?

I hope to use the knowledge and skills obtained during my degree to undertake this project. The degree has equipped me with good research skills that would be severely tested and enhanced through this project's completion. Furthermore, my intention in the future, is to further my skills through the design and development of a prototype to assist those with backup strategies needs. This phase would occur once the issues had become clear and all the relevant research was carried out, reviewed and analysed.

2.3 Project Objectives

The aims and objectives of the project are broken down as follows:

- To examine and evaluate the existing research in this area.
- To research and evaluate the available backup strategies and options.
- To use a quality survey to investigate people's backup strategies.
- To uncover interesting insights from the empirical research.
- To establish barriers to adequate backup strategies.
- To establish the important aspects of a good strategy.

- To suggest possible future directions of work.

Overall the main aim of this project is to examine computer backup strategies of individuals. The empirical research will highlight some of the reasons for adequate and inadequate strategies though an online survey. The project will be aided and guided by the existing relevant research in the area, by conducting the literature review and the state of the art.

2.4 Paper Outline

The purpose of this paper is to formally document the whole research process of the project. It details and accounts the review of the literature and state of the art, as well as the empirical research and survey analysis. The research section examines the existing research in the area, broken down into various sections, with the appropriate relevance to the individual and their backup strategies. Different types of backup options are also explained and examined. Existing backup solutions such as Google drive and iCloud are evaluated also. The empirical research section details the process involved, as well as an analysis of the online survey data. The analysis is broken down into different sections to give a general overview of the results and also a more focused perspective, regarding age and computer knowledge. The project evaluation section outlines the the different issues and factors that were faced during the project and looks at what future work may lie ahead. Finally, the conclusion outlines the overall result of the project, recapping and concluding the main points of the research.

3. Research

3.1 Research Overview

This section describes the research that has been undertaken for this project. Despite data backup being an important issue, there are not a vast amount of scientific papers surrounding the area, especially in regards to the individual and their backup practices. A search of the literature on computer backup strategies revealed varying and interesting results. Literature directly relating to the backup strategies of consumers and individuals were limited and difficult to find, especially during the original stage of the research. Backup strategies, related to topics such as businesses needs, infrastructure and architecture, IT, service providers and disaster recovery were frequently seen results for papers and articles. This became a common thread as research was sought through varies libraries and databases.

The relevant literature for this project gave interesting insights into individual's backup strategies and how they have changed over the years. There are of course a lot of facets to think of today but it is important to keep an eye on the stored data of the past too. The past can help when preparing for the future by recognising how backup options can change over time and understanding the issues for long term storage. Some individuals may have files and folders backed up from twenty years ago and losing such data may require a different recovery strategy than newer files, that have been lost or destroyed. This may be something not thought of at all when putting a strategy in place.

The importance of backing up data and the reasons for a good strategy, is something that may be thought about by people, but not entirely appreciated. Individuals need to have an understanding of what a backup strategy is and why it is needed. It may be a case of educating people on the importance of copying and backing up data, or even reinforcing this idea to those who are already somewhat aware. Delving into the many ways in which data can be lost is the starting place to understanding the need for an adequate strategy.

3.1.1 Data Loss

It is clear that data loss and backup strategies are intrinsically linked. A common thread in existing research is the loss of data occurring through various means. It is therefore, something that is prevalent in the literature and the main reason for the need of a good backup strategy. Knowing and being aware that data loss can occur and in many ways, is a key factor to understanding the need for an adequate strategy. With data loss it may simply not be a matter of if, but rather when will it occur.

There are numerous reasons for the loss of data, many of which will be familiar to computer users. As outlined in Smith's survey (2003), hardware failure, human error, software corruption, viruses, theft and hardware destruction are some of the reasons given for data loss. Hardware failure is something that could happen to anyone at any given time, hard drives can fail for a variety of reasons. Human error will always be a factor as users may delete data permanently without realising it or even drop their device causing damage. With the portability of laptops and the increasing number of smart phones and tablets, hardware destruction due to an accident is far more likely today. People don't always pay attention to where they leave their devices and therefore they are more susceptible to being damaged or destroyed beyond repair due to a fire or some other accident (Bergstra and Burgess, 2007).

A study by Kroll Ontrack (2010), argued that the leading cause of data loss is human error. This study asked those in the home and in other organisations such as governments, businesses and IT companies, what could be the reasons for their most recent loss of data. 40% of respondents felt or had a belief that human error was the main reason, while 27% were actually sure that it was human error. Since data loss is a major issue, users are advised to take proactive measures to ensure their data can be fully restored. Another interesting point from the study was that over 90% of respondents who have suffered data loss, 18% of them were unaware how it occurred. Users need to know how data loss happens in order to combat it in the future. There is a need to educate and inform people of the different aspects of data loss and recovery, so that the appropriate strategies can be put in place, to protect against data loss (Krollontrack.com, 2010). While it may not always be human error

that leads to the loss of data, it is certainly a factor and is something that people need to be aware of.

Businesses and organisations as well as individual's all have important valuable computer data that they own and wish to preserve. With the increasing nature of technological activity, there are more and more files and folders being of such importance today. There is of course a growing number of computer users in this day and age and with it there is a significant increase in the likelihood of data loss occurring. As such, there is a need for people to understand the importance of a good backup plan. With this, data loss has become prevalent and somewhat of a common problem, especially with individuals. Frequent and thorough backups are not done nearly enough as is necessary, to protect against data loss and to make a full recovery. This is true even though for most, it is obvious that their data, especially the important or critical data, should be backed up regularly (Santos and Bernardino, 2014).

For many people and also small businesses, adequate backup strategies are not in place to protect against data loss and to recover their data. To their detriment a lot of individuals do not backup their data and do not think of doing so until it is too late and they have lost important data. Doing nothing at all is simply not an option for anyone. Copying important data to an external hard drive is a least a step in the right direction, even if it is not anywhere near an adequate strategy. Those who think it is a full proof solution to guard against data loss or mistaken or misinformed. A more comprehensive strategy is needed, one where backups are automated, along with other solutions such as storing files online in the cloud (Santos and Bernardino, 2014).

It is evident that data loss can happen for a variety of reasons. The literature often focuses on the extreme cases of data loss but this is to show the importance of backing up data and being able to restore it. A good strategy will account for this by having a sound plan in place. It will also need to take into account different devices that a person uses. The cloud is one such solution that may be part of a strategy and help against data loss. It can also be an option for many of the different devices that are used today.

3.1.2 Cloud Storage

Cloud storage is a key area in regards to data backup and as such needs to be investigated. Research in this area has increased and coincided with its growth and rising popularity. Cloud-based storage has various components and thus the research comes from many different perspectives. The literature focuses on different facets of cloud storage, some being of an exploratory nature, using different methodologies to determine the best user performance. They examine specific aspects of cloud service providers, be it system architecture, the different capabilities, infrastructure, security and privacy issues and user concerns and assumptions.

The idea of cloud storage is one that individuals with a keen technological interest, or even those vaguely familiar with information technology, would have come across in some manner over the last number of years. Cloud computing as a service is one that is delivered over the internet, which users rely on for access to and handling of data. An important note is that the user has full legal control of the stored data. It is suggested that the user also does not need to be aware of the intrinsic details of the services servers and host operations and thus does not get such information. The term cloud computing therefore can be said to be a technical arrangement, where, under the control of other parties, a user's data is stored on a remote server rather than their personal computers, aided by software applications (Svantesson and Clarke, 2010). Users may not need to know the finer details of how the service is provided but it may behove them to become familiar with their rights and the terms at which their data is stored.

Nowadays when thinking of a backup strategy, a cloud-based solution may be seen as a viable option by individuals. Many different companies offer cloud-based options for consumers to store their data. Usually there are varying costs with different amounts of storage space offered depending on the price. Existing research investigates this backup option from various perspectives and often differs in approach from study to study.

Hu et al. (2010), take an in-depth look into four such cloud storage options that are available to consumers. To replicate a typical home computer and connection the researchers used an older Windows machine that ran XP with a standard residential internet connection. They also gave each of the offerings the same opportunity by carrying out the tests mainly at night. These offerings were Dropbox, CrashPlan, Mozy and Carbonite, which were evaluated in order to see if they meet the expectations that users expect from cloud storage strategies. For the study the researchers recorded the differences in each backup and restore process, taking into account what users are backing up, the possibility of data loss and issues with data privacy. (Hu et al., 2010) One major drawback of this approach is that it simply mimics what the researchers think an average individual's circumstance is. A different approach could have been implemented by using an established working circumstance. For example, willing participants could have used an existing situation that was deemed appropriate. Different tests could have been carried out and then analysed as happened in this study. This cuts out the need for simulating what an average user situation may be.

With cloud and online storage options so readily available and so many service providers to choose from, it is undoubtedly essential to ask the right questions in order to find the most suitable option for the consumer. The main focus of these services tends to be on the cost, ease of use and stability of such providers. It is argued to varying degrees of success, that what also should be taken into account is the architecture and performance, what guarantees are offered and the serious issue of the privacy and security of the data. With data loss being a prevalent issue, the authors conclude that users of cloud services should view them as a complement to their local backups. Cloud storage being the main backup strategy should not be an option as often restores can be slow and not everything will always be fully restored (Hu et al., 2010). Indeed, more than just a cloud-based backup of data is needed for a comprehensive backup strategy. Also privacy and security are always key factors for individuals. However, another important factor that is often highlighted but is a less considered factor, is the issue of the guarantees on offer and the limitation of liability outlined in the terms and conditions. These documents are not always considered when signing up to a service.

Users and consumers often assume they have more guarantees than are actually provided by cloud services. They may expect to have the same rights over their data in the cloud, as they would if it was stored at home on any of their devices. This is why terms and conditions and privacy policies are important aspects of any service. However, most users simply don't read them, as they can be very big documents. Also people simply believe that a major privacy issue wouldn't happen to any ordinary person who no one would have an interest in. It's important for individuals to understand their rights as "an alarmingly high percentage of users are unaware that their storage provider reserves the right to modify user data and disable user accounts at any time" (Ion *et al.* 2011).

Mendal et al (2014), take a different approach to investigating cloud storage. The threat of data loss is also a factor here and the researchers put forth four hypotheses, regarding this threat in relation to cloud use and the convenience and automaticity of cloud backup options. Through a survey, the research looks to ascertain "How does the threat of data loss affect a user's intention to back up their data in the cloud?" and "How do automaticity and convenience influence a user's intention to adopt a cloud-based backup solution?" (Menard *et al.* 2014).

