Is End User Feedback Considered During the Development of Information Security Policy?

David O’Shea
Robert David Stanley
Barbara - Justyna Pudlowska Pires

Monday 23rd of March 2015
Acknowledgements

As a team and as individuals we would like to thank the following people for their support, guidance and assistance during the course of this project.

• Kevin Foley Our Project Supervisor, for sharing his time, knowledge and direction which helped during this research project.

• Dr. Simon McGuiness Our Course Co-ordinator, for providing the challenge of this project and his continued support throughout.

• The interviewees and survey respondents, for taking the time to contribute to this project which provided a wealth of valuable information.

• Our families and friends for their unwavering patience and support throughout the course of our studies.
Permission to lend or copy

The team agrees to grant permission to the School of Computer and Statistics of Trinity College Dublin to retain an electronic version of this dissertation document and may lend copy or publish this dissertation document for the purpose of study and research.

______________________________
Signed - Barbara - Justyna Pudlowska Pires

______________________________
Signed - David O’Shea

______________________________
Signed - Robert David Stanley
Declaration

The team submitted this dissertation as part of requirement of final college year for the degree of B.Sc. (Hons) in Information System, Trinity College Dublin.

The team declare that the work in this dissertation is completely our own work, except where otherwise stated. It has not been submitted before as course work or a degree at this or any other university and has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics, Trinity College Dublin.

Submission date: 23rd March 2015

________________________________________
Signed - Barbara - Justyna Pudlowska Pires

________________________________________
Signed - David O'Shea

________________________________________
Signed - Robert David Stanley
Abstract

The purpose of this research project work was to conduct research into the main objective of this study “Is end user feedback considered in the development of Information Security Policy?” The research analyses if engaging with end users and collecting feedback through the development process has any benefit to the organisation and policy documents created and, if so, would this lead to an improvement in productivity and efficiency?

During the research team also looked at the value of end user feedback collected during the process of policy development and to what extent employees are aware of Information Security Policy in their organisations. A number of business reports highlight that there is an increase in the occurrence of cybersecurity incidents especially in the areas of misuse of policy, process and the misunderstanding of end users responsibilities within organisation. In the Global State of Information Security Survey 2015, PWC identified that security incidents caused by insiders are more costly and damaging compared with that of incidents caused by outsiders.

The risk of insiders is related to organisations failing to regularly update their documentation. Furthermore, processes that support day to day activities are not accurately updated and reflected within policy. Most importantly, end users are not well trained and engaged in the process of information security awareness and training. This research aim is to investigate if end users should be involved in the development process of Information Security Policy and to what extent, if any, end user feedback should be considered at any stage throughout the development phase. (PriceWaterhouseCooper 2015a)

To answer the main question of this study and all supporting questions, a review and full analysis has been conducted of existing secondary data in the form of literature review. To collect primary data, interviews and a survey of Information Security Policy were conducted. The main purpose of the literature review was to support the assumption of the team with relation to gaps identified within development process of Information Security Policy with a focus on end user feedback being not considered at any level.

The survey targeted variety of different business sectors and all type of users: Management, IT and End Users via LinkedIn groups and by distribution amongst our work colleagues. Interviews were primarily focused on Senior Management to understand their perspective. These methods provided the primary data for this study activity.

The research study explored that majority of end users are not participating during the development process of Information Security Policy, and also that there is no formal feedback process implemented in their organisations. Information Security Policy is becoming a mandatory framework for businesses. Processes supporting policy documentation are approved by managers and not necessarily implemented to suit the business needs but based on influence from outside. All declared information has been supported by secondary data findings from the literature review.

Information Security Policy drives end users behavioural adoption within organisational processes. It is very important that end users are engaged throughout the process of development and implementation of Information Security Policy.
# Table of Contents

Abstract .......................................................................................................................... 5

1. Introduction .................................................................................................................... 1
   1.1 Background .................................................................................................................. 2
   1.2 Objective ..................................................................................................................... 3
   1.3 Rationale ..................................................................................................................... 4
   1.4 Chapter Overview ...................................................................................................... 5

2. Literature Review ........................................................................................................... 6
   2.1 Introduction ................................................................................................................ 6

3. Methodology .................................................................................................................. 21
   3.1 Introduction ................................................................................................................ 21
   3.2 Multi-methodology Strategy ..................................................................................... 21
   3.3 Data Collection .......................................................................................................... 22
   3.4 Population / Participants ......................................................................................... 23
   3.5 Generating the survey and interviews ...................................................................... 25
      3.5.1 Self administrative survey ................................................................................... 25
      3.5.2 Implementing Survey ......................................................................................... 26
      3.5.3 Interview Methodology ....................................................................................... 26
   3.6 Conducting the Interview ......................................................................................... 28
   3.7 Secondary Data ......................................................................................................... 30
      3.8.1 Ethical Approval .................................................................................................. 30
      3.8.2 Ethics Issues ....................................................................................................... 31
   3.9 Data Protection .......................................................................................................... 31

4. Findings and Analysis .................................................................................................... 32
   4.1 Introduction to Findings and Analysis....................................................................... 32
   4.2 Participants response rate ......................................................................................... 33
   4.3 Data validation ............................................................................................................ 34
      4.4.1 Organisations questions ...................................................................................... 36
      4.4.2 Information Security Policy Awareness ............................................................... 37
      4.4.3 Information Security Policy and behavioural factors ........................................... 38
      4.4.5 Information Security Policy: Implementation process ....................................... 41
   4.5 Survey Open Questions Analysis .............................................................................. 44
   4.6 Interviews questions analysis .................................................................................... 47
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7</td>
<td>Summary of Data Findings and Analysis</td>
<td>48</td>
</tr>
<tr>
<td>5</td>
<td>Conclusion</td>
<td>51</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>51</td>
</tr>
<tr>
<td>5.2</td>
<td>The Research Question</td>
<td>52</td>
</tr>
<tr>
<td>5.3</td>
<td>Research Impacts</td>
<td>53</td>
</tr>
<tr>
<td>5.4</td>
<td>Possibility of Future Research</td>
<td>54</td>
</tr>
<tr>
<td>A.1</td>
<td>Survey &amp; Interview Questionnaires</td>
<td>58</td>
</tr>
<tr>
<td>A.1.1</td>
<td>Information Sheet for Prospective Participants</td>
<td>58</td>
</tr>
<tr>
<td>A.1.2</td>
<td>Informed Consent Form</td>
<td>59</td>
</tr>
<tr>
<td>A.1.3</td>
<td>Declaration</td>
<td>59</td>
</tr>
<tr>
<td>A.2</td>
<td>Statement of Investigators</td>
<td>60</td>
</tr>
<tr>
<td>A.3</td>
<td>Information Security Policy</td>
<td>61</td>
</tr>
<tr>
<td>A.4</td>
<td>Interview Questions</td>
<td>66</td>
</tr>
</tbody>
</table>
Table of Figures
Figure 1 - Kaspersky Labs average cost of cyber security incidents .......................................................... 10
Figure 2 - PCI Depth of Security Awareness ............................................................................................... 14
Figure 3- PCI Security Awareness Roles ..................................................................................................... 15
Figure 4 - PCI Security Awareness Program Record Template .................................................................. 16
Figure 5 - PCI Security Awareness Program Record Template .................................................................. 16
Figure 6 - PCI Security Awareness Program Record Template .................................................................. 17
Figure 7 - PWC Report Displaying IT Budget Decreases .......................................................................... 18
Figure 8 - PWC responses to survey asking sources of incidents (Insiders vs Outsiders) ....................... 19
Figure 9 - Formula for calculating sample size ......................................................................................... 24
Figure 10 - Data validation responses ......................................................................................................... 34
Figure 11 - Responses by Business Sector .................................................................................................. 36
Figure 12 - Responses by role in the organisation ...................................................................................... 37
Figure 13 - Information Security Policy decision results ............................................................................. 38
Figure 14 - Information Security Policy Awareness methods ....................................................................... 39
Figure 15 - Areas covered by Information Security Policy documentation ............................................... 40
Figure 16 - Cyber Security Threats Prevention ............................................................................................ 40
Figure 17 - Acceptance of Information Security Policy .............................................................................. 41
Figure 18 - PWC Report three areas to consider ......................................................................................... 42
Figure 19 - Evaluation of quality and effectiveness of Information Security .................................................. 43
Figure 20 - Measures taken to increase the efficiency of Information Security Policy ............................... 44
Figure 21 - Opinions of improvement on improvement of Information Security Policy ............................... 45
Abbreviations

CEO  Chief Executive Officer
CIO  Chief Information Officer
CISO  Chief Information Security Officer
COBIT  Control Objectives for Information Technology
CSFI  Cyber Security Forum Initiative
E&Y  Ernst and Yung
FFIEC  The Federal Financial Institutions Examinations Council
FISMA  Federal Information Security Management
HIPAA  Health Insurance Portability and Accountability Act
I.T.  Information Technology
ISACA  The Information Systems Audit and Control Association
ISO  International Organisation for Standardization
IEC  International Electro technical Commission
ISPA  Information Security and Privacy Awareness
NIST  National Institute of Standards and Technology
PC  Personal Computer
PCI  Payment Card Industry
PWC  PricewaterhouseCooper
SANS  United States Institute specialized in Information Security & Cybersecurity training
SCSS  School of Computer Science and Statistics
SME  Small Medium Enterprises
TCD  Trinity College Dublin
USB  Data Storage Device with an integrated Universal Serial Bus
1. Introduction

“You can’t hold firewalls and intrusion detection systems accountable. You can only hold people accountable.”

Daryl White, DOI CIO

This research project asks the following question:

“Is End Users feedback considered prior to Information Security Policy implementation?”

To answer this question, the project team decided upon a mixed-methodology approach. This consisted of three main research methods; literature reviews, surveys and interviews. The research methods chosen allow for both qualitative and quantitative data analysis. This approach combines the respective strengths of both methodologies providing more in depth analysis. (Tashakkori & Teddlie 1998)

Based on the professional experience of the team, the initial assumption was feedback was not widely considered prior to or following policy implementation. The literature review expands upon this in Chapter 2 and considers the various aspects of Information Security Policy and the international standards that can apply.

The research considers the end users perception and opinion on Information Security. It is necessary to understand the awareness of Information Security by the user and what level of involvement, if any, they had in the creation of Information Security Policy. This is central to understanding the role of end user feedback in policy implementation. In scenarios where feedback exists, it’s important to understand how formalised the process is and the benefit it offers.

Due to the significant increase in cyber security incidents attributed to insiders (PriceWaterhouseCooper 2015b) the research looks at the impact Information Security Policy has on end user behaviour. The research focuses on the importance of developing Information Security Policy with the consideration of end user behaviour and then aligns this with the risk of ignoring user feedback. The team develop this further by investigating if this is the result of the hierarchical culture prevalent in most organisations. (Atkinson 1997)

The aim of the survey was to target as many end users as possible. Of the respondents, 62% were not part of management. The team considered this response rate satisfactory given the scope of the project. The survey evaluates the opinion of users on various facets of Information Security and Policy implementation. Some of the key areas addressed focus on the awareness of Information Security and understanding the value of Information Security Policy. It’s also important
to understand the policy delivery methods and level of success users attributed to each delivery method.

The team analysed the data received from surveys and interviews to provide insight into why Information Security Policy is created and the methods used to educate users on the importance and necessity of such policy. Regarding the collection of feedback on Information Security Policy, 37% of respondents stated no form of feedback is collected. When feedback is not considered prior to or following policy implementation it is difficult for an organisation to ascertain how successful the implementation has been or the level of adoption of Information Security Policy by end users. All of this contributed to the conclusions found in Chapter 5.

1.1 Background

Information Security awareness stretches back to the 1960s with the realisation that sensitive information stored on computers could potentially be accessed by unintended persons. The idea that a computer could be a medium for theft developed throughout the sixties with people finding new ways to compromise computers to the point where they could steal or corrupt data. Such vulnerabilities lead to the development of computer espionage. In 1970, Gerhard Prager, an IBM employee in West German, was caught copying magnetic tapes and then passing them on to the Ministerium fuer Staatssicherheit, the State Security of East Germany. (Macrakis 2008)

The vulnerability of computers lead to innovation and development focusing on the improvement of computer security. This resulted in the development of protective measures such as assigning administrative privileges, file systems permissions and hashed passwords. Encryption of data transfers developed which lead to the implementation of published encryption standards. (Warner 2012)

The development of the Internet led to a global network of computers all with the potential to be the victim of remote intrusion. While the initial concern for compromised computers was the theft of sensitive information, the potential consequences of computers being manipulated to operate in unintended ways were fully understood after events in November 1979. This was the result of when the North American Air Defence Command (NORAD) reported that thousands of missiles had been launched by the Soviet Union. Operators assumed this was a real attack, however it was simply the result of a test program which simulates an attack loaded into the system. An act of human error could have realistic resulted in a world war and as such highlighted the potential of manipulated computers (Gates 2007)

Throughout the eighties and nineties the occurrence of cyber security incidents increased and cyber warfare developed into military application. With the increased sophistication of attacks, there were equally sophisticated countermeasures developed in an effort to inhibit the risk of such
attacks. Regardless of the sophistication of the security technology employed by an organisation or government, the human factor remains the weakest link in a security chain.

