Reasons Why Secure Systems Fail in Organisations

Hamad Mully

BSc (Hons) Computer Science

Yanlong Zhang

Manchester Metropolitan University

https://github.com/Zanoor/ResearchProject-on-SecureSystems.git

No part of this project has been submitted in support of an application for any other degree or qualification at this or any other institute of learning. Apart from those parts of the project containing citations to the work of others, this project is my own unaided work.

Signed Hamad Mully

Table of Contents

Reasons why Secure Systems Fail in Organisations

Research summary

Behavioural information management is an aspect in secure system management that entails controlling the organisation's informal structures while ensuring that the organisation has appropriate security systems (Baskerville & Myers, 2002). Organisations give different definitions for their informal structures, but the universal definition of an informal structure revolves around the understanding of the individual values and how they reflect on the organisation's objectives, organisational beliefs, and common behaviours as guided by the outlaid principles, as well as employees' perceptions on job responsibility (Baskerville & Myers, 2002). The concept of secure systems management is variably applied by organisations across the world and with changing technological infrastructure; five themes remain consistent with the detailed objectives. Secure systems management, according to the studies conducted remain consistent with the organisational security culture, improved internal assessment, and strategic implementation of secure systems, individual operational values, general organisational beliefs, and prompt training in areas related to security (Baskerville & Myers, 2002). The findings about secure organisational systems are generated from the field of sociology with a focus on current behavioural aspects of security governance. In general, organisational secure systems form the foundation of performance management since they focus on several fundamental assets of the organisation.

Introduction

Security is an important organisational concept that describes the process of protecting valuable assets that include an individual, a community, a state, or an organisation from any potential harm (Baskerville & Wood-Harper, 2009). Security provides controls that help to separate the valuable asset from the perceived threat, which can include instilling significant changes on either the threat or the asset (Baskerville & Wood-Harper, 2009). Insights linked to security tend to vary, and hence are poorly matched with reckonable objective security. Similarly, perceptions in relation to the effectiveness of secure systems employed may sometimes be distinct from the actual level of security offered by these systems (Haley, C. 2011, 133). This is because the presence of secure systems may even be confused for security itself. Two computer programs may, for example, be interfering and even limiting each other's effectiveness while the owner may on the other hand be thinking that she/he is receiving double the security from both programs. This shows that secure systems employed in organisations may not always succeed (Mather, T. 2009, 22).

The rising global industrial competition compels organisations to prioritize those activities that will ensure protection of the most sensitive areas of operations (Birman, 2007). Secure information system initiatives represent one of such plans that enhance protection and control of informational assets by creating a base for proper internal control processes alongside maintaining responsible and accountable behaviours in an organisational leadership structure (Baskerville & Wood-Harper, 2009). The mentioned cases of secure system failures point to the general fact that organisational management should base the managerial roles on contemporary informational system governance and other practices that are stringent for security issues. For example, the mentioned case of Water and Sewer department at San Diego is a description of instances that may occur if an employee is capable of accessing the most sensitive set of data or information that is meant for internal control and not for general viewing. Several of such cases where forms containing information about workers' taxes were inadvertently exposed to non-users and ended up affecting several workers indicate the level of threats in information systems security that is probable in organisational performances (Birman, 2007). Cases of management failures to control and/or prevent internal security breaches by those employed within the organisation indicate inefficient governance roles and inability to establish stronger foundations for information system security (Birman, 2007). This would mean that the strategies employed by the management team are ineffective and cannot address individual values in light of organisational objectives, or it would mean that the system management programs are inappropriately applied to encourage conformity with the organisation's policies.

Following the increasing incidents of secure systems failure, which have led to inefficient performance and poor control processes, it appears that the reasons why secure systems fail in organisations is under-researched (Brancheau & Wetherbe, 2011). It is logical to believe that organisational performance is based on proper control of assets, information, and data. Based on the mentioned secure systems challenges and their attached negative effects, this paper analyses the various reasons why secure systems in organisations fail (Brancheau & Wetherbe, 2011). The paper will also highlight various examples where such failures have occurred and to help come up with suitable recommendations on how this can be improved to allow for future management and development.

The purpose of the project

As already stated, behavioural information systems and secure systems governance should focus on the management of people and vital assets of the organisation. The major objective of behavioural security systems management is to ensure employees' conformity to organisational rules and policies (Collmann & Cooper, 2007). In most cases, organisations go to the extent of punishing deviant behaviours while taking deterrent actions to make sure employees follow procedures under the purview of the secure system governance (Collmann & Cooper, 2007). From the cases mentioned in this study, it is clear that people are the weakest link to information system insecurity; hence, it becomes necessary for system managers to offer continuous, dynamic and real time secure system management.

The main purpose of this project is to analyse how organisational secure systems may go wrong when inadequate decisions are made, especially where people from different fields are tasked with organisational responsibilities like system design (Dembe & Boden, 2000). For example, it is possible from the investigations conducted that at the production stage, disconnected ideas may make managers give different designs, which may conflict the performance objectives of the organisation (Dembe & Boden, 2000). Similarly, the project will also analyse the monetary costs of improving security and how such costs affect the workforce morale. The study will provide insights on trade-offs between risks and rewards, and whether reward is the best approach towards fixing system vulnerability, especially where the system is considered tight enough (Dembe & Boden, 2000). Where the proposed approaches are inefficient, the study project will provide alternative actions that will help organisations improve in areas of systems management under the section of recommendation. The project will use case histories of previous security failures that have been caused by lack of incentives and management skills. The case histories will provide background information on how organisations can learn from their mistakes while engaging in proactive actions to prevent occurrence or reoccurrence of the system failures.

Project objectives

1. To understand the security policies created by organisations following the risk management mechanisms.
2. To understand the reasons why people make certain decisions and how such decisions affect system security in the organisation.
3. To understand how system designs and projects can fail both at the formulation and at the implementation stages.
4. To understand the definition and causes of moral hazard and how it affects employees' incentives to engage in organisation's operations.
5. To understand how moral hazards may give rise to insecure systems in the organisation.

Literature review

Secure Systems within organisations

In this section, an overview of security policies created by organisations to avert risks associated with systems security breaches is conducted. The section further scrutinizes reasons behind different decisions made in institutions concerning system security and reasons why such decisions sometimes fail. Various analyses of moral hazard and other definitions coupled with an in depth understanding how system designs and projects can fail in organisations are done in this section. Similarly, the chapter analyses different, but relevant cases of histories of previous security failures within organisations providing reasons for such shortcomings and mitigations.

Lastly, a brief description of ways of improving security system in an organisation is given for consideration. Against these, a more secure system design for institutions must be one that vehemently reconciles the socio-technical aspect of the system with the organisational goals and objectives.

Background information on secure systems in organisations

System security in the 1940s was the core in the development of the digital computers and by 20th century, key inventions on security were significantly on the rise (Dhillon & Backhouse, 2001). From the wartime genesis, computers have evolved to be more powerful and complex with wider range of applications in different sectors of any viable economy. In essence, the use of computer technology is crucial and a necessity to most organisations in the operational and organisational designs (Dhillon & Backhouse, 2001). Therefore, there is need for more secure systems to safeguard the credibility of data and information in the organisations' databases. The ever increasing usage and reliance on information technologies for many businesses has further necessitated the need and desire to develop more secure and reliable designs to safeguard the data systems.