As is apparent, data loss can have a big impact or effect on any user, especially if the data is of importance. If a user is of a mind where they perceive or are aware that data loss can occur at any time, then they are more likely to use the cloud as an option to back up their data. If, however the opposite is true and users think that data loss is a less likely occurrence, then these individuals are a lot less inclined to use the cloud as a storage option for their data backups (Menard *et al.* 2014).

Interestingly, the study reveals how certain reasons influence whether users will positively intend to backup their data on the cloud. These reasons include user's awareness of data loss and its seriousness, being able to automatically backup data to the cloud, and also the duplication of data over various devices. Therefore, the study pinpointed the perception of automaticity and concurrency as two important facets that can sway users into using the

cloud as a backup. The studies findings appear to support the various hypotheses emphasised before the survey was carried out. Users who perceive convenience being associated with the cloud will have a higher tendency to backup their data in the cloud (Menard *et al.* 2014).

When it comes to cloud storage some individuals do have certain negative assumptions. Through their research, Ion et al (2011), investigate why people have such notions about the cloud. Their findings reveal that user's perceptions of the cloud is influenced by negative stories in the media and also the idea that their online data could be easily hacked. Individuals hold an overall view that the Internet is a precarious place. This leads to the storage of important data on hard drives, external and internal, in the home as opposed to on the cloud. Users reasoning for such behaviour is that in the cloud it is possible that their data can be viewed by sources other than themselves such as cloud providers, police authorities or other unwanted parties. It is felt that the home is the safer option for storing important data of a personal nature despite a cloud provider's security measures. An interesting insight that was highlighted was that many users prefer to use some form of mail based account and its limited storage as a cloud storage for their data. This gives them control over where exactly their data is, control that they feel is lacking with the cloud and can still be accessed from different devices (Ion *et al.* 2011).

Evidently more and more data is moving from computers and laptops to cloud-based storage. It can be argued that the many benefits of storing in the cloud has brought about this change in recent times. Now people can have access to their data on the go, across multiple devices and they can share and edit content from anywhere. (Ion *et al.* 2011). As has been alluded to, cloud storage can be a key facet of a good backup plan. It is a growing and important factor for data backup strategies, with a plethora of options available to the individual. Such a choice in this service is a good thing for consumers. However, having so many options can also be somewhat overwhelming, as there are of course different factors to consider and it can be difficult to decide which option is best suited to meet an individual's needs. As discussed, these important factors include the cost, storage demands, limitations of liability, the terms and conditions and of course privacy.

3.1.3 Privacy

Privacy can be a key concern to those users of cloud services. Hackers, bugs in the system and the likes are threats to exposing one's sensitive data. An average individual will not have the resources to fight back against such threats and thus must place much importance in security and privacy. Terms and conditions and privacy policies are not documents that are always read. It is often the case that free consumer cloud-based storage does not offer much guarantees and also are not at fault for loss of data from the cloud. They also can the disable accounts or the service could stop at any time without being held responsible (Ion *et al.* 2011).

In general terms, privacy is something that everyone should care about and consider, even if people feel they have nothing to hide. Without doubt, it is also a key component of cloud-based storage. No matter what is stored in the cloud, it is important that the cloud provider is not browsing through this data. Another aspect to consider is that cloud providers have little reason to protect its user's data. Other online traders and banks are under a legal requirement to protect their users and can be held liable if they don't. While certain data such as family photos may not be of concern to potential attackers, other data, such as information stored on email accounts may be valuable. Often emails accounts contain saved mail with passwords or other important information, that needs to be protected and secure. Not every email account will be rigorously maintained or secured and thus can be breached by hackers. The service providers, however will not take their share of the blame as they do not ensure or guarantee a person's data is protected, which is hidden away and stated in their privacy terms (Clark *et al.* 2015).

Keeping data secure and private should be important to everyone who uses or relies on the cloud. Some may have the simplistic idea, that because they are just an average individual, with nothing interesting to see, that their data won't be targeted or hacked. The iCloud leaks from 2014 may at first seem like just a problem for celebrities but it points to a bigger issue. Data stored in the cloud, is visible to anyone with the correct authorization or to those who can access or change the account's password. These files may be deemed private

but as is often seen, this is not always the case. People don't need to be famous for their data to be compromised. This is especially true with private videos and pictures. Nowadays, acts such as revenge porn and sextortion often take place, where someone's private videos or pictures are used to shame them online or extort money from them (Clark *et al.* 2015).

Encryption is a way to protect sensitive or important data, if it falls into the wrong hands. It is a form of security to protect the privacy of one's data. Threats exist out there such as identity thieves and hackers but there is also the risk of losing a device or having it physically stolen. Encrypting data, wherever it exits, in the cloud or on a laptop, is a security measure to help ensure that only the owner has access to them.

Data stored online can be encrypted to provide users with more security and privacy. Users can encrypt their data before storing it in the cloud, anyone without the key to decrypt the data will not be able to access it. Generally, the user has their own key for this and does not rely or or share it with the cloud provider. This gives a layer of security to the data to protect sensitive data stored online. Encryption, basically uses a complex algorithm to encode data. To fully unlock any encrypted information an encryption key is needed for decoding. Encryption is not immune to being cracked but is a good security measure for users (Trikha, 2010).

There is a need to educate users about privacy with cloud-based computing and storage. Make them aware of the pitfalls and issues, while also highlighting the benefits of storing data in the cloud. When fully aware of the facts, users will be capable of making informed decisions and can protect the privacy of their data. It may be a case that some users opt against using cloud-based storage or only store a minimal amount of data there. Instead storage media such as external hard drives or memory sticks may be used for a users sensitive and private data.

3.1.4 Hardware Storage

A more traditional backup method is the use of an external hard drive for storing data. Their price has come down as the years have passed and much more available to individuals than they once were. Storage capacity has also increased for the storing of more data. Much of the literature surrounding data backup includes the use of this storage option.

Hard drives can be used to store data in many different ways, in conjunction with the cloud, other software or simply done manually. Kljun *et al.* (2015) highlight an interesting point, that often when external hard drives are used to backup an individual's important files and folders manually, it can depend on an event or because of a feeling someone has. This means that certain events can trigger an individual into action. Examples such as data loss occurring, looming deadline dates, a full internal drive of a computer or the upgrading a computer. External hard drives are used to backup all of an individual's data, but preference is given to data that cannot be replaced easily, like documents collected over time, personal pictures and videos. Other data that could be easily replaced or found elsewhere online would be less likely to be backed up especially if storage space was limited. Hard drives are often used because the basic cloud package offers too little space and users have concerns over cost and privacy issues (Kljun *et al.* 2015).

Hard disk drives can have a varied lifespan and it may be between three and five years before they have failing parts. While this does not always mean the instant death of a hard drive it is an indicator as to how long they can last, especially since there are a lot of moving parts inside. The failure of, or damage to any one of these parts can cause a hard drive to completely stop working. The better quality hardware that is used, the more the consumer will benefit. It may be a case of spending some extra money to ensure a longer lasting hard drive. Flash storage such as solid state drives (SSDs) and flash drives can last for around ten years. It all depends on how quickly a devices memory degrades from the deleting and writing of information (write cycles). Again the better quality manufacture, who offer more write cycles the longer these storage devices will last (Morgan, 2013).

Trikha (2010), makes an argument against only using storage media, such as external hard drives as one's backup strategy. For some individuals, the greater storage space available on these hardware options the better. At first glance an external hard drive will meet their needs, but since an individual can have a lot of important data, storage can fill up quickly. An issue with hard drives, is the need to bring them everywhere with the person, which can result in them being more susceptible to damage, loss or theft. The cloud can therefore be an attractive alternative that is convenient and can be accessed from anywhere with Internet (Trikha, 2010). The fast paced nature of life today, may mean that using hard drives as the sole backup option just isn't feasible. Convenience is something that now applies more so than ever, with the use of so many portable devices such as smartphone and ready available Internet on the go.

3.1.5 Smartphones

The impact of portable computing devices has increased as the years have passed. People share and gather information in more and different ways than ten or fifteen years ago. The smartphone can be seen as an extension of a person and is used in everyday life for different means. It becomes almost like a habit to check one's phone throughout the day. The almost constant connectivity to the internet, along with its frequent use, allows for important data to be stored on these devices.

An ever increasing amount of people use devices such as smartphones or tablets in this day and age. With this increase in users and with devices now coming with better equipped specifications, important data and information is stored on these devices without a seconds thought. Therefore, users need to adopt a good solution to backup important data and contacts. It has been suggested that investing money and becoming familiar with such procedures would be beneficial in the long run and could save users from losing valuable data (Jewell, 2011).

The modern smartphone has the capacity to store gigabytes of data. Such data may be very important to the individual and could include pictures, contact information, documents, messages and so on. Due to the portable nature of the smartphone and its relatively small

size, it is more at risk to being accidentally damaged, lost or even stolen. They are also not immune from being infected with some sort of virus such as malware or spyware (Muslukhov *et al.* 2012).

Muslukhov et al (2012) conduct a qualitative study and suggest through their research, that even though users of smartphones believe that the security of their data is a serious issue, they are not inclined to take any preventative measures to ensure its safety. The paper focuses on the protection of data in smartphones but this naturally involves the backup of data on smartphones too. Participants who had experienced data loss acknowledged that they were more aware for the need of good backup activity. Some other of the participants revealed that they backed up valuable data whenever they felt they needed to, which is vague explanation and could mean anywhere from once a week to every six months. Reasons for such poor or occasional backup practice were a lack of time, a systems inconvenience and not knowing what data needs to be backed up.

Other findings revealed that some participants thought that personal computers or external hard drives were more secure than smartphones for storing data with again the main reason being the higher chance of a phone being stolen, damaged or lost due to its portability. Others had a similar thinking with regards online storage as they would prefer to store data at home in a more traditional manner rather than online (Muslukhov *et al.* 2012). Despite data protection being its main focus, the paper offers interesting insights in relation to data backup. It highlights as much of the relevant literature does, the threat of data loss occurring at any time, as well as putting forward some interesting reasons for users poor and indifferent backups of smartphones. Some of these reasons are inherently big issues and barriers to having a good backup procedure.

Chin et al (2012), focuses on smartphones data security. Once again data loss through theft, damages or virus attacks are mentioned as user concerns. It does also highlight issues with data backup and the lack of a good backup plan. An interesting recommendation for better security and improved user confidence, is superior data backup by individuals. This suggestion for smartphones, is accompanied by an example of the iCloud as a service that

shows the problem is at least being noted by companies in the industry. The researchers however feel that backup software can be challenging for the average individual to use and adopt. To aid the point they indicate a lack of a centralised mechanism on Android phones and the need for better user interfaces. where users could indicate the exact type of data to be backed up. The design of an easy to use backup service would help individual's backup important data on their smartphone (Chin *et al.* 2012).