The creation and implementation of Information Security Policy is necessary to ensure an organisation's confidential information is protected from theft or unauthorised access from nefarious third parties. While Information Security Policy is used first and foremost to protect an organisation, it also often encompasses a legal requirement to protect the privacy of employees and clients. The policy includes the governance of IT, the roles and responsibilities of IT Management, provides risk assessment and sets compliance standards for staff. Information Security Policy should be considered a necessity for any organisation with an online or technological footprint.

1.2 Objective

The primary objective of this research project is to understand how the End User is engaged in Information Security Policy and to ascertain the value of End User feedback to the implementation process. To address this, various aspects of Information Security were taken into consideration. Assessing the roles of both insiders and outsiders in relation to Information Security is important to understanding the threat of cyber security incidents. This is also factors into user behaviour which can help shape the best methods for policy implementation.

The team also looks at the potential of having a formalised feedback tool for Information Security Policy. By having a formal feedback tool in place, the impact of policy implementation on the end user can be appropriately captured which could potentially lead to amendments promoting productivity and a better working environment. The research also looks at the hierarchical culture found in organisations. It was important to understand the nature of top level management in the development of Information Security Policy. Is it a case of feedback being provided but dissolving in the leadership chain such that it can never have a meaningful impact?
1.3 Rationale

Information Security Policy impacts almost every person in the developed world either directly or indirectly. Information Security Policy directly impacts any employee who must abide by such policy ensuring the integrity of any sensitive data stored by their organisation. Information Security Policy affects almost every other person indirectly. People who have bank accounts, shop online or have their personal information stored in a database by their government are all indirectly impacted by Information Security Policy.

Given the global impact of such Information Security Policy, the team considered their professional experiences dealing directly with Information Security Policy. Past experience indicated that often, even when training is involved, the implementation process is more of a formality where the employee must signify their approval and understanding rather than a chance to educate the user to the value of Information Security Policy. This is supported by a study conducted by Enterprise Management Associates which surveyed over 600 respondents from a variety of organisations on Security Awareness Training. One of the most alarming findings from this survey is that “more than 56% of personnel, excluding security and information technology staff, had not receive security awareness training from their organisation.” (Monahan 2014)

“Actions that are taken by individual end-users the networks and devices we use, the files we send and receive, the apps we install and run, the links we click on, the emails we open are behaviours that result in a high percentage of security infections. Aberdeens Monte Carlo analysis quantifies the positive impact of investments in user awareness and training: by changing user behaviours, it reduces security-related risk by about 60%” (Brink 2014). The lack of security awareness training has a significant impact on user behaviour and reduces the effectiveness of Information Security within an organisation.

Research from the literature review identified a gap where there was minimal research previously conducted on Information Security Policy implementation, namely where feedback is considered. The team agreed to focus on the impact of feedback in the process of Information Security Policy implementation. It is assumed that a formalised feedback process could have a positive impact on the creation of Information Security Policy aligned to user behaviour as a result improving information security awareness. Such a process would also be beneficial post implementation for gauging the understanding and acceptance of Information Security Policy. The additional aim of this research is to conclude with suggestions which may improve the Information Security Policy implementation process.
1.4 Chapter Overview

Chapter 1: Introduction This chapter provides some background information and highlights the overall objective and the nature of the research.

Chapter 2: Literature Review This chapter focuses on the findings from the literature review which support the research conducted into Information Security Policy and the overall objective of the research project.

Chapter 3: Methodology This chapter describes the multi-methodology approach that was taken and the rationale for the research methods chosen.

Chapter 4: Findings and Analysis This chapter presents analysis of the primary and secondary data collected from the research.

Chapter 5: Conclusions This chapter provides the conclusions from the project and addresses the question posed by our research objective.
2. Literature Review

2.1 Introduction

The team reviewed a number of journals, articles and papers in order to identify areas that may not have been considered in the world of Information Security Policy decision making and implementation within organisations across a broad spectrum of industries. We also reviewed published surveys from websites such as Deloitte, PWC and Kaspersky Labs. Some of the articles will be included in the Lit Review section, while we also found some of the information learned from articles useful to support our findings from the methodology.

During the literature review we have sought to find some key information regarding users within organisations and whether or not their feedback is considered towards the formulating and implementing of Information Security Policies. In order to gain as much of an understanding as possible and see if we could identify a research subject of relevance within the timeframe of completing this research project; we identified some key areas to focus on. This report attempts to show a correlation between Information Security policies of organisations implementation and how the lack of involvement of users in that process is having in some cases, financial implications. Our hypothesis is during the implementation of Information Security policies, that end user feedback should be considered.

During the implementation of Information Security policies, should end user feedback be considered?

We needed to have a broad scope of literature researched in effort to build a strong foundation in order to form our thesis question. The more we analysed the literature that was available the more it was made easier for the team to identify the lack of previously conducted research that has led to the question regarding end user feedback consideration while creating and implementing Information Security Policies. To display the journey we took with the literature, we have separated those findings into the following sub sections within the Literature Review main section.

Where do Information Security Policies come from?

- Why it is important for organisations to implement Information Security Policies aimed at end user behaviour?
- Are Information Security Policies only for IT business sectors?
- Who is making the decisions when creating Information Security Policies?
- How are the policies being implemented by organisations?
- Is user feedback considered while creating or implementing Information Security Policies?
Where do Information Security Policies come from?

In this section we will discuss where Information Security Policies come from, or at least where some of the most industry standard recognised templates come from, which organisations can base their own policy upon. A description of the International Organization for Standardization (ISO) is given, followed by an example of recommendations of a Security Policy template for organisations. We note some differences in the policies and also some gaps that may be occurring across multiple organisations while creating their policies.

The International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) “define the basic procedures to be followed in the development of international Standards and other publications” (ISO 2015). It must be pointed out that these standards are voluntary and not mandatory. It is possible that the standards may become a requirement within the Information Security market at some future stage. The ISOIEC standards are referenced many times when reading literature regarding Information Security Policies.

The ISO creates Information Security Management Policy documents in which there have been several released such as:

ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirements (ISO 2013a)

At the time of writing this Literature Review the price for viewing these policy documents was €75 each and therefore reviewing these policies was beyond the scope of our research. There is an organisation called Praxiom Research Group Limited that describes their solutions as “ISO management standards translated into plain English” (Praxiom 2015). Contained within these policies are recommendations that Information Security Management Policy documents should contain the following a number of areas, for example “Asset Management”, “Physical and environmental security” and “Systems acquisition, development and maintenance”. The one policy mentioned within ISO/IEC 27001:2013 our team was concerned with, was the “Information Security Policies”, section 5.2.
5.2 Establish an information security policy

- Establish an information security policy for your organization
- Make sure that your information security policy is appropriate and supports your organization's purpose
- Make sure that your Information Security Policy either includes security objectives or can be used to establish these objectives
- Make sure that your information security policy makes a commitment to comply with all relevant Information Security requirements” (Praxiom 2015)

Many organisations will use the ISO/IEC standards as a template for composing their own policies which suits their own specific needs. Some organisations will mention that they are compliant or using the ISO/IEC standards as a template, while others will not.

One such policy template that does not mention ISO/IEC is “Building and Implementing an Information Security Policy” by the SANS Institute (Elmy-Liddiard 2002). At the beginning of the SANS Institute template they mention “A policy implemented without support may be seen as:

- A waste of space
- An attempt by I.T. departments to gain/enforce control
- A matter for I.T. and of no real relevance to non-I.T. staff” (Elmy-Liddiard 2002)

This was interesting as it would lead us to conclude that with the creation of the Information Security Policy they are recommending an all-inclusive acceptance. While researching this paper there was no mention of speaking with users when formulating the policy or receiving any feedback, however it does mention when defining standards that “Your standards should not be set in stone. They must be able to be challenged, reviewed and changed as your organisation’s requirements change, as long as the potential risks of any change are made clear to your organisation and said risks are accepted or mitigated.” (Elmy-Liddiard 2002).

The paper also discusses that in order to get a policy approved, it must be done so through the organisation’s board of management. Curiously, they advise the Information Security Policy creators to get all relevant information on composing the policy from areas such as Information Security websites, CISO colleagues from other businesses and other external sources (Elmy-Liddiard 2002). What was interesting is the advice to collect all relevant and necessary information for the policy creation from external sources and no mention of a collaboration or information seeking from within an organisation. This advice possibly causes a paradox regarding the ISO/IEC recommendations of “Establishing an Information Security Policy for your organisation” (Praxiom 2015). The paradox being that one is recommending it for an organisation (Praxiom 2015), while the other is recommending applying standards based on what everyone else is doing (Elmy-Liddiard 2002).

In the creation of the Information Security Policy in the example given by SANS Institute, all the decision making and creation was made at senior management level. CISO would approach
the board for approval of the policy. CISO would then compose the policy based on external existing policies and apply what they believed to be relevant to their own organisations. In the creation of the Information Security Policy for the US Government with regards to FISMA, it is done by Congress, National Agency Heads, Chief Information Officers and Senior Agency Information Security Officers. It is all senior management who consult with NIST on the requirements (National Institute of Standards and Technology 2013).

Why it is important for organisations to implement Information Security Policies aimed at end user behaviour?

In 2013 PWC released a report that claimed 80% of CEO’s would not be properly prepared to deal with a substantial cyberattack, if one were to occur against their organisations (PriceWaterhouseCooper 2013). Now in 2015 another report has been released in which the cost and the frequency of incidents are increasing, while the budget that IT departments are spending on their Information Security is decreasing.

As of September 2014, detected cybersecurity incidents have increased by 66% to nearly 43 million incidents per year since 2009. 32% of respondents claimed that incidents caused by insiders were more detrimental and harmful to an organisation than incidents caused by outsiders (PriceWaterhouseCooper 2015b). If cybersecurity incidents are increasing in cost and frequency, yet the budgets for one of the first line defences against such incidents are decreasing, it does beg the question of who is deciding on these particular policies, if in practical terms it may not seem to make logical sense. Reducing budget would be justified if organisations were confident that the information security policies they have in place are actually preventing, or at least reducing the opportunity for breaches, yet the evidence would seem to dispute this.

There is a real and serious cost from cybersecurity incidents for both large organisations and SMEs. In 2014 Kaspersky Labs released the findings of a survey they conducted from 3,900 respondents in 27 different countries. 2011 was the first time the survey was conducted. It found that nearly 27% of the companies lost confidential data due to an internal security incident. 19% of companies reported that they experienced data lost through the misplacement of devices by staff. It found that cyber security incidents damages can cost more than companies set aside for data security. The average cost of these incidents range from $649,000, while SMEs average $50,000. 29% of respondents said that staff were to blame for accidental leaks of data incidents, most of which was due to employees not familiar with Information Security Policies within those organisations (Kaspersky Lab 2014). The market value of a company can drop once the public become aware of an incident, as was the case with Choicepoint in 2005. Their stock price dropped nearly 20% after an incident where criminals accessed 163,000 consumer credit reports. The company was also fined $15 million, which was out of an earnings of $143 million. The average reported cost of incidents is $2.7 million, however the frequency of incidents that cost over $20 million has nearly doubled (Liginlal et al. 2009). Information Security Policies should be aimed at end users because end users are expensive when they do not follow policies.
Do Information Security Policies only affect end users within the IT business sector?

“No matter how large or small your company is, you need to have a plan to ensure the security of your information assets” (Gupta & Sharman 2012). An Information Security Policy is also not only applicable to the size of an organisation, it is applicable to every sector. When first identifying the general area of research as "Information Security", the team thought that mainly applied to the Information Technology (IT) sector. IT is probably the first sector that comes to mind when mentioning Information Security Policies, however while researching the topic, it was apparent that Information Security Policies apply to many industries and organisations of every size, large and small. This was beneficial as we realised the survey methodology to gain further understanding of our thesis topic could gain more information from multiple business sectors.

