

University of Portsmouth

Computing & Mathematics Programme Area

Final year project undertaken in partial fulfilment of the requirements for the
BSc (Honours) Degree in eCommerce & Internet Systems

Computer Security Policies: Towards a Secure and Open Alternative

By **Michael Pegg**

Supervisor: Dr Dave Billinge

Project unit: PJS30

2010

Abstract

Computer security policies are a matter of considerable importance to all companies that rely on electronic data storage to safeguard their information. Computers absent from these policies and guidelines may result in a loss of data and have a serious negative impact on the company.

The system security enforcement mechanisms that form computer system security policies are however, for many of the corporate and governmental companies and organisations that rely on them not published or viewable by other corporate entities that may benefit from this information.

This project critically discusses current policies, guidelines and standards that are currently in practice in real companies and organisations and progress to discuss the technologies that are currently available with the aim of envisaging a new concise framework of security policies for computer systems that would benefit all companies that choose to use its policies.

This new framework is open in nature and freely available to all that require it. This method of openness aims to give greater security for *all* companies that aim for a secure computer environment.

"The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts." William Osler 1849-1919

Keywords: security policies; open security; security models; security framework

Acknowledgements

Firstly I'd like to thank all the people who completed my user questionnaire; it helped me find some particularly insightful unique information. Special thanks must be given to the IT Security Managers who withstood my barrage of constant questions, thanks for sharing your time with me at no benefit to yourselves. My supervisor Dr David Billinge must also be thanked for his direction and general yes-but-have-you talks and not by any means least my friends and family for putting up with my many lost weekends; I'll stop working on it now, honest.

Table of Contents

1. Chapter 1 - Introduction	7
1.1. Background - No Computer Is An Island	7
2. Overall Project Aims	8
3. Research Questions	9
3.1. What relevance do security models have to security policies?	9
3.2. What computer security policies are currently being used?	9
3.3. What are the sources of current policies?	9
3.4. What are the opinions of computer security personnel to currently active security policies?	9
3.5. What do computer security personnel consider should be included in security policies?	10
3.6. Should security technologies be included in security policies? And if so which?	10
3.7. Are there any areas that need to be covered in policies that are not currently?	10
3.8. How much relevance do user passwords have to security?	10
3.9. What do system users think of current security policies?	10
4. Project Guidance	11
4.1. Chapter Overviews	12
5. Constraints	13
5.1. Coverage of Existing Security Policies	13
5.2. Security Techniques Available.....	13
5.3. Hardware and Software Limitations.....	13
5.4. Time.....	13
6. Models, Guidelines and Policies	14
6.1. Security Models.....	14
6.2. Security Guidelines.....	14
6.3. Security Policies.....	14
7. Chapter 2 - Primary Research	15
7.1. Overview	15
7.2. Methodology	15
7.2.1. Project Direction	15
7.2.2. Method of Research	16

8.	Interviews.....	17
8.1.	Scope Stated to Individuals	17
8.2.	Questions Asked.....	17
9.	Interviewees.....	18
9.1.	Interviewee #1.....	18
9.2.	Interviewee #2.....	18
9.3.	Interviewee #3.....	18
9.4.	Interview #1: EADS Astrium Feedback.....	19
9.5.	Interview #2: Company X feedback	24
9.6.	Interview #3: Company Y feedback.....	26
9.7.	Interview Review.....	27
10.	Questionnaire	28
10.1.	User Group	28
10.2.	Pre Questionnaire Statement	28
10.3.	Questions Asked.....	29
11.	Chapter 3 - Literature Review	30
11.1.	A recent history of ‘missing data’ from systems with secure policies.....	30
11.1.1.	November 2007.....	30
11.1.2.	July 2008.....	30
11.1.3.	January 2009	30
11.1.4.	May 2009.....	31
12.	Current Policy review.....	32
12.1.	ISO/IEC 27001:2005	32
12.1.1.	Plan.....	34
12.1.2.	Do	34
12.1.3.	Check.....	34
12.1.4.	ACT	35
12.1.5.	Advantages and Disadvantages of ISO 27001.....	35
12.1.6.	Critique	35
12.2.	Technical Risk Assessment	37
12.2.1.	Advantages and Disadvantages of the Technical Risk Assessment	40
12.2.2.	Critique	40

13. Chapter 4 – Discussion & Review of Information Gathered	41
13.1. Questionnaire.....	41
13.1.1. Question 1	41
13.1.2. Question 2	42
13.1.3. Question 3	42
13.1.4. Question 4	43
13.1.5. Question 5	44
13.1.6. Question 6	44
13.1.7. Question 7	45
13.1.8. Question 8	45
13.1.9. Question 9	46
13.1.10. Question 10	46
13.1.11. Question 11	47
13.2. Cross Referencing of Results	47
13.3. Questionnaire Summary	48
13.4. Technological Approach	49
13.4.1. Encryption	49
13.4.2. Passwords.....	50
13.5. Open Source	52
14. Chapter 5 - Conclusion	54
14.1. Research Questions.....	54
14.1.1. What relevance do security models have to security policies?.....	54
14.1.2. What computer security policies are currently being used?	54
14.1.3. What are the sources of current policies?	54
14.1.4. What are the opinions of computer security personnel to currently active security policies?.....	54
14.1.5. What do computer security personnel consider should be included in security policies?.....	55
14.1.6. Should security technologies be included in security policies? And if so which?	55
14.1.7. Are there any areas that need to be covered in policies that are not currently?	55
14.1.8. How much relevance do user passwords have to security?	55

14.1.9.	What do system users think of current security policies?	56
14.2.	Conclusion of Research Questions	57
14.3.	Suggestions.....	58
14.3.1.	Free.....	58
14.3.2.	Online	58
14.3.3.	Open Source	58
14.3.4.	Reasoning Stated.....	58
14.3.5.	Focus on Technology	59
14.3.6.	Constantly Updated	59
15.	Project Reflection.....	60
15.1.	Project Issues.....	60
15.2.	Decisions Made	61
15.3.	Project Management Issues.....	62
15.4.	Future Research and Development	63
16.	Bibliography	64
17.	Glossary of Terms	66
18.	Appendix A: Project Initiation Document.....	67
18.1.	Basic details.....	68
18.2.	Outline of the project environment and problem to be solved	68
18.3.	Project aim and objectives	69
18.4.	Project deliverables.....	69
18.5.	Project constraints	69
18.6.	Project approach	70
18.7.	Facilities and resources	71
18.8.	Log of risks.....	72
18.9.	Starting point for research	74
18.10.	Breakdown of tasks	75
18.11.	Project plan	76
18.12.	Legal, ethical, professional, social issues	76
19.	Appendix B: Ethical Checklist.....	77
	Ethical Examination.....	77

1. Chapter 1 - Introduction

1.1. Background - No Computer Is an Island

While it was once true that computers stood alone, unconnected and isolated from one another, this view has quickly and vastly changed. The networking of computers into Local Area Networks that started with larger universities and research labs with an interest and need to spread digital information between them has developed and evolved. Today through the work on ARPANET and the development of the Internet seventy percent of UK households now have access to the Internet (Office for National Statistics, 2009).

Through the many iterations of these computer networks; security models, policies and guidelines have been developed, issued and adopted for use in corporate and governmental use however, security on these computer systems that are 'protected' by these security policies are frequently vulnerable to hacker attacks, breached by easily correctable user errors and utilize outdated security methodology.

Current security policies are utilized as a formal model and are intended to show the steps that are required to be achieved to classify a system as secure. It is important to first recognise the purpose of these security models as the main barrier protecting business continuity and minimising damage or misuse of company data (Katzan, 1974) by minimising any negative impacts from computer security incidents. The policy exists to aid in the exchange of data whilst ensuring the protection of information and computing assets and must incorporate three basic components:

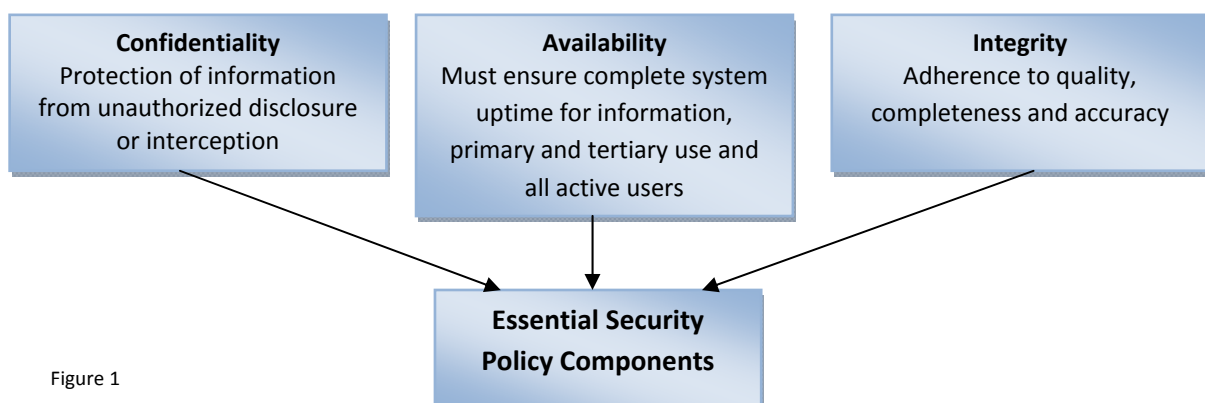


Figure 1

It is important within this project to criticise any and all assumptions on what makes a security policy secure. Computer security threats have increased year on year since the Internets conception (entrepreneur.com) however no current method of security policy has done enough to stand this tide, now is the time to develop and adapt to a new way of dealing with computer security.

Initial security models themselves such as the Bell-La Padula model which focused on enforcing access control in government and military applications serve as secure methods ideal for input and output of data and their secure procedures are now inherent in all

modern computer systems that deal with the granularity of access controls. These models created in the 1970's for mainly military purposes however do not themselves specify protection mechanisms, deal with systems that are connected to the Internet or any of the many other components of modern computer environments that exist and as such struggle to adapt to current security needs on multiple levels.

2. Overall Project Aims

This project aims to discuss computer security policies with an overall goal of producing new insight into a way of devising a computer security policy that deals with security at the layer of protection mechanisms, supports devices on secure local networks and also systems with connection to the Internet that require the highest level of protection possible all within a means that has the flexibility to be updated when current measures are compromised and in a manner that aids all that comply with it. This technique it is hoped aids in offering an easy to adopt set of secure system policies that are relevant, sourced correctly, deals acutely with the specified areas whilst also having the widest reach possible.

In addition to the overall project aims this project should also provide a useful tool for researchers, academics and students wishing to gain an insight into the current level and methods of computer security protection mechanisms, how companies deal with these issues and how they see the current security landscape.

Secondary research on existing security policies, models and the relevant protection mechanisms are gathered from academic texts including white papers and journals. Given the context of the issues of computer security secondary research from news sources are used, primarily to show past issues and the associated problems however, personal comments are kept to a minimum to avoid bias of any kind and only reliable information from authenticable sources is used. All literature reviewed for this project that is relevant and used to advance the project is the subject of a discursive review in relation to the project thesis growth.

Primary research is conducted via several stages interviews to gather information from current industry IT security personnel at sufficient level where decisions must be made and decided. This form of research is used to gather inputs on the current state of policies, issues and what they consider the future is for security policies. I also conduct a detailed questionnaire to issue to people working under these security policies to garnish a user prospective of technologies used, how secure they feel the computer security they use within their own environments are and to gather some usage patterns of what activities they do and do not conduct on these systems.

This project, using the methods mentioned above aims to provide a set of policies that broadly cover all areas discovered of concern within the computer security spectrum. By covering these areas a greater chance of adoption would be expected which would further aid in the security offered to all.

3. Research Questions

As this project deals with computer system security policies, research is engaged on background environment and understanding of the subject area. The research questions set answer questions relevant to the subject area and aid in the final conclusions gathered. The range of questions pondered as research questions aim to cover all available areas that are necessary to form concise decisions and what steps must be taken on final security policy decisions. The end date for the projects research date was set at the 31st of March, after this period no more inputs of data were accepted. With the speed of computer security and regular data breaches (and their inherent fixes), this limit was set to ensure enough time is reserved to reach conclusions which are well researched.

3.1. What relevance do security models have to security policies?

With this question I aimed to investigate what a security model is, what are the most common and what are the differentiators between them. I also look at how they relate to security policies and how access controls function in this environment.

3.2. What computer security policies are currently being used?

This question aims to divulge what computer security policies are currently in use in industry at companies that have an adopted set of security policies. This information is gathered from interviews with computer security personnel in a number of companies but also from published documents relating to active security policies.

3.3. What are the sources of current policies?

This question aims to discover the source of policies currently used be this from corporate documentation, industry standards or at the will of the security professionals enacting the policies. A review of available literature and through guided interviews I aimed to find only reliable sources as to what the sources are for current policies that are in use.

3.4. What are the opinions of computer security personnel to currently active security policies?

With respect to the currently active security personnel, what areas of currently active policies on the company networks and computer systems do they deem to be inadequate or not fit for purpose, which policies comply well to their purpose and which policies do they think need to be improved (regardless of if they have a solution).

3.5. What do computer security personnel consider should be included in security policies?

With this question I aimed to discover what security personnel consider needs to be included in the policies that govern their systems. This may relate to varying types of policies that specify certain restraints or limits; be this positive or negative and also could lead to initial thoughts on technologies.

3.6. Should security technologies be included in security policies? And if so which?

I aimed to discover if technologies such as encryption mechanisms should be included within security policies. If discovered to be positive this may lead to an investigation on technologies with related positive and negative implication.

3.7. Are there any areas that need to be covered in policies that are not currently?

With this question I aimed to discover what areas of policy are currently not present or lacking, be this in depth, relevance or method. I also aimed to discover with this question how the speed of updates reflects on policy alignment to company systems.

3.8. How much relevance do user passwords have to security?

Regarding password protection of systems, how much does this affect the security available on the system, what do security personnel feel about password systems used. Also I enquire directly to users about their passwords used on the systems.

3.9. What do system users think of current security policies?

I aimed to elicit how users of the systems discussed in this project consider the various aspects of the system to get a user overview of positive and negative statements.

4. Project Guidance

Due to the nature of this project (described in more detail in section 7) it is necessary to provide some guidance on its navigation to aid the reader in finding the information they require as this project does not follow a strict layout of introduction, literature review and conclusion as may be found in similar works.

Category	Headings and Page Numbers
Statement of project's context, aims and objectives	Introduction (p7-8), Overall Project Aims (p8), Research Questions (p9-10), Constraints (p13)
Critical review of relevant literature	Models, Guidelines and Policies (p13), Primary Research (p14-15), Interviews (p16-26), Questionnaire (p27-28), Literature Review (p29-30), Current Policy Review (p31-39)
Methodological approach	Methodology (p14-15), Project Reflection (p60-63)
Primary research & results	Review of Information Gathered (p40-52)
Evidence of project planning and management	Project Initiation Document (p63), Constraints (p12), Project Management Issues (p62), Project Issues (p60-61)
Summary, conclusions and recommendations	Conclusion (p54-59), Project Reflection (p60-63)
Overall understanding and reflection	Project Reflection (p60-63)

4.1. Chapter Overviews

Chapter	Title	Description
1	Introduction	Provides a brief introduction to the project and the environment.
2	Overall Project Aims	States what the overall aims of the project are and what I aim to achieve.
3	Research Questions	Describes what questions I aim to answer with my research.
4	Chapter Overviews	Aimed to give an overview of chapters included in this project to aid in finding the required information.
5	Constraints	What constraints will affect the project?
6	Models, Guidelines and Policies	Discusses the differences between the three different forms of computer security documentation.
7	Primary Research	An overview of what primary research I have conducted and what methodology I have used.
8	Interviews	How I conducted interviews and what questions I asked them.
9	Interviewees	Who I interviewed and what feedback they gave.
10	Questionnaire	Why I conducted a questionnaire, the questions asked and the pre-statement I gave to users.
11	Literature Review	A study on the recent history of data loss.
12	Current Policies	Discussion on policies discovered, this covers the ISO and TRA documentation.
13	Review of Information Gathered	Provides the feedback of information from information gather from questionnaires and interviews including a brief overview of some areas discovered.
14	Conclusion	A conclusion relating to the research questions asked and suggestions for project implementation.
15	Project Reflection	Feedback on how I conducted the project and what could be improved.
16	Bibliography	A list of the references used within the project.
17	Glossary of Terms	A list of terms that may provide useful for readers of this project.
18	Appendix A: Project Initiation Document	The initial Project Initiation Document that was generated before the start of the main project work.
19	Appendix B: Ethical Checklist	The ethical checklist to ensure ethical practice within the project.