3.1.6 Older Backup Options

Considering smartphones and the data stored on them as part of a backup strategy is relatively new. The ubiquitous nature of smartphones, means the data found on them will only become more and more important to the individual. In the future, as smartphones become more advanced, the way this data is stored on phones or the mechanisms for retrieving such data may change. Backup options in the not so distant past consisted of solutions that no longer are used today. Floppy disks are one such option that individuals may have used previously. This option became defunct over time for a variety of reasons and was replaced by devices such as flash drives. However, at one time floppy disks were commonly used for storing data. Of course PCs and laptops are constantly evolving to the point that newer machines nowadays, don't have CD drives built into them. Just like computers, backup options for the individual have evolved and moved on from the likes of the floppy disk (Trikha, 2010).

Smith (2002), discusses some of the main issues of computer backups such as computer failures or damages. It explores some of the available hardware options from the beginning of the century, that can help to save important data such as intellectual content, while also reviewing backup strategies. Some of the options of the time include floppy disks, Zip drives, CDs and extra hard drives. It also considers web storage options which were at a less advanced stage and tests backup systems for performance reliability. It also delves into what some commercial companies and their software offer for restoring data. The relevancy of this article is in the time period it was published. It alludes to an era that relied on floppy disks, CDs and DVDs for backup purposes. Additional hard drives, is another option that is mentioned but unlike floppy disks these would be still used today. Even

though a significant amount of time hasn't passed between then and now, there has been great advancement in technological terms. There are big differences in cost nowadays as backup options are obviously much cheaper. An issue that hasn't changed is how data loss can strike at any time, where things can go wrong for anyone and thus the need for a good backup strategy is so important (Smith, 2002).

Unintentionally this article inspires interesting thoughts on data from the past. Backed up data from years ago, stored or achieved on obsolete devices such as floppy disks, need some way of being accessed in the present. The storage of such data may also need to be updated or even restored for some reason by the individual. Furthermore, this could be something to be mindful of in the future, as some backup options used today dissipate and other newer better options become available.

3.1.7 Preparing for the Future

Long term storage may be seen as something that businesses and organisations should be concerned about. However, it may be something that the individual may need to consider also. Data can have different importance and within that importance lies how long it would like to be kept for. The exact point when one may need data may not be known but at some point it may needed and for that reason long term storage is an issue. People will always have some data with long-term value to be backed up. The digital nature of data nowadays may require people to keep backups of legal documents and the likes. Some laws require organisations to keep records of data, such as account information, for a period of time (Wan et al. 2014). While similar circumstances may not exist for the individual it is clear that the long term storage of their data needs to be something they must consider.

DSpace is an interesting idea, partly due to its long-term preservation of data and also because it can get one thinking on the right track about how to prepare for the future. DSpace is a repository software package, which is an open software initiative by MIT Hewlett Packard, that was developed around the beginning of the century for organisations. It is used for creating open access repositories for various forms of digital data, mainly for research, teaching and education. The rationale behind it was that everything was put in

there for redistribution, long term storage and preservation. The data content, as well as the software or means to access or edit it, was put into the repository and served as an archival system. It is an interesting aspect of the preservation of backup (Smith et al. 2003). Although its beginnings may have been with the concern for data in institutions and libraries, the individual can still take lessons from the project. When backing up data, especially with long term storage there is not much of a point having the data unless the software or appropriate mechanism to access and update it is available too. Therefore, the advancement of technology needs to be taken into account and the software to access the content may need to be backed up too.

So, the future is very much an important aspect to take in to account when backing up data. No doubt it is a difficult aspect to fully plan for, since nothing can be considered future proof when no one knows exactly what the future will hold. Technology moves so quickly, and will certainly be different in ten years' time, so the services and equipment at our disposal today will change or become obsolete. It is essential for individuals to firstly be aware of this very fact and secondly be prepared to update their plan to accommodate newer backup options. On a similar note, the current hardware that stores the data may need to be upgraded also as technology advances. Hard drives and media storage are likely to improve which may mean that current solutions eventually become unusable. At the very least these media storage devices have a shelf life and will eventually need to be replaced or upgraded, as they will not last forever (Lifehacker.com, 2016).

3.1.8 Forgotten Data

Other data that users may want to backup but may forget about or simply don't know how to, include important emails and bookmarks. These may be taken for granted or be hidden away in some folders where the user can't find them. Email is often used as a backup option but often the saved emails themselves can be of importance to users (Kljun *et al.* 2015). It begs the question, do individuals know exactly what data they want to backup and is there anything that they might take for granted like something as simple as emails.

Some users can also be unaware of certain data, as well as having data that they take for granted or forget about. This allows for questions such as; Is there data that people don't consider when thinking about what to backup? Is any of this data actually important? Do users know about everything they backup? Is there some data they do not realise, exits somewhere else? Email accounts is an interesting place to consider, as most computer users use email, albeit mainly as a communication device. Often older emails may be forgotten about, but have some value that and thus it can be said, should be backed up. Other such data may be software licences and keys or documentation. This type of data may not seem all that significant, hence why it gets forgotten about. However, once it is gone and can't be retrieved it becomes evident that it was in fact important.

Clark et al. (2015) suggest that people may not be aware of everything they have stored in the cloud. Again an email account may not be considered as a means to store data. There can be, however, a copy of every mail sent by the user, saved in the cloud. This is something that can be easy to forget or it may not even be apparent to the user at all. Data such as photos sent through email, are therefore saved in the cloud and can exist there without the user realising. With the best of intentions, users can take for granted that a photo is deleted, when in actual fact it very much still exists unbeknownst to them. These photos are intended to be private and is sensitive data that people do not want made public (Clark *et al.* 2015).

3.2 Discussion

As can be seen from the existing research, there is a lack of literature focused solely on the individual and their backup strategies. Individuals traits, issues and concerns are alluded to in some fashion, to a varying degree in the literature. One aspect that is common in much of research is data loss. This is obviously a serious issue and should be the main reason for anyone to have a good backup plan. It can happen for a number of reasons and nearly at anytime. There is a need for people to be educated on this issue.

Much of the relevant research highlights key areas and focuses on different elements of computer backup strategies. For instance, as discussed earlier in the report, cloud storage

is a viable option as part of a good strategy. Cloud-storage is an interesting and developing aspect. It is the main focus of several papers, as it is relatively new, interesting to researchers and is constantly evolving and growing. It is suggested that cloud storage should not be the sole or main backup method for an adequate strategy. There are of course benefits related to cloud-based storage but it is smart to also considered the issues and become fully educated before putting trust in a cloud provider. Obviously, there was a need to investigate the other options available for an adequate strategy as focusing on one area is limiting an individuals plan.

Software, hardware and newer devices such as smartphones are other areas that are solely the focus of many a paper. Other older literature also has a relevancy and focus on older techniques for data backups through archiving and the likes, which brings up other issues. Therefore, a lot of different factors have to be considered for one's backup strategy. It is important to understand that lessons can be learned from the past when preparing from the future. There is a need to know where important data exists and to not take for granted or forget certain content. The prevalent nature of smartphones means that there is valuable data stored on such devices and this needs to be considered also. There are indeed a lot of factors to consider when implementing a strategy.

This section examined the research relating to the backup strategies of individual computer users. It looked to tie together some of the important facets from the established existing research and focus in on the strategies of consumers and individuals. Overall there is a need to investigate individual's backup strategies as a whole, instead of studies focusing on one aspect or another individually. Some of the barriers and issues for not having an adequate plan in place have been highlighted. An understanding for what users need and how their important data can be stored has also been gained.

3.3 Types of Backup

This section of the research identifies some of the different types of data backup options and establishes their attributes. It is necessary to differentiate between these various options as they all can play a key role in an individual's strategy and recovery plan. The key is having knowledge of each type and then deciding which option best suits the individuals needs. These backup options can be used in relation to storage media, software or the cloud strategies. Encryption of data online is another issue briefly explored.

3.3.1 Full Backup

A full backup is a backup of all the data on a system. Every file and folder will be backed up and stored as one file. It is the most comprehensive backup and the starting point for any backup strategy. Full backups make sure that nothing is missed as it is a full copy of a systems data. This option can be time consuming as the process of backing up is slow. It also requires the most storage space. It can often involve having duplicates of full backups which leads to inefficient storage. An advantage of this option is that the last full backup is all that is needed to fully restore a systems files and folders and thus this is the quickest restoring option. (Nelson and Brown, 2011)

So the easiest way to protect from data loss is to copy the entire contents of the file system to a backup device. In the event of a loss of a lot of data or a damaged system a full backup can used to restore a system fully. However, such a large backup can take up quite a bit of storage and restoring a full system or large chunks of data can also be very slow. Files or data of a smaller nature can also be restored from a full back up. (Chervenak, A. L. et al. 1998)

3.3.2 Incremental Backup

An incremental backup is where any data that has changed or is new since the last backup gets backed up. For example, any file on a system that has updated or changed since the previous back up will be then be a part of an incremental backup while those files which have not changed will not be part of this process. This option saves time when it comes to the actual procedure of backing up data. It is the quickest form of backup and it also

requires less storage space. However, there is a disadvantage to this strategy which occurs when it comes to data recovery and restore. Every incremental backup since the last full backup must be restored to insure all the relevant data is recovered and restored to its most up to date state. (Nelson and Brown, 2011)

Incremental backups are therefore used for quicker backups and update only the data that has changed since the last backup occurred. The number of these files would be low and so the backup size would be small. They can be used in conjunction with full backups which would take place less frequently as the incremental would backup the modified files. (Chervenak, A. L. et al. 1998)

3.3.3 Differential Backup

A differential backup is a backup of all the data that has changed since the last full backup. For example, any file on a system that has changed since the previous full backup will be part of this backup. It is seen to be an option in-between an incremental backup and a full backup. This is because it is faster than a full backup but it also requires more time to restore data. However, it is not as fast as an incremental backup but it does take less time to restore data. This option does take up more storage space than an incremental backup but less than a full backup. When restoring data, the last full backup and also the last differential backup will both need to be restored to insure all the relevant data is restored to its most up to date state. (Nelson and Brown, 2011)

3.3.4 Mirror Backup

A mirror backup is an exact copy of the source being backed up. They can be quite useful and is an option often provided with some backup utilities. This type of backup allows for a clean and precise backup that doesn't copy old or redundant files. However, when data is deleted from the source or original, it will also eventually be deleted from the backup. If data is lost because of human error or by some other unwelcome means, then it may be lost forever if a mirror backup is relied upon. Some services provide a a period of time between deletion of the original and the copy as a way to combat this aspect of a mirror backup. (Nelson and Brown, 2011)

3.4 Existing Backup Solutions

There is a plethora of options that an individual can use as part of their backup strategy. Many of these options can be used across many devices and with different operating systems. Much of them have similar features and can often depend on an individual's preference. With so many solutions out there, it would take some time to evaluate each one. It is none the less important to investigate some of available solutions for different devices. The following is a brief overview of a few of these existing software solutions.