“Every employee needs to be aware of his or her roles and responsibilities when it comes to security. Even those who don’t even touch a computer in their daily work need to be involved because they could still be targeted by social-engineering attacks designed to compromise your physical security.” (AppliedTrust 2008). A company that has an Information Security Policy may also need to “comply with one or more standards defined by external parties”. We previously mentioned ISO standards and further on mention FISMA, who the United States Government use for their standards. There is the HIPAA: Health Insurance Portability and Accountability Act (HIPAA, Department of Health (HIPAA) 2015) which sets the standards that are applied in the United States.
for patient information within the medical sector. There is also the Payment Card Industry (Security Awareness Program Special Interesting Group PCI Security Standards Council 2014), which set the standards for the credit card sector.

Government Sector

The United States Government created the Federal Information Security Management Act (FISMA) in 2002 which was created to enable all federal government sectors to apply information security management systems. As mentioned previously there are Information Security Policy standards ISO/IEC and in the United States when composing the Federal Information Security Management Act, they utilised National Institute of Standards (NIST) accreditation for agreeing standards (National Institute of Standards and Technology 2013). FISMA is a thorough policy that is composed for states to follow. Even though such thorough policies are in existence does not mean incidents do not occur. Some examples of incidents occurring are from users within Government organisations mentioned in the paper “How Significant is Human Error as a Cause of Privacy Breaches” include when Homeland Security collected more data than was intended of airway passengers and also when the Ohio Secretary of State posted names and the dates of birth of citizens on their webpage (Liginlal et al. 2009). We are referring to workers within Government as the end users due to the context of Information Security Policies applying to those.

Financial Sector

The Federal Financial Institutions Examinations Council (FFIEC), which is the body that is “empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions” (FFIEC 2015) created an Information Security Policy for financial institutions within the United States (FFIEC 2006). This policy is created using models the National Institute of Standards and Technology (NIST), The Code of Practice for Information Security Management ISO/IEC 17799, Information Technology-Security Techniques-Evaluation Criteria for IT Security ISO/IEC 15408, The Information Systems Audit and Control Association (ISACA) and Control Objectives for Information Technology (CobIT) (FFIEC 2006).

Who is making the decisions when creating Information Security Policies?

“Information security is a significant business risk that demand engagement of the Board of Directors and senior business management” (FFIEC 2006). As the quote from the Information Security Policy of FFIEC states, it is the Board of Directors and senior business management for example the CEO, Directors and CISOs who make the decisions that affect all users within their respective organisations. In this section we use The Federal Reserve in the United States as analysis of literature released through their website such as the minutes of meetings, interviews and the Information Security Policy that they apply to their organisation.

An example can be the Information Security Committee of the Federal Reserve Division of Information Technology. This is the name of the committee for the Information Security within the Federal Reserve. Sharon L. Mowry who was appointed Chief Information Officer of the Federal
Reserve in April 2012 also sits on the boards of directors within the Federal Reserve. The Information Technology board consists of 17 people including the CIO. They are:

- Sharon L. Mowry, Director Chief Information Officer
- Wayne A. Edmondson, Deputy Director
- Lisa M. Bell, Associate Director
- Raymond Romero, Associate Director
- Kofi A. Sapong, Associate Director
- William K. Dennison, Deputy Associate Director
- Glenn S. Eskow, Deputy Associate Director
- Marietta Murphy, Deputy Associate Director
- Kassandra A. Quimby, Deputy Associate Director
- Sheryl L. Warren, Deputy Associate Director
- Rajasekhar R. Yelisetty, Deputy Associate Director
- Can Xuan Nguyen, Assistant Director
- Theresa C. Palya, Assistant Director
- Virginia M. Wall, Assistant Director
- Edgar Wang, Assistant Director
- Charles B. Young, Assistant Director
- Tillena G. Clark, Adviser

The occasions in which the board meet take place approximately eight times per year minutes for the meetings are released on the Federal Reserve website. According to the Federal Reserve Information Policy document the Information Security Committee should present written reports on the “effectiveness of the information security program at least annually”. Due to the restriction on resources during the research of this Literature Review section, our findings covered the period from 2012 to 2015 by analysing the publicly released minutes of the board meetings. Out of all the minutes during that period, we found only one instance where Information Security Policy was discussed at board level. That occurred on January 28th and 29th 2014. During that meeting the particular Information Security Policy approved was:

“By unanimous vote, the Committee amended its Program for Security of FOMC Information with minor changes to the review and reporting process for breaches in the information security rules and with several other minor updates and clarifications.” (Bernanke et al. 2014)
No member of the Information Technology committee has attended any of the committee meetings for the period of 2012 to 2015. Granted, there must be written reports sent to the board in order for approval or rejection, however the only time Information Security Policy change was discussed at board level was in January 2014.

Some questions arise from the, albeit limited analysis. Was an informed decision made if there was no member of the Information Security Committee in attendance? Was this amendment made to the Information Security Policy in response to any incident that may have occurred with regard to the “reporting process for breaches in the information security rules” (Bernanke et al. 2014)? At no point in the Information Security Policy is there a mention of inclusion of end user feedback in compiling information Security Policies, the only mention is of the CIO interacting with the Board of Directors. There may very well be a need for independence of the CIO from the Board of Directors and therefore no need for the CIO to attend the boardroom meetings. Should this be the case?

**How are the policies being implemented by organisations?**

Users that work in organisations of all sizes would most likely be familiar with Information Security Policy restrictions within their organisations, from no internet access, no USB peripheral access to the blocking of certain email attachments and having multiple passwords to access certain servers or locations within an organisations network. There must also be a mention also to users of PC, Laptop or smartphone device usage that would serve to reinforce the organisations Information Security Policy.

**Industry Recommended Template for implementing Information Security Policies**

All users should have a general security awareness. Across multiple research papers is the conclusion that users are the biggest threat to an organisation. “One of the biggest risks to an organization’s information security is…the action or inaction by employees and other personnel that can lead to security incidents”. A minimum security awareness should be recommended, “including formal training, computer based training, e-mails and circulars, memos, notices, bulletins, posters” (Security Awareness Program Special Interesting Group PCI Security Standards Council 2014).
This “threat” is addressed through communication, training and awareness by users, from either training programs, online tutorials, informational emails or company bulletin boards etc. All communications are one way, from the managers or the security awareness teams to the users. Using as an example, PCI Best practices for implementing security awareness where they advise a training awareness program may include “assembling a security awareness team, role-based security awareness, metrics, appropriate training content, and communications of security awareness within the organization”(Security Awareness Program Special Interesting Group PCI Security Standards Council 2014).
Figure 3- PCI Security Awareness Roles

PCI recommend any training awareness program that is created to use as reference the resources below:


The above are all industry standards, some of which we have mentioned previously in this chapter. Some examples of training material or suggestions are also supplied as you can see below.
### Figure 4 - PCI Security Awareness Program Record Template

<table>
<thead>
<tr>
<th>Sample Activity</th>
<th>Implementation Notes</th>
<th>Frequency</th>
<th>PCI DSS Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify methods for creating security awareness materials:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classroom training:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Consider third-party on-site training.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security Awareness Training team conducts training.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer-based training:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Also consider having a third party who has PCI experience train personnel.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Websites for training information—e.g.,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poster campaigns:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Display posters in break rooms and other employee areas.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Newsletters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Publish employee newsletters highlighting PCI DSS security and how it applies to the employees.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail communication:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• E-mails can be used to remind employees about security requirements responsibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen savers:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Screen savers can be used to remind employees to log off computers when away from their workstations and other useful security information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security meetings / roundtables / lunch-and-learn sessions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Have lunch-and-learns to discuss card data security and allow employees to ask questions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Team training:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Effectively train employees and other functions as it relates to security awareness.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The intent of this document is to provide supplemental information. Information provided here does not replace or supersede requirements in any PCI DSS standard.

### Figure 5 - PCI Security Awareness Program Record Template

<table>
<thead>
<tr>
<th>Sample Activity</th>
<th>Implementation Notes</th>
<th>Frequency</th>
<th>PCI DSS Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify methods for delivering security awareness training upon hire and annually:</td>
<td></td>
<td></td>
<td>Testing Procedure 12.6.1.b</td>
</tr>
<tr>
<td>Computer-based training:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Also consider having a third party who has PCI experience train personnel.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Websites for training information:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o <a href="http://www.mastercard.com/merchants/support/white/index.jsp">www.mastercard.com/merchants/support/white/index.jsp</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR onboarding (instructor-led training)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR onboarding (policy review and sign-off)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Team presentations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify methods for recording attendance on training:</td>
<td></td>
<td></td>
<td>Testing Procedure 12.6.1.b</td>
</tr>
<tr>
<td>Meeting agendas with attendees:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Prepare an agenda for security items to be discussed with employees.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed attendance sheets</td>
<td></td>
<td></td>
<td>Require signed acknowledgements that the employee understands and has completed security awareness training.</td>
</tr>
<tr>
<td>Sample Activity</td>
<td>Implementation Notes</td>
<td>Frequency</td>
<td>PCI DSS Reference</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------</td>
<td>-----------</td>
<td>------------------</td>
</tr>
<tr>
<td>HR onboarding checklists</td>
<td>Records of new hires requiring security awareness training.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer-based training records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure tracking and recording of who takes the training and whether it was completed successfully.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify methods for ensuring all employees attend training:</td>
<td></td>
<td></td>
<td>Testing Procedure 12.6.1.b</td>
</tr>
<tr>
<td>HR monitoring of attendance and/or checklists</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee performance reviews</td>
<td>Making security awareness part of the review process for personnel who have access to cardholder data helps ensure personnel attend training.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer-based training completion reports</td>
<td>Ability to pull reports from computer-based training that shows who took the training, date taken, pass or fail.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify methods for employees to acknowledge they have read/understood the information security policy at least annually:</td>
<td></td>
<td></td>
<td>Testing Procedure 12.6.2</td>
</tr>
<tr>
<td>E-mail acknowledgements</td>
<td>Employee e-mail acknowledgement of completion and understanding of the information security policy as proof of annual reviews.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed policies</td>
<td>Obtain signed employee acknowledgement of reading of the security policy as proof of the annual requirement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic signatures in computer-based training</td>
<td>Ability to electronically sign an acknowledgement that computer-based training has been completed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The intent of this document is to provide supplemental information. Information provided here does not replace or supersede requirements in any PCI SSC Standard.

Figure 6 - PCI Security Awareness Program Record Template

Alternatively there are companies such as Smarttech that believe in engaging with end users and increase their awareness through the Information Security & Privacy Awareness (ISPA) Program, which uses different modules including malware awareness, social engineering and phishing awareness. These training methods are aimed at engaging users in activities that would be easily understandable such as creating role playing games where the users use dummy email portals to help identify safe emails from more sinister phishing type emails.
What are the risks that organisations may be taking if they do not involve user feedback when creating Information Security Policies?

Organisations must be careful not to implement an oppressive Information Security policy as it could lead to the prevalence of “Shadow Security” within organisations. The paper discusses how, historically, Information Security policies within organisations were thought to have been either implemented or not. They believed there were only two options in relation to this. However, the paper discusses the emergence of a third option called “Shadow Security”. This describes where make use of workarounds circumventing Information Security policies that users find too restrictive in order to complete their daily tasks. These “workarounds” were something that higher management was not aware of.

The interest of this research paper was that its findings were based on interviews with users within an organisation. They found, that there was a lack of awareness amongst the employees of the security risks their actions were causing. The security policies which were implemented impeded employees work to such an extent that they felt the only workable solution was to be non-compliant with policies they were aware of. Some of the examples of user behaviour ranged from users writing down passwords, possessing a second laptop that was used to install restricted software and passwords to restricted locations not being changed after users leave the company. Users felt that any security concerns they raised were not being acted upon, to which they would act upon themselves. This in itself raises concerns as they were then acting outside of set Information Security policies (Kirlappos et al. 2014). Alternatively the Information Security personnel believed they had a good Information Security Policy by implementing security standard ISO2700, whereas those policies are created for an ideal environment that in practice does not exist. This in turn leads users adopting a non-compliant behaviour.

Figure 7 - PWC Report Displaying IT Budget Decreases

The average information security budget dipped to $4.1 million, down 4% over last year. Security spending remains stalled at only 3.6% of the overall IT budget.
Is user feedback considered while creating or implementing Information Security Policies?