Figure 2

5. Constraints

5.1. Coverage of Existing Security Policies

Due to the nature of existing security system policies the study of existing security policies must be restricted to that of major, publicised policies that exist within the possibility of research. Although it must be considered that policies are individual in nature for each individual company the range of possibly policies must be limited to what is discovered at companies and what is currently in use.

5.2. Security Techniques Available

With a project based around security hardware, with evidence based on primary and secondary research I must limit judging my findings on current working practice; this constrains me to use what techniques I find available and thus what is technically possible. If technologies are found to be appropriate this is mentioned however for the sake of review no technologies are mentioned that do not fit with known researchable techniques or techniques that have no support documentation.

5.3. Hardware and Software Limitations

The world of computing and the overheads associated with some levels of security protections such as encryption protocols must fall within a sensible barrier. A secure system that requires 60 minutes of processing time for each keystroke would be of little use. When considering implementation of techniques I do not consider any suggestions that would clearly be impractical to implement or are clearly not within sensible hardware or software limitations.

5.4. Time

Time was an important factor in the project development as all work had to be completed for the 7th of May 2010. During this period other projects and work had also to be completed. This limitation was factored in to the project development. Although time limitations clearly exist through clear project planning via the Gantt chart as seen in the Project Initiation Document (section 18.11) many of these issues were alleviated.

6. Models, Guidelines and Policies

Due to the similarity of models, guidelines and policies in the environment of computer security it is important to state early in the project the main differentials between these three different security documentation types.

6.1. Security Models

Security models are by definition “a scheme for specifying and enforcing security policies” (Krutz, 2001) and form the underlying schema of computer security infrastructure, some examples of security models are access controls (users, group and access permissions) with the most prominent being the Bell-La Padula model and the Clark-Wilson model, a model used in secure environment to form a foundation for “formalizing [] information integrity” (Clark & Wilson, 1987).

6.2. Security Guidelines

Security guidelines are a collection of best-practice procedures that have “no mandatory actions” (Axel, Gerrit, & Walter, 2005), often uses words such as “should” and “may” and are intended to aid users actions while utilising computer systems. They are intended to be used “to address an area of the security policy” (International Organization for Standardization, 2005) and as such are the least important of the three security documentation types.

6.3. Security Policies

Security policies form the decisions in which “constraints on behaviour [], mechanisms, [and] access by external systems and adversaries including programs and access to data by people” (Roberts, 1990) are decided. As such they form the core of what can be decided and set by security personnel, be this security mechanisms such as encryption, programs that have the required security or what minimal password settings must be used by users.

As such the focus of this project will be on security policies as it forms the core set of dynamics to computer security that can be changed and altered at the whim of security personnel to ensure a secure system to deal with security issues and vulnerabilities as they occur.

7. Chapter 2 - Primary Research

7.1. Overview

This project is concerned with computer security policies and unfortunately for research results in this field providing little in openness and sharing of information. There is generally a lack of academic research (Axel, Gerrit, & Walter, 2005) on this exact area of research coupled with the secrecy inherent in most companies behind security techniques. There are however, several published standards that most companies adhere to, which I will cover in secondary research.

The target audience for the primary research forms two distinct groups based on the research questions formed from the aims of the project. To address these questions, questions must be asked from that of an overview position from a person or persons who are capable to answer questions on how security policies were chosen, why they were chosen and work in the area the project covers. The second distinct group must be that of users of these secure policies to elicit answers on how the systems work for the users. Concerning user analysis for target audience no limits are to set for targeting due to the nature of the project goals.

7.2. Methodology

7.2.1. Project Direction

From the initial project initiation document I had a differing direction for my project based on producing a physical example of a security model and to “Design and implement a High Security Remote Data system model” that would have shown a physical example of my project with focus on enabling through the use of the security protocol the final project details a remote data system that would enable users to have greater security no matter of their location and was intended for military purposes. Due to the time constraints on the project however I was advised by my project supervisor to focus my attentions on production of a study project and that a physical artefact would be a minor step that may limit my reach and quality of the considerably more important study element of this project.

With this in mind I have produced this study project and through this document produced the necessary background to create, if required, a physical artefact of the policies listed.

7.2.2. Method of Research

To address the lack of information provided for use in the project I have conducted two types of primary research. These are direct interviews with IT managers who must be in a position to directly view and also change how security policies are set within the company, these interviews address many of qualitative questions set in the research questions section to elicit broadly how policies are set, why and from what sources. The second source of primary research is gathered from questionnaires. The questionnaires are only given to users of computers within a company that adheres to a computer security policy of some nature. This method of questionnaire issuing gives feedback to the other quantitative based questions set in the research questions based on user feedback on systems and also password based feedback.

To gather feedback to the questionnaire within the project constrains, mainly due to the time constraint I decided to use an online questionnaire off-the-shelf solution, this aided in time to construct the questionnaire and also to disseminate and gather results at a faster rate over a traditional paper based medium and also aids in removing any geographically limiting factors.

Firstly I will discuss the qualitative interviews before moving on to the quantitative questionnaires.

8. Interviews

8.1. Scope Stated to Individuals

The scope of the project explained to individuals, with effort made not to direct questions and limit possible answers given was issued as such at the beginning of the interview, this was done to give the individual an overview of the project without leading the individual to give certain answers based on preconceptions of what I wanted to achieve: “I am conducting a final year project on IT security policies and standards, their benefits and limits but also I am concerned with the associated technical surroundings including areas such as remote access to internet systems”

8.2. Questions Asked

The initial questions planned to ask were the following, however I ensured I let the individual give answers freely and deviate where necessary and referred to direct questions only when the individual had finished giving a response.

The Questions asked were:

1. *How many users do you administer IT security over?*
2. *Do you follow any IT security policies for IT security? (If so what are they? – ISO 27001)*
3. *How did you know to follow this policy?*
4. *How do you keep up to date with security changes?*
5. *What do you think of current policies?*
6. *Are there any areas you think policies should cover?*
7. *What remote access do you allow to connect to the internal system? (If so what are they?)*
8. *What is your password policy?*
9. *Any areas you think are relevant?*

9. Interviewees

Note: Interviewee number two and three wished not to be named directly and also for the company involved not to be named for security purposes. This reluctance to give freely any information about their security systems to individuals even for academic purposes shows how seriously security information is currently viewed by IT managers; I discuss this outcome later in the project reflection (section 15).

9.1. Interviewee #1

Company: EADS Astrium

Company Brief: Satellite engineering company for commercial and military.

Company IT headcount: ~10,000

Job role: European IT Security Manager

Name: Mr. Jim Cork

9.2. Interviewee #2

Company: Company X (Not stated at request of interviewee)

Company Brief: Telecommunications Company.

Company IT headcount: ~20,000

Job role: UK IT Security Manager

Name: (Not stated at request of interviewee)

9.3. Interviewee #3

Company: Company Y (Not stated at request of interviewee)

Company Brief: Human Relations Company.

Company IT headcount: ~3,000

Job role: Security Manager

Name: (Not stated at request of interviewee)

Note:

#Comments in this format# are directions to the interviewee to ensure the question stated is answered.

9.4. Interview #1: EADS Astrium Feedback.

EADS Astrium has 10,000 employees and all fall under the remit of the European IT Security Manager. His initial policy document is based on the EADS security policy and this covers most of the IT security issues for the company however, for the each nation country a set of deltas are issued to for fill the requirements for each countries specific needs and laws. For example the French and German EADS sites operate similar rigid standards while the Spanish and Italian EADS sites are more lenient with how IT policies are enacted. Commerical projects also differ to Military with the level of security that may be applied differing between them.

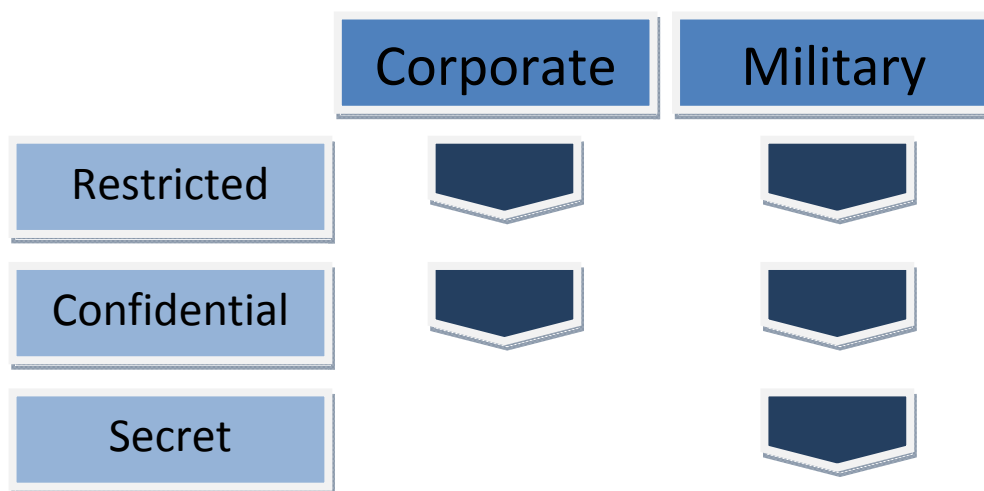


Figure 3

New projects that start at the company must fall broadly within the EADS policy however each projects security is given by the requesting company via the PSI (Project Security Instructions), which if not available as generally is the case by new customers this document can be worked on and decided by consultation between Astrium and the client. This document covers how the project itself will be run in a physical sense, the IT security itself although may be referenced in a physical sense is always running on the Astrium network and as such will largely will fall within the standard security remit. The PSI is the linchpin of security protocol to use for each project. For Astrium each satellite will have its own PSI document however, this document may well vary between countries where different government and company standards apply. The levels of security between commercial and military projects often have variation between their aims; this often pivots on what information they hold to be most important. Where commercial companies will be more secretive over test results, military companies will edge security to cover designs more.

To decide upon new security documents for a new project a typical flow would be



Figure 4

This flow shows the importance of the customer and the customer specification as it defines the initial input to how IT security policies in the project will be followed.

However, in some projects such as EuroSat3000 (and Galileo) government involvement meant a minimum of 50 of each nation's personnel must work on the project and as such initial specification was set not by the individual customer but by government involvement.

The projects data is owned by the project and not by the IT security personnel and they initially stipulate directly how cascaded security restrictions are within projects. This is often due to the customer knowing which data is more sensitive than others and this often plays within the write-up of the PSI.

The United Kingdom, Germany, Spain, Italy and France have agreed levels of national security and all follow the general security levels of Restricted, Confidential and Secret. These levels are used within projects that overlap many countries. However, these levels often follow different exact standards e.g. Germany and Italy run a level of encryption that falls below that of UK MOD requirements and as such concessions and adjustments must be made to work within these levels. When project data from Germany is imported to a UK MOD environment data is wrapped within tighter encryption to ensure it is accepted.

Relates to question 4:

To keep up to date with current security information conferences and web sources are used with the majority of work conducted to enhance IT security being done by Astrium personnel. Typical IT security budget of a FTSE100 company roughly €4m, Astrium budget £250,000. Astrium's external IT security focus is similar to a police approach with profiling of potential infringers as basis for security approach. ISO 27001 covers Infrastructure while ISO 27002 covers policy making. ISO 27002 is more relevant to the IT security approach taken at Astrium. He states that the problem with ISO 27001 is that it can cover only one section of development in a project or just one room in a company and as such adds little value however, he agrees it does form an ideal base to develop IT security protocols. Just because a company is ISO 27001 certified does not mean the whole business is or that even a whole project is. He argues that it is purely a "paper exercise" and does not relate directly to how security is run in the majority of companies.

Relates to question 5:

Current Standards (ISO 27001) can be easily manipulated and does not mean the IT security environment is secure. The standards only function as a base line. Day to day operations of most companies will not fall within these standards, even those that are 'compliant' to the standard. "Paper exercises" overhead like that of ISO 27001 can slow business processes more than the benefit it gives.

Relates to question 6:

Standards should be more pragmatic and should operate in a manner more related to facts each company. If standards are set, like in ISO 27001 people will only cover the bare minimum to be accredited. Impractical daily checks are the only way to currently make sure current standards are in place and working. Standards should be more goals orientated and based on forward momentum developed via project progression. Possibly different levels of accreditation on how well companies are accredited instead of pass or fail. External auditors only ask certain questions and as such companies will not offer failing areas for inspection. Technologies into standards although would be ideal would be impractical due to the fast changing nature of the IT security environment. Strict rule sets are often hard to set due to international regulations and customer specifications. The TRA or Technical Risk Assessment produced by the UK Cabinet Office however, does cover these protocols pragmatically. Instead of seeing if companies adhere to common goals it asks the company to show what it is doing and assesses it this way via a risk management matrix. The TRA is only available to government agencies and associates.

Relates to question 7:

Remote connections are currently only available via company laptops and via USB remote devices. These remote devices utilize a 3G wireless connection and connect to the company's network via a VPN. All remote connections must utilize a SSL connection. All data sent between the remote device and the company's network must comply with company policy. (At this point Mr. Cork points to issues with the system) Due to the USB connection it demands connections must be via devices with support USB and use existing drivers which are vulnerable to hacking. He would prefer a 'Secure ID' login system via a web browser which links to the company Active Directory system to authenticate and thus authenticates directly instead of connecting to the company systems before authenticating. Users of the current system must sign a user agreement stating where and when the remote connection may be used (airports for example are not acceptable due to security issues). A max number of remote users also exist.

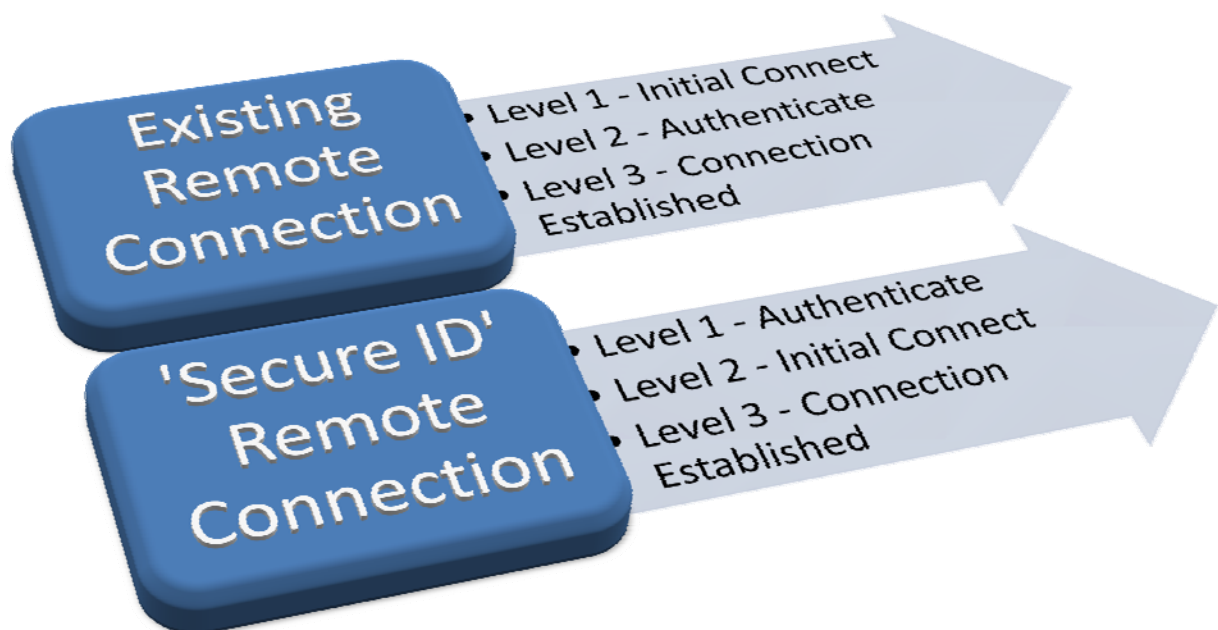


Figure 5

Relates to question 8:

Currently no password character limit set for minimum or maximum in the UK. #Begrudgingly Mr. Cork states that he would like# a minimum password of 12 characters which must include at least one capital letter, one lower case letter, one number and one none-alphanumeric character. He states he has not been permitted to set the password to this limit due to concerns of management that users will not be able to remember passwords. Mr. Cork rebuts that people should aim to set passphrases, not passwords such as 'mynameisjim1983' instead of a more obscure random assortment of characters that

would be hard to remember. This problem he states is an issue more with users than the system itself and is hard to overcome this user mindset. This setting of characters limits and range of character choices is aimed to stop hacking of user passwords. The system at EADS Astrium is set to limit the number of connections for each user account to five. After this limit has been reached the user account is locked and security informed if more connections are attempted. The eliciting of the password file from a system is the major concern for password security. This password file is encrypted however if this file is compromised and removed from the system a hacker will only be limited by time until he has access to all user passwords to the system. To ensure this file is secure measures are taken to ensure it is near impossible to transfer or copy.