3.4.1 Time Machine for Mac

Time Machine is a backup software option for Mac users and can be used with an external hard drive that is connected to a computer or Apple's Time Capsule. It can be used for full backups and incremental or differential back ups for individual files. This software backups data by taking recurring snapshots of a computers files and stores them on the user's hard drive. For efficiency the oldest backup gets deleted and the latest version replaces it. In the event of data loss, Time Machine can restore the full data or individual files. If the chosen external hard drive is not connected to the user's laptop, a local file is created so that it can backup at a later date. This feature called Local Snapshots, also allows for the daily or weekly back up of a computer. The downside to this feature is it uses some of the computers hard drive space, but to counteract that it will remove old backups when the computers space is below 20 percent (Imore.com, 2016).

3.4.2 Windows Tools for Backup

One tool available on Windows 10 is File History. This option can be used to backup a user's important data to a connected external hard drive. A benefit of this option is it allows users to restore versions of files that had been backed up some time ago. This gives the user the freedom to retrieve earlier versions of important data in the event of a mistake or change occurring. A full backup of Windows is possible with a full system image backup. This feature allows a user to create a backup plan that backups the important data on a computer as it changes over time. Backups can therefore be scheduled or automated and

stored data saved on an external hard drive or a network location. It also allows for the full restore of a system from a user's full back up (Thurrott, 2016).

3.4.3 Google Drive

Google drive allows its users to store their important data in the cloud and have access to them on any of their devices through their Google account. To begin with, users have a free 15GB of storage in the cloud storage. Files can be shared, managed and accessed from anywhere. Google drive can be used on a PC or laptop by installing its software. This allows users to back up important data to the cloud and can sync data with their other devices. Similarly, users can backup data on their phones to the cloud using the Google Drive app, so important photos or contacts can be stored and retrieved. If users need more storage space, they must purchase it online and the cost can vary depending on the storage needed (Google Drive Blog, 2016).

3.4.4 iCloud

One convenient option for Apple users is iCloud. This is an online service that can be used across Apples devices such as iPhones and iPads with a users synced data. It can work without the use of a Mac, and can be setup through a phone or tablet and data can be restored from an earlier backup using an Apple ID. If data loss happens for whatever reason, the important files can be retrieved easily for any device. Content such as iTunes music and applications are not backed up as they are perceived as easily accessible online and can be downloaded. Important data related to any such applications is stored so that the user can carry on from where the left off. Any documents created using an application that is linked to the iCloud, can be pushed to any of the users other Apple devices so they can continue to work on it. The iCloud provides Apple users with many features for the data on their devices (iMore, 2014).

3.4.5 Dropbox

Dropbox is another option for backing up data across many devices. Not only that but it also allows for the sharing of data with others who have an account. Different applications across platforms, have Dropbox features built into them for ease of use and access.

Choosing a laptop or computers files to sync to Dropbox is straightforward. It is as simple as moving them into a designated folder. However, it does only offer a limited amount of free storage, at just 2GB. This is hardly ideal and would not allow for a lot of storage. Extra storage can be expensive depending on how much is needed. Despite being a reliable option, with connection to many apps, it is not the ultimate solution as anything that is stored there must also be stored in a local Dropbox folder that can fill up quite quickly with limited storage (Hamburger, 2012).

4. Empirical Research

4.1 Overview

For this project, a quantitative research method, in the form of a survey was used to examine the backup strategies and practices of individuals. There are several methods associated with quantitative research, with different strengths and weaknesses. An online survey has advantages that were attractive for this project. These included the method being a fast and effective means of data collection, being able to target different participants through email and also it allowed for analysis of the data through statistical data processing. Having increased access to different kinds of people, with the survey being online was also of benefit.

4.2 Survey Process

With the empirical research for this project consisting of an online survey/questionnaire, it was important to approach the survey creation appropriately. This primary research followed a straightforward process in order to achieve the best possible outcome. Piloting and careful design allowed the survey to be relatively short, not overly complicated to complete and could assess different aspects of people's backup practises. It was distributed to a wide range of people of differing ages and computer literacy. The data returned was analysed to gain good insights and have a better understanding of the issues. For the survey, there was a need to focus on areas such as survey creation, testing, sampling, and distribution. The following were the steps involved in the process:

1. Create Survey Questions
2. Pilot Testing
3. Analyse Feedback
4. Implement Relevant Changes
5. Tested
6. Analyse Feedback
7. Implement Relevant Changes
8. Distribution of Survey

The existing research, through the literature review and state of the art, informed and helped shape the questions asked in the survey. An important aspect of any survey, is to pilot test it and this is something that this project required. Piloting takes place once the survey is initially made up, but before it is fully produced. It would include a smaller number of varied participants. This insures that the correct information is being retrieved from the questions being asked and reveals whether a survey is structured correctly or if it is complicated in any way. Overall it is essential as it quickly establishes if participants can follow the instructions of the survey and answer all the questions (Fink, 2012).

Initially, the survey had too many questions (Appendix 1), with an estimation of ten to fifteen minutes to complete. From feedback obtained through piloting, this was deemed too long of a survey, with some questions overlapping and producing similar answers. A reworked survey was designed and pilot tested again. Once this feedback had again been taken under consideration, changes were implemented and the finished survey was finally ready to be distributed (Appendix 2). Various groups were targeted to get a wide scope on participants, which was one aim of the survey and would also allow for a focused analysis.

4.2.1 Participants and Survey Distribution

Participants were recruited through email. They were tasked with completing the survey by answering a series of questions relevant to this research. For this survey no personal details were required other than the age group of the respondent. It was explained to participants that the survey was solely conducted to assess the adequacy of computer back up strategies of different people. They were made aware that their consent was given by clicking on the survey link and completing the questions. Also an information sheet was attached to the survey (Appendix 3), giving them full details about the project. The information was collected online through Google Forms and is stored securely and safely. Also a backup strategy was explained to them in the preamble of the survey.

Several considerations were to be accounted for from the outset. The email campaign hoped to get as high a response as possible, but this was never assured as surveys sent through email are often ignored. Participants had to represent a sample of the population

and it is important that individuals with specific characteristics (for example those who are computer literate) do not have a higher chance of being part of the sample over others. This is to ensure that the study had a broad spectrum of individuals in included, with differing computer knowledge and ability. The online nature of the survey, also provided participants with a scenario where they could answer the questions honestly and in private, without interference from the researcher. This benefits participants as they are less likely to alter their viewpoint, like they may do in a face to face scenario (for example in an interview).

4.3 Analysis and Findings

The survey remained open for three weeks, in order to get a good number of responses. Once this timeframe passed, the collection of the data and its analysis was the next step in the process. SPSS a software package used for statistical analysis, was used to analyse the data. The survey questions hoped to gain a better understanding of people's backup strategies and uncover some of the reasons as to why people do or do not have good strategies in place.

The responses, allowed for a good analysis and discussion on several interesting and key issues. Also the survey design, allowed for the partitioning of responses into groups. The analysis is therefore broken down into subsections. These subsections look at the general findings as a whole, before moving onto a more focused examination by looking at the role of age and computer literacy and also there is an analysis of those who have a backup strategy in place. Finally, it evaluates the strategies being used by the respondents and concludes the findings.

4.3.1 General Survey Analysis

The analysis is broken down down into different sections in order to gain a general viewpoint and a more focused understanding also. From the all the responses, it is important to explore the general results of the survey data obtained. Overall, 275 people participated in the survey. These participants can be divided into different categories of age

and computer knowledge (seen in the two pie charts below; figure 1 and 2), to examine the general number of varied participants for the different categories.

Figure 1, shows the different age categories of those who took part in the survey and as can be seen there is a rather even split between the ages, with over 60s being the lowest represented at 11%. The pie chart shows the different levels of computer knowledge, from 'Very Poor' to 'Excellent' and there is a good representation of the different levels. Age could now be assessed and analysed for older and younger people. Figure 2, shows the pie chart for the different levels of computer knowledge that participated. It shows that there was a varied response from people with different computer abilities. Those who rated themselves as 'Poor' or less can be seen to be was at 31%, while 'Good' or better is at 44%. In an ideal scenario, each level of the scale would be represented equally but, this distribution of computer literacy, allows for a good comparison none the less. These two pie charts show the different representation of the 275 responses.

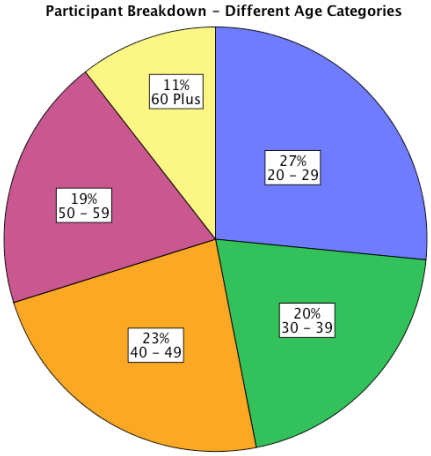

Figure 1: Pie Chart of Ages

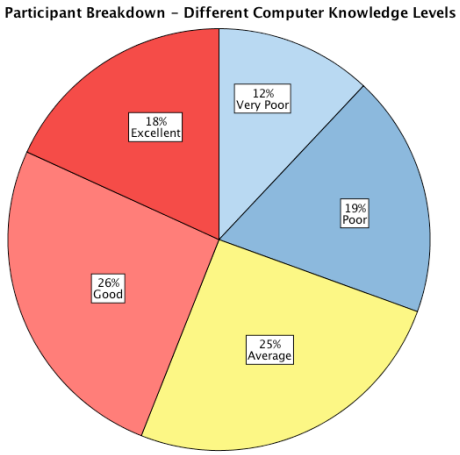

Figure 2: Pie Chart of Computer Knowledge

Followed on from the general number of participants, is the different devices that they use today. It is clear that technology is prevalent in most peoples lives today but it was important to see what devices are commonly used. Therefore, part of the survey looked to ascertain what devices were used, if important data was stored on said devices and if this data was backed up. There were 3 main devices that participants used, as can be seen in figure 3. Computers and laptops were the most used (94%), followed closely by smartphones (89%), with the tablet in third (53%). Participants felt that they stored important data on these devices but the survey also revealed that there was a difference in what data is considered important and what is actually backed up. Contact details is the biggest difference as seen in the charts. This highlights an interesting finding, that even though people may consider data important they don't always back it up.