In the all of the literature researched for the teams’ thesis one line of communication that is recommended countless times is from management and IT to the staff. The focus has been on management to understand and to communicate the policies of organisations to staff. A constant message has been to reinforce this message by compliance of staff to either sign non-disclosure agreements, attendance forms or for systems to be in place that confirm a user has completed their training. There are conflicting philosophies at play that we believe have identified. They are the mistrust management, Info Sec and in general IT have towards users. This mistrust is always present, no matter how well policies are communicated. Due to this mistrust we believe the majority of organisations that enforce Information Security policies, do so with one channel of
communication from the top to the bottom and little or no recommendations in any of the industry standards or practices to facilitate a channel of communication from the bottom to the top.

“Management needs to understand the organization’s security policy enough to discuss and positively reinforce the message to staff, encourage staff awareness” (Security Awareness Program Special Interesting Group PCI Security Standards Council 2014). This is in slight contrast to the paper Balancing the insider and outsider threat where they mention “Sometimes senior managers feel that their juniors never learn good habits by example; but one thing is clear bad habits are picked up immediately” (Walton & Limited 2006). There is a clear contradiction in the different philosophies here. How can management be expected to communicate to users effectively on Information Security policies if there is a clear mistrust between management towards users.

An oppressive regime must be avoided, the general atmosphere has to be one of trust but within a recognised culture of security responsibility. The message for employees needs to be you are trusted and together we need to ensure that trust is not misplaced or abused. The most important ingredient for achieving this is visible leadership from the top down (Walton & Limited 2006).

There is the paradox created by industry accepted opinions that users are the problem, whereas working with users may be the solution more so than organisations and Information Security Policy makers are willing to accept or consider. “Contradictory objectives, which are often inevitable, must be compensated for: security does not come first in end-users mind.” (Besnard & Arief 2004)

The only time we encountered “feedback” being mentioned in the literature we researched was in the paper “Balancing the insider and outsider threat”, which spoke about the period of time when users leave a company that “procedures should include an interview where the employee is reminded of his responsibilities… and given the opportunity to give feedback and discuss any security issues that concern him” (Walton & Limited 2006). This is promising, however it is as the saying goes closing the stable door after the horse has bolted. A hypothetical situation is a user is leaving the organisation because they do not like it. What type of feedback could be supplied as they are leaving the organisation. Wouldn’t it be more beneficial for the organisation as a whole to receive feedback from current users?

This is what focused the team on identifying a clear gap in the current literature and industry recommended standards, that user feedback is not being considered when creating Information Security Policies, nor is it being considered when implementing Information Security policies.
3. Methodology

3.1 Introduction

After conducting research into the plausible methodologies available for collecting data to complete the research project, many suitable methodologies were encountered for a project of this nature. We settled on three main methods we felt best allowed us to compile and analyse data. They are surveys, interviews and literature reviews. The following outlines the general approach taken by the team for research and data collection on the project. This outline will present the rational and objectives for the chosen topic and the conclusion the team arrived at.

3.2 Multi-methodology Strategy

The multi-methodology approach is one that collects data for research study work utilising more than one research methodology. In the case of this project, this is also related to the mixed methodology approach which includes both qualitative and quantitative data analysis procedures. The quantitative (statistical) method of research presents data in numerical form and it’s used within research forms such as those using questionnaires. Answers using a research technique of this nature are presented in the form of graphs or statistics, which in turn support the interpretation and organisation of data in the study. Mixed methodology improves the evaluation of analysed data by ensuring that the combination of two methods is balanced based on their respective strengths. The qualitative (non-statistical) method of research asks two main questions; why? and how? The data required for qualitative analyse is collected from techniques such as interviews or the categorisation of data. This can be presented in the form of pictures or video clips. The output of this method provides a deeper understand of survey responses and helps in the interpretation of their patterns.

Multi-method research combined of qualitative and quantitative methodologies supports the process of gaining more realistic and specific data on the subject of the research work. By using this method for a project of this nature, the big advantage over more stringent methods is the creation of a more realistic overall picture. All researches want their research to be useful, at least at some level in the real world. (O’Leary 2010). We feel our approach offers the best chance at real world relevance.

The team used this multi-methodology approach as it was agreed that both methods are appropriate for the research conducted. The primary objective of this research is to ascertain if end user feedback is gathered following the implementation of information security policy and if so, to what extent. In effort to collect the most relevant data, the focus will be on interviews and surveys. This resulted in the creation of a questionnaire for surveys and another for interviews. The team
believe the questions contained therein will allow for responses of authentic usefulness and practicality.

3.3 Data Collection

The term data collection usually refers to the process of gathering, collecting and measuring data to analyse the outcome from various sources. Data is collected for specific purposes, such as with this case research focusing on the specific topic on the gathering of end user feedback relating to the implementation of Information Security Policy. For data collection on this topic the team agreed upon an approach which included the collection of primary and secondary data.

Primary data is also known as row data. This is data which has been collected but has not been interpreted. This data is collected by researchers themselves by using interviews, surveys and experience from their work environment. While this method of collection takes a longer time to retrieve and analyse, it does provide more valuable real world information. There were two methods of primary data collection undertaken for the purpose of this project.

The Indirect Oral Interview Method is fairly self-explanatory. Primary data collection is gathered by indirect interviews with users related to the topic. A number of questions were prepared to facilitate the collection of information related to information security policy implementation. This method has no financial cost with the only resource invested being that of the time spent performing interviews. The second method used was the Mailed Questionnaire Method. This method is used for collecting primary data from questions in the form of surveys. The questions were documented and published via an online survey site, SurveyMonkey.com, with a formal request for honest answers.

Secondary data differs from primary data in that has been previously collected and already interpreted several times for the purpose of other research topics. Data of this nature is easily accessible and inexpensively available in form of journals, academic articles and books. It usually takes less time to analyse than that of primary data. The drawback of this data collection method is that is has already been conducted and analysed, so to ensure the team found data to suit the requirements, the process of identifying the relevant information may take longer.

“Secondary data must be viewed with the same cautions as any primary data that you collect (…) Secondary sources that appear relevant at first may not on closer examination be appropriate to your research question(s) or objective. It is therefore important to evaluate the suitability of secondary data sources for your research” (Lewis & Thornhill 2009).
3.4 Population / Participants

“One of the real advantages of quantitative methods is their ability to use smaller groups of people to make inferences about larger groups that would be prohibitively expensive to study” (Swanson & Holton 2005). The Central Statistics Office show that 1,869,900 people were in employment in Ireland between April and June 2013. Of these, over 38% work in sectors where Information Security Policy is likely to be prevalent. These sectors include public administration and defence, compulsory social security and information and communication (Central Statistics Office 2015). This gives us a base pool of 711,000 people as potential sources for information. Unfortunately there is limited information available on the true quantity of employees governed by Information Security Policy. Research into more precise figures would be another project in itself, so given the projects resources an assumption based on employment in relevant sectors is the most practical approach available.

As it is not viable to survey our entire population the team had to establish an appropriate sample size. The objective of this is to establish a plausible sample size where the results are likely to give a strong reflection of the overall demographic. There are various theories regarding the effectiveness of sample sizes. In the seventies, William G. Cochran developed a methodology to address the issue of error and variance. This involved specifying margins of error for the most vital areas of the survey. Thereafter by assessing the levels of risk and error the researching is willing to accept he developed a formula which provided the predicted ideal sample size (Cochran 2007).

In an effort to reduce the potential error and to ensure the confidence level in our responses remains high, the survey will be distributed through appropriate channels to receive only suitable responses. It’s important to understand if the assumptions are relevant only to the project teams work sectors or if they are shared by employees across various sectors. As our target demographic is only limited by the constraint that they must be end users, it’s possible to reach out to people across different sectors to get a better reflection of the opinion on Information Security Policy implementation overall. The particular sectors surveyed are further discussed in Section 4.4.1.

The formula below can be used to calculate the sample size based on three factors; population size, confidence level and margin of error. Population size is the total number of people whose opinion or behaviour will be represented by the sample. The probability that the sample is an accurate reflection of the attitude of the population is captured by the confidence level. The margin of error reflects the percentage of the populations’ responses which may deviate from the samples. Based on the formula below, by using the population size of 711,000, the confidence level as the industry standard at 95% and a margin of error at 10% the recommended sample size is 96.
\[ n = \left( \frac{K \times S}{E} \right)^2 \]

*Figure 9 - Formula for calculating sample size*

Based on the recommended sample size, the project team have set a target of receiving between 100 and 150 responses. The team decided it would be difficult to achieve more than 150 responses as users in specific organisations are not being targeted. Detailed analysis on the volume of responses received is presented in Chapter 4. The rationale discussed by O'Leary is supported by some of the market leaders in online surveys such as SurveyMonkey (SurveyMonkey 2015). As mentioned in Section 3.7.1 the survey will be distributed through online platforms to targeted groups known to the team. This was done to encourage a high response rate while lowering the risk to the potential margin of error. The interviews will be conducted with three people adhering to the best practices identified in Section 3.5.3 which will be further analysed within the Findings and Analysis of Chapter 4.
3.5 Generating the survey and interviews

3.5.1 Self administrative survey

As mentioned previously in Section 1.2 collecting primary data in the form of a survey questionnaire helped during the process of gaining more realistic and specific data on the subject of the research work.

The team have made the decision to create the self-administrative survey. This decision was influenced by the minimum information regarding end user feedback relating to Information Security Policy implementation from literature reviews. The team had fully agreed that self-administrative survey would offer confidentiality and anonymity within participants which helped to minimise the impact while awaiting ethical approval of such survey. We were fully aware that in order to publish and begin conducting the survey we had to obtain ethical approval from the Ethics Committee of Trinity College Dublin. This is a mandatory step for ethical approval and the submission was required in advance to mitigate the impact should the survey be rejected by committee. We had to take into consideration that big disadvantage of implementing the survey as a method of gathering primary data might be a low response rate. To offset this disadvantage we came up with a strategy implementation process when publishing the survey.

The process of drafting and re-drafting survey questionnaires was focused on keeping a low number of questions while focusing those questions on the three levels of survey participants: Senior Management, IT Team members and End Users. We have completed a number of face to face workshops and skype conferences in order to revise and remove unwanted elements from survey questions. The intention of all those meetings undertaken was the process of clarifying, simplifying and more importantly reducing the number of questions. They were also relevant for discussing what order all questions should be arranged to present their relevance and receive productive results. The team have agreed to use simple business language for the questions. This decision was made based on targeted group of participants. We wanted to ensure that this would help influence participants to be confident and honest while answering the questions and provide us with the participants’ thoughts, reaction and position regarding Information Security Policy.

As already mentioned in Section 1.2 the objective was taken under consideration. Some of the questions in the overall survey questionnaire were focused on targeted participants. Simple questions asked participants to identify which Business Sector are they in and what is their current role in the organisation they are working. The entire survey was dedicated to Information Security Policy implementation and factors that influence such policy existence in organisations. The team decided not to split the survey into sections, but to have all questions flows in particular order from simple to more difficult questions. The team have also included direct questions that supported our second thoughts about Information Security Policy implementation and end user feedback involvement being not consider prior to the process;” and you are involved in the creation of the Information Security Policy in your organisation, End user feedback is considered prior to the
implementation of Information Security Policy. There were also questions in the survey that were designed to test participant’s knowledge of the existence of such policy and what such policy contained and referred to.

The team have also included open-ended questions in the survey questionnaire. The purpose for this was to gather participants honest opinion based on their experience. We were fully aware that the relevant answers to those particular questions will be more impressionistic by their characteristics. Those questions were very helpful in analysis of data and supportive in taking an analytical approach.

Those open-ended questions provided more a qualitative characteristic to the research of our project. As part of the process while publishing the survey we were too in limited in terms of time and resources to run a pilot version of it. We have tested the survey between our team members prior to submitting for Ethics approval.

3.5.2 Implementing Survey

In order to be able to publish survey the team had to fill out formal forms for the ethical approval process. Those forms were formally submitted by our team to the Ethics Committee. The Ethics Committee responded with queries and requested additional information and declaration from the team in terms of a consent form for participants. As soon as formal approval was obtained, the survey was published via emails to individual participants and LinkedIn groups related to topic of Information Security Policy.

The platform used for our survey questionnaire as mentioned previously was SurveyMonkey. The team made decision to use a paid version of SurveyMonkey.com. Monthly charges fee for questionnaires of more than ten questions applied and the survey for our project contained 27 questions in total. We believed that the purpose of this project justifies paying £25 per month. The advantage of using such tool was that participants did not have to set up accounts while responding to questionnaires.

3.5.3 Interview Methodology

An interview is a purposeful discussion between two or more people (Kahn & Cannell 1967). The team have decided to conduct interviews as one of the methods used to answer or at least construct a question to be answered through the group dissertation. The book Research Methodologies for Business Students contained some insightful and valuable information and guidance when deciding how to construct the interviews.