Analysis of moral hazard and other definitions

Arguably, moral hazard can be defined as situation in which one party is involved in a hazardous situation with an assumption that it is cushioned and protected against associated risks. Such persons know that they will not incur any cost and are not committed in their work performances (Dhillon & Backhouse, 2001). Moral hazards in this context can be described as the availability of incentives to parties that incur expenses as a result of a failed system but are not obliged to bear the incurred costs. Just as the law recognizes a company or an institution as a legal person solely liable, a failure in security system pits the organisation as the sole bearer of the responsibility. Most system developers are, therefore, under less pressure when the system fails as they don’t have to bear the costs associated with the failure (Dhillon & Backhouse, 2001). This can result into low levels of commitments and responsibility from the developers and imminent system failures. Moral hazards occur where there is information asymmetry when one individual or party has more information about a system more than the others. For instance, the system developer may have some crucial information about the system but deliberately refuses to reveal the information in case the system fails. Moral hazards must be regulated and checked properly as some system developers enter into contracts in bad faith and in the process showing less level of commitment the responsibility demands (Dhillon & Backhouse, 2001). In overcoming moral hazards in an organisation, penalties should be placed on employees for bad behaviour that are contributory to the firm’s system failures. For example, the system operation manager may knowingly and out of bad intentions make questionable decisions like in the case of the nuclear reactor (Dhillon & Backhouse, 2001). Such decisions may hurt the general performances of the system and such managers should be punished appropriately if possible by a court of law. Similarly, the organisation should build in incentives to award employees with credible work performances and commitment.

In the analysis viability of secure systems within organisations, all the stakeholders relevant in the field of information and technology must be involved. Arguably, stakeholders in system theory refer to the organisation itself, its clients, and the external environment that are crucial in ensuring the safety and efficiency of the systems (Subashini & Kavitha, 2011). According to a study conducted by an IT firm in the UK, stakeholders were found to be the most crucial element in system design safety. Such stakeholders were identified as those who used and developed the systems, those who administered and owned the systems, and lastly, the security system experts

(Subashini & Kavitha, 2011). Stakeholders' participation in securing institutions' information systems cannot be underrated and is the first step towards system success.

Key to involving participatory elements revolves around pertinent viewpoints in achieving consensus and ranges from in-depth consultations and participation to consensual decision making processes (Subashini & Kavitha, 2011). Any conflict of interest, breach of trust, broken communication and consensus constitutes some of the crucial challenges facing systems within organisations. Consequently, failure to create a cohesive and coherent interactive environment that efficiently accommodates all stakeholders is the genesis of system failure in an organisation (Subashini & Kavitha, 2011). A study conducted to determine the feasibility and viability of stakeholders' role in systems safety ascertained that participatory approaches in managing Organisations' systems were central aspects.

Confidentiality, integrity and availability describe a secure system within an organisation and any breach in these entails organisational design failures. Confidentiality constitutes protection of the institutions' sensitive data and information from unauthorized access. Similarly, integrity involves sufficiently safeguarding the precision and entirety of information in the organisation's databases (Subashini & Kavitha, 2011). Correspondingly, availability comprises ensuring that all information and other critical services provided by an organisation are made accessible to all stakeholders when requisite. Therefore, systems security can be referred to as the processes of ensuring that the confidentiality, integrity and availability of data and crucial information are made possible. In addition, the systems should be dependable and reliable in the face of adversities, malevolence, mischance or even slip-up (Subashini & Kavitha, 2011). Securing the systems in a firm entails all the technical, cross-discipline expertise and supervisory procedures applicable in computer systems.

Any form of failure in an organisation may be detrimental to the enterprise employees and the external environment and should be mitigated appropriately. Though most systems are more susceptible to attacks from hackers and viruses, designing risk evasion strategies adequately prepares such establishments in averting such failures. Since different organisations protect their vital information and data differently depending on the value and importance, it is imperative for each and every organisation to remain vigilant and pro-active in protecting their systems.

The secure administration of an institution's information system in information savoir-faire organisations is most crucial in this current information savvy era. Coupled with the constant threats and resilient attacks on most major organisation's data sites, appropriate policies must be put in place to help identify and sort any potential mess. To this date, no viable research has been carried out on socio-technical designs in ensuring a safe system designs for organisations (Subashini & Kavitha, 2011). The data and information security systems in most business establishments are constantly facing breaches in their computer security databases. A study conducted in the UK to ascertain the extent to which the security systems in most institutions were at risk of being breached, it was found that most of these businesses surveyed reported at least one incidence security breach.

Understanding how system designs and projects can fail in organisations

Failure emanates first when system managers fail to comprehend or address the system performance requirements effectively and in the process causing unnecessary hiccups in the system (Subashini & Kavitha, 2011). Communications in such firms are relatively poorly coordinated in decision making processes and all stakeholders are not efficiently involved in the system functionalities. Most systems become obsolete with time and must be replaced or improved occasionally. Additionally, the system should be in line with the organisation's culture and core functions and acceptable among the workforce. By inadequately addressing cultural issues in the application of a technology, the system is bound to fail in achieving its core functions. Pitiable program system management and implementation procedures can also be attributed to the failure of a system in an establishment (Subashini & Kavitha, 2011). Moreover, poor system planning and risk management techniques in case of a system failure are common in some companies. Most system designs and projects failures in most establishments can be attributed to a number of development practices issues due to the complexity of the system software among other pertinent issues. Similarly, most system software developers incorrectly assume a number of system requirements that are necessary in securing the systems. Such faulty assumptions by system developers can stir major problems in an organisation as will be discussed in a case of the experiences at the nuclear regulatory commission in the US. In addition to these, inadequate involvement and training of all relevant stakeholders in the designing and usages of the systems can be detrimental to the general success of the systems (Subashini & Kavitha, 2011). For instance, a poor user interface significantly inhibits the use of the system and a possibility of shying off completely from applying the services of the system. This is particularly common in banks and other financial and accounting institutions and failure to mitigate or intervene may be detrimental in the long run to the applicability of the systems. Differently, faulty equipment in an establishment can severely cause a secure system to fail resulting in devastating effects. Though difficult to protect and secure, the organisation's hardware are crucial in achieving the operational and organisational goals in an establishment. Therefore, when the system is being designed, all the faulty hardware should be considered to help in minimizing any impact of a potential failure. In the same way, inadequately training the staff on the usability and applicability of the systems is instrumental in minimization of possible loss or failure. For instance, in a hospital setting, the introduction of online pharmacy and medication system, and disease detection and prescription processes required adequate training and orientation.

Lastly, the system should be one that fits the organisation's goals and objectives without many hiccups that may cause it to fail. A meagre fit connecting the system and the firm under consideration can result into severe system failure. For instance, when a country's asylum firm system developers limit its applicability to a few places or individuals in a country, it amounts to poor system management. Since the system should be serving all asylum seekers in a country, constraining it limits its primary purpose and scope and is described to be a poor fit between the system and the establishment.