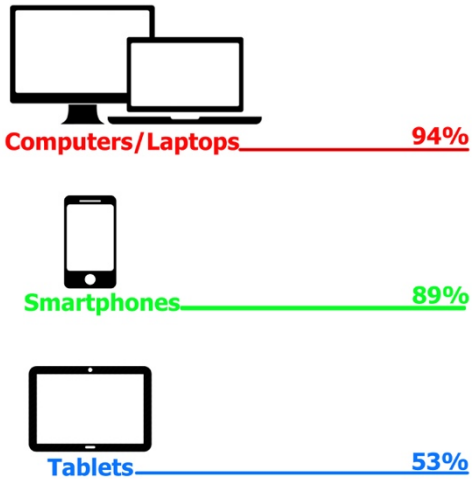

Figure 3: Devices Used by Participants

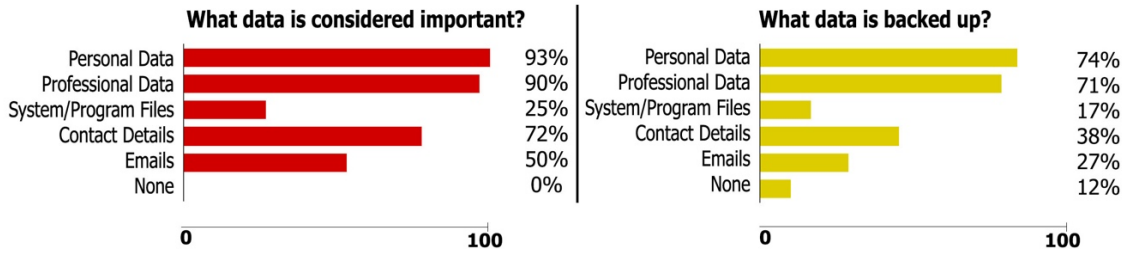

Figure 4: Breakdown of Important data versus data that is backed up

The following is the percentage breakdown between the difference in data that is backed up and what is considered important.

- Contact Details – 34%
- Emails – 23%
- Personal Data – 19%
- Professional Data – 19%

One of the issues that the survey looked at, was what impedes people's ability in backing up their data or having a good strategy. Since there is an obvious need for people to backup important data in case of loss, what is it that stops an individual from doing so? General laziness, apathy and putting off the chore of backing up were consider by some as impediments. Also alluded to, were cloud storage drawbacks, such as the need for good bandwidth speeds for uploading and downloading data, privacy concerns and the terms and conditions of service providers. Overall, time was the biggest factor at 63%, followed by convenience at 50% and a lack of knowledge at 48%. The cost factor was a lot lower than these issues at 22%. At first glance this may seem surprising but with so many options available today (some of which are free like Google Drive, albeit with limited storage), cost is indeed becoming less of an issue than it once was. The fast paced nature of life today may be a reason as to why time and convenience were the biggest barriers accounted for.

With cost being less of an issue another aspect that the survey examines is what storage options do people use. Figure 5, is a visual breakdown of some of the backup options that participants use. External hard drives, free cloud storage and memory sticks are the most used options. Backup Utilities such as Time Capsule for the Mac and Windows Backup and Restore are used less. One of the reasons that cost may not be an issue is that not many od the participants pay for cloud storage. Participants said that they used these options to a varying degree. On average, they backed up data the most on a monthly basis (30%), followed by yearly (22%), daily (20%), weekly (15%) and never (14%).

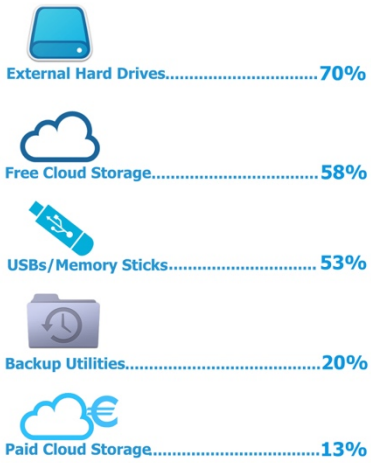

Figure 5: Backup options used

An important aspect for a backup strategy today is the cloud. It is a popular place to store data and there are a number of service providers available to the individual. How much important data do people store on the cloud, when considering some of the risks alluded to earlier and knowing that at respondents did say they used cloud-based services. Figure 6, shows in general, the average level of important data stored in the cloud. 35% said they

stored nothing of importance in the cloud. The amount of responses decreases, as the level of important data in the cloud increases. This may be for a variety of reasons outlined already in the impediments to a backup strategy.

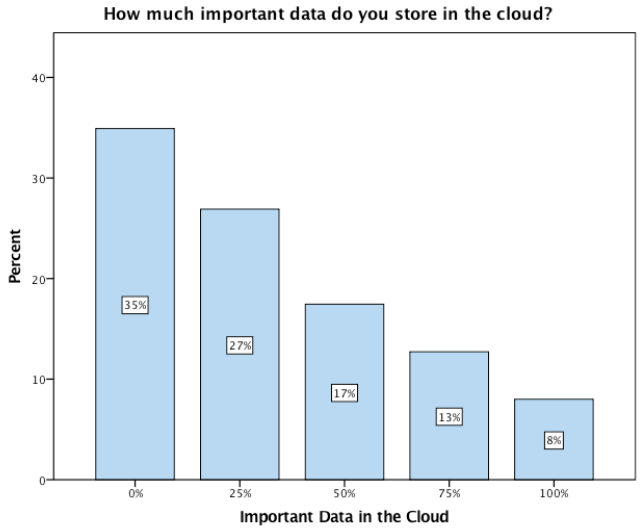

Figure 6: Bar Chart: Data stored in the cloud

The survey looked to ascertain if data loss had been experienced by participants and how it occurred. This was asked to see if data loss This was a thought provoking question, by getting participants to remember times when they'd lost data and how it can happen in various means. Device and hard drive failure were the highest at 41%. Accident was at 34% and computer virus was at 21%. Physical theft was the lowest at 18%. This highlights the different ways that data loss can happen and did happen to the participants. It is important to point out that 19% said they had never experienced data loss. This can be attributed to the older people who participated who had less data that they considered important.

With this all taken into account, in general, how did people rate their strategies? Figure 7, shows these different ratings for all participants. 52% rated their strategies as 'Poor' or worse, while 23% felt they were 'Good' or 'Excellent' strategies in place. Therefore, overall, more people felt they had poor strategies than good.

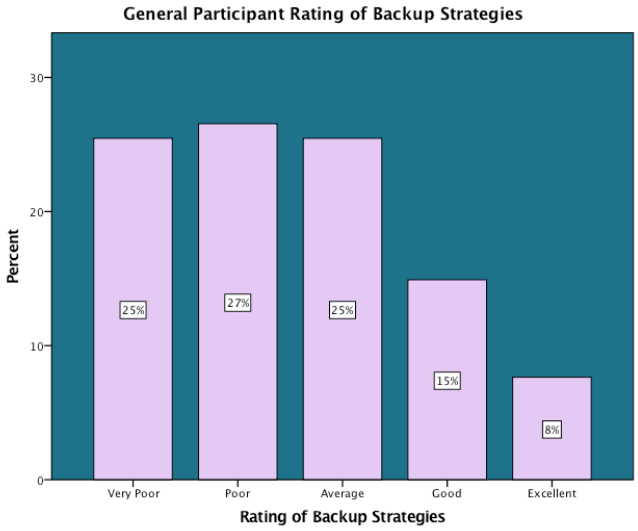

Figure 7: Bar Chart: General rating of strategies

4.3.2 Focused Survey Analysis

Now the analysis of the data will move focus and delve into the results for those participants who had a backup strategy in place. For examination, once again these participants can be divided into different categories for age and computer knowledge (seen in the two pie charts below). Figure 8, shows those over 60 are the lowest age group with a strategy at 6%, however there is a fairly even slpit between the rest of the ages. Figure 9, shows the different levels of computer knowledge and it is those with very poor computer knowledge that are the lowest percentage at 4%. This may be expected even before focusing in on the data. However, there is not too much difference between the rest of the knoweldge levels, which leads to a good anaylsis of those with a strategy in place.

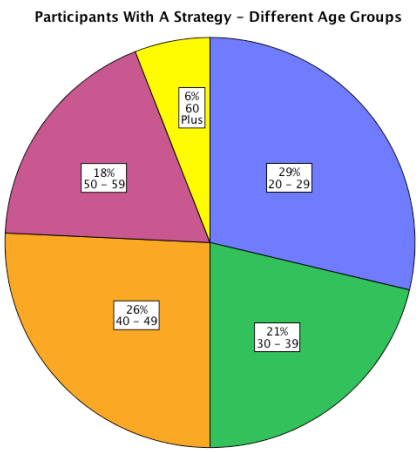

Figure 8: Pie Chart of Ages

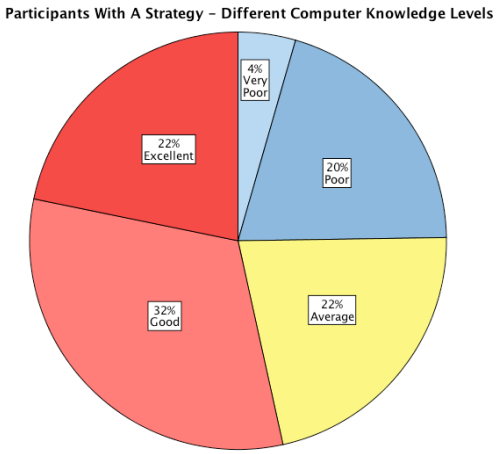

Figure 9: Pie Chart of Computer Knowledge

4.3.2.1 Role of Age in Backup Strategies

As mentioned already, one area that is of particular interest, is that of age and the role, if any, it plays when backing up data. Do those from different generations have widely differing approaches to backing up their data. Is it, that those who have grown up with technology, have good backup practises, while those who would be considered digital immigrants, do not? Those older may have taken to technology at a later stage in life and or may not have at all. These are general assumptions that can be made but may not be so straightforward.

The results from the survey suggest that age does play some factor. As seen in figure 8, those in the age categories of over 50 were the lowest percentage of those with a backup strategy. This was something that may be expected of an older generation. They may not have as much data that they want to backup or indeed some may not have the level of computer knowledge required to backup their data. Also those aged over 50, rated their backup strategies as very poor (Figure 10, below). This was the lowest any of the averages for any of the age groups. This only takes into account the age of participants. Also, there isn't too much of a discrepancy with the other age groups, so it is therefore important to look at people's computer knowledge also.