An example of interview techniques supplied in the book, used a section from Dragons Den where entrepreneurs are looking for investments from Dragons. It states that interview
questions must be clear and concise. The questions must probe in order to get as much relevant information as possible.

There are different types of interviews either structured or unstructured and formal or informal conversations. The research group conducted a number of informal unstructured interviews with work colleagues and users that would have an opinion on the general broad topic of research. The informal interviews were used as feelers for a general opinion of people working within the IT industry and familiar with IT Security policies.

Structured interviews are described in the book as a set of questions that are structured in the same way for each person that is going to be interviewed. The interviewer must ask the questions in a neutral tone, exactly as they are written on the paper. The neutral tone is to reaffirm a non-bias opinion when asking the questions. The reasoning for this method is to collect quantifiable data which are also described as quantitative research interviews.

Alternatively there are qualitative research interviews (Cassell & Symon 2004) which describe semi-structured or unstructured interviews. In this method an interviewer may omit questions and ask further questions based on the interviewees responses.

This describes the informal interviews that the research team initially conducted. There was a general theme that was agreed to conduct the interviews under and to record the opinions and feedback from the interviewees based on the agreed themes. Here there is no list of questions that are agreed on beforehand, just the general theme of topic that the research group is interested in. In our case it is IT Security policies and general opinions on how they are agreed upon, implemented and if user feedback is involved or considered along the process.

Qualitative interviews are a valuable resource for understanding the ‘what’, ‘how’, and also the ‘why’, for research papers. The data that was gathered from the semi-structured interviews was then used to structure our online questionnaire on survey monkey. It was also used to structure the questions for the structured interview. The semi-structured, informal interviews were extremely valuable as it really focused the question and area for the research topic.

The use of survey monkey online questionnaire was agreed amongst the research team as a means to gathering a large amount of data from a large pool of respondents. From speaking with previous members of other research teams, it was found that large pool of respondents is possible with online survey / questionnaires. The reference book for interviews mentions online questionnaires as a poor method for gathering data. The context of this opinion would seem to be based on users entering lots of text answers. The research group in this instance addressed this by deciding to minimise the amount of text based questions and focus on multiple choice responses.

The timing of the interview is recommended to take place during the morning, before lunchtime. When conducting the interview, there needs to be an active awareness not to introduce a bias when asking the questions. In that same regard, there needs to be a mindful awareness that the interviewee may have their own bias regarding the interpretation of the questions if they sense
bias in the way the question is asked. During the interview, in order to test the understanding of the interviewees’ answers, the interviewer may summarise briefly the answers given in reply to open ended questions.

### 3.6 Conducting the Interview

Based on the interview techniques research it was found that opening an interview with a question beginning with “what”, “how”, or “why” is the best practice. This gives the interviewee an opportunity to give an answer in their own words.

An example of an opening question could be: “How are you informed about the Information Security Policy within your organisation?”

Following on during the interview it would be beneficial to ask some probing questions. “What methods does your organisation use to evaluate the quality and effectiveness of Information Security in your organisation?” The probing questions can also be expanded on after the interviewee answers. Some of the examples of this might be “could you tell me more about that” or “how was that decision arrived at”. Other examples of expanding on a theme would be “why do you think the employees do not understand a certain policy”. Some specific questions we will be asking are “How many employees work in the organisation” and “What business sector you currently work in?”

The interview questions are going to be a more expanded version of those in the online questionnaire.

- What business sector are you currently working in?
- Which of the following describes your role in your organisation?
- Approximately how many employees work at your organisation?
- Are you aware of your organisations Information Security Policy?
- If yes, Are you involved in the creation of the Information Security Policy?
- If no, Is end user feedback considered prior to the implementation of Information Security Policy?
- If yes, Does end user feedback influence the Information Security Policies?
- If no, Would user behaviour within your organisation or external influences (i.e. trends or industry recommended) influence Information Security Policy decisions? Possibly both?

Would user behaviour within your organisation or external influences (i.e. trends or industry recommended) influence Information Security Policy decisions? Possibly both? How often is your organisations Information Security Policy updated? Does your organisation measure the quality and effectiveness of Information Security?
Some examples might be Regular assessment by internal audit department, regular assessment by a consultancy or official certification within the industry & international standards (PCI, ISO/IEC 27001 (ISO 2013a))

How are the employees (end users) informed of Information Security Policy within your organisation?

- Do you believe this informs them adequately?
- How often is information regarding Information Security policy distributed in your organisation?
- Could you give some examples of what is covered by your organisations Information Security Policy? (Passwords, clean desk rules etc?)
- Do you believe that Information Security awareness has a positive impact on your responsibility in the organisation?

Would you be fully aware of what is forbidden and what is acceptable in your organisation?

- If yes, possibly some examples?
- If no, why do you think that is?

How would you consider the level of understanding of Information Security Policy across your organisation? Is your feedback considered in relation to Information Security Policy implementation? Would you have any suggestions on improving Information Security Policy awareness in your organisation, or do you think there is a good awareness already?

- (If says good awareness, follow up with) what do you use to measure that awareness?

Is there feedback collected in relation to Information Security Policy within your organisation?

- If so, how is that collected?

Do you think there is a need to increase Information Security Policy efficiency within your organisation? Is your organisation concerned about the adoption of the Information Security Policy by employees?

- If yes, why?
- If no, why not?

What measures has your organisation taken to minimise a potential risk arising as a result of staff changes?

- If none, ask if thinks it would be beneficial

End of interview.
3.7 Secondary Data

As mention in Section 1.3 for data collection on this dissertation topic, the team agreed to include the collection of primary and secondary data.

Secondary data is a collection of already existing data. This data was collected by others and includes such sources like organisational records, data that was collected through process of qualitative methodologies and data collected as part of qualitative research work.

In this thesis paper we have also included secondary data from scholarly articles, journals, books, where topic on Information Security policy and factors related to it were available.

3.8 Ethics

3.8.1 Ethical Approval

A prerequisite to conducting research work in line with our final year project for the BSc (Honours) in Information Systems degree was obtaining ethical approval. This was a mandatory requirement for the purpose of the work we decided to carry out. The ethical approval was granted by the Research Ethics Committee, School of Computer Science and Statistics (SCSS), Trinity College Dublin.

Our team has followed the ethics application to completion in agreement with the ethics guidelines that are published and accessible on the Trinity College Dublin website via the following link: http://www.tcd.ie/about/policies/assets/pdf/TCDGoodResearchPractice.pdf

The first application was submitted on the 21st of January 2015 and the final approval was received from the Ethics Committee on the 16th of February 2015.

As mentioned in Section 1.2 our approach was to proceed along with qualitative and quantitative research methods. We have completed the ethics application to reflect these two approaches.

Our primary goal during the research project was to collect as much data as possible regarding the Information Security Policy implementation process. This includes feedback from users and their knowledge about Information Security Policy. To successfully answer the research question the team created survey and interview questions that were primarily focused on three groups of users: Management, IT Team members and End Users. The survey consisted of 27 questions in total. The interview questions were focus on only one group of participants: Senior Management. We decided to keep the number of interview questions to a minimum of 5 in total. This helped us to encourage users to participate to the point of completion in the survey. The communication to participants was in plain English. All questions designed by the team for the
survey and interview were focused on elaborating adequate scope in order to fully explore and analyse research questions. This was also to clarify the project objective.

Before publishing the survey we have decided the survey questionnaire would be distributed amongst contacts within existing networks of ours. This was our assurance that responses to the questionnaire where honest and that confidentiality was in place. The method of using existing contacts for the survey helped us target participate groups in batches to monitor a summary of responses from that particular group. This overall process allowed convenience for ourselves and predictability in terms of which group of participants would be targeted first. A similar approach was conducted for interviews by using existing contacts from Senior Management in our current work environments and other companies familiar to us. Given the nature of this project and the limited time available for completion, it was deemed impractical to develop new contacts and search for unknown participants. To further our reach with the survey, we utilised existing Information Security groups known to us via LinkedIn to gather more responses. We feel distributing the survey via LinkedIn provided a significant benefit to the research of our project.

3.8.2 Ethics Issues

The College Code of Ethics is highlighted in the policy document as mentioned in the Introduction section. We have adhered to this code.

The project researched team advised of potential conflicts of interest as we using existing professional relationships during the research of our project. All responses used in this project are anonymous.

3.9 Data Protection

The project research team has been made familiar with, and acted in accordance by the conditions set out in the Data Protection (Amendment) Act of 2003 and also the initial Data Protection Act of 1988 per the following links:

4. Findings and Analysis

4.1 Introduction to Findings and Analysis

The main purpose of this chapter is to present the results of the team work from the primary research surveys and interview questions. As mentioned in Section 1.2 Multi-methodology Strategy, the survey questionnaire and interviews were used to gather primary data which was very closely aligned to dissertation objective. All of the information was collected using twenty seven survey questions and including additional semi-interview questions. The interviews were conducted with three main individuals who were part of Senior Management within the Financial and Insurance business sectors. The survey questionnaire and interviews were conducted separately at different times. The survey was actioned first and then the interviews were completed. The findings from these two methodologies are combined and discussed in deeper context further on in this dissertation document.

The survey questionnaire was managed and actioned via the SurveyMonkey platform. The survey links were distributed to individuals and targeted LinkedIn special interest groups. The survey was active for ten days in total and was supervised by the team on a daily basis. The survey link was sent to one hundred and fifty (150) individuals of whom one hundred and twenty (120) participants responded to the survey. This equates to an 80% returned response rate.

The SurveyMonkey platform is only free where the survey contains less than ten questions. Our team agreed to invest in the paid option as it included more survey questions and had additional functionality such as statistics, response analysis and metrics reporting which was a big advantage for our project work. The overall perception of survey monkey was that it was a worthwhile endeavour to use the paid service offering. It assisted the team to review responses and monitor survey activity.

It is important to highlight that the team has carried out this study and research focusing on Information Security Policy implementation and existence across different organisations. During this process our team had to determine whether users were aware of their Information Security in their organisations and if end user feedback is considered regarding the implementation of such policies.

The team has also taken under consideration that strategy for implementation and/or existence of Information Security Policy might not be known by all respondents within their organisations during the research project. By not having such policies in place, organisations are exposed to vulnerabilities and weaknesses which might be used by their employees within their organisation. It would all depend on the overall process and structure across the business and particular departments. The team also had to consider security weaknesses, cyberattacks, and security incidents might not be exposed publically.
To ensure that the survey questionnaire was designed effectively to provide the most relative results, the survey was extended to include questions about specific areas that were directly focused on gathering such information about end user involvement in the process of implementation of policy. It also tried to address any type of measurement currently undertaken by reviews in organisations targeted throughout the survey. The project team included direct questions for the purpose to gather relative responses from the participants in order to support the project objective.

The project team had made a decision to publish survey questionnaire to all types of organisations. The team did not restrict the survey to any specific sector or business sector. To have responses from a different variety of business sectors gave team good insight to the process of implementation of Information Security Policy in organisations across a wide spectrum. The team directed this survey to colleagues and special interest LinkedIn IT Security groups, which consisted of members across a wide geographical area.

4.2 Participants response rate

The big advantage of using survey monkey platform was that it provided a response rate track on a daily basis for the overall survey and individual questions. This had positive influence on measuring the overall accomplishment of the response rate from participants. As mentioned previously the survey was published to targeted individuals and special interest LinkedIn groups that where these individuals and groups had a variety of experience with Information Security Policy. The team took this approach to make sure that abandoned rate of response would be comparatively low to that of the overall number of targeted users. The decision was supported by the guidelines from “Measuring Regulatory Performance. A Practitioner guide to perception surveys, OECD 2012” by following the full checklist of the following: design survey, run survey, select the respondents and analysis of responses. The team have also used interview methods as described by Kate Kelly in “Methodology Matters”. (Kelley et al. 2003).

The survey and interview questionnaire have been formally approved by The Ethics Committee on the 16th of February 2015. The team published the survey on the 16th February 2015. The survey was closed on the 27th February 2015. The interviews were conducted on the 27th of February 2015.

The project team published links to the survey on:

- Their LinkedIn profiles
- Cyber Security Forum Initiative – CSFI.

A number of individual emails were sent to colleagues to participate and complete the survey for the research work purpose. The team had full control over tracking responses via the
SurveyMonkey platform and by receiving email notifications that the survey has been complete. Individual email requests sent to workmates and colleagues had positive material impact on participation and overall responses rate. As mentioned in Section 4.1 the responses rate was in total 120. The team had targeted a minimum of 100 respondents so were satisfied with the overall response rate.

The project team had no way of tracking responses rate from special interest groups on LinkedIn, but the team did not feel that this impacted the research in a negative way.