Case studies of previous security failures within Organisations

The case on the "Data leakage Worldwide: The Effectiveness of Security Policies"

In a 2008 study dubbed "Data leakage Worldwide: The Effectiveness of Security Policies," Cisco conducted a survey of companies and their security policies. The findings of the survey indicated that 23 percent of IT professionals worked in companies with no security policies, and 47 percent and 77 percent of employees and IT professional respectively indicated the need for an update of the security polices in companies (Cisco 2008). Among the causes of failure of IT policies for many companies, the survey indicated, was breakdown of communication of the policies by the IT department. Specifically, the survey indicated that 11 percent of employees stated that the IT department did not communicate or educate them about the security policies (Cisco 2008).

Further, the survey indicated that most policy updates are communicated to employees via email, with the risk of deletion, disregard, or minimal likelihood of retention, as it would be the case if the updates were communicated in person (Cisco 2008). Even more from the survey was the discovery that although it is important to communicate security polices to employees, the action is futile if the employees have no comprehension of the policies, or do not comply with the policies. Therefore, apart from the mere communication of the policies to employees, it is important that the management do a follow up on the retention, comprehension and compliance to the security policies.

Yet another case study points to failure to update system security and reporting. The Atomic Energy of Canada designed the Canadian Therapy Machine, which was used in radiation therapy for the treatment of cancer patients (Dalal&Chhillar 2012). In two years (1985-1987), the machine gave an overdose of radiation to the patients, causing the death of three patients and injury of many others (Dalal&Chhillar 2012). According to Dalal and Chhillar (2012), investigation into the machines showed that there was an “inadequate system of reporting and investigating accident”. Indeed failure to update the software’s security and reporting systems dating several years since the installation of the software in the machine caused the overdose and eventual death of three patients.

The need to update security policies, protocols and upgrading of a system is the responsibility of the management of an organisation. The management should therefore be proactive in the security protocols and systems especially after a security breach. Sony is however currently facing two class action lawsuits by employees whose information including social security numbers and medical information was leaked to the public by hackers who had earlier breached Sony’s data security (Ellis 2014). The plaintiffs in the lawsuits claim that given a previous data breach and warnings, the company remained negligent, paving way for the security breach. The Anonymous group of hackers had hacked the company's PlayStation network earlier in 2011 making some games unplayable and making away with millions of user accounts. Moreover, the group had informed the company of the impending breach several days in advance, of which the company took no action in implementing safeguards to insulate the system (Ellis 2014). Yet even after the 2011 breach, the company could not prevent attacks on the PlayStation and Sony Entertainment networks, both of which suffered massive breaches in August 2011 and the most recent (November 24), even after warnings from the North Korean government (Ellis 2014).

The case of system failure at the US Military

Studies conducted by a UK research firm confirmed that as one of the principal causes of system failures, pitiable development practices in most institutions was in fact identified as a major detriment. A case of a system failure at the Pentagon, the Office of the National Reconnaissance identified a number of deprived development practices as the derivation causes of the adversities. These entailed insufficient trials of the delivery systems of the Titan IV rocket carrying nuclear missiles (Haley, 2011). The US military being technology savvy is widely driven by complicated installations based on technological innovations, and this make computer security in the military a necessity. Most US military hardware is costly and is as a result of expensive scientific research works funded by the US Federal Governments (Haley, 2011). The communication systems at the US military bases must, therefore, be sufficiently secured against any attack or potential hacks. The future of any viable military at the global level depends primarily on information and communication systems and development of robust hardware based on technological innovations (Haley, 2011). All this dictates a more refined and encrypted secure system that can easily detect security breaches. Buoyed with a vibrant logistic and inventory management system, the US military operates solely on information technology.

Against these, the loss of the Titan IV rockets indicated a clear failure by the military in securing their systems. This was as a result of the inability of the National Resonance Office to deploy a defence program (satellites) that could ward off an imminent loss of the military hardware. The director of the Reconnaissance Office ascribed the slip to an ‘omitted decimal point’ in the military software that was to control the movement of the rocket. In testing an already operational military system, it was necessary to adequately prepare to counter any malfunction or general failure of the system (Haley, C. 2011). The US military failed to put in place workable development practices in deploying and testing its weaponry and other crucial installations. This case is of particular importance since the rocket was carrying the US nuclear missiles and was supposed to be subjected to higher monitoring and protection given the danger a possible loss to the US enemy poised to the country. The systems failed to protect the rocket carrying nuclear weapons and the credibility of the security technological systems was questioned. These ranged from failed electronic detection and authentication systems that were to detect and monitor the movement and use of the rocket (Mather, 2009). The failure was blamed entirely on national command authority centre at the pentagon and the alarm systems.

Similarly, the failed systems of the US military were portrayed when a truck carrying explosives and detonators in Kabul exploded (Mather, 2009). This incidence was attributed partly to negligence and partly to problems in the management of US munitions by the personnel. A comprehensive and coherent development practices in the military is clear on weaponry assortments and transportation procedures (Mather, 2009). A feasible system will detect when explosives are put in the same truck with detonators and give prior warning signals. In this case, the system failed and as a result, a life was lost and expensive military equipment destroyed in the process.

The case of system failure at the US Nuclear Regulatory Commission

The scientist and system developers at the US Nuclear Regulatory Commission came up with a program they named Shock II to test models in a nuclear reactor. The test model miscalculated some crucial calculations necessary in ensuring that the nuclear reactors withstands and survive any strong earthquake (Subashini & Kavitha, 2011). The developers summed the components and changed the vector into a magnitude instead of adding absolute values. This amounted to an error in the earthquake testing systems and was only discovered after the completion of the construction processes of the reactors. The Federal Government, therefore, had to close down a number of nuclear reactors to carry out a robust background check and to reinforce the whole system (Subashini & Kavitha, 2011). Arguably, this resulted into a loss of crucial time and resources that could have been channelled to other crucial sectors or systems within the organisation. These background checks and reinforcement procedures took a considerable amount of duration during which most companies had to do without power supply. By incorrectly assuming some specific requirements of the model in the nuclear reactors, the developers contributed to the system failure and to the ensuing loss of time and resources.

The case of system failure at an investment bank

A pitiable user interface at an investment bank in the US was recognized as an instrumental aspect in ensuring that the financial and accounting system of the bank was either a success or failure (Siponen, 2000). A bank employee who had issues with the bank’s system user interface introduced unnecessary data and information to the system. As a result, the employee sent an invoice to a customer but in a wrong currency and to another client a credit note instead of an invoice. Ultimately, this made the system to be seen to have failed in its core mandate and was subjected to severe public scrutiny (Siponen, 2000). This, however, was attributed to the bank's accounting software and user abuse or inability to use the computer systems. The US Accounting and financial systems can sometimes be complicated to use without prior adequate training and maybe erroneous causing the systems to fail in its core functions.