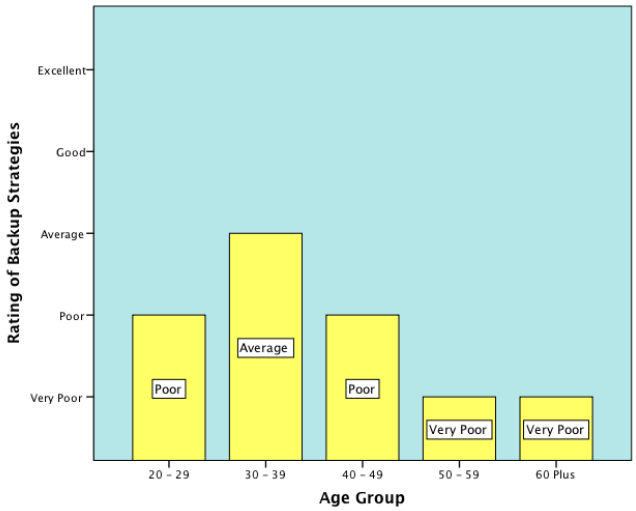

Figure 10: Bar Chart: Average rating of Backup Strategies for different Age Groups

4.3.2.2 Role of Computer Literacy in Backup Strategies

Another key facet of this survey was an individual's computer knowledge and literacy. While age can play a certain part, it is not always the case that a young person is more computer literate than an older person. It can therefore very much depend on the individual.

To ascertain respondent's computer knowledge, the survey asks the participants to rate themselves on a scale, between 1 and 5 (from 'Very Poor' to 'Excellent'). Figure 11, shows the average rating of strategies for different levels of computer knowledge in a bar chart. It shows an incline as the individual's computer knowledge increases, showing that there may indeed be a relationship between having a good strategy and one's computer knowledge.

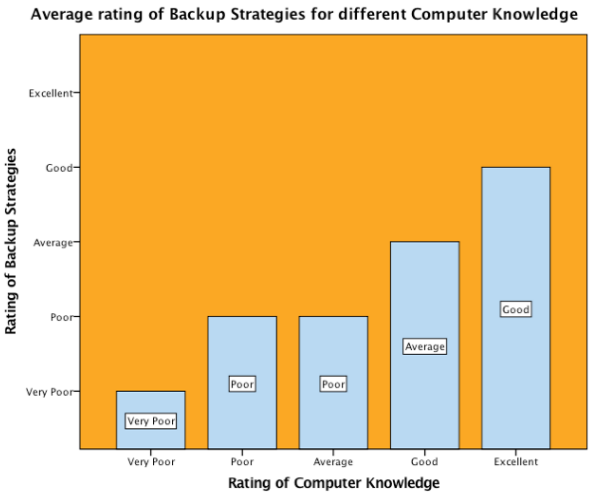

Figure 11:Bar Chart: Average rating of Backup Strategies for different Computer Knowledge

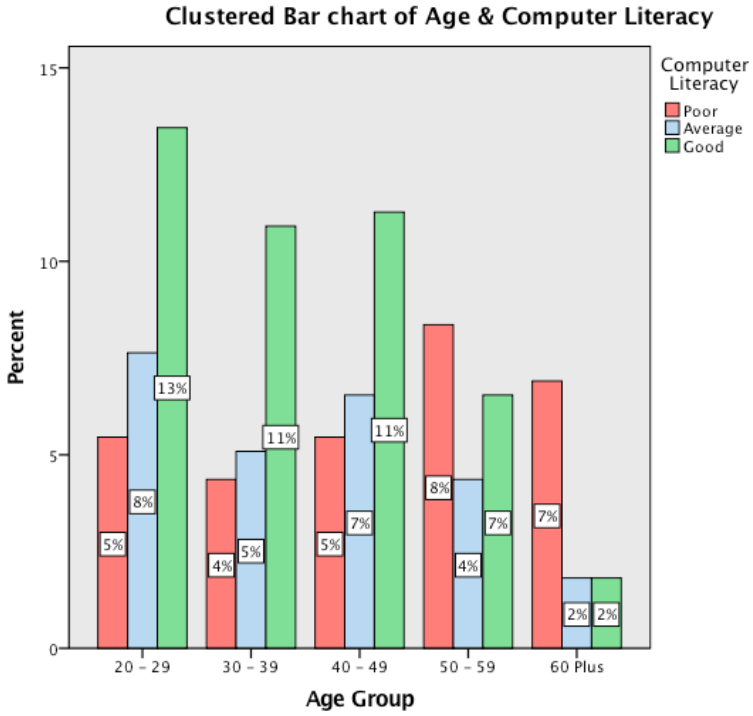

Figure 12 Bar Chart: Different levels of computer knowledge for age groups

Figure 12, is a clustered bar chart, showing the differing levels of computer knowledge for each age category. It is a good breakdown of both the two prominent aspects that the survey looked at. The green bar represents good or excellent computer knowledge, the red bar is for poor or 'very poor' and blue is for average. As is evident from the chart as age increases good computer knowledge becomes less of a factor.

4.3.3 Analysis: Testing Backup Strategies

The analysis now shifts focus towards those who said they had a backup strategy in place and if it was tested. Figure 13 below, is a breakdown of the question *"Do you have a backup strategy in place?"* Of all that responded, 73% said yes they did have a strategy, with 23% saying they didn't. A small number of 3% of people said they did not know if they had a strategy or not. These responses came from older, less computer literate participants. A reason for this is that maybe a backup plan is put in place for them by a more knowledgeable person or relative. Overall a good number of respondents did have a backup strategy.

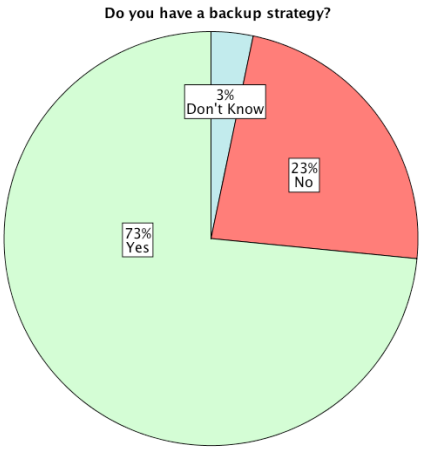

Figure 13: Pie Chart: Backup Strategy Breakdown

An important aspect of any backup strategy is the testing of it, to make sure it can be relied upon in the event of data loss. If not tested, an individual cannot be fully sure if their strategy will allow them to fully restore their data. A simple question in the survey asked participants to say whether or not they had tested their strategies. Interestingly, of those that said they had a backup strategy in place, 54% said they had not tested their strategy, as can be seen in figure 14 below.

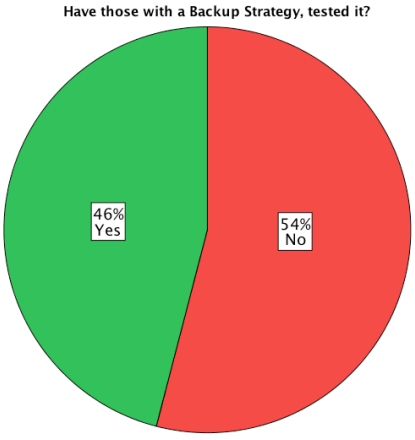

Figure 14: Pie Chart: Testing Breakdown

There isn't a big difference between the percentage that answered yes and no to this question. However, it is important to note that many people's backup strategies have not been tested. A good strategy most certainly needs to be tested before data loss occurs. After the fact these individuals may find their strategy wasn't good enough and their data is permanently lost. In order to have the best possible strategy in place, it needs to be tested, in order to know that it can be used if and when it is needed.

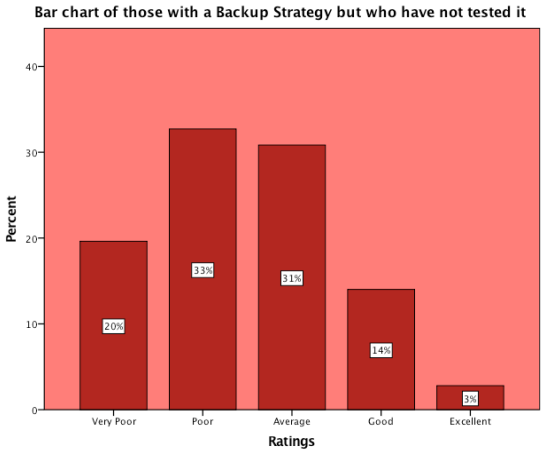

Figure 15: Bar Chart: Have not tested their strategy

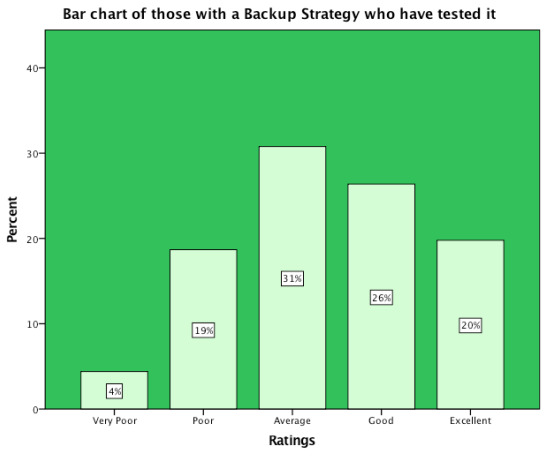

Figure 16: Bar Chart: Have tested their strategy

For further evidence, the responses can be again separated out, as part of the analysis. These results show different ratings based on who tested their strategy and those who didn't. Figure 15 shows the ratings for those who did not test their strategy. The ratings here showed these strategies as 'Poor' or 'Very Poor', at 53% with much less respondents rating their strategies as 'Good' or 'Excellent' at 17%. In contrast, figure 16 shows the ratings for those who did test their strategy. Here the chart shows better ratings for 'Good' and a marked rise in those who said 'Excellent'. The 'Average' rating is consistent in both bar charts at 31%, which indicates that overall there is room to improve strategies even if they are tested or not.

However, it is also important to exercise prudence when analysing these results. Testing is indeed important, but the full picture may not be known. Testing may vary depending on different factors. For example, how much data is being backed up and how frequent do these backups occur? The type of backup, also may need to be taken into account. Testing can vary depending on several variables. It is not known when last the participants had tested their strategies. It may be that it was quite some time ago and that there is a fault with the strategy now, meaning a full restore could not take place. The frequency of testing is not taken into account or indeed how vigorous it is. So some caution needs to be exercised here.

4.4 How adequate are people's Backup Strategies?

A key question for in the survey, was how good are people's backup strategies? Participants were asked to rate their strategies on a scale between 1 and 5 (1 being 'Very Poor' and 5 being 'Excellent'). The question was positioned last in the survey and looked to ascertain how adequate, people felt their strategies actually were. By having the question asked last, it allowed participants to reflect on their answers to the previous questions and give their strategy an honest rating. Figure 17, shows the results for this question in a bar chart.