Relates to question 9:

Be aware of all possible risks to the systems and ensure you keep up to date with attack possibilities via constant risk assessments. To ensure this is done you must ensure you have the technical skill and awareness to address these issues as they arise accordingly. A policy is not directly enough to safeguard security as differing levels of security must be used for different users. HR staff for example who have little technical knowledge must be able to adjust user accounts and temporary workers in some areas must have access to secure environments. Policies such as the ISO 27001 show maturity over initial standards but do not relate enough to ensure system security. For some customers they require ISO 27001 for initial launch but are in-flexible keeping up to date with issues of security and technological advances. Customers broadly do not ask for us to be ISO 27001 compliant due to its limited value. ISO 27001 is only a paper process, it is useless to state compliance with it as it is infrequently checked to ensure it is all still in order.

Any reported hacks are discussed with the company appointed Government Security Advisor (this is due to working on MoD projects). This individual discusses issues back and forth of what to expect but also expects to receive reports on attempted or successful hacking within the organisation. TEMPEST (a codename referring to investigations of electrical emissions) investigations and issues are conducted and secured. This TEMPEST requirement observes that electrical signals may leak from cables and be detected and hacked much like an unsecured wireless connection if the right equipment is available. To address these issues insulated cables are used to address this problem.

9.5. Interview #2: Company X feedback

Company X has 20,000 employees and all computer security in the UK is controlled by the UK IT Security Manager. The UK IT security manager must adhere to worldwide security policy however; almost all decisions are set within the UK. This decision was made to ensure decisions can be made with affectively.

Relates to question 2:

The company have been accredited to ISO 27001 previously however it is has been five years since the company was last accredited. (The manager comments that the company may not pass it if assessed today but does not seem worried by this). The company however does adhere to a document issued by the UK Cabinet Office called the Technical Risk Assessment, this document issued to companies working on government projects functions similar to the ISO 27001 accreditation but functions differently. It has no firm suggestions on how to rectify problems but instead deals with each area of risk and asks how the company is aiming to address this problem. The manager states this will always be more affective at securing systems instead of a loose set of steps that must be accomplished as with the ISO standards.

Relates to question 3:

ISO27001 accreditation is the industry standard and is heavily discussed on internal documents and educational courses. The Technical Risk Assessment however was issued to us on agreeing to take on government projects. To complete work for government agencies it was required that we achieved accreditation by the auditor, which we completed two years ago. We happened to be one of the few companies taking it at the time as it was relatively new so worked through the process with little past experience of companies who had taken it.

Relates to question 4:

Within our team we focus on day to day tasks however all members of the team check several websites, the main one being securityfocus.com, this site is the most commonly used for sharing and updating security issues with systems, hardware and software so it's ideal for our purposes, it also has a rather active community of other security personnel so word of issues gets around pretty quick. Some warnings on primarily software updates come from the cabinet office and some warnings however these are quite infrequent and only on severe issues and can't be relied upon. Adopting new security policies generally a matter of knowing what we are using on all the systems and rolling out automatic updates once the machines are in a sleep state although a couple of systems do require us to physically be at the machines, these are generally the ones where the computer is not in a bootable state yet.

Relates to question 5 and 6:

Current standards are working well for us; they enable us through ISO 27001 and the Technical Risk Assessment to get new work on these accreditations alone and give us a broad system for knowing what is and what is not covered however, the issue still exists that especially with ISO 27001 that they do not cover technologies or updates that happen on a near weekly basis. These written, printed and assessed standards are things that take time to complete and cannot deal with issues that are updating at these speeds.

Relates to question 7:

We do not allow remote connections to any of our systems. #Pressed for further information# We feel that remote connections give too much risk for too little benefit, if we enabled remote access via most methods that would have to be complied with for most applications the overhead of securing it would not be beneficial.

Relates to question 8:

Our password policy is set within the terms and conditions of employment and requires the user to set a new password once a month and this password must be at least six characters. We feel this is a good balance between security and the user being able to remember the password. Password loss is still common however a direct call to the helpdesk can restore it. I would always like to improve this with alpha numeric passwords etc but it is just not feasible. Most attempts to break into our systems are via passwords but little can be done to stop this other than setting a maximum number of connections.

Relates to question 9:

I would like to see technologies play a larger part in policy setting, why can't technologies such as encryption be set and agreed upon? I suppose it could be argued that policies are set to be broad but I think it is more a matter that they are made broad because due to the speed of changes they are unable to keep up to date. I think a system that all could agree with would be a useful asset if it was updated on a near-daily basis if accreditation of-sorts could also be agreed, otherwise it may purely be another overhead.

9.6. Interview #3: Company Y feedback

Company Y has 3000 employees and has a single Security Manager who deals with all security issues at Company Y. The company works in the sector of Human Relations and has a large number of temporary workers on-site and at other companies. The Security Manager sets all policies within the company and has direct control over any and all changes.

Relates to question 2:

As a relatively small company in terms of computer infrastructure we are more aimed at ensuring systems are secure and security is tight. #Asked again on standards with reference to ISO standards# We have looked at getting ISO 27001 accredited however the time and effort spent would give us little real-world benefit and only distract our security personnel. We have not looked specifically at any other standards other than single technical solutions.

Relates to question 3:

As I stated earlier we do not follow any standards directly but we do keep up to date with security from multiple channels. We ensure we keep aware of any issues stated from the main antivirus and antimalware companies and review many security websites that keep us up to date with any issues or changes in the world of computer security that we must stay aware of. There is a strong community of security personnel who work together to solve any problems that arise. How do I know if it is wise to implement a solution to alleviate one problem when I cannot see how they came to this solution? I may well be creating another problem.

Relates to question 4:

Security websites give us the main information for current issues and what must be solved. We then decide based on what the consensus for updating and correcting problems is from these sources, discuss it within and team and change as appropriate.

Relates to question 5:

As I stated earlier current policies require much time to implement and give us little benefit. I can see benefit that these policies may be useful if our customers requested them but I don't see this happening in for foreseeable future. If the policies themselves covered more exact topics that were relevant to keeping the day-to-day security checks updated it would be considerably more useful to us, not only would it cut down time for us to check any issues but also ensure we were at a high standard of security within our company.

Relates to question 6:

Technological issues would be a real benefit for us. Being a small company ensuring we have covered all issues is a real concern and all time must be spent ensuring this is the case. Ensuring we meet overall standards must always be a secondary issue to this. General guidelines exist in various forms for what are good ideas for setting security but when this is not sourced it is near impossible to tell if this is valuable information. For example when dealing with passwords there are multiple sources of information on what should and should not be set. The American department of defence has guidelines but the reasoning for

these reasoning's are harder to find due to their nature. At the end of the day most security personnel have to set a certain limit between security and usability of the system.

Relates to question 7:

We allow remote access to our systems over a VPN solution. The user logs into our website using their corporate login and this enables them to connect via Active Directory to their system. This is the only way other than basic email retrieval we offer to connect to our systems from outside the local network.

Relates to question 8:

We ensure passwords are changed every three months. #asked for more detail on any limits# we do not set any limits on minimum or maximum passwords or ensure any character limits, we feel this will not particularly raise the security only ensure people will write down passwords to ensure they remember them.

Relates to question 9:

I would like to see policies cover more on-hand issues such as passwords as you mentioned earlier but also technological issues so as and when issues arise the security community could agree on a set of standards and move forward as a group.

9.7. Interview Review

From the interview feedback gathered from several varied security managers it has become evident that many problems exist in the environment of security policies. With the information gathered from the interviews conducted this aids in generating what further information should be investigated in certain technical areas, security communities investigated and more exact questions and phrasing of questionnaires for secure systems generated. I will now move on to ask questions of security system users to aid in answering the other questions based on the research questions.

10. Questionnaire

To address several questions asked in the research questions (set out in the aims of this project, section 3) that could not be gathered from interviews I generated the following questions to enquire about them. The interviews conducted also aided in shaping and refining the following questions.

10.1. User Group

To ensure questions can be answered in the correct way I ensured the questionnaires were only been issued to individuals who have experience of working on secure computer systems and purposely did not issue any questionnaires to the general public. To ensure confidentiality, names were not taken and redundant questions that do not aid in answering research questions were not asked, such as sex of the user.

10.2. Pre Questionnaire Statement

The following statement was issued at the top of the questionnaire to give individuals a preface to the project scope, offer thanks and ensure anonymity and confidentiality assurance:

This questionnaire is part of my research for my final year project and as such, any help to complete this survey would be greatly appreciated. The project itself asks many questions about computer security and I hope the information gathered here will aid in answering some of those questions.

I would ask that you complete this questionnaire accurately and remember truthful answers are worth more than any other.

All answers given in response to this questionnaire are anonymous and confidential. If you wish to contact me regarding this questionnaire, please email me at mikepegg@gmail.com

Regards, Michael Pegg.

10.3. Questions Asked

I have issued eleven questions to users, all of which aim to answer research questions. The questions asked are as such:

1. What is your current occupation?
2. How many years have you worked in a business computer environment?
3. Have you ever been given access to a company's internal system from an external environment (e.g. Company laptop, home computer)
4. In this business environment, were you made aware of computer security protocol? (e.g. What should and should not be done)
5. Do/did you feel secure accessing the World Wide Web when using a computer in this environment? (Select all that apply)
6. If you had any questions on what the security protocols were/are in this business computer environment, do/did you know exactly where to visit or ask?
7. When using a computer in this business computer environment, how secure do/did you think you are?
8. Have you witnessed any security problems/breaches in this business computer environment?
9. Would you be willing to sacrifice computer speed to operate in a more secure environment?
10. In this business computer environment, is/was your password forcibly changed by the computer system?
11. In this business computer environment, what does/did your password contain?

11. Chapter 3 - Literature Review

11.1. A recent history of 'missing data' from systems with secure policies

11.1.1. November 2007

As was widely reported in the press (BBC News, 2009) two compact disks that contained the personal details of all families with a child under the age of 16 went missing. This data amounted to the personal details of 25 million UK citizens. This major data leak led to the resignation of the head HM Revenue & Customs and even though a reward of £20,000 was offered as a reward for returning the data, no further sign of this data has been seen since.

The two compact disks containing the HMRC's entire data on child benefit were password protected but were not encrypted in any way and posted via internal post (using public courier TNT) from the HMRC to the National Audit Office. This failure, affecting over 42% of all families (Office for National Statistics, 2007) led to a justifiable public concern of the security of their personal details

11.1.2. July 2008

The Ministry of Defence admitted (BBC News, 2008) having 658 laptops 'stolen', 89 'lost' and 121 USB memory storage devices falling somewhere between the two categories since 2004. Concerning the devices lost during 2008, nineteen were labelled as containing "restricted" information and three contained information labelled "secret". This information regarding loss of devices shows the levels at which devices are being lost by what should be the organization at the forefront of the nation's defensive capabilities. Following this loss of devices and information contained within, a report was carried out by Sir Edmund Burton which looked at MoD policies and procedures. This report (Burton, 2008) gave 44 recommendations on ways to improve security, mainly focused on training and restating policies at various levels set out by the HMG Security policy (Cabinet Office, 2009) as issued by the Cabinet Office for civil servants as a whole. Relating to hardware security the Burton Review led to one major change, this being for the MoD to begin recalling and encrypting 20,000 laptops that were previously not encrypted and putting out of service 2000 that were incapable of encryption. This recommendation would mean all current and future laptops for use at the MoD were encrypted. The date for this department wide activity was set to January 2009 (Burton, 2008).

11.1.3. January 2009

A health worker at HMP Preston lost a USB memory device with medical records of over 6000 current and ex-prisoners (BBC News, 2009). The device that was lost contained information relating to "surnames, their broad age range, prison number", "cell location" and records of "mental and sexual health". The memory device was, as required (ICO, 2009) by their regulating body the Information Commissioner's Office was encrypted, however the

password to the device was attached at the time of its loss, in direct contrast to the advice and guidance given out by the ICO.

11.1.4. May 2009

Hard drives containing “500 highly sensitive files, containing details of individuals' extra-marital affairs, debts and drug use” relating to “tens of thousands of personnel” (BBC News, 2009) was noted as missing from RAF Innsworth in Gloucestershire, a Ministry of Defence site. A spokesman for the MoD stated “Two of the drives are believed to have contained potentially sensitive personal data” and that the drives were “subject to physical protection standards consistent with the [Burton] Review” (Gloucestershire Echo, 2009).

12. Current Policy review

As gathered from interviews with the security professionals at EADS Astrium, company X and company Y all had reliance on ISO standards (namely ISO 27001) to base security choices for their environments, also evident was the option of companies working on government projects to also use the Technical Risk Assessment. I now investigate these policies with the aim of ensuring understanding of their environment and consider them outside of potential bias from interviews conducted. After I have investigated the policies I then move to critique where possible the advantages and disadvantages of each and how these can be used in future policy creation.

12.1. ISO/IEC 27001:2005

ISO/IEC 27001 is the standard published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). ISO/IEC 27001:2005 is the latest revision of the document, last revised in July 2007. The current standard however is the 2000 version, a word-for-word copy of the British Standard document BS 7799-1:1999. I, for the purposes of this project focus on the latest revision as was found from interviews with security personnel as this gives a true depiction of how these companies actually function.

The 27001 standard is intended for use by information security professionals who require an Information Security Management System to ensure the security of information on their computer networks, as a whole it contains a comprehensive list of best practice techniques for this purpose.

Some software is pre-listed in the documentation as being secure, for example Microsoft Outlook and requires less auditing on known software thus less known software may take longer.

Within ISO 27001 four stages of operation are present to ensure issues are resolved, these are Plan, Do, Check and then Act and each involve several actions to ensure they are successfully checked and completed. Within each of these four areas the sections break down into:

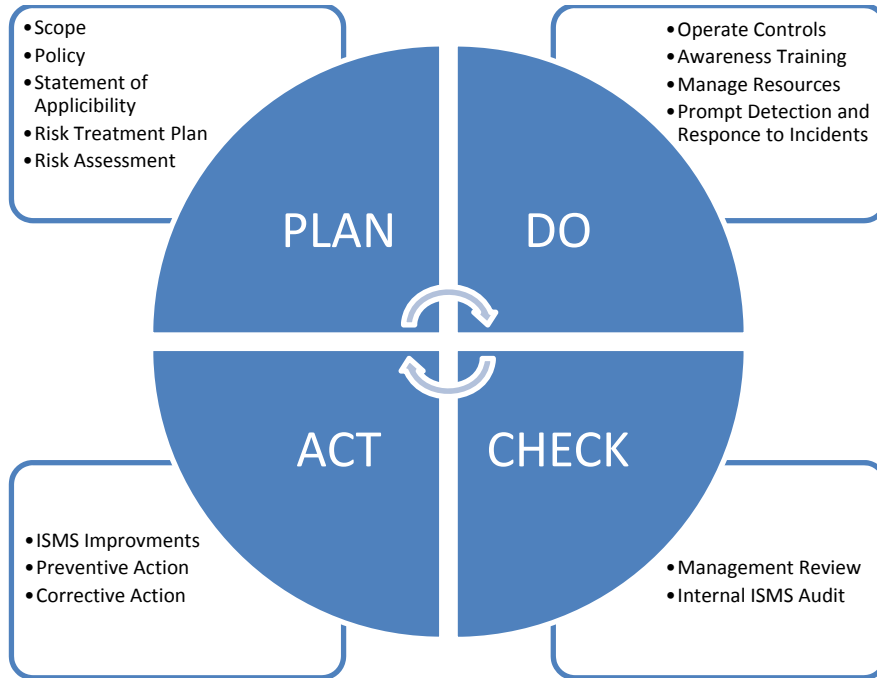


Figure 6

12.1.1. Plan

Plan involves setting the Scope of the project; this is generally the organisation as a whole but could be for instance, one particular site. The setting of Policy involves defining what needs to be achieved but also looks at constraints and existing policies and codes of practice. After the Scope and Policy are set two level of risk must be looked via the Risk assessment, this involves plotting all possible risks on the provided Area of applicable risk chart as seen in figure 6 to ensure all areas of possible risk has been investigated and planned for. This chart is then followed by the risk treatment plan, detailing the plan to overcome the recognised risk.