Similarly, the bank lost a number of its reliable and loyal customers crucial account information and a number of employees were fired as a consequence. Notably, the foundation of any bank's operations is rooted on its relation with the clients and its ability to safely store the clients' crucial records without many hiccups (Siponen, 2000). For these reasons among others, the bookkeeping system must be efficient and constantly updated with credible and trustworthy employees in place. The procedures involved in bookkeeping must be secure to ensure no unauthorized access to secret information is permitted. Correspondingly, the banks teller machines being the public face of the investment bank had to be probated from any form of malfunctioning or attack. John's card was stolen while travelling in a commuter train though kept his he personal identification number (PIN). After one week of frantic search, he reported to the bank but unfortunately, he was too late. His account balance read zero as the thief had managed to hack his pin and withdrew all his savings (Siponen, 2000). This was attributed to the imminent failure by the bank to properly and adequately authenticate transactions and to protect clients' assets (Siponen, 2000). The bank's teller machine system and the general physical security systems had loopholes that the credit thief exploited.

In another instance at the bank, the vaults of the highly guarded currency safe room was broken into and a considerable amount of cash stolen. Despite the vaults being connected to a robust and active alarm system, the thief still managed to access it. This was attributed to the failure of the alarm security technology at the bank that allowed manipulations and false impressions of a workable and reliable system.

The case of system failure at a local hospital

The hospital management settled on the web based technology as a measure to revolutionize their service delivery and to increase profitability. The online system revolved around ensuring that patients' records were well stored and easily retrieved when needed and to avoid unauthorized access to the records (Sindre, 2005). Drugs prescriptions and purchase was designed to be done online to ease the time a patient waited in line to get served or attended to by the medical staff. The personal systems identifying each patient's record ever treated at the hospital was designed and widely applauded as a great milestone. Joan was among the very first beneficiary of the system during the first weeks of its launch and operations (Sindre, 2005). When her son fell ill, upon arrival at the institution, the system failed to retrieve her son's help records on time and she had to wait in the queue longer than expected. The hospital staffs were very slow and inefficient when using the system, too slow even compared to the old manual system. Similarly, the hospital administrator claimed that the system had been attacked by a virus contributing to the slow response the system was facing. The service provision at the hospital generally stalled and the viability of the new technology introduces was under sever public scrutiny and criticism (Sindre, 2005). This was a clear case of a failed system due to insufficient back up plans and security measures relevant to the system's functionality. Similarly, the medical staff had insufficient training on the use and applications of the new technologies introduced at the hospital and as a result were slow in their service provisions. This can also be attributed to scarce system orientation programs for the staff at the hospital creating limited time for the majority of the staff to get used to the new system.

Improving security system in an organisation

Though an expensive undertaking, it is imperative that the management of an establishment take necessary and relevant steps in improving and maintaining a secure work environment (Miller & Whitford, 2007). The expenses incurred in setting up new systems and improving the existing ones must be solicited from whatever avenue to ensure the systems remain updated and pertinent. For instance, this can involve setting up new surveillance systems and locking up server rooms to prevent unauthorized access to the systems (Miller & Whitford, 2007). All vulnerable devices and secret information should remain locked in the server rooms and be placed under strict surveillance. Appropriate backing system devices should be developed to help in recovering of lost data and information in case of a system failure. Training and orientation programs on the use and application of a new technology should be implemented to improve users interface and to minimize potential system misuses (Miller & Whitford, 2007). Lastly, physical security at an institution should be enhanced to prevent unauthorized entry and access to the firm's systems.

Methodology and Design

This section presents a detailed description of the methodology and study design and how it impacted on the results obtained. Some of the key areas discussed under this section include research design, description of the study area, target population, sample population, sampling procedure, data collection methods and data analysis methods.

Research design

The research was carried out in form of a cross section survey of organisations, institutions or businesses that have faced cases of insecure systems. The study focused majorly on the systems of communication between departments and employees or among employees. Prominent in this case was the use of emails to communicate with internal uses of information or data sets. Some of the areas that were considered for investigation included the number of emails received by employees each day, number of important emails, confidentiality issues attached to the use of email, whether emails are appropriate means of communicating organisational changes, clarity of emails as a channel of communicating organisational changes, overall security posture and industry practices, strategies used by the organisation or institution to address security breaches and whether such communication practices motivated employees.

Questionnaire and Interview as the methods of Data Collection Techniques

I used questionnaires and interview schedules in a set form to draw information from respondents. The respondents had the opportunity to fill the questionnaires on their own. However, my presence during the scheduled interview was considered important as far as the investigation was concerned. Emailed questionnaire was considered most appropriate by me because it was easy to administer, reduces the time and cost of study and also gave the respondents opportunity to respond without any interference. However, not all the respondents sent back the questionnaires with their responses. I only received 420 responses out of the 910 emails sent.

Target population, sample and sampling techniques

The study targeted employees from various organisations and institutions that have faced instances of security breaches and system failures. The study focused on both private and public institutions and their respective systems of communication, data processing and transmission and how these systems become open to security challenges.

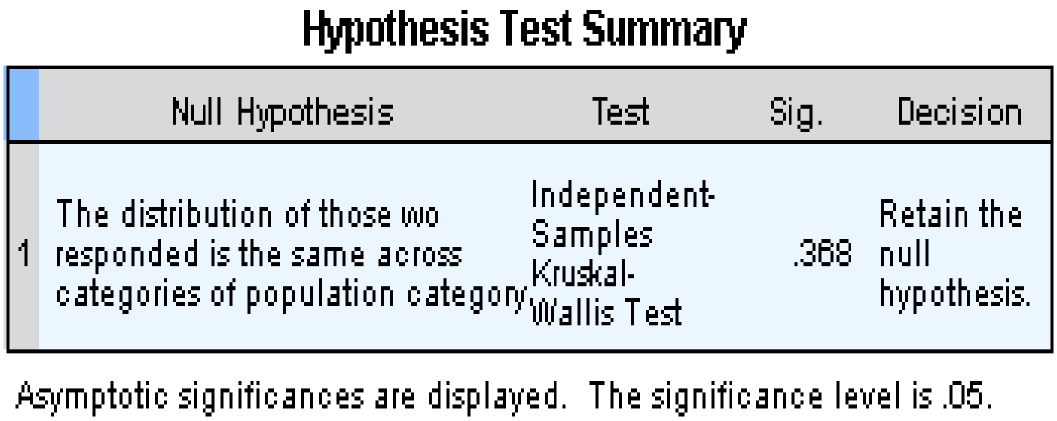
For convenience, the target population was clustered into groups with similar experiences on issues of system security following the highlighted areas of investigation. A sample size of 910 employees was drawn from a population of 3361 individuals. A set of 8 questions were presented to each employee in form of questionnaire. Some of the questions were ranked using ordinal scales while other questions were restrictive and only required a yes or no answer. The use of rigid questions and, or response through ranked values was important for the purposes of uniformity in response and easy analysis. Out of the 420 respondents, about 66.7 percent were female while the rest were male. The higher female figures showed that women are more sensitive to issues of system insecurity and would note any slight changes in system operations, especially in areas of communication. The table and graph below shows the sample representation for the emailed questionnaires.