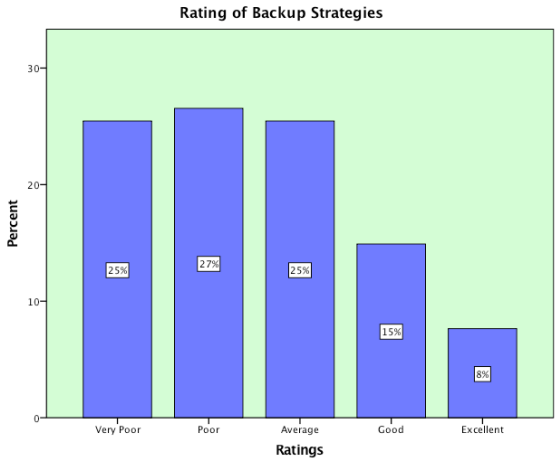

Figure 17: Bar Chart: Participant Backup Strategy Ratings

As can be seen from the bar chart, the results show that people rated their strategies as mainly 'Average' or worse. Over half of those that took the survey, felt their strategies were 'Poor' or 'Very Poor', while 23% rated theirs as 'Good' or 'Excellent'. For the most part, the results show that there may indeed be a need for people to implement better strategies in order to protect and keep their data. It at the very least can be said, that there is room for people to improve their strategies, from the indication given by over three quarters of the people that completed the survey.

4.5 Limitations

Since this survey aimed to have individuals who are computer literate and also those less so, of various ages, it could be considered somewhat biased. The bias appears when targeting certain groups through email. Although not completely biased those of an older and younger age were did partake in the survey, as well as different groups who who have

varying levels of computer knowledge. However, as certain groups were targeted the results are therefore not an overall reflection of the population. For example, those of different employment status or other such criteria were not considered when recruiting participants. These factors may have had an impact on the results. However, since certain groups were targeted in a similar way, age and computer level was the only way to analyse and separate participants. Indeed, these were the two separating factors when designing the survey.

The quantitative nature of the research also has some limitations. It doesn't allow a deep analysis and instead relies on deduction of the data returned. A mixed methods approach may have been beneficial. A qualitative interview could have gained rich insights into the many issues and give a deeper understanding to individual's backup practises. This along with the survey would have allowed for a greater analysis with the possibility of greater insights.

4.6 Discussion on Findings

It is important that people know and understand the value of data and indeed where it exits. They can then decide what data is important enough to backup or if they can tolerate losing data. Evidently data loss can occur for a variety of reasons and people have experienced important data loss on various different devices. It is more than likely they will experience data loss in the future when learning the lessons of the past. Many barriers exist when backing up data. Lack of knowledge, time and convenience are notable issues that people have. A plethora of options are out there and are being used by people but may not be used as part of a good strategy.

The survey results show that age and computer knowledge can play a part in the adequacy of computer backup strategies. A case can be made showing that older and computer illiterate have no plan in place or indeed have no sensible, coherent plan. The analysis shows that younger and computer literate fair much better, but they can still improve their backup strategies. An individual's computer knowledge plays a big role it seems, even more so than age. Those with greater computer skills had higher ratings for their strategies.

Those who tested them, rated their strategies the best of any participants, as they knew they could rely on their strategies if needed to. Planning and being prepared is a must, to guard against data loss. Therefore, as seen, testing one's strategy is important to the success of any good strategy. It can be strongly argued, that it is only worth creating a backup, if it can be fully restored when needed. It may be necessary to regularly test a backup by trying to restore it fully. By doing this it prepares the individual in two ways, first by knowing how to retrieve and restore data and secondly by testing if the plan in place actually works.

Overall, after analysis the survey data, more people felt they had poor strategies than good. As discussed age and computer knowledge can play a role. In general, the analysis shows there is room for most people to improve their strategies. Those with an adequate strategy in place is not as high as it should be, when the many backup solutions available are considered. The issues and barriers alluded to give some reasons as to why this is the case. It is necessary that people become aware of the need for an adequate backup strategy, that could prevent the loss of important data no matter what device it exists on.

5. Project Evaluation and Future Work

5.1 Evaluation

The aim of this project was to examine the adequacy of people's backup strategies, in the fast paced technological world of toady. Its intent was to gain an understanding and insights, through an evaluation of the relevant literature and by conducting empirical research through an online survey.

The review of the literature proved to be an interesting aspect of the project. Finding relevant research, focused on the individual, was challenging at times, especially at the outset of the project. A lot of the literature in this field, is more centred around the backup practises and structures of businesses and organisations. Infrastructure, IT and other such aspects, that the average individual would not have to consider, are explored thoroughly in many a paper. As the project progressed relevant research continued to be uncovered, detailing different aspects of backup strategies for the individual.

Many factors related to one's backup strategy were examined in the reviewed literature. It was necessary to break down the existing research into different sections, detailing the various components in the area. Some of these sections included, the reasons for needing a backup strategy, different backup solutions, the importance of data and older backup mechanisms. The evaluation and critique of the existing research allowed for a good understanding of the issues, while also providing guidance for the empirical research.

The survey process was a more complicated and longer aspect than first was envisioned. Even with several factors take into consideration, such as the need for pilot testing and the redesigning questions, the process was not without its issues. The initial response to emails was poor and not encouraging. However, after a more targeted emails, responses increased and data analysis could begin. The survey in general proved to be beneficial in unearthing various aspects of people's backup strategies, their issues and practices. A high number of respondents provided good information and allowed for a good analysis of the data returned. It would have been beneficial to ask different questions for more insights and to possibly target a wider group of participants.

Good time management is key to any project and it proved the case for in this instance too. In an ideal world the survey distribution and analysis would have been completed at an earlier date. This would have allowed for the possibility of a qualitative approach, through interviews to gain further insights and to have a more detailed and focused views to analysis along with the quantitative nature of the survey. This mixed method approach may have uncovered different issues and given detailed explanations, where the survey alone could not.

The project proved to be a challenge but ultimately was rewarding. Personal and academic objectives were accomplished through its completion. Having had some research experience in past modules over the years, this project allowed for a different level of research and intensity, that pushed and tested various skills. It developed my skill set overall and gave me a greater understanding of the different facets of primary and secondary research, through the examination of a real world issue. It also also allowed for the envisioning of what future work might consist of.

5.1 Future Work

As this project was research based, the future work would entail some form of practical support, to aid those who have inadequate of none existent strategies. More primary research could be carried out, to uncover more of the issues and to fully understand the barriers that prevent people from having a sound backup strategy in place. As alluded to this could be done through a mixed method approach, with qualitative interviews and possibly another survey.

The practical element could be designed for those with a lack of knowledge, time, resources or for convenience. These were some of the backup impediments, found in the analysis of the survey. Service design or indeed a web based application could be beneficial in aiding certain individuals.

Once the relevant research is fully complete, a prototype phase could begin. A prototype would be designed in its various stages and tested on users. This would be an iterative

process moving, from low fidelity to high fidelity and based on user centred design. The users would have a key role in the process, from beginning to end. The prototype could be some form of application on a smartphone, since it is a common device used by many today and data such as contact details is often forgotten about or not properly backed up. Once the prototype phase is finished, the actual development of the application could take place.

6. Conclusions

This project highlighted the need for individuals to have an adequate backup strategy for their data. This was achieved through two different means of research. Firstly, a review of the literature and a state of the art was conducted by evaluating the existing research in the area. Then primary research was carried out in the form of an online survey, to investigate and evaluate people's backup strategies and practises.

As is evident, many people use technological devices nowadays. Laptops, tablets and smartphones are commonly used. Data is stored on these devices without a seconds thought. The portable nature of all these devices makes them more susceptible to damage, loss or theft. Depending on how important the pictures, documents and items found on these devices are to the individual, some or all of this data may need to be part of one's strategy.

Data loss can occur for many reasons, especially when data exists in many forms and on many devices. Lost files and folders can vary in significance but important data needs to be backed up properly, in order for it to be fully restored. Good backup solutions are then needed as part of one's strategy. If such strategies are inadequate, valuable data can be lost forever or not properly restored.

A strategy basically involves the copying and archiving of computer data. This strategy can then be used to restore the original data in the event of it being lost. Many existing solutions are available for people to use. These include, but are not limited to, cloud-based storage, hardware devices (e.g. external hard drives) and backup utilities (e.g. time capsule for the Mac and Windows backup and restore). Knowing these solutions strengths and weaknesses can be of benefit to an individual. A combination of these options form the basis of a strategy. Different types of backups can be performed depending on what is necessary and best suits someone. These can be full backups, incremental or differential.

It may seem simple, an individual backs up their data and it can be restored if needs be. However, there are several reasons as to why it is not so straightforward. People may have a lack of knowledge about the need for a strategy or how to implement one. They may lack appropriate computer knowledge or skills. People can have apathy for the problem and put

off dealing with the issue. Todays fast paced nature of life may explain some of this as time is a key issue when baking up data. It may also be a reason as to why those with good computer knowledge, don't always display the best backup practices.

The empirical research shows that there is room to improve people's strategies and practices. Many felt their strategies were average or worse when they were rated in the survey. An adequate strategy, incorporating different backup solutions and is tailored to protect the individual's important data against loss is a must, for anyone who does not want lose the data that is important to them. To implement a strategy an individual should analyse what needs to be backed up, plan on how best to use the solutions available, implement the plan fully, test the strategy appropriately and review the process after a period of time.

7. References

Bergstra, J. and Burgess, M. (2007). *Handbook of network and system administration*. London: Elsevier.

Chervenak, A., Vellanki, V. and Kurmas, Z., 1998, March. Protecting file systems: A survey of backup techniques. In *Joint NASA and IEEE Mass Storage Conference*, available: http://www.storageconference.us/1998/papers/a1-2-CHERVE.pdf [accessed 13 Dec 2015].

Clark, J.W., Snyder, P., McCoy, D., Kanich, C. (2015) '"I Saw Images I Didn't Even Know I Had": Understanding User Perceptions of Cloud Storage Privacy', ACM Press, 1641–1644, available: http://dl.acm.org/citation.cfm?doid=2702123.2702535 [accessed 8 Mar 2016].

Fink, A. (2012). How to conduct surveys. 5th ed. Sage Publications.

Google Drive Blog, (2016). *Meet the new Google Drive*. [online] Available at: http://googledrive.blogspot.ie/2014/06/meet-new-google-drive_25.html [Accessed 1 Jan. 2016].

How to Back up and Restore Your Mac with Time Machine [online] (2016) *iMore*, available: http://www.imore.com/how-set-and-restore-time-machine-backup [accessed 1 Jan 2016].