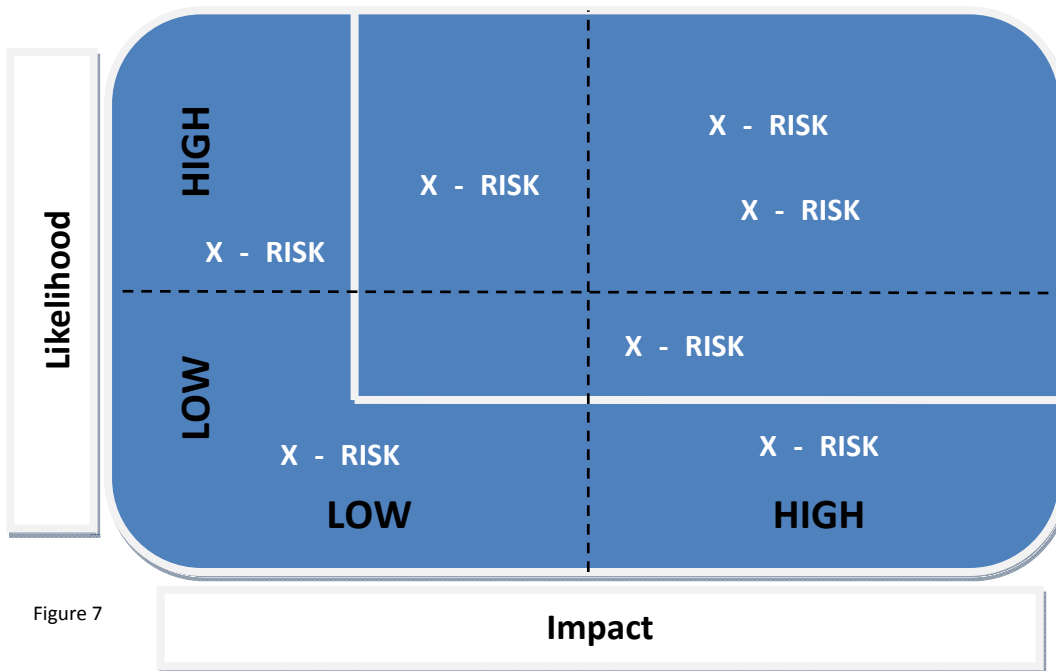


Figure 7

Statement of Applicability is the final stage in planning and must be completed; this involves checking all 133 controls set out in the ISO 27001 document and ensuring all controls have been set. This rigid system is intended to ensure no errors will occur during the planning stage to aid in maximum success.

12.1.2. Do

This step focuses around operating the controls set in the planning stage ensuring all areas of risk are maintained and mitigated as planned while the work is completed. This stage also includes security staff awareness and training needed to successfully complete the task. The final stage ensures all resources are assigned correctly to complete the task, complete risk assessment and complete, if required, training of staff.

12.1.3. Check

Now work has begun from the Do step the planned controls and objectives are checked via multiple available methods, the two mandatory checks are a review of management and an

internal ISMS audit. These two steps are one of the few areas that are allowed to be reviewed and audited internally outside of the ISO 27001 auditing scope.

12.1.4. ACT

The final step in the ISMS ISO 27001 cycle involves any action that is required to correct any issues found during the Check step, these corrections may be of three types, corrective, preventive and improvements. This is the final step in the cycle however if more work is required above that deemed acceptable the cycle may well begin again until all work is successfully completed.

12.1.5. Advantages and Disadvantages of ISO 27001

Advantages

- A clear cycle of steps ensures planning; risk and checking are involved in all processes.
- Due to its common use it is recognised at the industry standard for security compliance.

Disadvantages

- For the document to get updated to the 2005 revision (which included the latest technical updates) it took over two years.
- Minimal technological areas are covered.
- Only covers specified areas regardless of environment or company.
- Users must pay \$995 to obtain the full ISO 27001 (and 27002 checklist) documentation.
- Requires an external auditor to ensure compliance.
- Certain software gives faster auditing

12.1.6. Critique

A company who shows an auditor a full drive encrypted laptop would pass the ISO 27001 audit on laptop security. If this same company decided to give users the same username and password to all users they would still pass the audit. This tick-box method of security shows how when rigid controls that do not adapt to method are set for technology compliance that the standard is, as stated by the European IT Security Manager for one of the world's largest defence companies "a pure paperwork affair with little real world benefit".

The ISO 27001 standard itself says little about how an organisations information security actually is defined in an absolute way and specific and common security controls such as firewalls and antivirus programs and not involved in any part of the ISO 27001 standard and would not be investigated during an audit. Instead these security controls are presumed and

while 47% of UK firms (King, 2009) claim compliance with ISO 27001 “over half” (Tarzey, 2009) of them engaged in practices that would ensure a failing with ISO 27001 compliance, the main reasons stated for these breaches are “restricted [administrators]”, “inability to adapt to [software]” and “changes in technology [such as encryption methods]”. This research shows that although ISO 27001 is the industry standard companies and the IT security personnel that are in control of the companies systems either find it too time consuming, too restrictive or of too little benefit to wish to utilize it.

12.2. Technical Risk Assessment

The Technical Risk Assessment is a standard published by the UK Cabinet Office and is issued to companies to ensure IT security on projects it is associated with. The standard itself describes it as “HMG’s approved technical risk assessment and risk treatment method for ICT systems” (Office, 2009). It performs a similar task to that of the widely used ISO 27001 however for a standard this widely used it is deemed not sufficient enough for UK government projects. I first encountered this document via interviews with the security personnel at EADS Astrium and Company X. The security personnel at these companies valued it above that of the ISO 27001 standard. The document currently has a yearly refresh to ensure it is still relevant to current issues. The Technical risk assessment does not require an auditor to ensure areas are checked, instead when the document is completed and the assessment completed for the task the document is sent externally to a Cabinet Office member for approval.

The assessment assesses systems in the format of a top-level risk assessment, with areas specified including integrity, confidentiality and assurance to the security control. However, where this assessment differs to that of the ISO 27001 is how aspects such as business risk of a change and the appropriate threat of any change without a tick-box methodology being used to assess an issue with multiple possible issues. The scenario stated in the critique of ISO 27001 of the encrypted laptop but with a weak password system would not happen under a system compliant with the Technical Risk Assessment. The assessment also factors in with each risk assessment a request for a straight forward statement from the security personnel without being limited to a statement within the boundaries of the stated question and how this change will be affected and could be affected by users themselves.

Within the documentation many useful examples that should relate directly to companies are offered to aid in company's transition to be compliant. A major part of these examples is the Model Catalogue which presents a system for relating potential levels of impact on two levels.

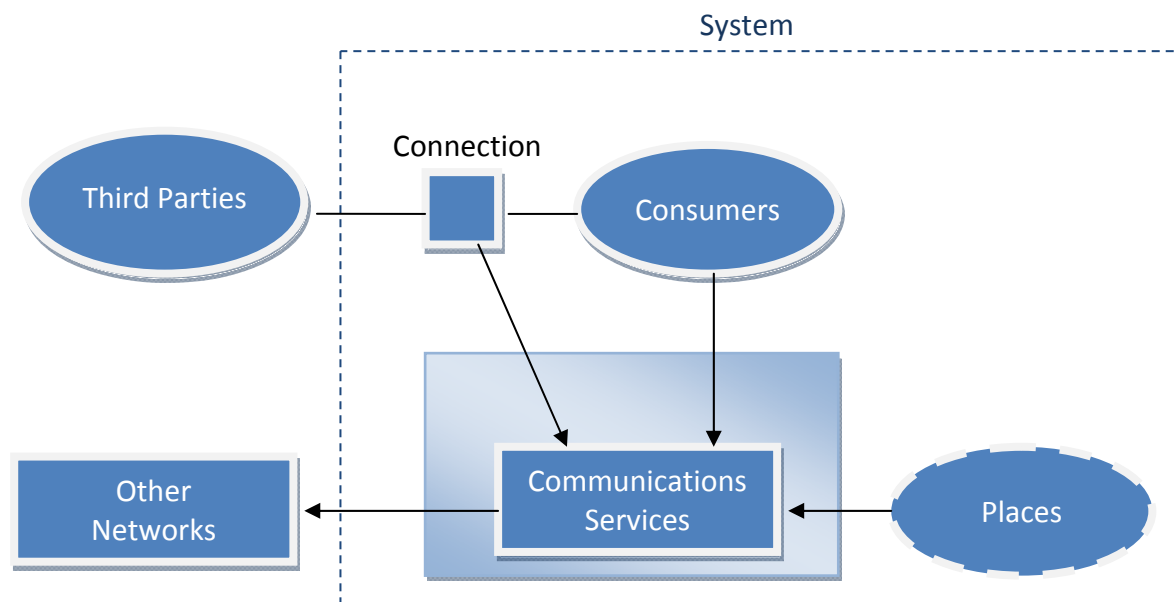


Figure 8

Model Object Identifier	Description	Immediate Impact (1 Low - 5 High)	Long-Term Impact (1 Low – 5 High)
Communications Services	Represents all the equipment that the project will be supplying to provide the communications services and the people who will provide and manage the services.	3	3
Places	Represents all the places where the equipment providing the communications services are located, including the communications equipment at consumer sites.	n/a	n/a
Consumers	Represents all the account holders of all the systems that use the communications service can support a wide range of systems.	4	4
Connections	Represents all the equipment and people involved in providing and controlling the exchange of business information between consumers and third party systems.	4	4
Third Parties	Represents all the account holders of all the systems that have direct or indirect connections to the consumers of the communications services.	4	4
Other Networks	Represents all people and equipment involved in the existing communications services that the project will use to provide external bodies. This includes public telephone services and the Internet.	n/a	n/a

Figure 9

Figure 8 and 9 show a typical example of a secure system and its interconnections. It is useful to note how these examples of what should and should not be included when assessing risk account for a wide range of activities and areas but do not force the user to specify which particular methods they will use only how they plan to address the risk in the immediate and Long-Term. This system for addressing risk relating to how the user wishes to address the problem and providing the tools to address them shows why this has proven to be a popular method of providing IT security within their organisations.

12.2.1. Advantages and Disadvantages of the Technical Risk Assessment

Advantages

- Enables the security personnel to state their identified risks.
- Enables the security personnel to state their methods of addressing or deferring risk.
- Is adaptable to many system layouts due to its design.
- No internal audit is required, external documents sent only.

Disadvantages

- Updates are faster than the ISO 27001 document but still yearly.
- Minimal technological areas are covered.
- Users must be working on UK governmental projects
- Lack of a 'check box' method could enable some areas of risk to be overlooked.

12.2.2. Critique

Unlike the ISO 27001, IT security personnel appreciate the framework offered to them for use assessing risk via the Technical Risk Assessment. The design of the assessment enables multiple projects to be covered in a way specified by the security personnel for both identifying and addressing all risks that may occur within the organisation however, there are still issues with the document. The lack of a 'check-box' method to address risk that in one instance may prove useful in the hands of experienced security personnel may cause the same areas of risk to be overlooked by less experienced personnel, this problem is hard to address and a risk itself that must be met by the organisation itself.

Any document, such as this one used by one organisation to a limited group of companies is going to be limited in ease of support and growth of update, this problem is fundamental to one of the major problems within security documentation. If a lack of use and growth is evident within any project a lack of support and fix for any problem will be hard to find. Limit the spread and limit the effectiveness. The document also fails to cover technological areas to any level adequate for ensuring risk of these areas is protected.

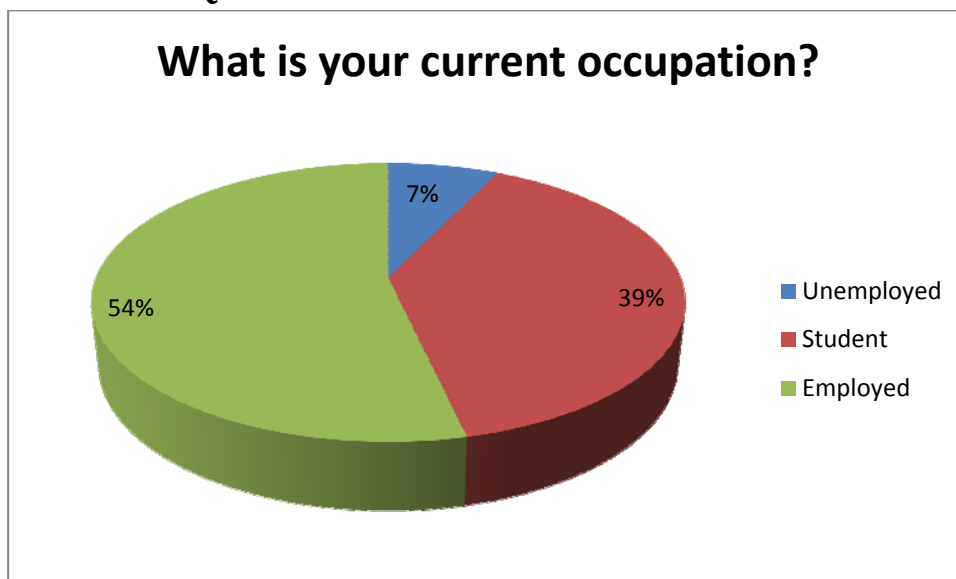
13. Chapter 4 – Discussion & Review of Information Gathered

13.1. Questionnaire

Questionnaires were issued only to computer users who work within a secure security policy controlled environment. From the results gathered I have listed the results which I have listed from question one to question eleven. Each answer has been assigned the correct percentage, exact figures shown for total responses and any possible answers that were not answered shown. Eighty four individuals completed the questionnaire. No individuals started but did not end the questionnaire nor did any individuals choose to contact me to enquire about details or to question privacy concerns.

The following responses to questions have been gathered:

13.1.1. Question 1



Exact numbers per answer:

06 - Unemployed.

33 - Student.

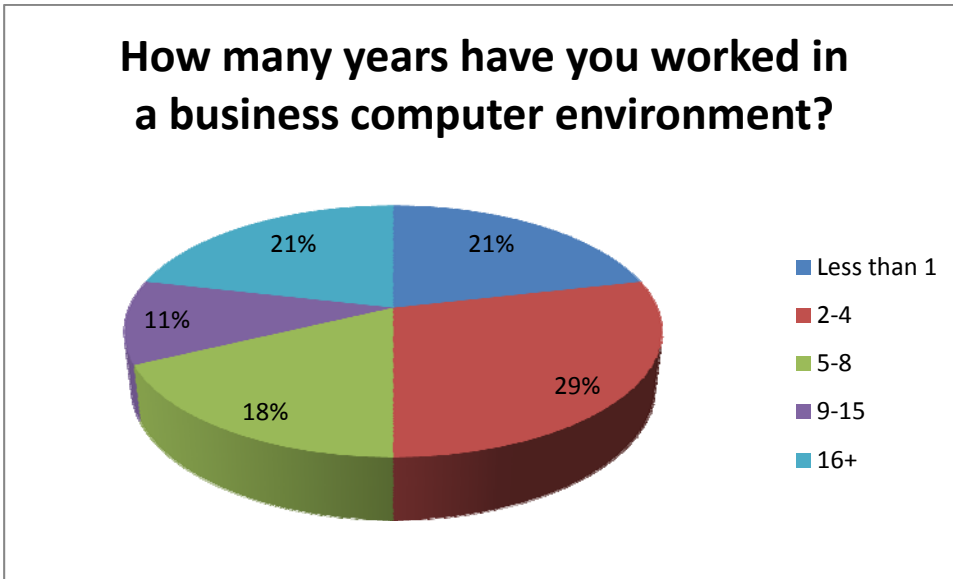
45 - Employed.

Answers with no responses:

00 - Retired.

Information gathered: As this questionnaire was only issued to users who work or have worked on a secure computer environment and many contacts were that of current students who most likely had worked in this environment whilst on placement years the spread of results is as would be expected. With the current rate of unemployment standing at 8% (Office for National Statistics, 2010) the percentage of unemployed answers also seems apt. No users to the questionnaire were retired; this is also not an unexpected result as it was not issued to anyone who would have been in this occupation.