4.3 Data validation

The survey began with consent form of declaration to participate in the survey and agree or otherwise to participate. Three participants did not agree, from which one was a test performed by project team before publishing the survey, to make sure that individuals wouldn’t be able to continue with filling in the survey while disagreeing with the consent form.

![Data validation chart]

Figure 10 - Data validation responses

The project team do not know the reason for the two participants choosing not to complete the survey questionnaire.

The overall summary of responses was 120 so the project team decide to use all of them as valid responses. The individual participants for the survey were targeted across number of business sectors, different roles and responsibilities level in the organisations: Management, IT
Team members, End Users and Others. The survey was targeted at organisations of all sizes. The team have not included a demographical questions, as it was not related to the objective or this research.

None of the questions in the survey were mandatory. A number of days into the survey, the team noted that participants had not responded to all questions. The project team has acknowledged that not having all individuals answering all questions presented a gap in the data. As part of the requirements of the Ethics Approval, the team could not make all survey questions mandatory. All survey questions had to be optional.
4.4 Survey Data Analysis

4.4.1 Organisations questions

At the beginning of the survey, the participants were asked questions to specify the business sector they are currently working in, their position within the organisation and also the size of the organisation.

The following sectors were dominant in the survey response. Of the 103 respondents, 37.86% (39 responses) were in the Insurance sector, followed by IT and Telecom of 28.16% each (29 responses) and 24.27% (25 responses) from the Financial sector. There was also low number of responses from other sectors including Legal, Healthcare, Consumer Goods and Government.

![Figure 11 - Responses by Business Sector](image)

Of the total number of responses to the question related to their role within their organisation, members of the IT team equated to 42.7% with Management accounting for 37.9%.
Teams with lower response rates were from Finance, Marketing and Information Security & Risk Management. (12.62%) As the research objective was also to include End Users, there were 6.8% of participants identified in the survey from End Users.

![Figure 12 - Responses by role in the organisation](image)

The dominant percentage (82.52%) of individual responses to the survey question on the size of the organisation came from organisations with more than 250 employees. 12.62% of responses came from organisations sized between 50-250 employees and the lowest response rate (4.85%) for this particular question came from those in organisations with less than 50 employees.

### 4.4.2 Information Security Policy Awareness

The majority of responses to this question (56%) responded that that they are well aware of the existence of Information Security Policy in their organisation. Their response was that they strongly agree with being aware of it. 39% participants responded that they only agree that they are aware of the Information Security Policy. 5% of participants to this questions disagreed with the statement, which gave us the information that they do not know and/or are not informed about Information Security Policy.
In contrast to this question, 39% of participants responded that they are involved in the creation of the Information Security Policy and 45% of participants responded that they are not involved in this process. 44% of those answers highlighted that the End User feedback is considered prior to implementation of the policy, 29% disagree and 28% of participants neither agree nor disagree, which would indicate that they are not involved in this process. Almost equal to that, 43% of participants responded that the creation of Information Security Policy in their organisation is influenced by feedback received from End Users, 21% think that End User feedback is not considered and 36% remained neutral.

4.4.3 Information Security Policy and behavioural factors

"As we have noted, more than 40% of security professionals report that their greatest security concern is employees accidentally jeopardizing security through data leaks or similar errors” (AlgoSec 2013).

The majority of responses to this section (94.7%) agree that decisions regarding Information Security Policy are very much influenced by user behaviour and external influences like industry recommendations, such as aligning with IT controls and regulations. Only 5.3% specified that they are not sure and/or they don’t know. According to a number of reports, employees are the biggest concerns for any type of security issues.

It was not surprising to see that the majority of participants responded that user behaviour and external influences are results of the creation and existence of Information Security Policy across organisations.

![Figure 13 - Information Security Policy decision results](image)

---

Page | 38
This section can be compared to Section 2.x (shadow security section) which discusses shadow security and how users will find a work around if they find the recommendations of Information Security Policy too restrictive. As mentioned previously, there are several reasons for users adopting non-compliant behaviour. Some of the factors include:

- Lack of awareness - employees not aware of security risks.
- High Compliance costs - the security policies impede employees work that they feel the only workable option open to them is non-compliance.
- Compliance impossible - where employees find ways to work around the policies.

Data collected via the research survey presents that information about Information Security Policy is circulated via the following methods: email (66.67%), induction training (56.32%), personal and/or group training (27.59%) and intranet (17.24%). The majority (77%) strongly agreed that the form of receiving information about Information Security provided was adequate and satisfactory.

![Figure 14 - Information Security Policy Awareness methods](image)

According to Wombats it is not enough to educate employees about issues like phishing, smashing and social engineering existence. This won’t reduce data breaches and malware infections. Employees should be fully aware and understand how security threats present themselves in daily situations. They should be aware of impact they have on the day to day protection of the network, data and assets.

The following responses have been received from individuals in relation to what is their understanding of what is covered in the Information Security Policy document within their organisation:
The majority of participants are fully aware of areas covered in the Information Security Policy documentation within their organisations. Across different business sectors awareness and information related to the Information Security Policy is distributed bi-annually/annually (47.7%), quarterly (26.7%) but there are also cases where information is distributed more frequently; monthly (14%) and weekly (2.3%). 9.3% of findings presented that information regarding Information Security Policy has been never distributed in their organisation.

Of the respondents, 85% strongly agreed that regular awareness in the organisation has a positive impact on their responsibilities. There was also high response from 70% who indicated that they strongly disagree with Information Security Policy having a negative impact on their ability to work effectively and efficiently. Only 15% of participants remained either neutral or disagreed with the statement and almost equally as 20% didn’t specify if Information Security Policy had a negative impact on their day to day work. By regular distribution of information related to Information Security across the business, the majority (86%) of individuals strongly agreed that they have full awareness of what is forbidden and what is acceptable within their organisation. A very low rate of respondents (9%) disagreed with such statement and few individuals (4.7%) didn’t take a position and neither agreed nor disagreed. The team believed that this is also strongly supported by Information Security Policy acceptance being mandatory within the organisations where the majority (85.1%) declared that acceptance of policy is mandatory. Only a minority response rate (4.6%) declared that acceptance of policy is not a mandatory and some responses (10.3%) stated...
that they are unsure about such process which also indicates that they might not be aware of
Information Security Policy.

![Pie chart showing percentages of Yes, No, and Unsure responses]

**Figure 17 - Acceptance of Information Security Policy**

### 4.4.5 Information Security Policy: Implementation process

When it comes to cyber security, CEOs and boardrooms are not adapting. While it's understood there is a danger and the threat of cybersecurity is discussed more actively, this doesn't equate to
greater allotment of financial resources. The most common resolution for addressing the issue
appears to be training. Could this potentially lead to an experience gap, where the focus is too
heavily on training and less so on acquiring proven talent to address potential issues? Cyber security
threats have traversed from being the sole domain of the IT department to something every
department in a company must protect against and as such, CEOs must be proactive in
understanding and addressing the threats. Serious attacks can cripple companies financially and
damage their brand, in extreme cases beyond recovery. It's best to address the issue now as when a
threat is realised, it may be too late.

As per PWC (PriceWaterhouseCooper 2013) reporting there are at least three areas an
organization should initially consider when assessing their cybersecurity posture, posing questions
that can be answered only at the executive level and above:

1. Advancing the security posture through a shared vision and culture.
2. Enhancing the cybersecurity strategy and capability
3. Understanding and adapting to changes in the security risk environment.

The below chart represents participants responses that are related to PWC reports data which is a representation of shared vision and culture in the organisation that relates to the Information Security Policy and also evaluation of the effectiveness of Information Security across organisations.

![Chart showing participant responses]

Figure 18 - PWC Report three areas to consider

In relation to enhancing the cybersecurity strategy and capability within organisations, participants responded that the following evaluation has been performed to assess the quality and effectiveness of Information Security Policy.

<table>
<thead>
<tr>
<th>Area</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>It has been reviewed and updated within the year</td>
<td>89.9%</td>
</tr>
<tr>
<td>It was formally approved by Senior Management</td>
<td>91.4%</td>
</tr>
<tr>
<td>It has been communicated to all relevant staff (including staff, contractors, temporary employees and third parties)</td>
<td>84.9%</td>
</tr>
<tr>
<td>It contains a definition of the organisational structure of information security</td>
<td>70.5%</td>
</tr>
<tr>
<td>It addresses the legal aspects associated with security</td>
<td>57.7%</td>
</tr>
<tr>
<td>It regulates the role and duties of employees</td>
<td>78.5%</td>
</tr>
</tbody>
</table>
According to data collected throughout the survey, we can say that organisations take into consideration the necessity for adaption to change in the security risk environment as per the below chart. The majority of responses (~ 60%) strongly agreed with additional measures taken place within their organisation to improve Information Security processes.

**Figure 19 - Evaluation of quality and effectiveness of Information Security**
4.5 Survey Open Questions Analysis

During process of designing survey questionnaire, the team have decided to create two open questions, where respondent would be allowed to enter free format text in relation to the questions below.

What, in your opinion, (if any) would improve Information Security policy awareness in your organisation?

The project team have separated responses into two groups; positive and negative. Some comments received indicate a good awareness of Information Security Policy in organisations. There are also comments that mostly highlight gaps within the organisations in terms of training not being provided regularly and most frequently not enough budget and resources to focus on the Information Security Team. The below table represents all responses collected.
<table>
<thead>
<tr>
<th>Positive Feedback</th>
<th>Negative Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;I think awareness is high in our organisation, everyone is very aware of the need for information security.&quot;</td>
<td>&quot;I'm not particularly aware of AVNIS; Policies in our company, if it was communicated to staff in plain English, that would help.&quot;</td>
</tr>
<tr>
<td>&quot;I feel we're quite well informed as an organisation and this is largely due to an active and dedicated Security Team. Yearly training is required and a weekly news email is sent. Internal tests such as phishing scams are carried out regularly.&quot;</td>
<td>&quot;Security understanding business flows&quot;</td>
</tr>
<tr>
<td>&quot;Lunch and Learn Sessions, video transmissions (all new staff had to recently complete an online security course, pass this and inform personnel when it had been completed)&quot;</td>
<td>&quot;A layman's explanation of why and how&quot;</td>
</tr>
<tr>
<td>&quot;An internal or even external industry incident always alert awareness. Continued ISO certification at least ensures ongoing management and reviews&quot;</td>
<td>&quot;More updates/training&quot;</td>
</tr>
<tr>
<td>&quot;Not an awful lot. A reference to the information security policy is everywhere in the organisation. On documents, on desktops, in meetings, etc.&quot;</td>
<td>&quot;Have it in a simple, readable non-technical format that can be easily read and understood.&quot;</td>
</tr>
<tr>
<td>&quot;All practical steps are taken to improve awareness already.&quot;</td>
<td>&quot;Simulated phishing attacks simulations of info sec incidents.&quot;</td>
</tr>
<tr>
<td>&quot;I think it's fairly good&quot;</td>
<td>&quot;Awareness should be interesting to the end users. It needs to have a touch of the realities associated to them in terms of personal and as well official - Awareness should be more targeted based on the incidents internally and externally and should have relevance to the practices in place in the organisation.&quot;</td>
</tr>
<tr>
<td>&quot;Currently working towards 27001 certification will increase awareness&quot;</td>
<td>&quot;More regular updates&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Annual updates presentations&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;More education on the value of company information and the impact to the company and its employees when data is lost, stolen or compromised.&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;More group training with end users&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Ensuring standards and policy requirements are translated into plain English for process and training documents to be consumed by the business, e.g. Terminology, references to ISO standards (what standard and what that means)&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Information Security is influenced too much by parent company which bears little resemblance operationally to our business. Should be tailored to suit our own business.&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Regular Awareness email training and e-training that people should respond to on a regular basis. There should be &quot;ty&quot; or &quot;prr&quot; displays with monthly topics on security&quot;</td>
</tr>
</tbody>
</table>

Figure 21 - Opinions of improvement on improvement of Information Security Policy
In general, the respondents indicated that having additional training, awareness, and more frequent updates in relation to Information Security Policy would be a big advantage for both the end users and the organisation.

On the same vain, we have seen that there is number of organisations that currently adapt to standards and have well defined process for circulating awareness of Information Security Policy. It would be good to see the adaptation of Information Security Policy training being a regular activity in the organisations and also the collection of feedback from the end user. In fairness all areas of business are affected of Information Security Policy, not only IT. All users should be well aware of impact that can be caused by breaching policy and it’s supporting processes.

**How is feedback related to Information Security Policy collected within your organisation? (If feedback is not collected please enter N/A)?**

The survey results to this question were relatively low (52%). 37% of individuals declared that feedback related to Information Security Policy is not collected in their organisation at all.

Other participants declared that feedback is collected through forms such as: email, intranet, informally via managers or team leaders, semi-annual survey, via HR and ad hoc feedback. What was very interesting is that the majority of responses indicate that feedback in relation to Information Security Policy does not exist. The Policy becomes mandatory for organisations but no one really asks the important question: what are the gaps and is it realistic to adapt to documentation that was not designed for the way an organisation operates? From the overall responses rate to this question, it is visible that the collection of feedback process does not exist in most of the organisations and end user feedback is considered neither prior to implementation nor post implementation of policy.

From the other side it was positive to receive information that there are already organisations that have “Monthly Information Security discussion” and “Monthly Security Governments”. Unfortunately the team had not received deeper details as to what those meeting are concluded with but it would be of significant advantage to see the feedback process being formalised in organisations as part of the Information Security process.

Following on from the above point, there was a comment in the survey which said: “You will probably find that Information Security is a field that is only just becoming visible to Senior Management as potential tool to protect organisations as much as one to drive enterprise”

From analysing the response, it would indicate if Information Security would become an enterprise it would have to be adapted by most of organisation as a mandatory requirement. It would make life much easier as all users would understand Information Security as overall processes and procedures not only as existing documentation.
4.6 Interviews questions analysis

Following on from the survey questionnaire, the project team have aligned three participants for interviews. Those interviews were conducted straight after the survey questions had been completed. The interviews were conducted with individuals from the Insurance and Banking business sectors. All participants are part of Senior Management within their organisations. The roles of the individuals within their organisations are: Head of Risk & Compliance, System Manager and IT Manager.

The project team have decided to keep the interviews short and align them to the dissertation objective of finding out if users can submit feedback in relation to Information Security Policy.

Project team have decided to keep the interviews short and align to dissertation objective of finding out if users can submit feedback in relation to Information Security Policy.

Q1). Does your organisation have any facility available where users can submit their feedback regarding Information Security Policy Implementation? If so, what types of facilities are present?
Q2). Does/would your organisation find such a facility beneficial, if so how?
Q3). Does/would such a facility impact policy implementation and further amendments/changes through your organisation to such documentation?
Q4). Does your organisation conduct an impact analysis following Information Security Policy Implementation? If so, what types of measurements are present? What does this information indicate?
Q5). Does/would you as a member of an IT Management Team find the impact analysis beneficial and if so, how would you use such information for further changes documentation and processes

The project team have received a mixture of responses from the three individuals. In all cases the participants declared that in their organisation there is no facility for collecting feedbacks from end users. One individual declared that Information Security Policy documentation is too mature to be visible to end users in the organisation. Their business is focused to protect clients and not focused on insiders. In all organisations related to participants, Information Security Policy is reviewed by such departments as: HR, IT, Risk and Legal. There are formal feedback processes that are submitted within organisations via gap analysis documentation for the minimum requirements of policy to Security Unit Management.

In regards to such a facility being beneficial, individuals offered different answers to this question. Some believe that having feedback from users would allow local variances in the operational model without reducing group policy to the lowest common denominator. They also believe that having such a process would improve processes in the organisation across all business
areas. There was also a response which specified that having feedback from end user would have no benefits to organisation.

When asking individuals about such a facility impacting Information Security Policy, all agreed that they don’t see a reason why a feedback mechanism could not be put in place, allowing users to recommend additions or adjustments to policy content. All have also declared that prior reviews have taken place in their organisation, however only on management level, users are not considered during this stage of the process.

Regarding gap and impact analysis being performed to assess Information Security Policy, two participants responded that they do not perform such action in their organisation. We have also received a proper process description in which a full gap analysis is performed in one of the Insurance organisations to comply with minimum policy requirements. All requirements are assessed and non-compliance gaps are highlighted. The measurement that is presented concludes two forms of assessment: design and operating effectiveness of policy. Design effectiveness is a process which describes what type of documentation exists in the organisation to support Information Security Policy.

Operating effectiveness is a process which detects all processes and day to day procedures that are cumulated accordingly to the ISO 27001 standardisation and presented in the form of a scorecard in monthly Information Security meetings. All government material is then formally submitted to the Head of Information Security within the organisation for review and discussion. This process was declared as most beneficial one to the organisation. Impact analysis is a beneficial step in adaptation and implementation of Information Security Policy as information underpins a continuous integration process. All participants conclude that impact analysis is beneficial and helps support the understanding of fundamental processes as part of policy documentation.

4.7 Summary of Data Findings and Analysis

The total number of responses to the survey was satisfactory to the project team. The main objective of the survey was to target end users and receive high responses from this particular group. Even that the majority of responses were heavily represented by IT Team members (43%) followed by Management (38%). The team have decided to include “Others” to the End user group, which in total representation of End users equates to 19%. It was not surprisingly to see the wide range of industries represented in the survey responses, but surprising to see the influence of the Insurance sector (38%) over Financial Services (24%) followed by IT and Telecoms (28.2%) and the minority in sectors such as: Government (5%), Healthcare (2%) and Others (2%).

When asked about existence of Information Security Policy in the organisation, the majority of participants (56%) responded that they are fully aware of the policy in their work place. In contrast to awareness 39% of individuals declared that they are also involved in the creation of the policy. 44% answered that End User feedback is considered post implementation of policy.
documentation, but this process is not formalised. These individuals can provide their concerns or ideas via email, or informal discussion with their managers, as indicated by the survey but the issue here is that this information ends up not being passed on to the relevant people within the company. The majority of responses (57%) declared that they do not take part in creation of the policy documentation and this includes those answering in disagreement and from neutral position. 21% of those strongly agree, declaring that End user feedback is not considered prior to the creation of Information Security Policy and 39% of them took a neutral position which would suggest that they either do not know about such processes and/or are not involved in creation, publication or the providing of feedback.

52% of 59 respondents to the question in relation to feedback being collected in their organisations declared that such action doesn’t exist. They highlight that this process is not formalised and there is no legitimate tool for collecting user opinions and/or ideas. One of the responses from the open question was as follows: “As the CIO I am a stakeholder in the group development process around information security”. This indicates that a review of policy documentation effectiveness it is only reviewed at senior management level and does not include lower level employees and end users. User behaviour is an extremely important factor while developing processes supporting information security, so engagement with end users would be a useful element during this process.

As mentioned previously according to secondary data reports, employees are the biggest concerns for any type of security issues but no one really considers their opinions nor their feedback during the implementation of not only Information Security Policy but also day to day processes that are supposed to improve the efficiency and productivity in the business. 94.7% individuals agreed that the decision regarding Information Security Policy is very much influenced by user behaviour and also by external influence, but they are unsure if the comments submitted via emails to line managers are taken under consideration. There is lack of capturing end users feedback during the process phase in the implementation of security policy.

According to Ernest & Young Survey, 57% of employers polled listed employees as the most likely source of cyber-attackers. This secondary data report highlights that Policy documentation is decided on by Senior Management and enforced by the IT Team for the good of end users. The question here would be: are End Users aware that they are perceived by employers as the biggest threat and also as the most likely source of a cyber-attack? Is this why End user feedback is not considered regarding the implementation of Security Policy? One of the well-known training companies Wombat, which provides a service that educates the workforce of an organisation on the cyber security threats. It does through a number of role playing scenarios that in their opinion educating people on the serious threats that exist is not enough.

Wombat believes that people need to be made aware of their role in the overall cyber security defence. This opinion is also backed up by Denis Besnard Nadn and Budi Arief in their paper which focuses on how computer security can be impaired by legitimate users (Besnard & Arief)
2004). They recommend not only the educating of staff, but also that procedures should be understood rather than followed to the letter. Security should not be an end user task and companies should also be wary of contradictory objectives; don’t ask users to focus on security without expecting a trade off in performance. There is a potential gap between a company training its staff on the cyber security threat and the staff understanding their roles within the defence of that threat. There is also a possible gap between the understandings of how staff perform their jobs compared to the restrictions of policies put in place. The policies are created for security reasons to protect an organisation from threats, although they may also cause a hindrance to peoples work. The reason for this might come from users being mostly affected by policy rules, but not being included in the process of creation those rules.

While all of the concerns regarding users as a vulnerability are not unwarranted, there is a possibility that more trust is required between the policy implementers and the users that are expected to adhere to all of the rules. In the paper “Balancing the insider and outsider threat”, it concludes that there must be more trust between the system administrators and their personnel but team believes that this would require additional research work to identify if this is the case or if simply End User feedback should be considered regarding policy implementation.

While talking about cybersecurity issues we often hear that people are the biggest concern, not technology. In the article “Understanding Insiders: An analysis of risk-taking behaviour” Farahmand and Spafford clearly point out that insiders or those that discover themselves as insiders can be educated on risk elements that can be outcomes from their actions (Farahmand & Spafford 2013). They discuss that those insiders that are fully aware of being caught in committing fraud they are less likely to do so. They also talk about SETA Program (Security Policy Education Training and Awareness) of security policies, where they indicate that each process might have discouraging effects on their possible intention of exploiting the Information System. Their survey figures present that organisations do not focus enough on their employee security education, training and awareness. The highlighted fact is also that users should be engaged in the security adventure process. End Users should be trained on risk related to misuse and breach of Information Security Policy and all supporting processes in their work environment. Again this presents a possible gap where users are enforced adapt to documentation and procedure they do not understand. While creating policies, effort should be made to develop a standardised approach to understand risk across different business areas. This standardised approach would include employee engagement in the process and understanding their opinion about risk and their relation to risk and the consequences of breaches.

From data received throughout the survey and from secondary data that supports this research objective, we can define that organisational management should include end users point of view on risk, understating the concept of Information Security in the process of creation and implementation of Information Security Policy. Engaging with End Users throughout the process of putting into practise Information Security Policy and any other supporting policy documents would create a positive working environment.
5. Conclusion

5.1 Introduction

The main purpose of this research work was to discover adequate answer to the question “Should End user feedback being considered regarding the implementation of Information Security Policy?” The following efforts were undertaken to answer this question. The literature review was conducted and reviewed, primary data was collected from survey questionnaires about Information Security implementation and semi-structured interviews were performed. This was to gather information as to what the primary benefits are from the collection of feedback from end user in regards to the creation of Information Security Policy. Furthermore, secondary data in the form of statistics and national survey results (Business reports) were analysed and explored.

The literature review part provided an indication into the historical and current view of cybersecurity. It presented how cybersecurity importance has increased during the evolution of computer security in organisations all around the world. It also highlighted that peoples behaviour is an important factor throughout the process of creation, implementation and adaptation to Information Security Policy. End user actions are exposed to the possibility of attack and/or can cause misuse of systems and processes with high impact to the business.

The primary data that was collected via survey questionnaire and semi-interviews was purely qualitative. It demonstrated the participants’ opinions and knowledge about Information Security Policy in their organisations, rather than assessment of qualitative data already provided via other sources. Survey questionnaire and semi-interviews were decided as a primary method to gather data. This data was fully analysed and statistics examined to identify what factors could be used to conduct and support research work.

Statistics from primary data was analysed and compared with and against secondary data sources from business reports (PWC, Deloitte, Ernest & Yung), journal articles related to cybersecurity and information security in general. Data and findings from those resources supported the project team’s idea during research analysis.

All the above research activities was undertaken to investigate the research question and clarify any assumptions that arise during this operation work.
5.2 The Research Question

After analysing the interview and survey responses, there were several things identified to be taken into consideration. The majority of respondents from the survey were management which was then followed by IT members. The relatively low response rate from End Users highlights that more focus could be placed on the end user.

Following the question based on Information Security Policy and behavioural factors, 95% of respondents agreed that decision making for Information Security Policy is influenced by both user behaviour and external factors. The question that remains is what element of user behaviour is considered? Does this focus on the negative impact users can have in contributing to breaches, cyber security incidents and generally increasing the potential threat to the organisation?

Much of the research conducted in the literature review supports the theory that training alone is not enough for acceptable levels of security awareness. Employees should be made fully aware of the impact Information Security Policy has, such that they understand the potentially threats and security breaches that can result from users not abiding by the standards set in policy. To this end, users should be engaged to get their understanding of policy.

Awareness of Information Security Policy does exist which is already a big step in the right direction. 85% of respondents strongly agree that regular awareness has a positive impact on their responsibility within their organisation. When this occurs, users are fully aware of not just Information Security Policy but also other policies within their organisation such as acceptable usage.

It’s clear that the implementation of policy comes from Senior Management at the top of the hierarchical structure within organisations. While the end user shouldn’t be part of the approval process, it would be beneficial to have the end user engaged in the requirements gathering process. This would have a positive effect on policies the end user must abide by and also improve the end users security awareness.

A shared opinion from the survey is for organisations to improve awareness of Information Security Policy within their organisation more frequent training sessions and updates are required. The methodology used for educating users understanding and awareness of security impacts should be tailored for the end user. This should be simple and easy to understand from the end users perspective. Information security awareness within an organisation should be realistic and aligned to each individual organisation rather than a bespoke training package from an external provider. With this in mind, respondents feel information security should be tailored to suit their own business needs, limiting the influence from outside.

It may be worth considering the theory that information security could become an enterprise within an organisation, where the continuance of an awareness plan is part of the day to
day process. This promotes the possibility of organisations aligning relevant people with the implementation process.

There was a surprisingly low level of responses to the question regarding feedback in relation to the overall implementation policy. Only 52% of respondents answered this question, and of these, 37% stated feedback was not collected or considered in their organisation with no formal process for collecting feedback present. Others said it was possible to provide feedback through various means such as via e-mail or through their direct manager, however none were aware of the direct impact of providing such feedback. Given the high number of non-responses to this question at 48%, it may be the case that many users are unsure of the feedback process within their organisation. It is possible channels exist in their organisations with the users just need to be made aware of them.

The feedback from the interviews suggested it would be worth the effort involved to implement feedback process. The analysis of the feedback could then be aligned to both the gap and impact analysis of policy itself.

In closing, Information Security Policy should be aligned to the business needs with the focus being on that of the primary audience; the end users.

5.3 Research Impacts

During the research work on this thesis document project team came across number of factors that created limitation during the study.

The project team believes that the research analysis submitted within this thesis document presents a relatively high level overview and view of implementation of Information Security Policy process within organisations and also in the consideration of end user feedback prior to and following the policy implementation of this process. However, the biggest limiting factor during this research project, was the limited time available. This project work has been fully completed alongside our day to day family lives, working lives and student lives. The team believes that these particular issues are related to all students and that it may highly impacted other projects. The biggest weakness during this process was to balance other college requirements and continuous assessments within the project cycle. The project team feels that possibly having longer time frame for this research, more deep analysis would have been completed and more relevant data would be detailed in the documentation. We are fully aware that the requirement for completing this course is to finalise the research project while also balancing work between other studies and academic requirements for other subjects.

The project team believes that within given time constrains the full effort has been accomplished to fulfil college requirement and complete this study.

The other factor that limited research work was lack of responses to the self-administrative survey that team have undertook as part of the primary data collection and analysis.
Within the given tools, the team was not in position to track number of non-responses, but team believes that non-responses were part of assumption that participants had no familiarity with the subject of Information Security within their organisations. According to O’Leary, the lack of response might be an outcome from not having enough trust in the project team and/or enough confidence in participating in survey (O’Leary 2010). The team concluded that it wouldn’t be the case but more likely the factor of individuals not having enough knowledge and awareness about the topic.

Another limiting factor during this research activity was the limited skill regarding academic research and academic writing within individuals of the project team. The team had no expertise either independently or collaboratively in the academic research area (writing and analysis of secondary and primary data). The Team took into consideration that this is one of the limitation for all students in this academic course at Trinity College Dublin.

Although, team accepts that all the above factors might have potential negative effect on content and quality of the document. However, the best intention and commitment was given in order to submit this research work.

5.4 Possibility of Future Research

During research work on gathering information about Information Security Policy and computer cybersecurity, the team came across a number of areas where further research could be performed. With a longer time frame, the team believes that topic of Information Security could be expanded and enhanced by the inclusion of interviews being conducted with End Users to gather their opinion included in the project as analysis on its own. A targeted population of End Users would improve the quality of statistics and extend the work to focus more on users. Furthermore, research that would include the majority or equal share of responses from End users would support more detailed and inclusive results.

The findings presented from the primary data suggest that avoiding security incidents within organisations means engaging with end users during the process of the implementation of Information Security Policy. If not including the End User opinion and point of view during the implementation process of policy as part of a day to day process to improve efficiency and productivity, should they be included in such process at all? End Users are those that must adhere to this documentation, so the question that arises here is: “Is a training and awareness program considered enough?”

A study presented that educating, training and completing awareness is not enough. End users should be fully engaged during the process of creation, adaptation and implementation of policies, processes and procedures in organisations.

A more detailed project could be undertaken with the focus on the End Users perspective, including their approach, attitude and behavioural factors on limitations that arise from following Information Security Policy requirements and rules.
References


ISO, 2015. Directives and Policies, Available at: 

ISO, 2013a. ISO-IEC 27001:2013, Available at: 

ISO, 2013b. ISO-IEC 27002:2013, Available at: 

ISO, 2010. ISO-IEC 27003:2010,

Kahn, R.L. & Cannell, C.F., 1967. The Dynamics of Interviewing: Theory, Technique, and Cases, Wiley. Available at: https://books.google.ie/books?id=h7gCLgEACAAJ.


Lewis, P. & Thornhill, A., 2009. Research methods for business students,


PriceWaterhouseCooper, 2013. *10 Minutes on the stark realities of cybersecurity*,


Appendix

A.1 Survey & Interview Questionnaires

A.1.1 Information Sheet for Prospective Participants

Please be advised of a potential conflict of interest as we are using existing professional relationships to further advance the research of our project.

The online survey participation should take no longer than 10 minutes to complete. You are free to exit the survey at any time.

Your participation in the online survey is completely anonymous. There is no need to enter any identifiable information regarding yourself or your place of work. Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.

We will ascertain the impact of policy implementation from a broad spectrum of users. We will analyses the relevant results for presenting them in our dissertation document. This will be published to the School of Computer Science and Statistics of Trinity College Dublin. The aim of the online survey is to examine Information Security Policy implementation within an organisation.

Interview participations should last no longer than 20 minutes.

The interview will consist of several questions related to Information Security Policy Implementation within your organisation. You have no obligation to answer these questions and you may opt out at any time without penalty.

Should you have any questions or wish to have any of the information provided omitted from the Interview or online survey our contact information will be provided below. In the unlikely event that any illicit activity is reported, we will be obliged to report it to the appropriate authorities.

Participant and third-party anonymity will be preserved in analysis, publication and presentation of resulting data and findings.

If you have any questions, please contact lead researcher David O’Shea on oshead5@tcd.ie Thanks and regards
A.1.2 Informed Consent Form

LEAD RESEARCHERS: David O Shea, Barbara Pires, Robert Stanley

We are conducting research regarding Information Security Policy implementation and the adoption of policy within organisations.

PROCEDURES OF THIS STUDY

There is an interview that should take no longer than 20 minutes to complete and there is an online survey that should take no longer than 10 minutes to complete. There is no obligation to answer the questions and both the interview and online survey can be concluded at any time.

PUBLICATION: This will be published to the Computer Science and Statistics faculty of Trinity College Dublin.

Individual results may be aggregated anonymously and research reported on aggregate results.

A.1.3 Declaration

I am 18 years or older and am competent to provide consent.

I have read, or had read to me, a document providing information about this research and this consent form.

I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.

I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.

I understand that if I make illicit activities known, these will be reported to appropriate authorities.

I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.

I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.

I understand that my participation is fully anonymous and that no personal details about me will be recorded.
I have received a copy of this agreement.

A.2 Statement of investigators

Responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS: oshead5@tcd.ie, pudlowsb@tcd.ie, stanlerd@tcd.ie

Date: 02/02/2015

1. Declaration
2. Agree
3. I Do Not Agree

Q1: What Business sector are you currently working in? (Please select one)

Financial Services
Government
Healthcare
IT and Telecom
Insurance
Consumer Goods
Other (please specify your business sector, we do not require the name of your organisation)

Q2: Which of the following describes your role in your organisation? (Please select one)

Management
Part of IT Team
End User
Other (please specify)

Q3: Approximately how many employees work at your organisation? (Please select one)

Less than 50
Between 50 & 250 More than 250
A.3 Information Security Policy

Q4: You are aware of your organisation's Information Security Policy (Please select one)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q5: You are involved in the creation of the Information Security Policy in your organisation (Please select one)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q6: End user feedback is considered prior to the implementation of Information Security Policy (Please select one)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q7: End user feedback influences the Information Security Policies created for your organisation (Please select one)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q8: Does user behaviour within your organisation influence Information Security Policy decisions or is it a result of external influences? (Please select one)
User behaviour
External influences (e.g. Industry recommended standards)
Neither Agree or Disagree
Disagree
Both
Other (Please specify)

**Q9: Information Security Policy decisions are the result of:**

User behaviour
External influences (e.g. Industry recommended standards)
User behaviour and external influences

**Q10: Your organisation’s Information Security policy (Please select all that apply)**

- It has been reviewed and updated within the year
- It was formally approved by Senior Management
- It has been communicated to all relevant staff (including staff, contractors, temporary employees and third parties)
- It contains a definition of the organisational structure of information security
- It addresses the legal aspects associated with security
- It regulates the role and duties of employees

**Q11: Your organisation evaluates the quality and effectiveness of Information Security in the following methods (Please select one from each row)**

- Regular assessment by internal audit department
- Regular assessment by a consultancy
- Comparison with competing organisations
- Official certification within Industry & International Standards (PCI; ISO/IEC 27001)
- Self-assessment by staff, IT and IS Department

**Q12: How are you informed about the Information Security Policy within your organisation? (Please select all that apply)**

- Induction Training
- Online Training
- Personal / Group Training
- Via email
- Other (please specify)
Q13: How are you informed about the Information Security Policy within your organisation? (Please select all that apply)

- Induction Training
- Online Training
- Personal / Group Training
- Via email
- Other (please specify)

Q14: This method informs you adequately of the Information Security Policy (Please select one)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q15: Information regarding the Information Security Policy is distributed within your organisation :( Please select one)

- Weekly
- Monthly
- Quarterly
- Bi-annually / annually
- Never

Q16: Is your acceptance of the IT policy mandatory? (Please select one)

- Yes
- No
- Unsure

Q17: The following are covered by your organisations Information Security Policy (Please select all that apply)

- Data / Information classification
- Data / information storage / destruction
- Data privacy / protection of personal data
- Passwords requirements process
- Rules for clean desk / desktops
- Use of mobile and portable devices (tablet, Smartphone, flash drive etc.)
- Use of internet and e-mail
Q18: Information Security awareness has a positive impact on your responsibility in the organisation (Please select one)

Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree

Q19: You are fully aware of what is forbidden and what is acceptable in your organisation (Please select one)

Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree

Q20: The Information Security Policy has a negative impact on your ability to work (Please select one)

Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree

Q21: There is a good level of understanding throughout your organisation of the Information Security Policy (Please select one)

Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree

Q22: Your feedback is considered in relation to Information Security Policy implementation (Please select one)

Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree

Q23: What, in your opinion, (if any) would improve Information Security policy awareness in your organisation? (Open question)

Q24: How is feedback related to Information Security Policy collected within your organisation? (If feedback is not collected please enter N/A) (Open question)? (Open question)

Q25: The following measures are taken to increase the efficiency of Information Security within your organisation (Please select one from each row)

- Implementation of additional security tools
- Implementation of automated access control and account management
- Implementation of continuous improvement, monitoring & controls process
- Implementation of key performance indicators (scorecard)
- Outsourcing of selected activities in the area of security
- Standardisation based on a unified system of control procedures

Q26: Your organisation is concerned about the adoption of the Information Security Policy by employees (Please select one)
- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

Q27: Your organisation has taken the following measures to minimise the potential risk arising as a result of staff changes (Please select one from each row)

- Development of a knowledge management program
- Regular review of user access management procedure (Leavers / Departmental transfers)
- Evaluation and improvement of monitoring / controlling of changes within information systems
- Implementation of data leakage prevention
- Other (please specify)
Q28: We would like to thank you for taking the time to complete our research survey. If you have any feedback or suggestions then please complete the comment box below (Open text box)

Q29: Do not submit, exit without submitting (Only tick if you do not want to submit your survey)

A.4 Interview Questions

1. Does your organisation have any facility available where users can submit their feedback regarding Information Security Policy Implementation? If so, what type of facilities is present?

2. Does / would your organisation find such a facility beneficial, if so, how?

3. Does / would such facility impact policy implementation and further amendments / changes through your organisation to such documentation?

4. Does your organisation conduct an impact analysis following Information Security Policy Implementation? If so, what type of measurements is present? What does this information indicates?

5. Does / would you as a member of Management Team fined the impact analysis beneficial and if so, how would you use such information for further changes documentation and processes?