Results

Before analysing the data collected from the field, it was important to conduct a test to determine whether there was randomness in the sample selection. I conducted a non-parametric test for randomness where I fed the data in figure 1 below in SPSS to help with the processing and output display. The results for randomness according to SPSS indicated that the distribution of those who responded was the same across the category of the population as well as those who did not respond.

Figure 1: sample distribution table

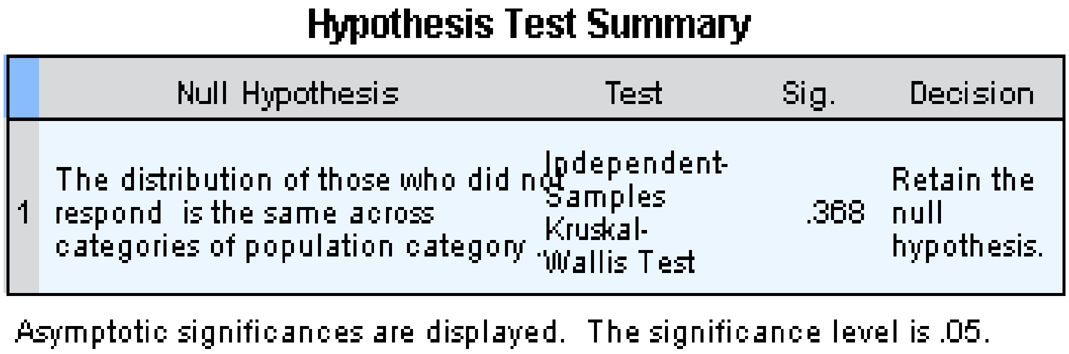
Population category	Those who responded	Those who did not respond	Total Sample representation
Males	140	315	455
Females	280	175	455
Total	420	490	910



Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of those wo responded is the same across categories of population category	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of those who did not respond is the same across categories of population category .	Independent-Samples Kruskal-Wallis Test	.368	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Since the numbers of those who responded and those who did not respond were equally likely across the categories of population, the test met my objective of randomness and therefore the analysis of the information on system security was to be conducted.

The response from the questionnaires collected were as presented in figure 2 below and represented employees perceptions on the use of mails as one of the channels of communication. With the rising changes in communication technologies, organisations' systems of communication are exposed to threats of insecurity.

Figure 2: summary of employees' response

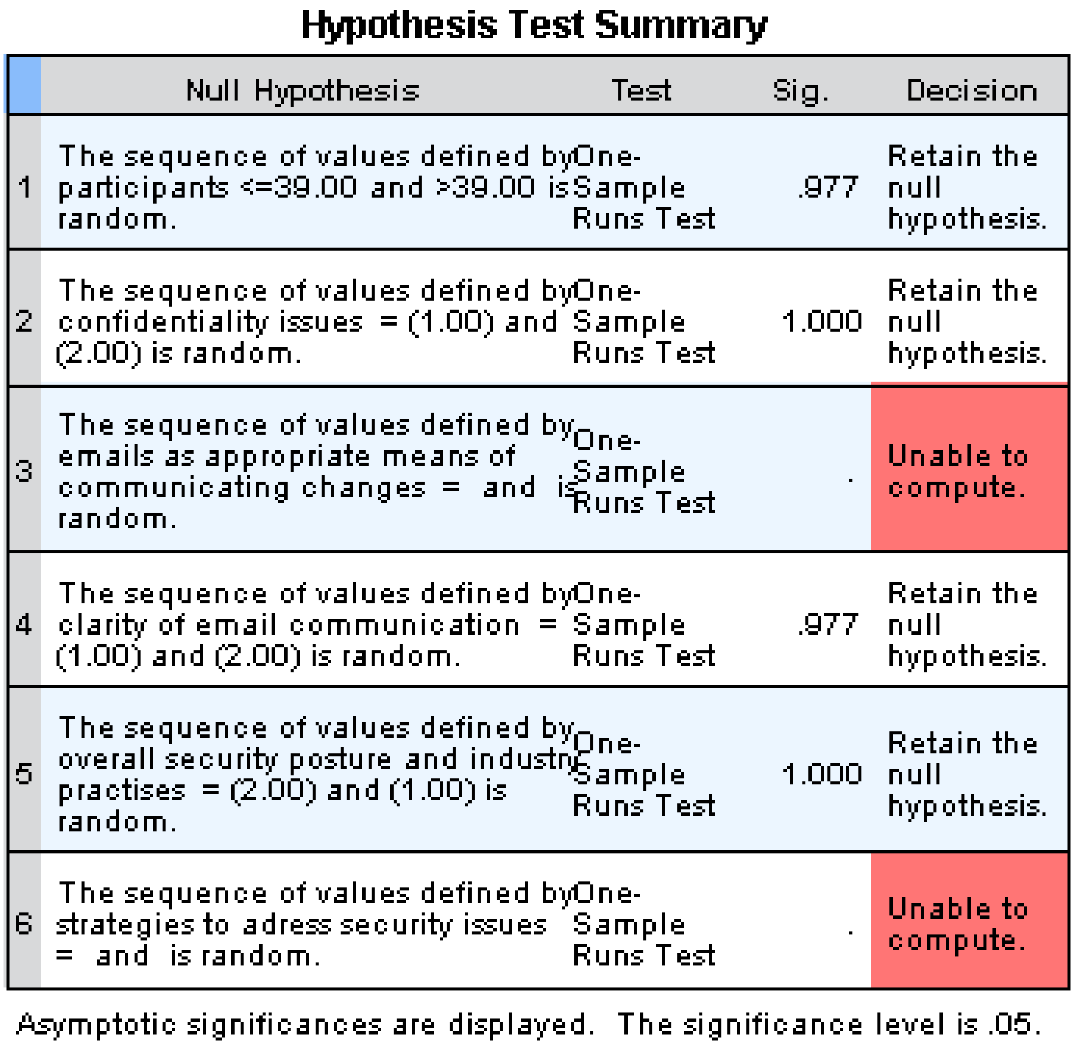
Participant	Number of emails received daily	Number of important emails	Confidentiality issues	Emails as appropriate means of communicating changes	Clarity of email communication	Overall security posture and industry practices	Strategies to address security breaches	1 hour email free sufficient to motivate employees
51	**0-4**	1-3	Yes	4	Yes	No	1	3
44	**15+**	10+	Yes	5	No	Yes	1	5
33	**15+**	4-6	Yes	1	Yes	Yes	5	5
40	**15+**	10+	Yes	5	Yes	Yes	3	4
37	**10-14**	1-3	Don't know	5	No	No	1	3
24	**10-14**	4-6	Yes	4	No	No	4	5
45	**15+**	10+	Yes	5	Yes	Yes	1	1
39	**15+**	7-9	Yes	5	Yes	Yes	5	3
26	**15+**	4-6	Yes	4	No	No	4	5
36	**10-14**	4-6	Yes	3	No	No	1	5
45	**5-9**	1-3	Yes	3	Yes	Yes	5	5

The precise areas that were in line with the study objectives included confidentiality issues, whether emails are appropriate means of communicating organisational changes, overall security posture and organisational practices and strategies to address security issues. For the purpose of analysis, I gave the yes-no responses nominal values of 1 and 2. That is to mean, 1 represented a yes response while 2 represented a no response. Figure 3 below gives the precise information and data that were used for the analysis and generation of the results obtained discussed in this study.