13.1.2. Question 2



Exact numbers per answer:

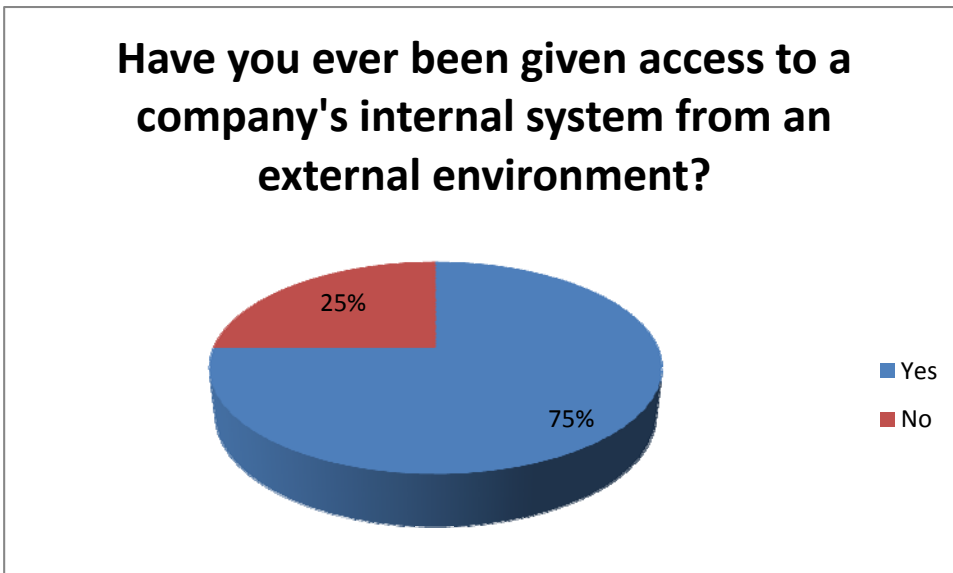
- 18 - Less than 1.
- 24 - Between 2 & 4.
- 15 - Between 5 & 8.
- 09 - Between 9 & 15.
- 18 - Greater than 16.

Answers with no responses:

- 00 - None.

Information gathered: The spread of answers show that all people that answered the questionnaire had worked in a business computer environment however, 50% had only been in this environment for four years or less. This result most likely reflects the high percentage of student answers from question one. The other 50% of users have worked in the environment for 5 years or above, this is a strong result as experience in the field is essential for answers in other questions.

13.1.3. Question 3

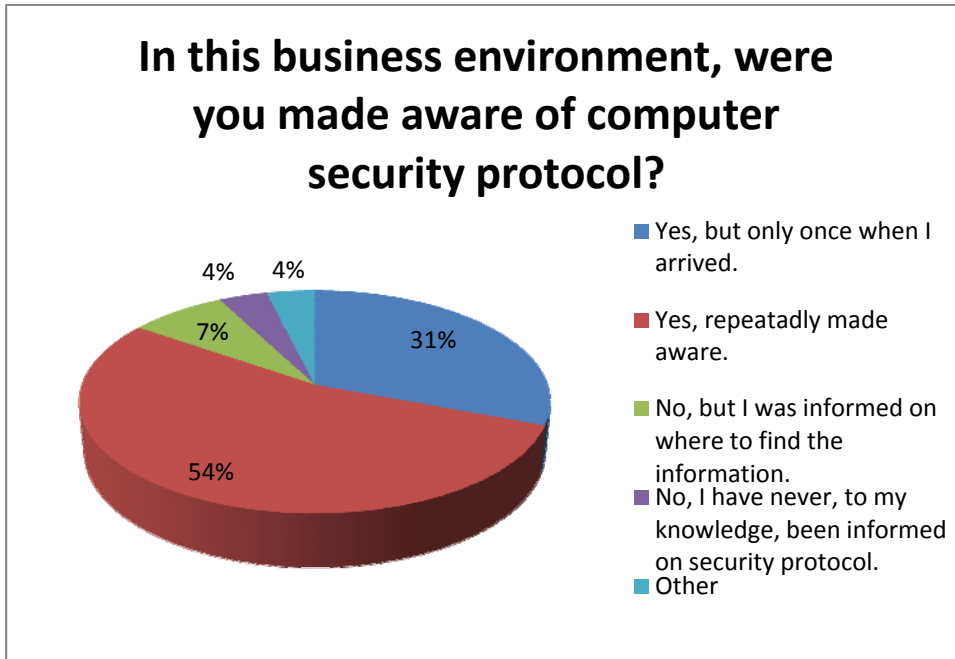


Exact numbers per answer:

- 63 - Yes.
- 21 - No.

Information gathered: a 75% result for users who had been given access to a company's internal system from an external environment shows that while the IT Security Managers in the interview stage considered this access infrequent access is certainly taking place and to a large extent.

13.1.4. Question 4



Exact numbers per answer:

24 - Yes, but only once when I arrived.

42 - Yes, repeatedly made aware.

6 - No, but I was informed on where to find the information.

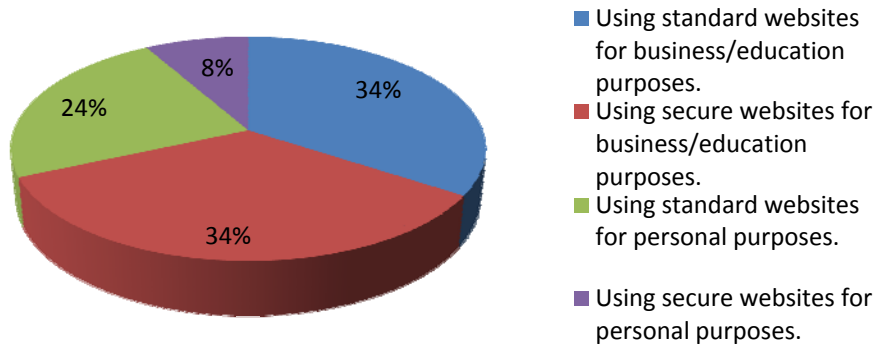
3 - No, I have never, to my knowledge, been informed on security protocol.

3 - Other

Information gathered: 85% of users answered that they had at least at some point been informed what security protocol in the environment where they were working however in this group 36% stated they had only received this information once on first use of the system. This percentage is possibly worrying as received from question two that 79% of users had worked in this environment for a period greater than one year. 11% of users stated they had never been informed on the security protocol used on the systems; this is exceptionally worrying given the nature of the secure environment and the possible repercussions.

13.1.5. Question 5

Do you feel secure accessing the world wide web when using a computer in this environment?



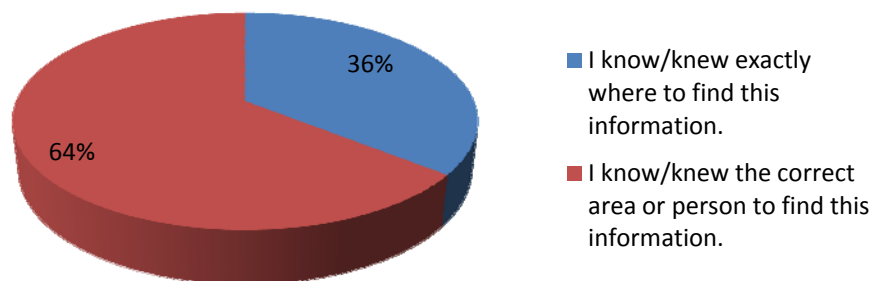
Exact numbers per answer:

- 66 - Using standard websites for business/education purposes.
- 66 - Using secure websites for business/education purposes.
- 45 - Using standard websites for personal purposes.
- 16 - Using secure websites for personal purposes.

Information gathered: 58% of users state they feel secure accessing standard websites while at work, this figure relates to known figures (snapshotspy.com, 2008) on personal internet usage however, only 42% of people feel secure accessing secure websites for personal reasons showing that even in secure environments people do not feel completely secure accessing secure websites be this for tracking reasons or otherwise.

13.1.6. Question 6

If you had any questions on what the security protocols are in this business computer environment, do you know exactly where to ask?



Exact numbers per answer:

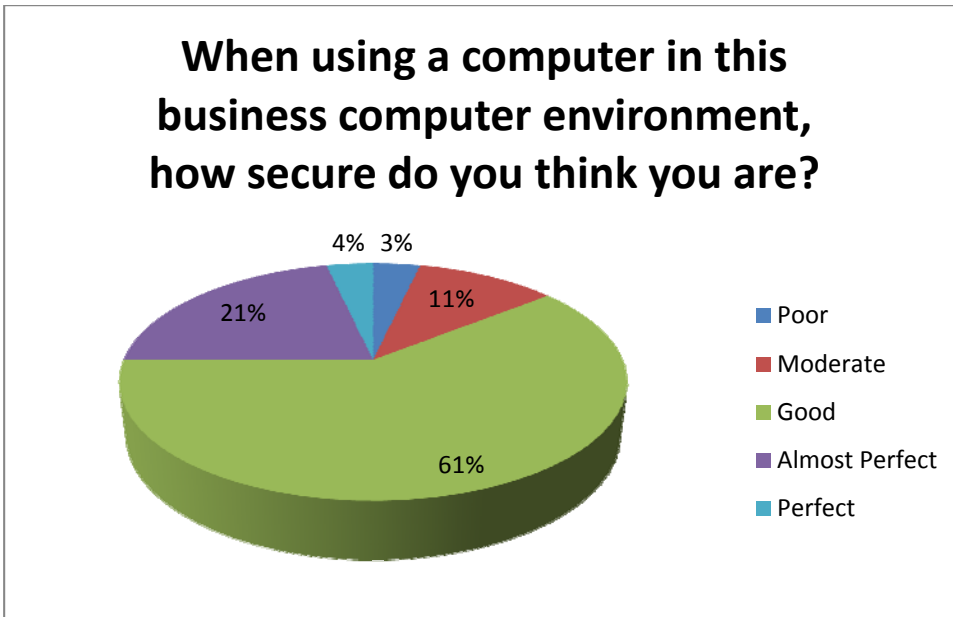
- 30 - I know/knew exactly where to find this information.
- 54 - I know/knew the correct area or person to find this information.

Answers with no responses:

- 00 - I don't/didn't know who to ask or where to visit.

Information gathered: All users stated they either knew or knew where to find information on security protocols. This feedback is particularly interesting as it shows users know to find any information required if they have any concerns about security.

13.1.7. Question 7

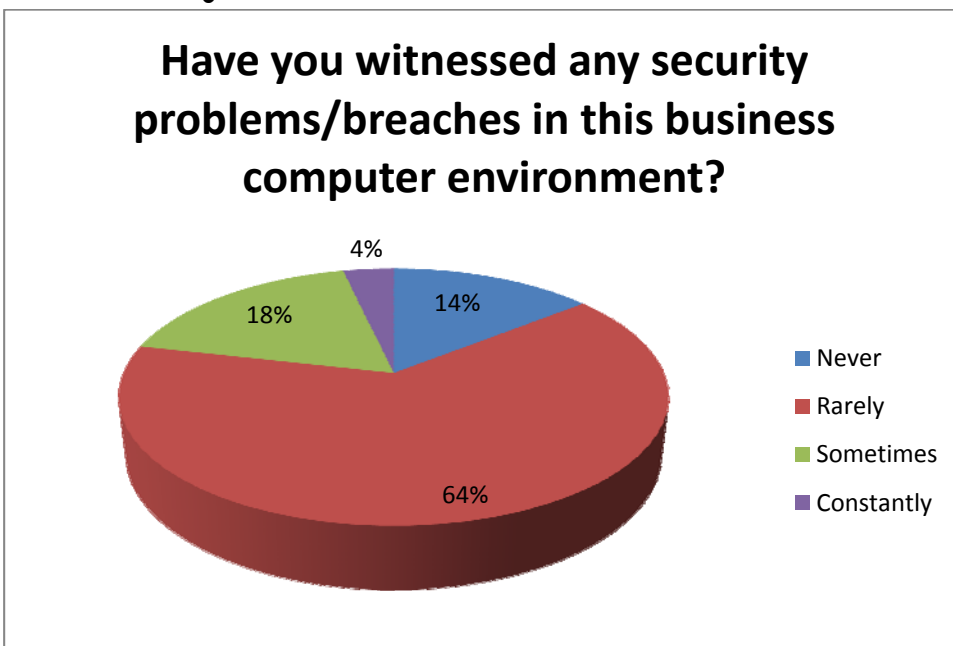


Exact numbers per answer:

- 03 - Poor.
- 09 - Moderate.
- 51 - Good.
- 18 - Almost Perfect.
- 03 - Perfect.

Information gathered: 86% of users stated they believed they had either Good or better security on their computer environments whilst only 3% said security was Poor, this shows very few people think they are not secure.

13.1.8. Question 8

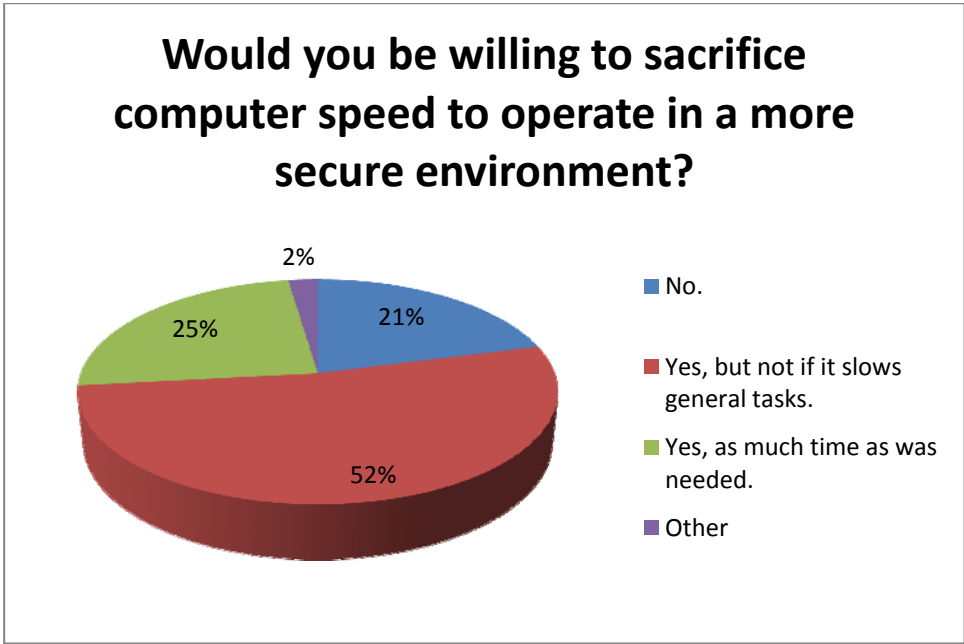


Exact numbers per answer:

- 12 - Poor.
- 54 - Moderate.
- 15 - Good.
- 03 - Almost Perfect.

Information gathered: 86% of users stated they have experienced some sort of security issues in their business computer environment which shows a worrying level of issues on an environment that should ideally not be experiencing any issues relating to security. Only 14% of users said they had never experienced any issues.

13.1.9. Question 9

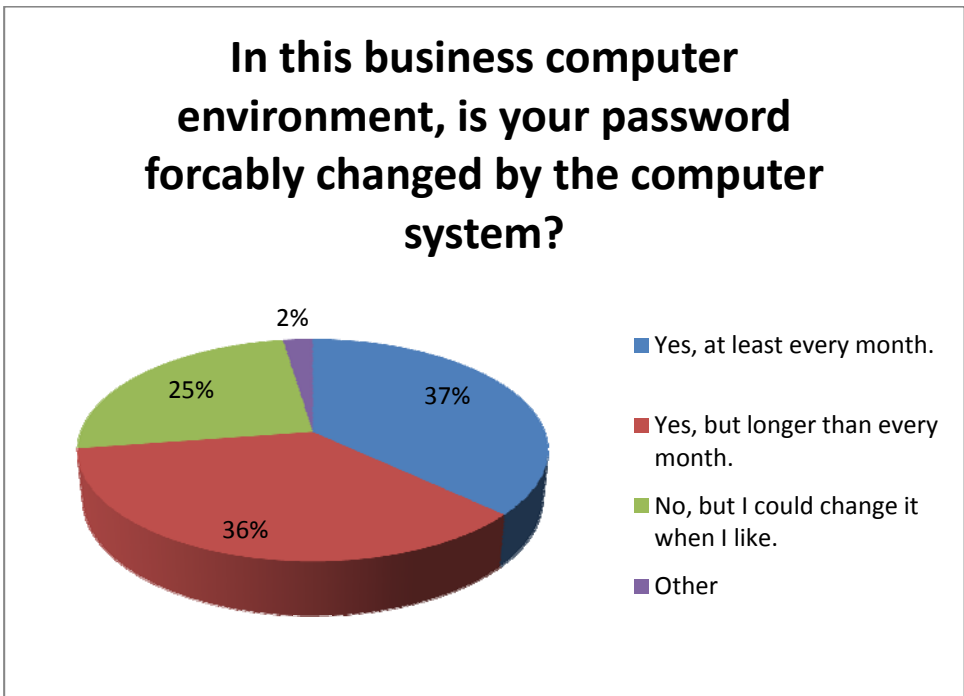


Exact numbers per answer:

- 18 - No.
- 45 - Yes, but not if it slows general tasks.
- 21 - Yes, as much time as was needed.
- 02 - Other.