Hamburger, E., 2012. Google Drive vs. Dropbox, SkyDrive, SugarSync, and others: a cloud sync storage face-off. *The Verge*.

Hu, W., Yang, T., Matthews, J.N. (2010) 'The good, the bad and the ugly of consumer cloud storage', *ACM SIGOPS Operating Systems Review*, 44(3), 110–115.

iMore, (2014). *iCloud*. [online] Available at: http://www.imore.com/icloud [Accessed 4 Jan. 2016].

Ion, I., Sachdeva, N., Kumaraguru, P. and Čapkun, S., 2011, July. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In*Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 13). ACM.

Jewell, S. (2011) 'Productivity via Mobile Phones: Using Smartphones in Smart Ways', *Journal of Electronic Resources in Medical Libraries*, 8(1), 81–86.

Kljun, M., Mariani, J. and Dix, A., 2015. Toward understanding short-term personal information preservation: A study of backup strategies of end users.*Journal of the Association for Information Science and Technology*.

Krollontrack.com. (2010). *News*. [online] Available at: https://www.krollontrack.com/resources/press/details/61462/technology-users-believe-human-error-is-the-l/ [Accessed 24 Feb. 2016].

Lifehacker.com. (2016). [online] Available at: http://lifehacker.com/5904275/whats-the-best-way-to-back-up-my-data-for-the-long-haul [Accessed 13 Mar. 2016].

Menard, P., Gatlin, R. & Warkentin, M. 2014, "THREAT PROTECTION AND CONVENIENCE: ANTECEDENTS OF CLOUD-BASED DATA BACKUP", *JOURNAL OF COMPUTER INFORMATION SYSTEMS,* vol. 55, no. 1, pp. 83-91.

Morgan, C. (2013). Data storage lifespans: How long will media really last?. [Blog] Storagecraft. Available at: http://www.storagecraft.com/blog/data-storage-lifespan/ [Accessed 10 Mar. 2016].

Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K. (2012) 'Understanding Users' Requirements for Data Protection in Smartphones', IEEE, 228–235, available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6313685 [accessed 28 Dec 2015].

Nelson, S. and Brown, R. (2011). *Pro data backup and recovery*. [New York]: Apress.

Santos, A., Bernardino, J. (2014) 'Open Source tools for remote incremental backups on linux: an experimental evaluation', *Journal of Systems Integration*, 5(3), 3.

Schofield, J. (2014). *Follow Schofield's Three Laws of Computing and avoid disasters | ZDNet*. [online] ZDNet. Available at: http://www.zdnet.com/article/follow-schofields-three-laws-of-computing-and-avoid-disasters/ [Accessed 30 Nov. 2015].

Smith, D.M. (2003) 'The cost of lost data', *Journal of Contemporary Business Practice*, 6(3), 1–9.

Smith, M., Barton, M., Bass, M., Branschofsky, M., McClellan, G., Stuve, D., Tansley, R. and Walker, J.H., 2003. DSpace: An open source dynamic digital repository.

Smith, R. 2002, "Computer Backups: The Gotcha Factors",MultiMedia Schools, vol. 9, no. 4, pp. 40.

Svantesson, D., Clarke, R. (2010) 'Privacy and consumer risks in cloud computing', *Computer Law & Security Review*, 26(4), 391–397.

Thurrott, P. (2015). *Windows 10 Feature Focus: Backup and Recovery - Thurrott.com*. [online] Thurrott.com. Available at: https://www.thurrott.com/windows/windows-10/4279/windows-10-feature-focus-backup-and-recovery [Accessed 1 Jan. 2016].

Trikha, B. (2010) ‘A Journey from floppy disk to cloud storage’, *International Journal on Computer Science and Engineering*, 2(4), 1449–1452.

Wan, S., Cao, Q. and Xie, C., 2014. Optical storage: an emerging option in long-term digital preservation. Frontiers of Optoelectronics, 7(4), pp.486-492.

8. Bibliography

Damaschke, P. (2002) 'Online strategies for backups', *Theoretical computer science*, 285(1), 43–53.

Fernando, N., Loke, S.W., Rahayu, W. (2013) 'Mobile cloud computing: A survey', *Future Generation Computer Systems*, 29(1), 84–106.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P., Wetherall, D. (2009) 'When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1993–2002, available: http://dl.acm.org/citation.cfm?id=1519004 [accessed 01 Apr 2016].

Odom, W., Zimmerman, J., Forlizzi, J. (2011) 'Teenagers and their virtual possessions: design opportunities and issues', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1491–1500, available: http://dl.acm.org/citation.cfm?id=1979161 [accessed 05 Apr 2016].

O'Hara, J. (2012a) 'Online Data Backup (2012)', available: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=1122&context=utk_mtastech [accessed 05 Apr 2016].

Sun, D., Chang, G., Sun, L., Wang, X. (2011) 'Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments', *Procedia Engineering*, 15, 2852–2856.

Toka, L., Amico, M.D., Michiardi, P. (2010) 'Online data backup: A peer-assisted approach', in *Peer-to-Peer Computing (P2P), 2010 IEEE Tenth International Conference on*, IEEE, 1–10, available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5570003 [accessed 05 Apr 2016].

Traeger, A., Joukov, N., Sipek, J., Zadok, E. (2006) 'Using free web storage for data backup', in *Proceedings of the Second ACM Workshop on Storage Security and Survivability*, ACM, 73–78, available: http://dl.acm.org/citation.cfm?id=1179574 [accessed 10 Mar 2016].

9. Appendices

9.1 Initial Survey Questions

1. **How many years of computer use do you have?**

2. **How knowledgeable do you consider yourself about using computers?**

   Not knowledgeable 0-10 Very knowledgeable

3. **What type of computer is this main device?**

   Personal Desktop, Personal Laptop, Work Desktop, Work Laptop, Other

4. **Do you have a backup strategy in place?**

   Yes, No, Don't know

   a. **If yes, do you use the following?**
      Software Automation, Manual Backup, Other

5. **How often do you backup your main computer?**

   Daily, Weekly, Monthly, Don't Know Other

6. **Which of the following do you use to backup data?**

   External Hard Drives/USBs, CDs/DVDs, Cloud Storage, Email, Company/College Drive, Other

7. **What data do you backup?**

   Personal data, Professional data, System files, Software, Other

8. **Have you ever experienced important data loss?**

   a. **If yes, what data type was lost?**

      Pictures, Video, Other Media, Documents, Program Files, Contacts, Other

   b. **How did you lose data?**

Virus, Hard Drive Failure, Theft, Accident, Other

9. What are you most worried about losing on your computer?

10. Could you restore important data if you lost it now?

Yes, Not the most up to date version, No, Don't know

11. Do you own a Smart Phone?

a. If yes which of the following do you backup?

Everything Contacts, Apps, Messages, Photos, Documents, Videos, Email, Other

b. Where do you store backups of this data?

Phone Storage (SD Card), Cloud, Other

12. Do you own a Tablet Computer?

a. If yes which of the following do you backup?

Everything Contacts, Apps, Messages, Photos, Documents, Videos, Email, Other

b. Where do you store backups of this data?

Phone Storage (SD Card), Cloud, Other

13. Do you use Cloud Storage?

a. **If yes, is this important data?**

Yes, No, Don't Know

b. **If yes, how much data do you estimate you store there?**

0-20%,20- 40%,40%-60%, 60%-80%,80%-100%

14. How do you rate your current backup strategy?

Very Poor 0-10 Excellent

9.2 Final Survey Questions

1. **What age group do you belong to?**

   Under 20

   20 – 29

   30 – 39

   40 – 49

   50 – 59

   60 plus

2. **How would you rate your computer knowledge?**

   Very Poor 0-5 Excellent (Scale)

3. **Do you have a backup strategy in place?**

   Yes/No/Don't Know

4. **Have you ever tested your backup strategy?**

   Yes/No

5. **Which of the following devices do you use?**

   Computer/Laptop

   Smartphone

   Tablet

   None of these

   Other

6. **What data do you consider to be important?**

   Personal Data (e.g. Pictures, Videos, Sensitive Data)

   Professional Data (e.g. Files, Documents, College Work)

   System or Program Files (e.g. Operating Software, Other Software)

   Contact Details

   Emails

   None

7. **What data do you backup?**

   Personal Data (e.g. Pictures, Videos, Sensitive Data)

   Professional Data (e.g. Files, Documents, College Work)

   System or Program Files (e.g. Operating Software, Other Software)

Contact Details

Emails

None

8. **Have you ever experienced important data loss due to any of the following?**

   Computer Viruses

   Hard Drive Failure

   Device Failure

   Physical Theft

   Online Theft

   Accident

   Never Lost Data

   Other

9. **Do you use any of the following backup options?**

   Free Cloud Storage

   Paid Cloud Storage

   External Hard Drives

   USBs/Memory Sticks

   Backup Utilities (e.g. Time Machine, Windows Backup and Restore)

   None of these

   Other

10. **How much important data do you estimate you store in the cloud?**

    0%

    25%

    50%

    75%

    100%

11. **Do any of the following impede your ability to backup your data?**

    Cost

    Time

    Lack of Knowledge

    Convenience

12. On average, how often do you backup your data?

Daily

Weekly

Monthly

Yearly

Never

13. How do you rate your current backup strategy?

Very Poor 0-5 Excellent (Scale)

9.3 Participant Information Sheet

INFORMATION SHEET

Dear Participant

My name is David Leen and I am currently undertaking a Final Year Project at the University of Limerick under the supervision of Brian Fitzgerald. The title of my proposed research is "Adequacy of Computer Back up Strategies". The purpose of this project is to undertake a study of available backup options and conduct a survey into the extent of actual use of these options by the technically literate and those not so. It will also evaluate the adequacy of the various strategies being used.

Participants will be expected to complete a survey by answering a series of questions relevant to this research. This research does not require personal details or even names; it is conducted to assess the adequacy of computer back up strategies of different people. By clicking on the link and completing the survey, you the participant have agreed to give your consent. The information will be collected online through Google Forms. This information will be stored securely.

You can withdraw from participation at any time during the survey for any reason. The survey should take no more than five minutes to complete. However you are not obliged to participate in this research.

If you have further questions regarding this research please feel free to get in touch with either myself or my supervisor using the email addresses listed below.

If you have concerns about this study and wish to contact someone independent, you may contact: The Chair, Faculty of Science & Engineering Research Ethics Committee, University of Limerick, Limerick. Tel: 061 202802

Yours sincerely,
David Leen

David Leen
Researcher
Digital Media Design
Email: 12040193@studentmail.ul.ie

Brian Fitzgerald
Supervisor
Email: Brian.Fitzgerald@ul.ie