Figure 3: data and information for analysis

Participant	Confidentiality issues	Emails as appropriate means of communicating changes	Clarity of email communication	Overall security posture and industry practices	Strategies to address security breaches
51	1	4	1	2	1
44	1	5	2	1	1
33	1	1	1	1	5
40	1	5	1	1	3
37	2	5	2	2	1
24	1	4	2	2	4
45	1	5	1	1	1
39	1	5	1	1	5
26	1	4	2	2	4
36	1	3	2	2	1
45	1	3	1	1	5

Essentially, I conducted a Runs test to determine the randomness in individual responses based on the questions asked. From the analysis, it was clear that the responses given by individuals had not been predetermined or influenced by anything I said. Therefore, the null hypothesis that each respondent's response was based on personal experiences with the organisation system security still remained significant according to data output given below.



Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The sequence of values defined by participants <=39.00 and >39.00 is random.	One-Sample Runs Test	.977	Retain the null hypothesis.
2	The sequence of values defined by confidentiality issues = (1.00) and (2.00) is random.	One-Sample Runs Test	1.000	Retain the null hypothesis.
3	The sequence of values defined by emails as appropriate means of communicating changes = and is random.	One-Sample Runs Test	.	Unable to compute.
4	The sequence of values defined by clarity of email communication = (1.00) and (2.00) is random.	One-Sample Runs Test	.977	Retain the null hypothesis.
5	The sequence of values defined by overall security posture and industry practises = (2.00) and (1.00) is random.	One-Sample Runs Test	1.000	Retain the null hypothesis.
6	The sequence of values defined by strategies to adress security issues = and is random.	One-Sample Runs Test	.	Unable to compute.

Asymptotic significances are displayed. The significance level is .05.

After determining whether there were randomness in sample selection and responses, I needed to obtain the means of the responses in order to understand the normality of data distribution, hence the validity of the result obtained. The analysis of normality and validity of individual argument is represented in both figure 4.1 and 4.2 below.

Figure 4.1: confidentiality issues overall security posture and industry practises strategies to address security issues * emails as appropriate means of communicating changes

emails as appropriate means of communicating changes		confidentiality issues	overall security posture and industry practises	strategies to address security issues
	Mean	1.00	1.00	5.00
1	N	1	1	1
	Std. Deviation	.	.	.
	Mean	1.00	1.50	3.00
3	N	2	2	2
	Std. Deviation	.000	.707	2.828
	Mean	1.00	2.00	3.00
4	N	3	3	3
	Std. Deviation	.000	.000	1.732
	Mean	1.20	1.20	2.20
5	N	5	5	5
	Std. Deviation	.447	.447	1.789
	Mean	1.09	1.45	2.82
Total	N	11	11	11
	Std. Deviation	.302	.522	1.834

Figure 4.2: confidentiality issues overall security posture and industry practises strategies to address security issues * clarity of email communication

clarity of email communication		confidentiality issues	overall security posture and industry practises	strategies to address security issues
1	Mean	1.00	1.17	3.33
	N	6	6	6
	Std. Deviation	.000	.408	1.966
2	Mean	1.20	1.80	2.20
	N	5	5	5
	Std. Deviation	.447	.447	1.643
Total	Mean	1.09	1.45	2.82
	N	11	11	11
	Std. Deviation	.302	.522	1.834

Other than the means of communication (emails), it was clear from the analysis that organisational system security depended on factors such as confidentiality issues, overall security posture and industry practices, as well as strategies to address security issues (Baskerville, 2010). Let Y represent system security while channels of communication, confidentiality issues, overall security posture, industry practices and strategies to address security issues be represented by X_1, X_2, X_3, X_4, and X_5 respectively, then Y would be modelled into a regression equation as shown below.

$Y = X_1^{\beta 1} + X_2^{\beta 2} + X_3^{\beta 3} + X_4^{\beta 4} + X_5^{\beta 5} + \mu$, where $\beta = 1, 2, \ldots, 5$ represents factor endowment in each of the independent variables while μ represents all other factor defining system security other than X_1, X_2, X_3, X_4, and X_5. From the analysis I determined how the changes in each of the independent variables would affect the overall security system of an organisation as follows.

$\partial Y = \beta_1 (\partial X_1^{\beta 1\text{-}1}) X_1 + \beta_2 (\partial X_2^{\beta 2\text{-}1}) X_2 + \beta_3 (\partial X_3^{\beta 3\text{-}1}) X_3 + \beta_4 (\partial X_4^{\beta 4\text{-}1}) X_4 + \beta 5 (\partial X_5^{\beta 5\text{-}1}) X_5$

In this model β_1, β_2, β_3, β_4 and β_5 are the response strategies an organisation can use to ensure all its systems are secured and free from access by unauthorized person. In other words, they define the strategic plan for an organisation facing security threats from external users of the systems.

Evaluation

From the study conducted, it is prominent that inappropriate decisions are some of the major causes of system failures, which in most cases have adverse effects on critical operations and asset management (Anderson & Moore, 2006). The common threats to secure system management according to the information gathered include intruders, system hackers, disgruntled employees, natural calamities and to a lesser extent terrorists (Anderson & Moore, 2006). According to the respondents, communication through emails could be beneficial to the organisation's performance and may also have various disadvantages. The research also revealed the possibility of estimating the likelihood that security threats will exist is based on the historical information and judgments of system managers (Anderson & Moore, 2006). Since organisations at times operate in a free space and depending on the decisions provided by employees or other staff members, controlling people's actions become hard. The decision by most organisations presented in this study to rank assets that could be affected should there be threats to security systems is important (Anderson & Moore, 2006).

From the surveys conducted, it is imperative that organisations conduct risk assessments to understand the causes and effects of secure system failures (Ash & Bates, 2005). For example, the use of email to deliver sensitive information to employees could be one of the causes, or mismanagement of security systems like computers and other applications. Even though the respondents believed that data on threat likelihood and its associated costs to the organisation could be lacking, the limiting factors like costs of management and skills should not prevent effective exploration (Ash & Bates, 2005), understanding, and information security ranking. Most respondents believed that system managers could present procedures and allow people to contribute through discussions as a way of ensuring that the risks associated with secure system management were periodically addressed and common management grounds reached.

Conclusion

Secure systems play a crucial role in promoting the daily activities of a business organisation, thereby promoting its capacity to accomplish its missions and goals (Anderson, 2008). Security policies generated from risk management mechanisms and inadequate decisions may however be attributable to failure in secure systems within organisations, thus, affecting security as a whole. Being uncertainty averse rather than risk averse involves organisations creating inadequate security policies that only allow organisational leaders to deal with security issues intuitively. Inadequate decisions to adopt limited internal controls, activity displacement, and solving the wrong problems may cause secure systems in organisations to fail (Anderson, 2008). Organisations should, however, learn that adopting science-based engineering procedures as well as aiming to address complex problems could prevent secure systems from failing.