Information gathered: Only 21% of users stated they would be unwilling to sacrifice some computing speed to give greater security when operating in a secure environment, while 25% stated they would be willing to sacrifice as much time as was needed to ensure a more secure environment. 77% of users gave a positive response to sacrificing computer speed for more security.

13.1.10. Question 10



Exact numbers per answer:

- 31 - Yes, at least every month.
- 30 - Yes, but longer than every month.
- 21 - No, but I could change it when I like.
- 02 - Other.

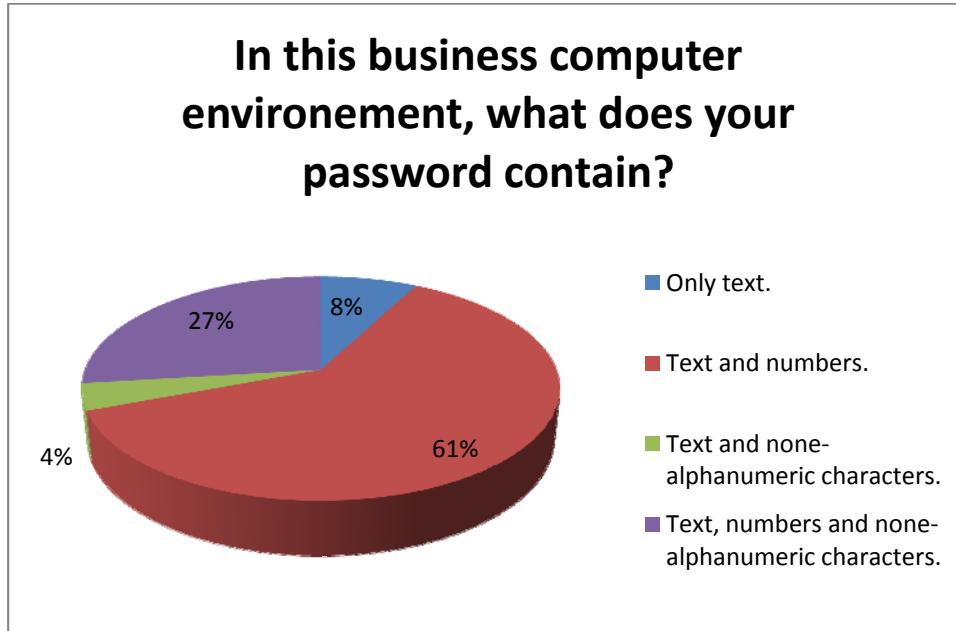
Answers with no responses:

- 00 - No, and I cannot change it.

Information gathered: No users stated they cannot change their password; this is as expected but shows standards are followed in these environments and users are not unable

to change passwords if needed. 73% stated they are forced to have passwords changed, this high figure relates to the interviews conducted on best practice however a higher figure would be more ideal to ensure a secure environment.

13.1.11. Question 11



Exact numbers per answer:

06 - Only text.
 48 - Text and numbers.
 03 - Text and none-alphanumeric characters.
 21 - Text, numbers and none-alphanumeric characters.

Answers with no responses:

00 - Password is not known.
 00 - Other.

Information gathered: Only 8% of users stated they only use text for passwords and none said they use all numeric for passwords, this is a strong answer as these two states are the weakest form of passwords. The other 92% had the required minimal password standard for minimal security with 27% stating they use 'Text, numbers and none-alphanumeric characters', the most ideal format for a password in a secure environment and advised by Microsoft (Microsoft). Still the highest percentage 61% uses just text and numbers and therefore could be improved by the addition of alphanumeric characters.

13.2. Cross Referencing of Results

Patterns observed during a review of the questionnaire became apparent, these patterns are not initially visible from the feedback however are visible from a cross referencing of result patterns. Possibly unsurprisingly users who had worked in a secure computer environment for less than five years also had only rarely observed security breaches however they also had no users whose passwords contained none-alphanumeric characters and hence may also be part of the problem. Users who stated they used alphanumeric characters in their passwords also believed they are very secure operating on their computer systems, this tells us that at-least in the minds of this user base they feel more secure. This same user base also largely stated they would not be willing to sacrifice

computing speed for advanced security, in this way we may consider this a more advanced range of users who, given their feedback feel their security is adequate for purpose.

13.3. Questionnaire Summary

Many interesting results have been found from the questionnaire results, I have found 75% of users state that they have access to their companies internal networks from outside this environment and at the same time 11% of users state they have never been informed of what the security protocols are and thus this form of access must studied in more depth. 86% of users stated they had *experienced some sort of security issues in their business computer environment which shows a worrying level of issues on an environment that should ideally not be experiencing any issues relating to security, this shows that according to the actual users of these networks a serious number of them witness problems and prove that the current state of protocols could indeed be improved upon. 77% of users gave a positive response to sacrificing computer speed to operate in a secure environment; this will give some evidence for tighter security mechanisms even if it impacts operational speed.*

13.4. Technological Approach

From interviews with several IT Security Managers one aspect arose more than any other, the lack of technology standards. It was the most frequent complaint that was not covered by either ISO 27001 or the Technical Risk Assessment. The reasons for this lack are based on issues particularly fundamental to the release and design of the policies themselves. A paper published document requires issuing, publishing and sending out to users, it is purely not capable of delivering a source of information on every technological advised solution or updating it when necessary. From the interviews and critique of the two before mentioned documents encryption and passwords were both mentioned as current issues, I will now investigate current best practice on these two issues.

13.4.1. Encryption

Encryption is the most common form of protecting information from unintended parties. It works by using an algorithm called a cipher to make the information unreadable to anyone who does not possess the correct key. Encryption within organisations is most commonly split between two functions (Schifreen, 2006), to encrypt a user disk drive to ensure only a registered user can access the drive itself and a secondary function to secure the data within-transit between external or secure sources.

For drive encryption many solutions exist, the MoD for instance as mentioned in the 'Recent history of 'missing data from systems with secure policies' section had severe problems with loss of information on disk drives either being on memory stick or laptop computer. To correct this problem the MoD invested in BeCrypt software based encryption on all disk drives (Davies, 2008). One month after the completed recall and rollout of BeCrypt on all MoD laptops a free downloadable tool (McGrew Security, 2008) usable with little experience became available rendering software based encryption considerably less valuable as a method for securing data.

The bypass this vulnerability a technique called 'Hardware-based full disk encryption' is the next most obvious solution to ensure current safety in disk drive encryption. This technique involves using a symmetric encryption key independent from the CPU and thus removing any possible memory based attacks.

The speed in which technology for security is invented, invested in and cracked or hacked is of major concern to all those who wish to operate in a secure environment.

13.4.2. Passwords

Passwords form a major obstacle between IT Security Managers and users. They are the gateway between the user's access to the system and the security to restrict it. The consensus between the IT Security Managers was that while they acknowledge secure passwords are necessary to keep unwanted individuals from accessing their systems passwords also need to be easily remembered by users to ensure users do not constantly forget them or worse, write them down or choose an overly simple password.

A recent incident on the social networking site RockYou highlighted this problem. The website, with 32 million users was the recipient of a SQL Injection hack (Siegler, 2009). Shortly after the incident a file containing user's usernames and passwords was posted on the Internet. This incident, potentially damaging shows just how important password security must be and also provides us with an interesting insight into users password habits.

The top ten passwords of users on the social networking site RockYou are as follows (Leyden, 2010):

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

Almost 50% of users passwords are that of "names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys)" (Leyden, 2010) within the RockYou leaked database, this shockingly revelation shows that when setting password restrictions for users, it is particularly important to ensure it is impossible to set a password that is this simple.

Within the database of passwords I processed a simple test, Within 24 hours, how long would it take to crack passwords within the file with a simple free tool (I used 'John the Ripper password cracker').

The results were as follows:

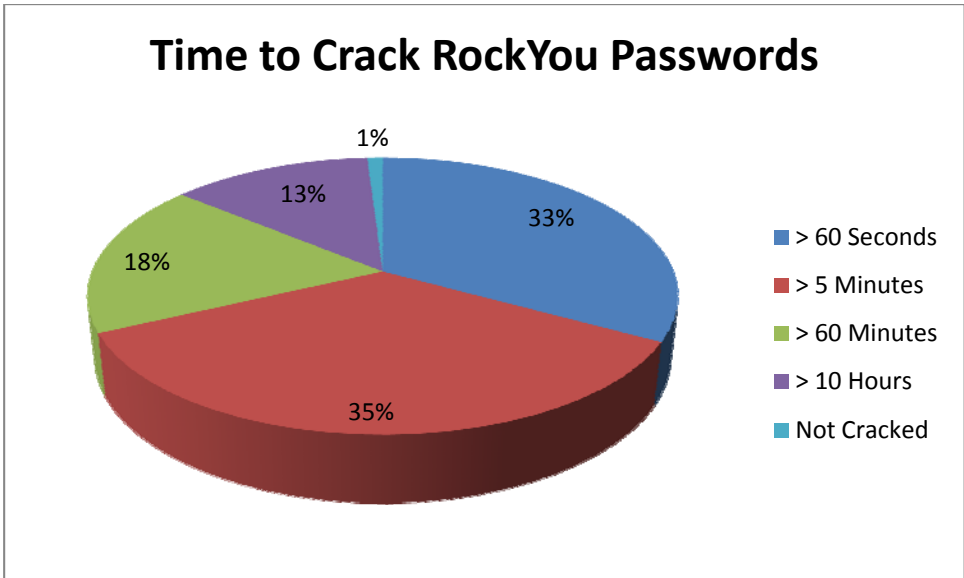


Figure 10

Within an hour the tool had cracked 86% of passwords in the file. This is a shocking result for what is the only factor stopping an individual gaining access to restricted information.

Microsoft provides a strong list (Microsoft) of what makes a secure password that forms a similar definition as mentioned by the European IT Security manager at EADS Astrium. This table provides strong steps on how to ensure user passwords are of enough complexity to not be easily cracked and also be remembered by users.

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest. I keep mine secret. (10 words)
Turn your sentences into a row of letters.	Use the first letter of each word.	Iacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	Uppercase. IACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	IACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?IACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?IACpAs56IKMs" (14 characters)

Figure 10

13.5. Open Source

An open source approach offers many benefits over a more traditional approach to production and development. It is capable of enabling “better quality, higher reliability, more flexibility, lower cost, and an end to [internal company secrecy]” (Open Source Initiative) and as such is of worthy consideration for any project. This approach to production and development is achieved by “promoting access to [the] source materials” (Fogel, 2005) of the project and thus this approach is not always considered wise if giving access to this information would compromise the operations of the associated business or project.

In the many stages of research gathering for this project, particularly the Interviews conducted with IT security personnel it became apparent that while system diagnostics and checks were done via existing documentation such as the ISO or TRA certification all input on security issues other than direct governmental influence came from information gathered on the internet (primarily securityfocus.com) which is published freely. This information however is only available in the form of posts and while some discussion takes place on message boards, this information is also freely available via the internet.

The open source approach requires all involved to publish and share any development done that within the open source project while working within the method for the benefit of all users of the project. With this method all updates and changes to improve the project are required to be shared, for security, this could involve for example what encryption methodology is used, why and what deployment of software used. The same could also be used for what password limit is set for users, what software versions are used and how numerous other security restrictions are used.

To use an open source approach to this project would require a wealth of data and personnel to manage and update however, the more data and personnel that did partake in this approach would further improve the information available and aid in project in growing and developing.

It must be considered that while this approach may indeed function to the benefit of gathering data for the use of protection anyone wishing to immediately know which version a company that joined this approach was running on their systems would be able to find this information without any issue. This issue may also limit how management may see this development, is it better to publish your security information even if you know it will be better protected for intruders generally? The approach would require security staff to update as advised by the policy as fast as possible on their systems, to ensure when a possible vulnerability becomes known it can be dealt with before an intruder compromises the system.

An open source approach to the implementation of security policy would seem a wise move for a project that's major inputs are freely available but all current company development remains a protected secret.

14. Chapter 5 - Conclusion

14.1. Research Questions

When this project was formed, it was decided ideal given the range and environment of the issues to investigate to set a series of research questions which were then subsequently aimed to be answered via either interview questions with IT Security professionals or users of secure computer systems. The answers gained to the research questions and their evidence provided for each answer is listed below.

14.1.1. What relevance do security models have to security policies?

My initial research laid out the major differences between security models and policies (section 4), this being while a policy is a definition of what it means to be secure, a model however is the underlying scheme (such as access controls) that the policy layer operates on.

14.1.2. What computer security policies are currently being used?

This question I initially directed at the interview stage of my primary research. From the staged interviews with the IT Security Managers at EADS Astrium and company X and Y (section 8) I was able to elicit the two formal set of policies that were in use for security governance, these being ISO 27001 (section 12.1) and the Technical Risk Assessment (section 12.2). I then conducted further investigation into these two documented standards.

14.1.3. What are the sources of current policies?

From the interviews conducted (section 8) I was able to elicit what the sources for current policies were (section 12), these were the ISO and TRA documentation. The sources for these documents were the UK cabinet office and the International Organization for Standardization, both current working standards requested by customers for work completion. Additional policies were decided within the department most commonly sourced from internet websites or message boards. The security manager of Company X stated that the ISO documentation is “heavily discussed on internal documents and educational courses [and] The Technical Risk Assessment [] was issued to us on agreeing to take on government projects” similarly the security manager at EADS Astrium stated that “To keep up to date with current security information conferences and web sources are used”.

14.1.4. What are the opinions of computer security personnel to currently active security policies?

Many areas of current security policy were deemed inadequate or not fit for purpose. The IT Security manager at EADS Astrium stated that “Current Standards (ISO 27001) can be easily manipulated and does not mean the IT security environment is secure. The standards only function as a base line [and that] Day to day operations of most companies will not fall within these standards” and referred to the ISO standard as a “Paper exercise”. With this

statement he is saying he seems their primarily function as a form of administration on top of true business practice and not how to correctly secure a system. At company Y it was stated that they “do not cover technologies” and as paper based documents “cannot deal with issues that are updating at [such] speeds”. Feedback from company Y focused on the “time to implement” the entire policy giving “little benefit [to smaller companies]” and that they would be more valuable if they were more “relevant to keeping the day-to-day security checks” in place.

14.1.5. What do computer security personnel consider should be included in security policies?

The IT Security manager for EADS Astrium stated that if policies operated in a “more pragmatic” manner and “more related to facts [for] each company” they would adapt better to the work actually conducted to ensure security. Current standards like the ISO 27001 were felt to “only cover the bare minimum to be accredited [and contained] Impractical daily checks” it was felt that the way this is conducted in the TRA documentation is much more practical solution. Company Y felt that as a small company “Technological issues would be a real benefit” as “all time must be spent ensuring [current security]” and that proper sources for why security decisions have been made should be properly sourced as this enables them to “tell if this is valuable information” or not.

14.1.6. Should security technologies be included in security policies? And if so which?

A clear positive method from all three interviews stated they would all wish to have security technologies included within the policies to ensure the highest level of security possible on their systems however; the possible negative aspects of this inclusion must not be overlooked.

14.1.7. Are there any areas that need to be covered in policies that are not currently?

Possible inclusions to current policies was largest answered in question five however no specific items that felt must be included were discovered as proven by all companies taking part if at least one form of current security policy standard.

14.1.8. How much relevance do user passwords have to security?

Feedback from interviews suggested that although the IT Security Managers felt that it was of serious issue would like to in the case of the IT Security Manager at EADS Astrium set “a minimum password of 12 characters which must include at least one capital letter, one lower case letter, one number and one none-alphanumeric character” they are unable to due to “concerns of management that users will not be able to remember passwords”. The information gathered via the case at RockYou (section 13.4.2) showed that weak passwords are common place and via the cracking of the leaked password file can be easily defeated.

This outcome proves that considerable relevance must be placed on strong passwords to ensure this simple method of entry is secure.

14.1.9. What do system users think of current security policies?

From the questionnaire issued to users 86% felt they were secure in their environment however the exact same figure 86% stated that they had at some point experienced some sort of security issues in their business computer environment which shows a worrying level of issues on an environment that should ideally not be experiencing any such issues. This result shows that while they may feel secure about the majority of issues it is clear improvements can certainly be made to ensure this figure of 86% is dramatically reduced.

14.2. Conclusion of Research Questions

From the large quantity of information gathered in this project some serious issues on current policies have been stated. It has been said that they are purely 'paper exercises' concerned with nothing more than getting a box ticked, they don't relate to actual security that is conducted, are too slow to update and that due to their printed format the inherent cost and delay in publishing ensures it is largely not fit for purpose when it is available for use by IT security personnel.

The world of computer security is a complicated environment, not least due to the rapid pace of computer development. Computer security threats rise annually without hindrance (entrepreneur.com) yet still no method to halt or decrease this rise is being offered. Whilst computer security policies exist to 'classify a system as secure' it is clear from the evidence gathered that is not the case and they are far from 'being secure'. To remedy this situation using the research carried out in this project and with the cooperation of current IT Security Managers come to six suggestions to be used to create a set of security policies that if used correctly will greatly improve computer security for secure systems.

14.3. Suggestions

The following justified suggestions are now stated to be utilized in envisaging a new system for computer security policies:

14.3.1. Free

The cost of the most commonly used policy (ISO 27001) at just under \$1000 is too high for emerging markets and small companies, as shown by company Y's lack of interest. By removing this limitation you remove the hindrance to investigate, read and utilise the policy by anyone who wishes to learn more. There is no greater incentive to a solution than if it is at no cost to the user. To enable it to be free a similar method to open source software (as discussed earlier) or the establishment of a charity based organization (similar in function to the website Wikipedia) would permit all those that wished to use and maintain the policy to read the policy whilst simultaneously have an active interest in ensuring its survival.

14.3.2. Online

Current limitations inherent in physical paper based documentation such as requiring printing, publishing in a final manner and not being able to make adjustments simply when required can all be alleviated by publishing the document in an electronic format to the Internet. Not only this but utilization of the internet to disseminate its information will enable maximum reach, near instant updates and enable collaboration on a vast scale.

14.3.3. Open Source

By ensuring the policy is open source will enable "better quality, higher reliability [and more] flexibility" (Open Source Initiative). This method of delivery promotes access to the source materials of the policy and anyone who wishes to modify, improve or utilize is bound to post these improvements for all to benefit. No longer will IT security personnel be forced to work alone with ideas not shared, instead all work generated will be used for greater security for all who participate.

14.3.4. Reasoning Stated

As reasoned by the IT Security Manager at company Y "how do I know if it is wise to implement a solution to alleviate one problem when I cannot see how they came to this solution? I may well be creating another problem". When all reasoning is stated when overcoming an issue, why it is being used becomes clearer and enables IT security personnel to make informed choices relating to their own implementation. It also enables any future issues such as a new software vulnerability to be seen in context of past issues so future issues can be addressed at a faster pace and without the need for prior personal experience.

14.3.5. Focus on Technology

Considerable feedback was gathered from the interviews with IT Security Managers that the majority of focus to ensure security on systems was based on technological based issues, be this encryption, software versions or otherwise. Current policies are unable to cover technology primarily due to their current method of delivery and as such are unable to cope with the speed of updates needed to maintain its security hence it is left outside the scope of current security policies. Enabling technological focus within the policy will enable IT Security Managers incorporate these updates giving the running of this policy greater worth and increase its use within day-to-day operations.

14.3.6. Constantly Updated

A “purely paper exercise” is what the IT Security Manager of EADS Astrium considered current security policies; this does not have to be the case. A constantly updated policy ensures complete relevance to what is necessary to ensure a system can be considered secured and if utilized correctly will become the only necessary source to ensure complete computer security.

15. Project Reflection

15.1. Project Issues

From the initial cursory investigation into computer security before moving into how security policies work and following thorough into detailed investigations of policy documentation, discussions with IT Security personnel and through questionnaires a large number of users I decided certain ways of working to achieve each new goal. The ways in which I chose to structure each new goal or objective were however at some parts in the project limited by certain constraints or factors that limited their reach and/or effectiveness.

The initial constraints I identified from the PID stage of the project and supplemented in the constraints (section 5) were in the end project not sufficiently identified to alleviate all possible problems and although many of the choices made at a later stage were difficult to predict more investigation into the areas concerned could have aided in enhancing the project. In addition to the constraints specified (section 5) I encountered issues with the following areas:

- IT Security Manager contact – Given the time restrictions of the project and from starting from an unknown position beginning contact with people in charge of computer systems was a difficult task. I achieved contact through either personal contacts in companies and emails to contact email addresses publicly listed. To give greater depth and worth to the interview stage of this project a higher number of interviews could have been conducted. This change would have likely increased the number of security policy documentation studied and given the project an increased reach.
- IT Security Manager confidentiality – When contact was made with the security managers and questions asked in both the cases of Company X and Company Y confidentiality was requested, this was an unexpected repercussion of attempting to elicit details of security details from companies who wish to keep such information as secure as possible in the mindset that this will give them greater security. Unfortunately these confidentiality requirements by IT Security Managers forced me to not state what companies or names was Company X or Y. To alleviate this problem I have used the alternative names stated. Unfortunately this was unable to avoid if I wished to gather the information required.
- Questionnaire Focus – When deciding on questions to ask users, questions were based on answering the research questions that could not be asked by staged interviews with IT Security Managers. This decision to phrase questions in this way did aid in answering the questions stated however it also limited the feedback given especially as it was conducted with no reflection time given to answers gained from the interviews. If extra time had been given to either reflection from interviews or a second phase of questionnaires issued this

may have increased the quality of research questions answered by ensuring all were successfully covered in sufficient depth.

- Questionnaire numbers – To ensure feedback for the research questions that related to user aspects were answered to a sufficient level, questionnaires were issued to people who had worked in a secure environment for a minimum of one year. This restriction to a specific user group limited the sample size and limited the range of answers given. To alleviate this issue I could have greatly increased the number of people who the questionnaire was given to however I would still be limited by only being able to use answers by people who have spent time operating on computer systems that operate in a secure environment. The Eighty four responses received gave a satisfactory however possibly simplistic view to some research questions where more answers would have given greater quality.

15.2. Decisions Made

Some decisions within the project had to be made to ensure research questions were answered and goals were met. The introduction of interviews and questionnaires both introduced to meet certain research questions. The interviews with IT Security Managers aided me answers questions needed relating to exact policy questions such as how they are implemented, sourced and any problems encountered. It was not possible to also ask the same group of IT Security Managers questions on system use as they may have given biased answers and as with many experts try to give answers that they feel are correct instead of answering the questions. With the issuing of questionnaires I aimed to answer questions that related to user experiences of security policies such as what user had experienced in security issues and breaches, if they knew what policies were and if they had any issues did they knew where to gather the correct information.

15.3. Project Management Issues

When beginning the project I set a clear set of goals and dates to achieve them as stated in the Gantt chart (Figure 11). As I progressed with the project it became more difficult to stick to this rigid plan of actions and dates, specifically with the interview and questionnaire gathering. With regard to the planned Interviews the time to send, receive and plan times for Interviews was largely taken out of my control and largely planned by the IT Security Managers due to other time commitments. This problem was hard to alleviate however the project planning via the Gantt chart could have had more time planned for this activity as this would have aided in future task planning that relied on it. The questionnaire feedback was unfortunately slow on issuing it to users and little time was planned to receive answers, this section could also have done with more allocated time in the Gantt chart as I was forced to elongate the allocated time and do tasks that were not planned to be conducted so soon such as the Interview and technology discussion sections.

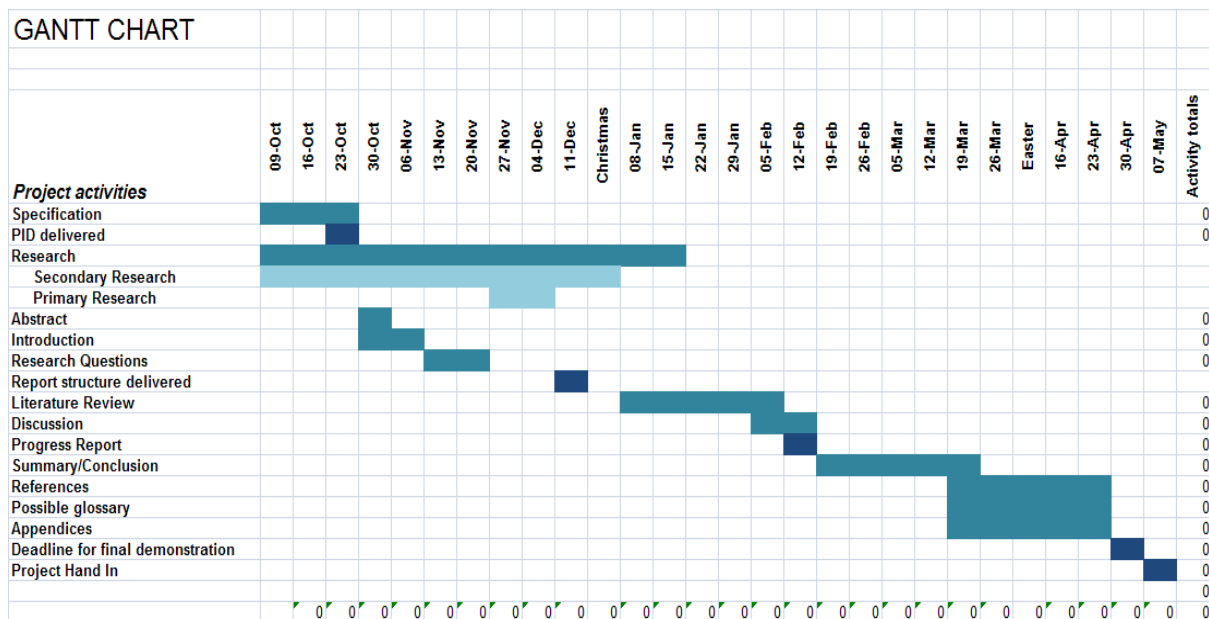


Figure 11

15.4. Future Research and Development

Many possibilities are possible for future research, the most obvious being a physical development of the security policy this project envisions. The suggestions stated in section 14.3 should ideally serve as the initial reasoning and justification to begin development of a security policy that greatly improved security on computers in reigns over. By making a free, online, open source, resource stated, technology stated and constantly updated security policy future research in this area should be greatly improved in a logical and dynamic way.

Due to the research conducted in this project it will also serve the purposes of other concerns. The research conducted on user feedback in the questionnaires gives an insight into user habits that may well be useful for Information Technology staff and Management into how users regard secure systems. The Interviews conducted are of unique value to academics, students or anyone wishing to gain an insight into how IT Security Managers regard the security policies that are intended to safeguard their systems.

16. Bibliography

- Axel, H., Gerrit, T., & Walter, B. (2005). Service Oriented IT Management: Benefit, Cost and Success Factors. In *ECIS 2005 Proceedings* (p. 98).
- BBC News. (2009, May 25). *Blackmail fear over lost RAF data*. Retrieved November 13, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/uk/7449927.stm>
- BBC News. (2008, July 18). *MoD admits loss of secret files*. Retrieved November 6, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/uk/7514281.stm>
- BBC News. (2009, January 9). *Prisoners' medical details lost*. Retrieved November 13, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/england/lancashire/7820338.stm>
- BBC News. (2009, November 20). *UK's families put on fraud alert*. Retrieved November 06, 2009, from BBC NEWS: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
- Burton, S. E. (2008). *Report into the Loss of MOD Personal Data*. London: Ministry of Defence.
- Cabinet Office. (2009, May 07). *Security Policy Framework*. Retrieved November 13, 2009, from cabinetoffice: <http://www.cabinetoffice.gov.uk/spf.aspx>
- Clark, D., & Wilson, D. (1987). *A Comparison of Commercial and Military Computer Security Policies*. Oakland: IEEE Press.
- Davies, J. (2008, May 09). *Encryption software deployed on 20,000 MoD laptops*. Retrieved March 10, 2010, from Computing.co.uk: <http://www.computing.co.uk/computing/news/2216316/encryption-software-protect-mod>
- Fogel, K. (2005). *Producing Open Source Software: How to Run a Successful Free Software Project*. New York: O'Reilly Media.
- Gloucestershire Echo. (2009, May 25). *RAF Innsworth staff at risk after personal data stolen from site*. *Gloucestershire Echo*, p. 3.
- ICO. (2009, November 13). *About the Information Commissioner's Office*. Retrieved November 13, 2009, from Information Commissioner's Office: http://www.ico.gov.uk/about_us.aspx
- International Organization for Standardization. (2005). *ISO/IEC 27001*. London: ISO Press.
- Katzan, H. (1974). *Computer data security*. New York: Van Nostrand Reinhold Company.
- King, L. (2009, October 22). *Almost half ISO 27001 'compliant' firms break with security*. Retrieved 02 05, 2010, from networkworld.com: <http://www.networkworld.com/news/2009/102209-almost-half-iso-27001-compliant.html>

Krutz, R. (2001). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. New York: John Wiley & Sons.

Leyden, J. (2010, January 21). *RockYou hack reveals easy-to-crack passwords*. Retrieved March 21, 2010, from The Register: http://www.theregister.co.uk/2010/01/21/lame_passwords_exposed_by_rockyou_hack/

McGrew Security. (2008, July 8). *Information and Tools*. Retrieved March 12, 2010, from McGrew Security: <http://www.mcgrewsecurity.com/tools/msramdmp/>

Microsoft. (n.d.). *Strong Passwords*. Retrieved April 3, 2010, from Microsoft Online Safety: <http://www.microsoft.com/protect/fraud/passwords/create.aspx>

Office for National Statistics. (2010, April 21). *Employment*. Retrieved April 21, 2010, from National Statistics Online: <http://www.statistics.gov.uk/cci/nugget.asp?id=12>

Office for National Statistics. (2009, August 28). *Internet Access Households and Individuals 2009*. Retrieved October 30, 2009, from UK National Statistics: <http://www.statistics.gov.uk/pdffdir/iahi0809.pdf>

Office for National Statistics. (2007, October 4). *Overview of Families*. Retrieved November 6, 2009, from UK National Statistics: <http://www.statistics.gov.uk/cci/nugget.asp?id=1865>

Office, U. C. (2009). *Technical Risk Assessment*. London: UK Cabinet Office.

Open Source Initiative. (n.d.). *The Open Source Definition*. Retrieved April 3, 2010, from opensource.com: <http://www.opensource.org/docs/osd>

Roberts, D. (1990). *Computer Security: Policy, Planning and Practice*. London: Blackwell Publishers.

Schifreen, R. (2006). *Defeating the Hacker: A Non-technical Guide to Computer Security*. Hoboken: John Wiley & Sons.

Siegler, M. (2009, December 14). *One Of The 32 Million With A RockYou Account? You May Want To Change All Your Passwords. Like Now*. Retrieved March 20, 2010, from TechCrunch: <http://techcrunch.com/2009/12/14/rockyou-hacked/>

snapshotspy.com. (2008). *Employee Computer & Internet Abuse Statistics*. Retrieved April 11, 2010, from snapshotspy.com: <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

Tarzey, B. (2009, December 01). *Straight Talking - Why you must rein in your power users*. Retrieved February 6, 2010, from quocirca.com: <http://www.quocirca.com/media/articles/122009/440/PUM%20for%20Silicon%20PDF.pdf>

17. Glossary of Terms

Term	Meaning
ISO	The International Organization for Standardization, producers of all ISO standards discussed.
ISO documentation	The ISO/IEC 27000 family of documentation regarding Information Security Management Systems. The main document referenced is 27001.
TRA	The 'Technical Risk Assessment' security documentation issued by the UK Cabinet Office.
Wikipedia	Wikipedia is a free, web-based, collaborative, multilingual encyclopaedia project supported by the non-profit Wikimedia Foundation

Figure 12

18. Appendix A: Project Initiation Document



**School of Computing
final year project**

Michael PeggPJE30

**Project Initiation
Document**

**High Security Remote System
Model**

Project Initiation Document

18.1. Basic details

Student name:	Michael Pegg
Draft project title:	High Security Remote System Model
Course:	Bsc (Hons) E-Commerce And Internet Systems
Client organisation:	EADS Astrium
Client contact name:	Mervyn Thomas
Project supervisor:	Dave Billinge

18.2. Outline of the project environment and problem to be solved

The protection of corporate and governmental data has in this digital age has become a hot topic for all the wrong reasons. In the conception of the public this data is not seen as secure, instead the possibility of risk now exists where it should not, and not without reason. In recent times an increasing number of media reports have focused on of vast amounts of lost, mishandled or stolen data and this has lead to giving digitized data a negative stereotype. A significant majority of these leaks have been due to data been taken off-site, primarily on laptops and USB memory sticks.

In July 2009 the MoD admitted it had lost 658 laptops and 121 portable USB memory sticks since 2004. This set of guidelines issued after a major case of data loss in 2004 are clearly not adequate and no formal model exists for dealing with the security of data in remote locations or otherwise.

High security environments for the MoD, ESA or otherwise are of little use if taken away from these secure networks that exist to protect them. Data is transferred and worked on all over the world yet data is stored on laptops with only password protection, little or no wireless encryption, too few cases or weak hard drive encryption and with no way of tracking the hardware itself.

This problem is widespread and applies to the vast majority of companies and agencies be they governmental or otherwise. For companies and the general public to regain confidence in their own data storage this problem must be solved. A model must be devised to end, wherever possible the loss, mishandling and otherwise misuse of digitized data.

18.3. Project aim and objectives

Overall Aims:

- To discuss and explain the current security guidelines and standards of the companies and agencies including the MoD showing weaknesses, flaws and how a different model would improve security and confidence.
- To explain how encryption works and other hardware based techniques, why it is important and to produce a detailed study on varying types and forms.
- To explain the advantages and disadvantages of varying types of guidelines and security models that currently exist, how they are implemented and what can be learned from them.

Overall Objectives:

- Design and implement a High Security Remote Data system model
 - Must comply with methodological techniques.
 - Varying levels of delivery
 - Explanation of why this is important
- Based on an open source schema.
- Discuss hardware techniques available
- Discuss security techniques current available and in corporate or governmental use.

18.4. Project deliverables

- A design and requirements specification gathered from information sources and Astrium management.
- A thorough explanation of encryption types and forms.
- An explanation of the HSRD clearly showing advantages and why it should be implemented.
- A project report to show conclusions gathered and a discussion of how the project progressed including a list of potential solutions to issues discovered.

18.5. Project constraints

- Coverage of existing security models and guidelines – Due to the lack of an existing highly utilized security system model the study of existing security policies must be restricted to that of major, publicised policies that exist within the possibility of research.
- Security techniques available – With a project based around s security hardware, with evidence based on primary and secondary research I will be judging my finding on current working practice, this will constrain me to use what techniques I find available.

- Hardware and software limitations – The world of computing and the overheads associated with some levels of security protections such as encryption protocols must fall within a sensible barrier. A secure system that requires 60 minutes of processing time for each keystroke would be of little use.

18.6. Project approach

The research itself on existing security models will come from secondary research derived from academic texts including white papers, journals. Given the context of the issues of computer security secondary research from news sources will be used, primarily to show past issues and the associated problems, however personal comment will be kept to a minimum to avoid bias of any kind and only reliable information from authenticable sources will be used. Primary research from Astrium itself on security policies and what would be required will be gathered by me with input derived from Astrium management.

Two methodologies will be used to complete the aims specified. A prototyping methodology will be used to approach the task of constructing the artefact as the input of the client are important to ensure credibility and hopeful implementation of the model and this methodology will give the flexibility to make changes to the specific artefact as iterations are shown.

A methodological approach will also be used to aid in directing the project as a whole from initialization, through managing the boundaries of the project to closing the project so all the requirements have been met successfully in a manner that is structured within a clearly defined framework.

The skill set required to carry out this project requires the ability to garner the requirements successfully from the client without bias or direction, to ensure a successfully garnished list of requirements that are truly required to merge with the requirements needed to ensure a successfully secure system. Skills in system development and knowledge of the workings of operating systems are also a useful tool to aid in the development of the model and reading of secondary research on the associated subject.

18.7. Facilities and resources

The project will be completed on the hardware side with personal computer equipment (desktop and laptop computers, memory stick etc) and with university facilities for research tools such as academic books, journals and the library search tools.

The white papers and sources of information on encryption not available from academic books in the university library or not sufficiently up to date will be sourced primary from the internet but only from verifiable sources.

Resources from EADS Astrium such as current security policies of itself and the greater MoD will be important to gain knowledge of what is current and in use and also as a source of employees who must adhere to them. This specific resource is thankfully been made available upon request within work hours and security clearance granted to gain access and ask related questions.

The software used to write all report aspects of this project will be open source and require no additional funding. Ideally all the software used in the artefact will also be open source to keep the project free and available to the maximum of people, however this is entirely dependent on which software is required.

The library and also EADS Astrium are open normal working hours and have no known issues for access, or use and no cost constraints are expected to affect this project.

18.8. Log of risks

There are a number of risks that could affect the project, the risk; chance and plan of avoidable are listed below:

<i>Risk</i>	<i>Chance</i>	<i>Plan of Avoidance</i>
Hardware failure (artefact)	Low	The artefact itself will be deliverable on any medium capable of supporting an I/O based operating system so an image will be backed up on desktop and laptop computers and external memory drive.
Hardware failure (report tools)	Low	If my personal computers for writing up my report become unavailable the use of university supplied computers will function adequately.
Personal Illness	Low	Correct planning on the project should give enough flexibility to withstand small breaks for mild illnesses of myself or my supervisor without compromising the development of the project.
Loss of supervisor	Low	If my project supervisor becomes unavailable for long periods of time I shall consult the project moderator.
Loss of Data	Low	All project data will be synchronised between personal desktop computer and laptop and also to external data storage in a different location to ensure protection from local issues.
Lack of client availability	Medium	This variable is outside of my influence. If the client became unavailable research will be shifted to a more generic security model and an artefact delivered without the clients specific requirements.
Time constraints	Medium	The final delivery date for this project is unchangeable. To aid in avoidable of time slip correct project planning should ensure time used on the project is used wisely and to a plan.

Personal bias of news articles	Low	To avoid this issue news items relating to security will only come from verifiable sources and statements made reviewed by my project supervisor.
--------------------------------	-----	---

The reviewing of these risks will be stated in the project plan and will be reviewed regularly to ensure any negative impact risks may have on the project are dealt with in a timely and none intrusive manner.

18.9. Starting point for research

Thorough secondary research of academic literature on computer security primarily and its associated models from the university library.

Secondary research of current white papers on computer security will be utilised to gain sufficient knowledge of recent insights, breakthroughs and current best practice.

Initial research will focus on the following sources:

The two most prominent secure system models and their initial sources:

- Bell-La Padula model *Secure Computer Systems* - Bell, David Elliott and La Padula, Leonard J. (1973)
- Clark-Wilson model *A Comparison of Commercial and Military Computer Security Policies* - Clark, David D.; and Wilson, David R (1983)

These Sources may also prove valuable:

- BBC News. (2009, May 25). *Blackmail fear over lost RAF data*. Retrieved November 13, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/uk/7449927.stm>
- BBC News. (2008, July 18). *MoD admits loss of secret files*. Retrieved November 6, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/uk/7514281.stm>
- BBC News. (2009, January 9). *Prisoners' medical details lost*. Retrieved November 13, 2009, from BBC NEWS: <http://news.bbc.co.uk/1/hi/england/lancashire/7820338.stm>
- BBC News. (2009, November 20). *UK's families put on fraud alert*. Retrieved November 06, 2009, from BBC NEWS: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
- Burton, S. E. (2008). *Report into the Loss of MOD Personal Data*. London: Ministry of Defence.
- Cabinet Office. (2009, May 07). *Security Policy Framework*. Retrieved November 13, 2009, from cabinetoffice: <http://www.cabinetoffice.gov.uk/spf.aspx>
- ICO. (2009, November 13). *About the Information Commissioner's Office*. Retrieved November 13, 2009, from Information Commissioner's Office: http://www.ico.gov.uk/about_us.aspx

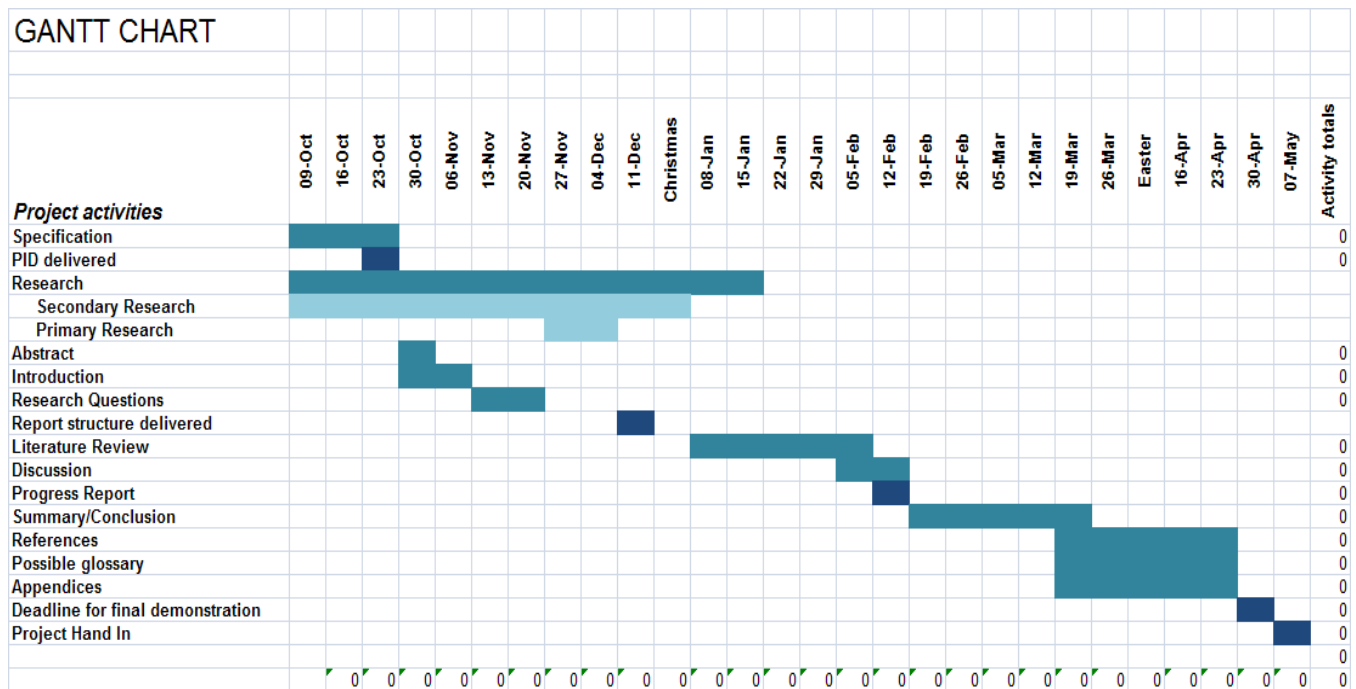
- Office for National Statistics. (2009, August 28). *Internet Access Households and Individuals 2009*. Retrieved October 30, 2009, from UK National Statistics: <http://www.statistics.gov.uk/pdfdir/iahi0809.pdf>
- Office for National Statistics. (2007, October 4). *Overview of Families*. Retrieved November 6, 2009, from UK National Statistics: <http://www.statistics.gov.uk/cci/nugget.asp?id=1865>

The initial research should also lead to the creation of a matrix to clearly show the advantages, disadvantages, limitations and what functionality is missing in current systems to aid in the creation of a matrix to show advantages possibilities of an updated security model.

18.10. Breakdown of tasks

1. Research / Gathering of functional requirements
 - a. Research into secondary sources of existing secure system models
 - b. Primary research from Astrium and requirements gathering to expand on information gathered from secondary sources
 - c. Research into current best practice and recent developments.
2. Design Specification
 - a. Matrix produced to show current issues.
 - b. Matrix produced to show model development possibilities.
3. Design
 - a. Model framework development.
 - b. HSRD system model specified
4. Development
 - a. Development construction.
5. Evaluation
 - a. Review and discussions
 - b. Conclusions gathered
 - c. Potential further work, how it could develop.

18.11. Project plan



18.12. Legal, ethical, professional, social issues

See Ethical Checklist in Appendix B.

Signatures

	Signature:	Date:
Student		
Client		
Project supervisor		

19. Appendix B: Ethical Checklist

PJE30 and PJS30

2009/2010



Ethical Examination

Undergraduate Final Year Projects

School of Computing

Faculty of Technology

Ethics Information: 12-point Checklist

<p>1. Will the human subjects be exposed to any risks greater than those encountered in their normal lifestyle?</p> <p><i>For example: could the study induce psychological stress or anxiety; is more than mild discomfort or pain likely to result from the study; will the study involve prolonged or repetitive activities?</i></p> <p><i>Investigators have a responsibility to protect human subjects from physical and mental harm during the investigation. The risk of harm must be deemed to be no greater than in their normal lifestyles.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>2. Will the human subjects be exposed to any non-standard hardware or non-validated instruments?</p> <p><i>Human subjects should not be exposed to any risks associated with the use of non-standard equipment: anything other than pen-and-paper, or typical interactions with desktop, laptop PC's, tablet PC's, PDA's or mobile phones are considered non-standard (for example, using a VR room) nor should they be subjected to non-validated instruments e.g. unscrutinised questionnaires.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>3. Will the human subjects voluntarily give consent?</p> <p><i>If the results of an evaluation (for example) are likely to be used beyond the term of the project (for example, software is to be deployed or data is to be published), then signed consent is necessary. A separate consent form should be signed by each human subject. Return of a consent email can constitute written consent if this has been made clear to the human subject.</i></p> <p><i>Otherwise verbal consent is sufficient and should be explicitly requested in the introductory script (Information Sheet).</i></p>	<p>Yes No</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/></p>

<p>Comments:</p>	
<p>4. Will any financial, or other, inducements (other than reasonable expenses and compensation for time) be offered to human subjects?</p> <p><i>The payment of human subjects must not be used to coerce them against their better judgement, or to induce them to risk harm beyond that which they risk without payment in their normal lifestyle.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>5. Does the study involve human subjects who are unable to give informed consent (for example: children under 18, people with learning disabilities, unconscious patients).</p> <p><i>Parental consent is required for human subjects under the age of 18. Additional consent is required for human subjects with impairments, and people assessed to be lacking in mental capacity. If consent is gained from a person other than the human subject themselves e.g. a parent, then written consent must be obtained.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>6. Are you in a position of authority or influence over any of your human subjects?</p> <p><i>A person in a position of authority or influence over any human subject must not be allowed to pressurize them to take part in, or remain in, any study.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>7. Are the human subjects being provided with sufficient details of the study at an appropriate level of understanding?</p>	<p>Yes No</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/></p>

<p><i>All human subjects should be able to understand the information provided in any documentation and/or verbal information they receive about the experiment or study. They have the right to withdraw at any time during the investigation, and they must be able to contact the investigator after the investigation. They should be given the details of both student and supervisor as part of the debriefing. This information should be in the introductory script (Information Sheet).</i></p> <p>Comments:</p>	
<p>8. After the study, will human subjects be provided with feedback about their involvement and be able to ask any questions they may have about this involvement?</p> <p><i>If the human subjects request further information, the investigator must provide the human subjects with sufficient details to enable them to understand the nature of the investigation and their part in it.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/></p>
<p>9. Will the human subjects be informed of the true aims and objectives of the study?</p> <p><i>Withholding information or misleading human subjects is unacceptable if human subjects are likely to object or show unease when debriefed. It must be clear to human subjects if information is being withheld in order to elicit a true response. This should precede any analysis of the data.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/></p>
<p>10. Will the data collected from the human subjects be made available to others (where appropriate and only in relation to this research study), and be stored, in an anonymous form?</p> <p><i>All human subject data (hard-copy and soft-copy) should both be stored securely and, if appropriate made available, in an anonymous form. Making human subject data available to a third party may be relevant where a student is taking</i></p>	<p>Yes No</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/></p>

<p><i>part in a wider research project eg. for a member of the University staff, in which case anonymity of human subject data must be preserved.</i></p> <p>Comments:</p>	
<p>11. Will the study involve NHS patients, staff, or premises?</p> <p><i>If yes, then an application must be made to the appropriate external NHS Local Research Ethics Committee (LREC). For projects other than postgraduate research studies, the length of time for gaining external approval may not fit into a project timescale.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>
<p>12. Will the study involve the investigator and/or any human subject, in activities that could be considered contentious, morally unacceptable, or illegal?</p> <p><i>If yes, then further approval must be sought. For example: a project involving the study of pornography on the web will fall into this category. It is possible that the project may not be allowed to proceed.</i></p> <p>Comments:</p>	<p>Yes No</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/></p>

=====

By signing this form, I AGREE to abide by the decisions made in the above points.

If at any time during my project, my answers would change from a white box to a grey box, then I MUST seek re-approval for my project. I understand that if I do not do so, then it is possible that I may FAIL the project component of my course.

Student name: Jupiter number:

Student signature: Date

=====

Supervisor signature: Date