Now on a more personal note; throughout the year I have been intellectually challenged and stimulated and at the beginning of my project I felt overwhelmed by the amount of research needed to be done and disappointed in how my topic of interest has been somewhat overlooked but also this gave me the opportunity to perhaps make a small contribution and that motivated me. I tackled this project by researching and evaluating on the objectives I set for myself thereby constructing a hypothesis and using data extracting techniques to amass results and evaluate. What I would like to have done differently should I have the opportunity would be to target my investigation to a more relevant audience not just within universities and peers but to people who actually work within industries and secure systems however I feel that to accomplish such a task requires better investigative techniques, one which can be possible through further research as currently I have not done enough. I do believe that with better understanding and more research we can employ better risk management and managerial techniques within the industry and promote better practises which can benefit security, employees and businesses as a whole. Having a deeper understanding has given me more confidence to work in management industry as I feel more conscious of the problems that can arise from decision making and I feel I can relate more with the workforce through experience of my own.

References

Anderson, R 2008, *Security Engineering: A Guide to Building Dependable Distributed Systems,* Wiley, Indianapolis.

Anderson, R., & Moore, T. 2006. The economics of information security. *Science*, *314*(5799), 610-613.

Ash, J. S., & Bates, D. W. 2005. Factors and forces affecting EHR system adoption: report of a 2004 ACMI discussion. *Journal of the American Medical Informatics Association*, *12*(1), 8-12.

Baskerville, R. L. 2010. Investigating information systems with action research. *Communications of the AIS*, *2*(3es), 4.

Baskerville, R. L., & Myers, M. D. 2002. Information systems as a reference discipline. *Mis Quarterly*, 1-14.

Baskerville, R. L., & Wood-Harper, A. T. 2009. A critical perspective on action research as a method for information systems research. *Journal of Information Technology*, *11*(3), 235-246.

Birman, K. P. 2007. *Building secure and reliable network applications* (pp. 15-28). Springer Berlin Heidelberg.

Brancheau, J. C., & Wetherbe, J. C. 2011. Key issues in information systems management. *MIS quarterly*, 23-45.

Collmann, J., & Cooper, T. 2007. Breaching the security of the Kaiser Permanente Internet patient portal: the organisational foundations of information security. *Journal of the American Medical Informatics Association*, *14*(2), 239-243.

Dembe, A. E., & Boden, L. I. 2000. Moral hazard: a question of morality?. *New Solutions, 10*(3), 257-280.

Dhillon, G., & Backhouse, J. 2001. Current directions in IS security research: towards socio-organisational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Haley, C. 2011. "Security Requirements Engineering: A Framework for Representation and Analysis," *IEEE Trans Softw Eng,* 34 no. 2, pp. 133-153.

Mather, T. 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* O'Reilly Media, California.

Miller, G. J., & Whitford, A. B. 2007. The principal's moral hazard: Constraints on the use of incentives in hierarchy. *Journal of Public Administration Research and Theory*, *17*(2), 213-233.

Sindre, G. 2005, “Eliciting Security Requirements with Misuse Cases,” *Requirements Eng,* 19 no. 3, pp. 34-44.

Siponen, M. T. 2000. A conceptual foundation for organisational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Subashini, S., & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Bibliography

CISCO, 2008, *Data Leakage Worldwide: The Effectiveness of Security Policies*. CISCO Systems

Dalal, S. &Chhillar, R. S. 2012, “Case Studies of Most Common and Severe Types of Software System Failure”, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 8, pp. 341-347

Ellis, R. 2014, “Lawsuit says Sony Pictures should have expected security breach”, *CNN*. Available from http://www.cnn.com/2014/12/20/us/sony-pictures-lawsuits/

Herath, T. & Rao, H.R. 2009, "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, vol. 18, no. 2, pp. 106-125

Shore, J. 2004, “Continuous Design”, *IEEE Software*. Available from http://www.martinfowler.com/ieeeSoftware/continuousDesign.pdf

Smith, A.D. 2014, "E-security issues and policy development in an information-sharing and networked environment", *Aslib Proceedings,* vol. 56, no. 5, pp. 272-285

Waldo, J. 2006, *On System Design*. Portland, Oregon: Sun Microsystem

Yayla, A. A. & Hu, Q. 2011, “The impact of information security event on the stock value of firms: the effect of contingency factors”, *Journal of Information Technology,* vol. 26, pp. 60-77

Appendices

Appendix A - Terms of Reference

If I were to describe my project in one (long) sentence, it would be to find the reasons as to why secure systems fail in organisations with examples of where and when this occurred and what we can learn from our failures and how to improve for future management and development.

This leads to many questions which needs answering such as, how can lack of incentives in organisations cause securities to fail? How can managers learn from their mistakes? How can we make people care about bugs and vulnerabilities? Why can designs (waterfall, spiral evolution) fail?

The reason I’m undertaking this project is because not a lot of attention has been given to this field and there is potential to unearth a productive area of research. This can be used by organisations that are developing systems, software and creating projects that can learn to minimise security breaches and not make the same mistakes repeatedly.

My aims are to analyse how security goes wrong when inadequate decisions are made or where people from different fields are tasked with making a product – programmers, testers, designers and managers for example will have different approaches and may not be able to speak in the same language and understand each other (Behavioural psychology and moral hazards)

Analyse the monetary cost of improving security and how it affects the workforce's morale. The trade-off between risk and reward, is it worth doing? Sometimes it may not be worthwhile to fix vulnerabilities especially if security is already tight enough. Maybe explore how we can focus alternatively.

Compare and collect case histories of previous security failures caused by lack of incentives in organisations. And to learn from these mistakes, see why and where things go wrong and how to foresee a problem before it occurs.

List of Objectives:

1.) Understand security policies created from an organisations risk management mechanism and make a decision on whether organisations tend to be more risk averse or uncertainty averse.
2.) Understand why people make the decisions they do and how it affects security as a whole.
3.) Understand how system designs and projects can fail
4.) Understand the definition and causes of moral hazards and how it affect the incentives of people which then give rise to security issues.
5.) Compile and critically analyse a collection of case histories of previous security failures within organisations.

The resources ill need to make my project possible would be case studies and reports regarding organisations and their various security problems. Such as, LJ Heath, *'An Analysis of the Systemic Security Weaknesses of the US Navy Fleet Broadcasting System 1967-1974 as exploited by CWO John Walker'* J McGroddy, HS Lin, '*A review of the FBI's Trilogy Information Technology Modernization Program,'* and Microsoft Word so I can document my findings.

Key References:

Anderson R, '*Security Engineering a Guide to Building Dependable Distributed Systems' (2011, pages 815 – 855*

Appendix B – Ethics Check Form

Project and Applicant Details

Name of applicant (Principal Investigator):	Hamad Mully

Telephone Number:	07446809911
Email address:	zanoor@live.co.uk
Status:	Undergraduate Student
Department/School/Other Unit:	School of Computing
Programme of study (if applicable):	Computer Science
Name of supervisor (if applicable):	Yanlong Zhang
Project Title:	Reasons Why Secure Systems Fail in Organisations
Does the project require NHS Trust approval?	NO

Ethics Checklist (Please answer each question by ticking the appropriate box)

	Yes	**No**	**N/A**
1. Will the study involve recruitment of patients or staff through the NHS, or involve NHS resources?		✓	
2. Does the study involve participants who are particularly vulnerable or unable to give informed consent (e.g. children, people with learning disabilities, your own students)?		✓	
3. Will the study require the co-operation of a gatekeeper for initial access to the groups or individuals to be recruited (e.g. students at school, members of self-help group, nursing home residents)?		✓	
4. Will the study involve the use of participants' images or sensitive data (e.g. participants personal details stored electronically, image capture techniques)?		✓	
5. Will the study involve discussion of sensitive topics (e.g. sexual activity, drug use)?		✓	
6. Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?		✓	
7. Will blood or tissue samples be obtained from participants?		✓	
8. Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?		✓	
9. Is pain or more than mild discomfort likely to result from the study?		✓	
10. Will the study involve prolonged or repetitive testing?		✓	
	Yes	**No**	**N/A**

11. Will it be necessary for participants to take part in the study without their knowledge and informed consent at the time (e.g. covert observation of people in non-public places)?		✓	
12. Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?			✓
13. Is there any possible risk to the researcher (e.g. working alone with participants, interviewing in secluded or dangerous)?		✓	
14. Has appropriate assessment of risk been undertaken in relation to this project?			✓
15. Does any relationship exist between the researcher(s) and the participant(s), other than that required by the activities associated with the project (e.g., fellow students, staff, etc)?		✓	
16. Faculty specific question, e.g., will the study sample group exceed the minimum effective size?		✓	

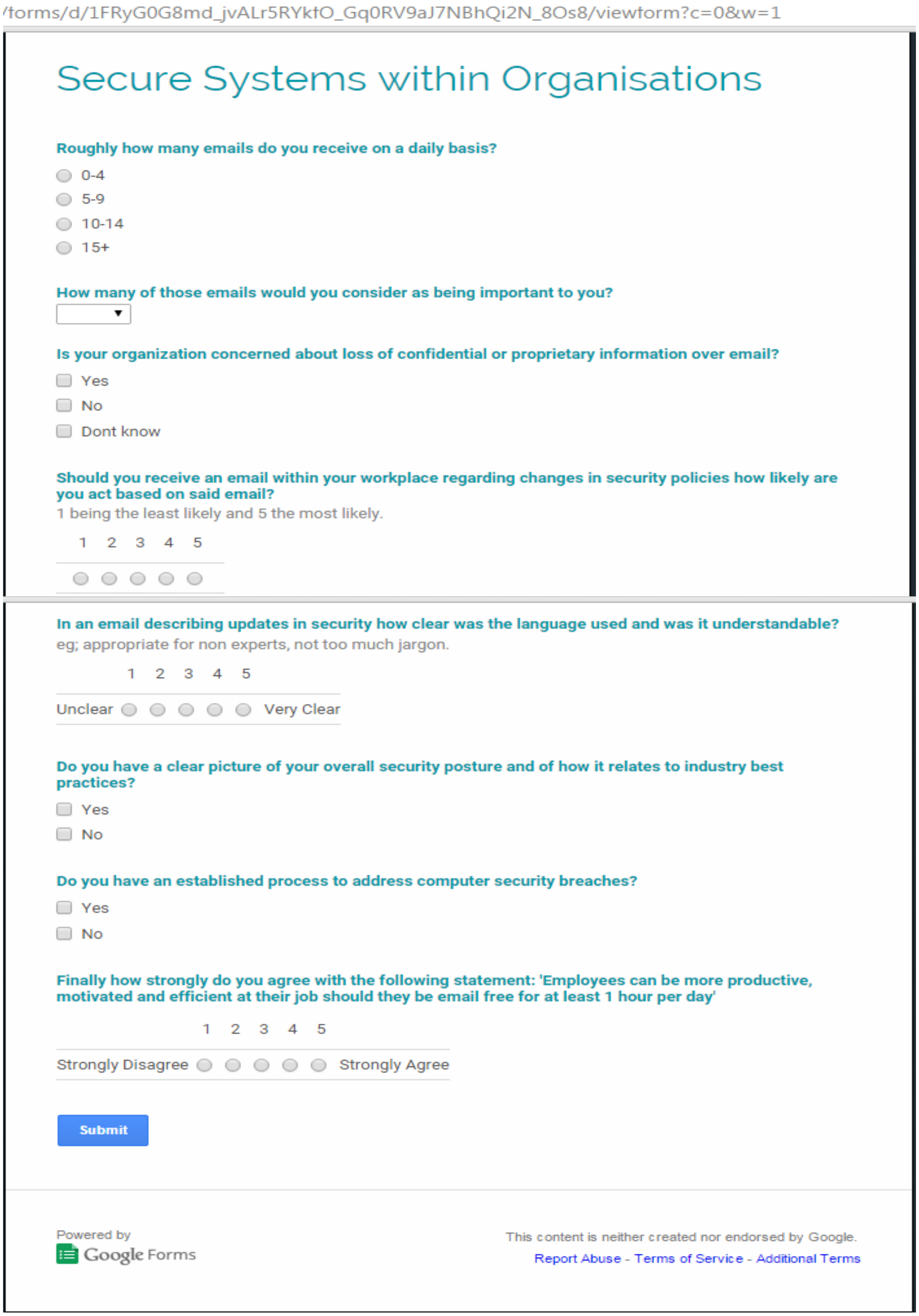
Approval for the above named proposal is granted

I confirm that there are no ethical issues requiring further consideration. *(Any subsequent changes to the nature of the project will require a review of the ethical consideration(s).)*

Signature of Supervisor (for students), or Manager (for staff): ___________________________________

Date: _______________

Appendix C – Questionnaire



/forms/d/1FRyG0G8md_jvALr5RYkfO_Gq0RV9aJ7NBhQi2N_8Os8/viewform?c=0&w=1

Secure Systems within Organisations

Roughly how many emails do you receive on a daily basis?

○ 0-4
○ 5-9
○ 10-14
○ 15+

How many of those emails would you consider as being important to you?

▾

Is your organization concerned about loss of confidential or proprietary information over email?

□ Yes
□ No
□ Dont know

Should you receive an email within your workplace regarding changes in security policies how likely are you act based on said email?

1 being the least likely and 5 the most likely.

1	2	3	4	5
○	○	○	○	○

In an email describing updates in security how clear was the language used and was it understandable?

eg; appropriate for non experts, not too much jargon.

	1	2	3	4	5	
Unclear	○	○	○	○	○	Very Clear

Do you have a clear picture of your overall security posture and of how it relates to industry best practices?

□ Yes
□ No

Do you have an established process to address computer security breaches?

□ Yes
□ No

Finally how strongly do you agree with the following statement: 'Employees can be more productive, motivated and efficient at their job should they be email free for at least 1 hour per day'

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree