BALANCING RISK APPETITE AND RISK ATTITUDE IN REQUIREMENTS: A FRAMEWORK FOR USER LIBERATION

Daniel G Dresner
Visiting Academic, School of Computer Science,
University of Manchester, Manchester, M13 9PL.
Email: daniel.dresner@manchester.ac.uk

Joy E Garfield
Worcester Business School, University of Worcester,
Worcester, WR1 3AS.
Email: j.garfield@worc.ac.uk

Abstract

The tendency to throw controls at perceived and real system vulnerabilities, coupled with the likelihood of these controls being technical in nature, has the propensity to favour security over usability. However there is little evidence of increased assurance and it could encourage work stoppages or deviations that keep honest users from engaging with the system. The conflicting balance of trust and controls, and the challenge of turning that balance into clear requirements, creates an environment that alienates users and feeds the paranoia of actors who assume more ownership of the system than necessary. Security therefore becomes an inhibitor rather than an enabler for the community. This paper looks at measuring the balance of an organisation's or a community's risk appetite with the risk attitudes of its members in the early stages of IS development. It suggests how the dials of assurance can be influenced by the levers of good systems practice to create a cultural shift to trusting the users.

Keywords: Security, risk, requirements, trust, non-functional.

1.0 Introduction

The importance of secure systems is increasing with the broad range of technological advancements within every domain of human society (Dubois and Mouratidis, 2010) not least with the developing ubiquity and pervasiveness of the Internet of Things (O'Neill, 2014). As the sophistication of security threats continues to evolve, organisations must take steps toward preventing the losses from these threats (John, 2000).

The increase in technology-driven services is matched by an increasingly diverse range of stakeholders in the systems that provide or are involved with those services (Alexander, 2007). Security always assumes some degree of trust in its mechanisms (Dubois and Mouratidis, 2010). Trust is a state of positive expectation that one's vulnerabilities will not be exploited (Riegelsberger, Sasse, and McCarthy, 2005). So, in an attempt to engender the desired trust, all software-based systems have to compensate for an environment over which the law of requisite variety (Ashby, 1957) will allow them little control. The various elements that must struggle for the control of the system within the environment – stakeholders, users, relevant laws and regulations – will influence the security aspects of the system (Islam, Mouratidis, and Jürjens, 2011). Security requirements analysis and security-related decision making requiring the analysis of personal and organisational goals of the stakeholders participating in the system due to the subjective nature of security are important (Elahi et al., 2010). The challenge for those who develop or change information systems is that stakeholders have conflicting requirements with respect to the assets that comprise the system (Fabian et al., 2010).

In this study we have considered: (a) how the vagaries of the risk attitude (Hillson and Murray-Webster, 2007) can be translated into programmable security requirements; (b) how to balance the security requirements with risk appetite of the organisation as represented by the security controls it embraces (ISO/IEC 27001, 2013); and (c) how the balance of risk appetite and attitude can be measured and assured.

Systems that trade security for ease of use are likely to be used incorrectly resulting in security risk which may include wilful circumvention (Beckles, B et al., 2005). In this paper we look at the early stages of development and discuss the good, the bad, and the ugly in the problem space of building security into an information system so that it does not stand out as a feature whilst the system is in use (Bevan, 1995) and then carry this through to test the method with users. We suggest that this practice is a critical success factor to enable the usability of a system at its simplest and to encourage acceptable use of the system at its best.

If security is implemented well then it will be invisible to the users. However if it is implemented badly then security controls are in place but their implementation makes for inelegant use of the system, and in the worst case scenario poor consideration of security in the realisation of requirements can lead to anguish where users create their own workarounds and data migrates to the unintentional information system.

We shall suggest that the challenge of articulating security requirements may be met by enabling secure systems operation through a framework for user liberation, and conclude with an assessment of examples where it would appear that by accident or by design, the mechanisms to achieve security objectives through the system in use have been successful.

2.0 The problem space: unintentional information systems

There is a challenge to find those who do not pay sufficient attention to risk and the very *human* nature of losing their sense of emotional literacy in an effort to achieve personal goals or just to get the job done (Hillson and Murray-Webster, 2007). We have articulated this in our research questions (*see 1.0 Introduction above*). Ignoring risk may have no malicious intent but it may have significant consequences well beyond the immediate environment of the individual. Even shocks that can trigger appropriate emotions at one time may be relatively short lasting. For example, would-be Liverpool football club spectators who wanted to break into the Champions League final against AC Milan (23 May 2007) (McNulty, 2007) where a lack of available tickets had led to their exclusion from the ground. The emotions governing their desire to see the game overcame their appreciation of what had happened at a match between Liverpool and Nottingham Forest when 96 people died after supporters tried to enter an already overcrowded stadium (15 April 1989) (BBC News, 2009). The challenge is to maintain an awareness of the risks to many when individuals distance themselves from the consequences of their actions. Information systems not only need to provide opportunity to share and transform information but also need to remind users of the outcomes of their actions of using the system. For example, what consideration do people give to the consequences of publishing holiday photographs or personal information on a ‘Web 2.0’ social network (House of Lords, 2007) and how much thought does a user give to continuing e-mail correspondence using the ‘Reply-to-All’ function? At the other extreme, how many are prevented from making decisions or taking actions which would be unlikely to lead to a risk being realised? There is a tendency for overcompensating day-to-day; to be become obsessed with the high impact, low probability risk. For a comprehensive approach, sensitivity to the weltanschauung of each user is required as it could be said that risk is in the eye of the beholder.

The term ‘unintentional information systems’ was coined by Professor Bob Wood (Dresner, 2011) to describe the movement of data from the intended places of processing, transit, and storage to places where that data should not be. The data is handled by people outside the information system that was designed for it by legitimate users who want to do things their way, or by nefarious ‘users’ who have their own objectives – the system ‘misuse’ case.

Human factors are still not sufficiently addressed in the process of engineering secure software systems (Faily and Flechais, 2010). It is important to ground usability decisions in information gathered about real people, potentially including them in the design process (ibid.). Security lock-down should not result in security lock out. There should be no expectations that the user will apply much thought process to the reasons for having to navigate security controls when they stand between a risk – however calculated and however likely – and getting a job done. The calamity occurs when the workaround damages the workflow resulting in stunted operations or worse – a failure to operate. The intentional, designed system is no longer able to protect data and any capability in the system for self-preservation (business continuity) is moot.

This work is needed to improve security by default without which there will be active failures through both technical and social vulnerabilities (Flechais, Sasse, and Hailes. 2003) As well as designing for the people who will use them, secure systems also need to be designed for the environment they will be used in. Delivering security for the user means a balance of human factors with security requirements so that an acceptable level of risk is maintained.

3.0 Literature review

3.1 The challenge of articulating non-functional requirements

Information system acquisition, development, and maintenance needs to have a complete and consistent set of security requirements – within itself and with relation to the other requirements for the system (Fabian et al., 2010).

Although many factors contribute to information system failures, the concentration and emphasis on the early phases of development holds particular significance. Every system of consequence needs good requirements (Orr, 2004). Without knowing the requirements of customers and users it is difficult to build the right product (Kauppinen, 2005) and without good requirements, project risks, such as costs, schedules and performance, increase dramatically (Orr, 2004). In spite of many research efforts and the development of a range of Requirements Engineering (RE) techniques for a system's functionality, system failures still continue to be attributed to, among other factors, requirements issues.

Crosby's Quality Management Grid (Crosby, 1979) shows the cost of quality, based on removing defects. The sooner the defects are removed in the life cycle, the reduced cost of removal, and the increased maturity of the organisation required to achieve this. Security flaws may be expressed as quality defects. Security is a non-functional requirement or a primary system/software quality characteristic (BS ISO/IEC 25010, 2011) so information security vulnerabilities and breaches are manifestations of quality defects and can therefore be evaluated using Crosby's grid.

The most challenging projects often involve multiple stakeholders from differing organisations, subcontractors, divisions, etc., who may have a diversity of expertise, come from different organisational cultures and frequently have competing goals. When requirements are based on information gained from users or customers, there is a link to project success and a lower proportion of Requirements Engineering in the project costs (Kujala et al., 2005). However since people involved in RE processes (Alexander, 2007) have various roles (for example, user representative, system developer, maintenance staff, financial officer), together with different skills and knowledge, each has his or her own understanding of the system to be built or changed (Pohl, 1994; Krogstie and Solvberg, 2003). And there is a risk of losing sight of the security requirements when an incomplete set of users are consulted (Carr, Konda et al., 1993).

Typically requirements stem from two main sources, namely user-defined - usage world – and domain-imposed – subject world (Jarke and Pohl, 1993; Rolland and Prakash, 2000).

Security requirements are consequences of threats to the system (Fabian et al., 2010). A threat is posed by someone – who may be a counter-stakeholder – or something that threatens something that stakeholder values (ibid). Conflicting stakeholder views introduce the challenge of conflicting requirements. All views must be considered to synthesise a consistent set of system requirements. A process of reconciliation and compromise is needed to effect this to a level of acceptable risk to all stakeholders and ultimately the system owner.

The user can be locked out by security, either literally or psychologically. This can result in stunted operations and system operational failure. This threatens the ability to protect data and the ability for self-preservation in a state of business continuity. However security risk countermeasures are necessary to allow an information system to protect, operate and self-preserve. Therefore human factors need to be balanced with security requirements. We shall show how the barometer of success can be shown in a heat map (see Figure 3).

People who specify requirements for products or services that store and process information may find that the association of certain words can either inhibit or enable specifications that require interpretation to move from intention to realisation. Stating that an information system must be, for example, 'secure' may result in the implementation of hardware, software, and processes which restrict access to such an extent that users – with no malicious intention – work around the security constraints and inject information into unintentional information systems or, conversely fail to realise the possible protection with safe outcomes. Security is a state. It is affected by the realisation of risks to that state. Management of risk in the context of information security and cyber security is attributed to the application of controls which may vary from anywhere between 4 or 35 (Australia, 2012) and 20 critical controls (SANS, 2013) to 135 (ISO/IEC 27002) and many more (NIST 2013, HIPAA 1996, PCI DSS 2010). The standards that set out these controls do little to separate out clear risk management processes and the feedback they require to adjust the state of security within acceptable boundaries that match risk appetite. A requirements specification is challenged with being detailed enough to represent complexity whilst being simple enough to be unambiguous and understandable and not attenuating the description of the information system it models. It risks (sic!) creating requirements for controls whose combined complexity dampens the ability to manage quality attributes such as security.

The challenge is how much can we dare to tamper with the constraint of security locks to free the user and how do we turn the security controls into non-functional requirements meeting obligations of protection and system objectives simultaneously. This is the risk and requirements conundrum that we address in this paper. We do this by proposing a framework (Figure 2) for user liberation that may reduce the risk of security incidents and increase the risk of successful operations. The term ‘risk’ is used to mean both negative and positive possibilities throughout this paper to divorce the usual association where risk management is defined in terms of negative connotations.

3.2 Security: the good, the bad and the ugly

Poor security has been said to be worse than no security (Townsend, 2000) because it is false security. However, we propose that at least some security is better than none providing that it doesn’t eschew reliance.

Any measure of security is transient and requires periodic – if not frequent – re-evaluation. The information that users are provided with needs to be understandable. The temptation to label users as ‘the weakest link’ (Sasse, Brostoff, and Weirich 2001) should not lead to a belief that user education will be a panacea (Ranum, 2005). It should however be used to suggest that careful elicitation of user-oriented requirements may be applied to treat the risks from the detected human vulnerabilities. These treatments may include user education but only from the perspective that any education will only be effective if users believe in the risk (Sasse, 2003), and cost effective, secure systems design (Flechais, Sasse, and Hailes, 2003) which sets policies and targets to assure risk management within the context of the software in use (the policies and targets being the regulators of the protection of information in the system). The software needs to believe in the risk on behalf of the users. Reworking the software will be desirable but is unlikely to have the speed of return that is needed – standards beyond those for good development practices will be required, as well as enticing the implementation of the good practices which are already known.

The obligation is on the system designers to develop systems that enable the fulfilment of objectives. Security controls need to be unobtrusive to the honest user but not to those that would seek to damage the system.

3.3 Quality and security engineering in software

Although there are a number of security Requirements Engineering methods few take into consideration different stakeholder views, attitudes or appetites to risk. Such methods include Security Quality Requirements Engineering Methodology (SQUARE) (Mead et al., 2005); KAOS (van Lamsweerde, 2007); Secure Tropos (Mouratidis and Giorgini, 2007; Masscci and Zannone, 2006); Secure i* (Liu, Yu and Mylopoulos, 2003); Multilateral Security Requirements Analysis (MSRA) (Gurses, Berendt and Santen, 2006). MSRA also proposes steps to address the issue of contradictory security concerns amongst stakeholders where compromises must be made. However MSRA does not cover threats. UML based approaches such as Misuse Cases, Secure UML and UMLsec do not take environmental issues into account. Misuse cases allow early focus on security by describing security threats and then requirements without going into design (Sindre and Opdahl, 2005). Alexander (2002) used misuse cases to successfully determine threats and requirements and subsequent resolution of design conflicts. And Breivik (2002) used misuse cases to represent security threats from the Open Web Application Security Project (OWASP, 2001) in pattern form. However Misuse cases are not equally suitable for all kinds of threats and they could lead to analysis paralysis due to weak method guidelines.

Security requirements were able to be leveraged successfully with usability and cost constraints taken into consideration within SECUR, an RFID-based off-site data storage management system that significantly improves the security of the backup data life cycle (Lopez-Carmona et al., 2010). This was achieved through arranging security controls in a set of ten security tiers, of which the level of security increases with high level tiers. Houmb et al (2010) applied the SecReq approach to elicit security requirements for Internet Protocol Television (IPTV). SecReq, a security standard ISO 14508 Common Criteria driven security requirements elicitation and tracing approach, that also uses a heuristics requirements editor and UMLsec. This made it possible to gain repeatable feedback from core stakeholders throughout the requirements elicitation process.

Elahi et al (2010) proposed a requirements engineering framework to support the elicitation of security requirements based on the effects of vulnerabilities on security requirements. However the framework assumes knowledge of vulnerabilities , potential attacks and countermeasures or that they can obtain such information.

4.0 Designing successful security requirements

Security is a *non-functional* requirement of an information system (BS ISO/IEC 25010, 2011) that must be as clearly defined as the colours, (data-formatting for example) that are usually associated with other *quality attributes*, such as *usability* or *interoperability*. However, words associated with the specification of security are so riddled with their own semiotic baggage that they are either used inappropriately, too often, too little, or not at all. Words such as ‘control’, ‘restrict’, ‘legal’, or even ‘risk’ suggest the red terminology of protection or danger and suggest barriers to the user.

In the specification of information systems that handle data in a way that is commensurate with all reasonable expectations of the impact resulting in compromise to their confidentiality, integrity, or availability, we need a method to build information systems that can be adapted to the risk literacy of both those who specify the information system and those who must apply that specification in development, implementation or use. It is the manifestation of the human behaviour principle of IT governance (BS ISO/IEC 38500, 2008). This would manifest in a method to support the development of secure information systems by reducing the risk of inappropriate data processing and increasing the risk of containing the information in an accurate state and available where it is genuinely needed. Success is when a requirement is identified and the security measures increase the likelihood that requirements will be realised and are not by-passed in use.

Designing is a necessary activity amongst stakeholders when working towards a solution for an information system which is compatible with their needs. Everyone designs who devises courses of action aimed at changing existing situations into preferred ones (Simon, 1969).

Design thinking enables the creation of ideas that better meet consumers' needs and desires, rather than making an already developed idea more attractive (Brown, 2008). It is also often seen as a way of dealing with complex problems in systems development (Saffer, 2005). This enables not only the determination of stakeholders' needs but also the best possible outcome to be ascertained in the balance between business impact (CESG, 2009), and end user contentment (Adams and Sasse, 1999).

5.0 A Framework for user security liberation

5.1 Methodology

The objective of this research was to determine whether the attitudes of individuals to risk may be usefully correlated to the acceptable level of risk that is expected by the 'risk culture' in which they work. Knowing this to be true, and how so, is a foundation for understanding what training, improved awareness, or other mechanisms - namely applying standards as regulators (Beer, 1993) or controls - are needed for changes in risk culture or to maintain a current, appropriate risk culture. This was to be tested by creating a scale of measurement for attitudes to risk. A questionnaire was constructed to determine where on the scale a user should be placed and whether they sit within, or outside, the attitude that is acceptable to the owner of the network. The creation and refinement of the questionnaire and the evaluation of the responses determines the application of the method as a practical tool to evaluate the appropriateness of implemented policies (or standards) for risk management in information systems.

5.2 Profiling the user

The methodology complements the technical and quasi-technical countermeasures deployed for use against well-known outsider threats such as hackers or the malicious software of criminal programmers. Technical measures would include intrusion detection and prevention systems, antivirus or spyware detection and removal programs and firewalls (both hardware and software). Quasi-technical measures comprise a technical implementation which may, for example, use technology to distract a criminal from gaining inappropriate access to a computer network such as a honeypot which may imitate a legitimate network or part of a network with otherwise redundant information stored thereon. The common characteristics were isolated and are represented by the formula in **Figure 1** which is explained below:

System Vulnerability at the point of use = **Environmental circumstances + Personal circumstance + Path(s) + ICT literacy + Risk literacy + Emotional literacy**

Where

Risk Literacy = **Knowledge of risk + Knowledge of treatment + Willingness to deploy treatment**

Figure 1. Profiling the user in an information system

The context in which a type of person or organisational role is assessed for being a human vulnerability has the two aspects of environmental circumstances of where they use information systems (often a workplace), and a set of personal circumstances or profile. The environmental circumstances were considered in the questions (and the rules designed to evaluate the results) by taking into account the environment and context in which an individual is operating. The method recognises that where a user engages with a network, the context of use will depend on the profile of the user in terms of their ICT skills, the tasks that the user expects, or is expected, to achieve, the equipment such as hardware or software that gives the user access, the physical and social environments in which engagement takes place, and the stability of the organisation in terms of its existence or propensity for change. For example, appropriate risk taking for a private individual accessing personal e-mail with a mobile device is not likely to be appropriate for another user engaging with a network managing a safety-critical SCADA system. However, common areas that would secure the use of both would appear in the attitude tests for all users.

The presence or absence of expected security measures and the propensity for users to show emotional intelligence in the face of risk were allocated scores to rank the quality of the security controls and the reaction to everyday threats. This created a weighted ranking method that allowed quantitative representation of essentially qualitative measures. Part of the inherent challenge of collecting information for this type of analysis is in the accuracy of the responses and hence the quality of information collected. *Table 1. Options for investigation*, shows how segregating the respondents considered the quality of information by providing some independent judgement. This table considers who can offer the best answers to questions about the organisation with the research objective of eliminating bias in the responses. This control is centred on having someone profile the respondent to the questionnaire first. This improves quality of the analysis of the responses based on the assumptions (that is, acceptable risk) that the supervisor and the individual will not collude, or that the response should not be an opportunity to transfer risk from supervisor to individual. Again, quality assurance would expect the supervisor to undergo the same scrutiny (Quis custodiet ipsos custodes – Who will keep watch over the guardians?).

Options	Questions answered by:			Relative quality of data expected 1 = low 5 = high.
	(a) Questions about the Organisation	**(b) Questions about general network users/ stakeholders**	**(c) Questions about specific individual(s)**	
1	Supervisor/ Security or Risk officer	Supervisor/ Security or Risk officer	N/A	**2**
2	Supervisor/ Security or Risk officer	N/A	Supervisor/ Security or Risk officer	**3**
3	Supervisor/ Security or Risk officer	N/A	Specific individual	**4**
4	Supervisor/ Security or Risk officer	N/A	Profile information by the Supervisor, Security or Risk officer; Purely risk attitude questions by the specific individual	**5**

Table 1. Options for investigation

5.3 The liberating route map

Figure 1 shows the proposed User Liberation Framework. This framework comprises the key components of a process to elicit and manage the security requirements that can be reflected in a system's security controls. These controls would be sensitive to the attitude of the users who are responsible for handling information and are to be built into the system (Bryant, 2013) to assure the steering of the information with the boundaries necessary to achieve the business objectives for which the system was intended. The organisation's risk appetite would be assessed using the active security control metrics, followed by assessment of individuals' risk attitude using reactions to scenarios relevant to the organisation. A comparison of the risk appetite to risk attitude would produce a value to be used in the heat map (Figure 3) and inform iterations of security requirements. It is particularly pertinent to consider both organisational and stakeholder influences on requirements, as Chmura and Crockett (1995) note that when defining functional and non-functional requirements individuals often consider only their personal requirements, without thinking about the company's overall goals.

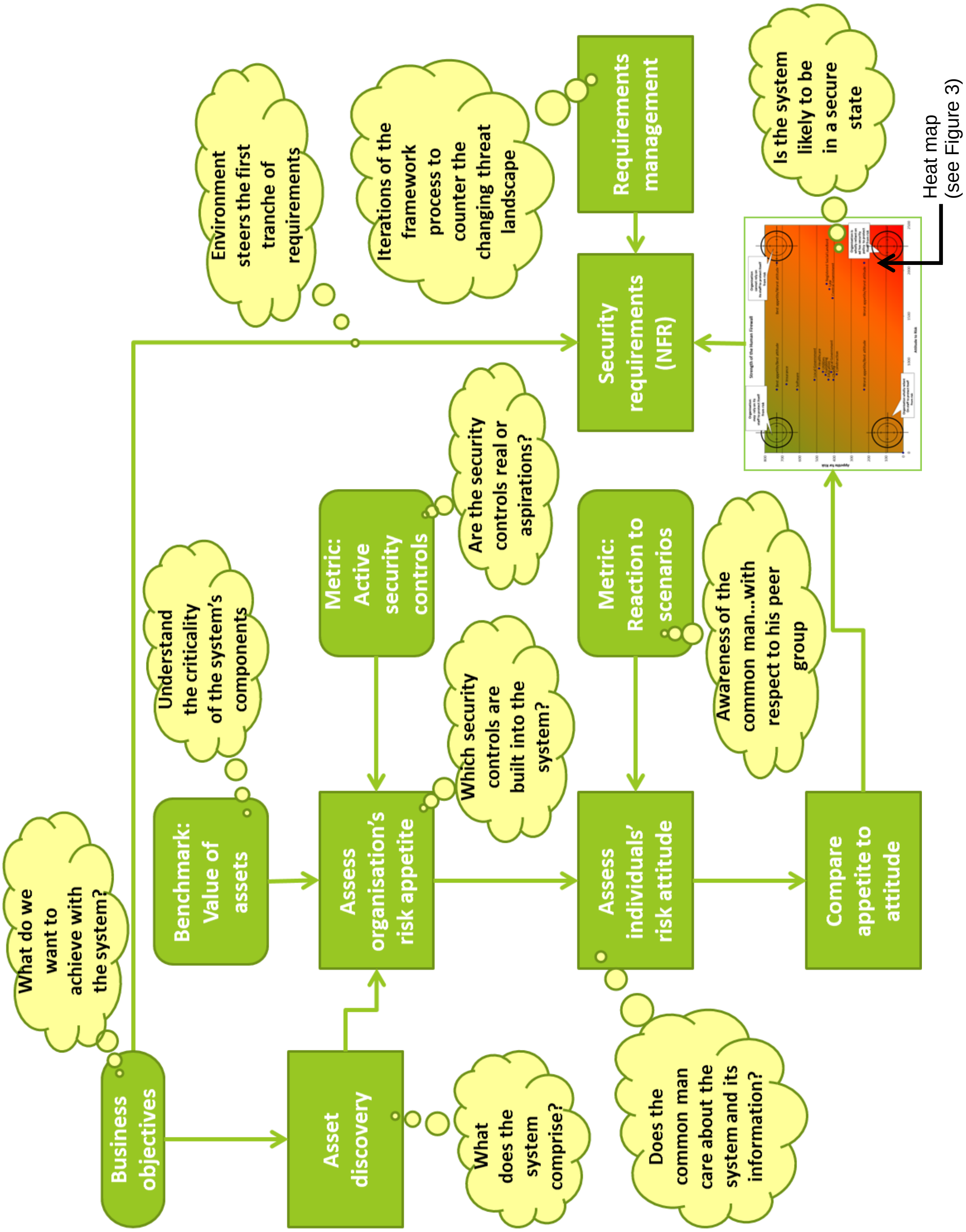
Business objectives
What do we want to achieve with the system?
Asset discovery
What does the system comprise?
Benchmark: Value of assets
Understand the criticality of the system's components
Assess organisation's risk appetite
Metric: Active security controls
Are the security controls real or aspirations?
Which security controls are built into the system?
Environment steers the first tranche of requirements
Iterations of the framework process to counter the changing threat landscape
Requirements management
Security requirements (NFR)
Assess individuals' risk attitude
Does the common man care about the system and its information?
Metric: Reaction to scenarios
Awareness of the common man...with respect to his peer group
Compare appetite to attitude
Is the system likely to be in a secure state
Heat map (see Figure 3)

Figure 2. User Liberation Framework

Key to all information security management is the understanding of the target of protection (BS ISO/IEC 27001:2013) and if not already know, the entry point for the framework is asset discovery to enable considered and appropriate controls to be selected rather than creating overly complex control matrices to protect items that are no longer important or do not exist. The axes on the heat map are created by establishing as series of questions that establish the relative measure of the organisations attitude to risk (Y axis) as benchmarked by the degree to which the organisation has adopted identified controls from the risk-based information security standard ISO/IEC 27001. This is plotted against a weighted ranking of an individual's attitude to risk (X axis). So, questions are asked to discover (for example) whether information risk is regularly addressed in projects, operations/IT service delivery, and at board level, whether staff may use their own IT equipment for business use (PCs, telephones, PDAs, USB sticks/pen drives). These questions are designed to paint a risk landscape to understand if the environment that the users are to be found in expose day-to-day, system agnostic risk and does something to protect against the losses that may be caused by their realisation. The stability of the organisation is itself scrutinised with consideration of whether it is undergoing, likely to undergo, or may be rumoured to be undergoing some merger or acquisition or internal reorganisation. Questions look at practices such as the place of screening staff screened for background, qualifications, during selection and during changes of employment and their access to information tailored accordingly. This considers the arrangements that change unskilled users to skilled individuals who may be expected to manage some risk as an instinctive reaction. This is balanced with the question as to whether staff have their work monitored for accuracy for a period until competency through experience is assured or other validation mechanism is deemed sufficient. The effect of the user on the reference architecture is considered by asking if alterations to how company equipment is set up can only be done through qualified staff.

The richness of the security environment is weighted by the answer format which ranks answers as describing a better quality of environment for working securely on the assumption that the best security control is not only implemented but that it should also be documented, communicated, and audited. The worst case is where there is no policy to say whether a control is used or not.

Attitudes to risk are measured by a similar system of representing responses as to the level of concern that the interviewee shows for good and bad information security practices – a combination of risk and emotional literacy. Whether or not the user tends towards the high-risk profile is analysed by whether they feel threatened, unfamiliar, uncommitted to, or comfortable with the risk and/or the risk treatment that is present or applied respectively.

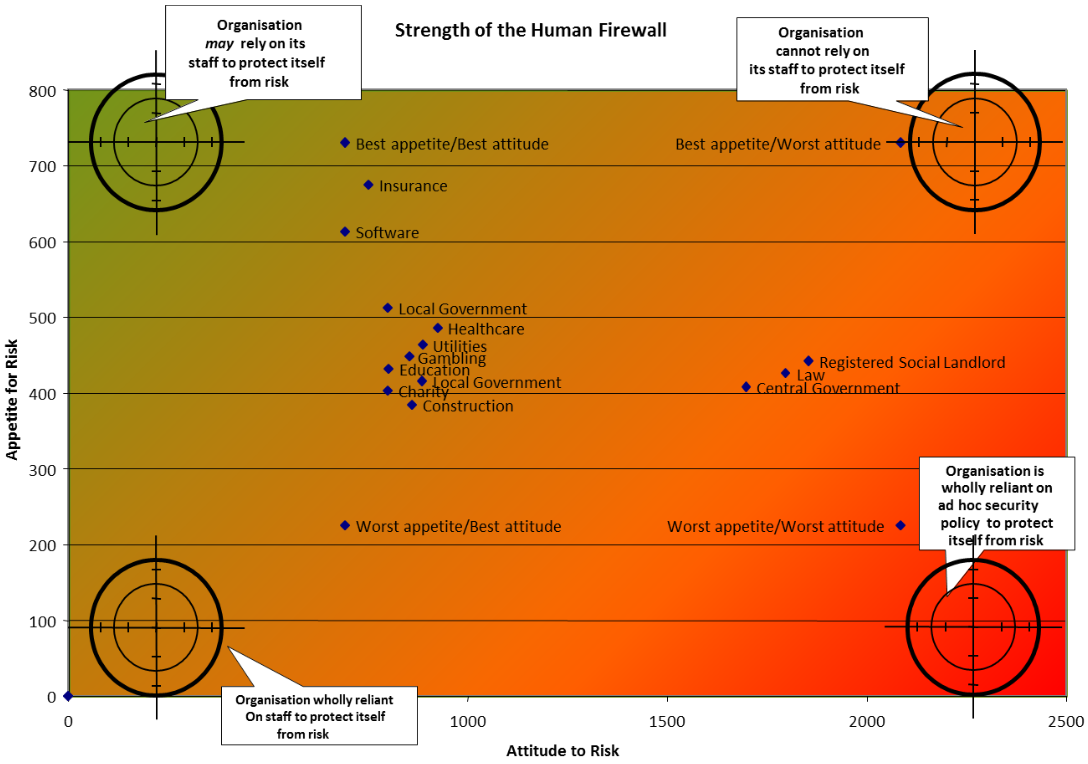

Figure 3. Heat map for showing a balance of human factors with security controls

In the ideal zone (Figure 3) - with low attitude to risk and low appetite for risk values - there is a good balance of implemented and audited security policy with staff attitudes. A low attitude to risk and high appetite for risk may mean that an organisation with weak security may rely on its staff to protect itself from risk. In contrast a high attitude to risk and low appetite to risk indicates that the organisation is wholly reliant on enforced security policy to protect itself from risk. And a high attitude to risk and high appetite for risk indicates that an organisation with weak security cannot rely on its staff to protect itself from risk.

5.4 Utility – deriving requirements from the framework

The heat map is the pivotal tool for deriving requirements that should be built in to the system – as determined by the Trustworthy Software Framework, (Bryant, 2013). It has been designed to recognise that attitudes are harder to change than security policy and so it can be experimented with to adjust the controls of the system (ISO/IEC 27001 and ISO/IEC 27002, 2013) to bring the information systems plotted exposure to risk into an acceptable zone on the heat map. The controls can be defined as system requirements and managed through the acquisition process.

The more sensitive problem of the attitude of the user can be tackled by awareness education which can be benchmarked for progress using the attitude questions that are used to plot the people component of the heat map.

This was tested by investigating the development environment of the IT department of a County Constabulary. The department comprises system designers, implementers, support and maintenance staff, and management and administration. The department is responsible systems that handling information classified to Business Impact Level 3 (defined as confidential according to HMG Infosec Standard No. 1, CESG, 2009). The education programme that offered the opportunity to validate the security awareness benchmarking was requested by the organisation's information security officer so that he could discharge its obligations under government requirements for mandatory information assurance training. Information assurance is defined by CESG as 'the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users'. The training was designed specifically for the IT department. This realised the responsibility of system developers to manage requirements and create systems where usability would not be compromised by the poor design of the security controls (Flechais, Sasse, Hailes, 2003). Each session comprised a presentation with an exercise to test the risk awareness of the staff. It is worthwhile noting that the IT department agreed to the training under sufferance as it was not seen to be a priority.

In several training sessions the questions measuring risk attitude were completed at the start and end of the session and benchmarked against the original answers. The results were used to see if the training had improved the attitude of those attending by increasing their awareness of risk and what was considered as acceptable treatments for those risks.

The IT department comprised 83 staff who were involved with the development, support, and maintenance of information and communication systems for the organisation, and administrative support for the department. The staff attended the training sessions in groups of 12 or less with little or no knowledge of why they were required to attend. Each session started with an explanation followed by a review of their information security attitude. This was taken with the risk appetite measure for the organisation which had been calculated by interviewing the information security officer using the questions about the organisation's status, and the content and quality of deployment of the organisation's information risk management policies. His responses were added to the spreadsheet, leaving the questions about the local attitude to risk to be asked during training sessions with the IT department. This plot was made with the version of the questions used by the in-depth questionnaire so that the trainees could not only see where they were placed in relation to themselves before and after the training but also with respect to other organisations. An example from one session is shown in Figure 4. The objective was to show the collective risk attitude of each group.

The training session for each group contained material to educate attendees in the basics of information assurance, teach them how to apply proportionate treatments to information risk, and help them appreciate the stakeholders who will make risk treatment effective. This was exercised with a fictional case study about handling sensitive information to which the controls of BS ISO/IEC 27002 (2005) had to be applied to link risks with policies and countermeasures.

5.5 Measuring the attitude of the user

Seven sessions were run which included most of the department in the training. As the programme was run, it became more and more challenging to deliver the sessions with some of those attending being distracted by their perception that the training was a low priority in relation to their day-to-day responsibilities. Priority was given to delivering the presentation material and encouraging participation in discussion and the risk treatment exercise. Only three of the seven sessions completed the benchmarking exercise. The results are shown in Table 2.

		Session 1	**Session 2**	**Session 3**
	Appetite Score	**Attitude Score**	**Appetite Score**	**Attitude Score**
Training session: first measure	301	324	486	287
Central Government	424	1698	1698	1698
Construction	396	861	861	861
Law	426	1797	1797	1797
Registered Social Landlord	442	1854	1854	1854
Local Government	434	886	886	886
Insurance	675	752	752	752
Education	432	803	803	803
Software	613	694	694	694
Utilities	463	886	886	886
Gambling	460	848	848	848
Local Government	512	800	800	800
Charity	403	800	800	800
Healthcare	473	925	925	925
Training session: second measure	301	209	137	137

Table 2. Before and after training – measures of risk attitude

5.6 Analysis of the results

In all sessions, the coordinates of the group under scrutiny were moved further into the heart of the green zone of the chart. Figure 4 shows the improvement measured from the first session. It is worth noting that the organisation scored well from the outset with regard to both risk appetite and risk attitude. This is likely to be because of the nature of the organisation's work which require it to habitually regard security as important as part of its business which often requires it to enforce security for others. This is further exemplified by the existence of the full time information security officer and the mandate for the information security awareness training.

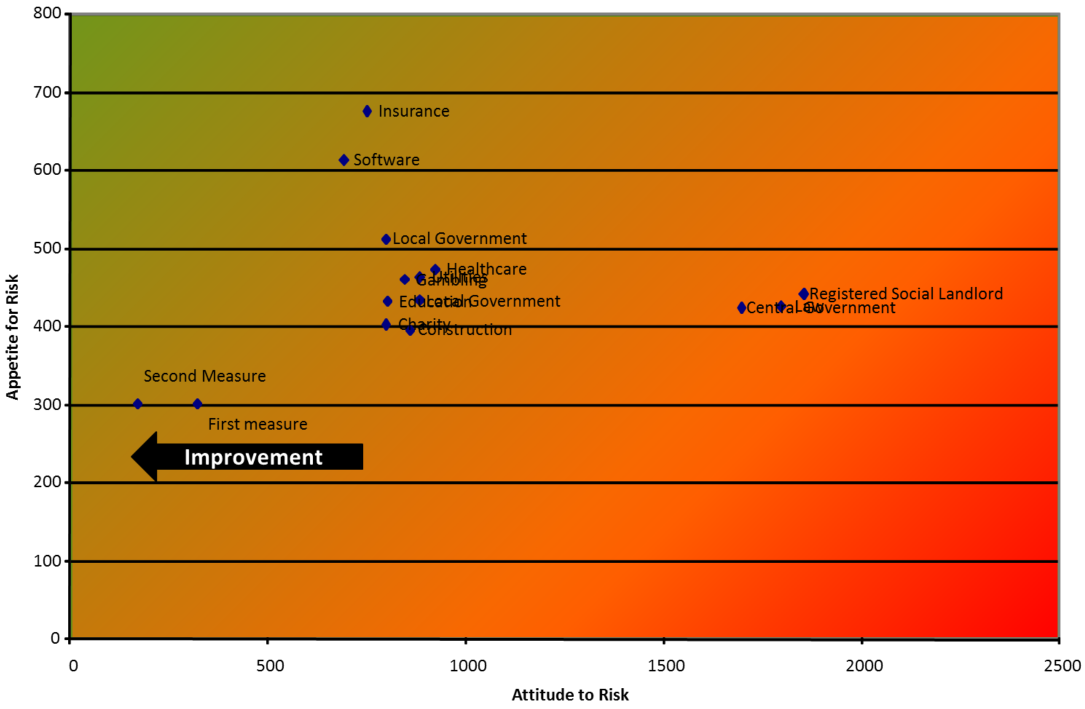

Figure 4. Improvement in risk and treatment awareness measured in the first session of training

6.0 Conclusions and future work

There is a clear need for a solid foundation to be established for information systems development, as an important detail missed at an early stage can lead to large problems later in development. The User Liberation Framework (Figure 2) presented in this paper focuses on the early stages of IS development and attempts to measure the balance of an organisation or community's risk appetite with the risk attitudes of its members.

Research tends to concentrate on what is required in terms of system security from an organisational perspective rather than focusing on the human usability aspect, showing the causal links between security breaches and people's behaviour and the system. There also tends to be a gap between organisational expectations and user actions and technical capabilities. For example research by Mannan and van Oorschot, (2007) highlighted the emerging gap between banks' expectations and users' actions related to security requirements of online banking.

In this study we have shown: the opportunity provided by modelling the human vulnerabilities in information systems to synthesise programmable security requirements (a), how the realisation of those requirements can be used to check the balance of security requirements with risk appetite of the organisation as represented by the security controls it embraces (b), and how the balance of risk appetite and attitude can be measured and assured by representing them on a heat map (c).

Supporting research around the language of risk is still needed to support the promulgation of a tool for detecting human vulnerabilities in information systems. Are the terms *risk attitude* and *risk appetite* sufficiently defined and understood? How does one describe appetite which may vary from one organisation to another, yet be good enough for each depending on the risk treatments deployed and the respective residual risk that remains? Some of this is addressed in the model for connecting organisations with a standards-based approach (Dresner and Wood, 2007). The term *good* is used here to describe individuals who appreciate their responsibilities to manage a degree of risk and whose awareness encompasses the organisational measures in place to allow risk-managed access to the information system.

References

Adams, A, and Sasse, M. A, (1999) Users are not the enemy, *Communications of the ACM CACM*, 42(12), 40-46.

Alexander, I.F. (2002) *Initial Industrial Experience of Misuse Cases in Trade-off Analysis*, In Proceedings of the 10th Anniversary IEEE International Requirements Engineering Conference (RE’02), Essen, Germany.

Alexander, I.F. (2007) *A taxonomy of stakeholders: human roles in system development*, In Stahl, C.B. (Ed) Issues and trends in technology and human interaction, De Montfort University, UK: IRM Press, 25-71.

Ashby, W. R., (1957) *An introduction to cybernetics*, Second Impression, London: Chapman and Hall Limited.

BBC News (2009) *How the Hillsborough disaster Happened* [online] Available from: http://news.bbc.co.uk/1/hi/uk/7992845.stm [Date accessed: 28 January 2014].

Beckles, B. Welch, V., and Basney, J. (2005) Mechanisms for increasing the usability of grid security, International Journal Of Human-computer Studies, 63(1-2), 74-101

Bevan, N. (1995) Measuring usability as quality of use. *Software Quality Journal*, 4, 115-150.

Breivik, G.F. (2002) *Abstract misuse patterns – a new approach to security requirements*. Masters Thesis, Department of Information Science, University of Bergen.

Bryant I, (2013) *Trustworthy Software Framework* (*to be published as BSI PAS 754*) Trustworthy Software Initiative, Cyber security centre, De Montfort University http://www.uk-tsi.org.uk/

Brown, T. (2008) Design thinking. *Harvard Business Review*, 86(6), 1-9.

British Standards Institution, BS ISO/IEC 27002:2005 BS 7799-1 (2005) *Information technology - security techniques - code of practice for information security management*, (Previously ISO/IEC 17799)

British Standards Institution, BS ISO/IEC 25010 (2011) *Systems and software engineering. Systems and software quality requirements and evaluation (SQuaRE).* System and software quality models.

British Standards Institution, BS ISO/IEC 27001 (2013) *Information technology — Security techniques — Information security management systems — Requirements.*

British Standards Institution BS ISO/IEC 38500 (2008) *Corporate governance of information technology.*

Carr, M.J., Konda, S.L., Monarch, I., Ulrich, F.C. and Walker, C.F. (1993) *Taxonomy-based risk identification*, Software Engineering Institute, Carnegie Mellon University.

CESG, (2009) HMG IA Standard No. 1 Technical Risk Assessment, Communications-Electronics Security Group

Chmura, A. and Crockett, H. D. (1995) Tools to align goals and information systems, *IEEE Software,* 12(3), 108-111.

Crosby, P. (1979) *Quality is free: the art of making quality certain,* London: McGraw Hill.

Dresner, D.G. (2011) *A study of standards and the mitigation of risk in information systems*, A Thesis Submitted to The University of Manchester for the Degree of Doctor of Philosophy in the Faculty of Humanities.

Dresner, D.G., and Wood, J.R.G. (2007) *Operational risk: acceptability criteria*, The Third International Symposium on Information Assurance and Security (IAS 2007), IEEE CS Press.

Dubois, E. and Mouratidis, H. (2010) Guest editorial: security requirements engineering: past, present and future, *Requirements Engineering*, 15, 1-5.

Elahi, G., Yu, E. and Zannone, N. (2010) A vulnerability-centric requirements engineering framework analysing security attacks, countermeasures and requirements based on vulnerability, *Requirements Engineering*, 15, 41-62.

Fabian, B., Gurses, S., Heisel, M., Santen, T. and Schmidt, H. (2010) A comparison of security requirements engineering methods, *Requirements Engineering*, 15, 7-40.

Faily, S. and Flechasi, I. (2010) A meta model for usable secure requirements engineering, In *Software Engineering for Secure Systems, 2010. SESS '10. ICSE Workshop*, 29-35. May, 2010.

Flechais, I., Sasse, M.A., Hailes, S.M.V. (2003) *Bringing Security Home: A Process for Developing Secure and Usable Systems*, In NSPW '03 Proceedings of the 2003 Workshop on New Security Paradigms, ACM.

Gurses, S., Berendt, B. and Santen, T. (2006) *Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments*, In Berendt, B., Menasalvas, E. (Eds) Proceedings of Workshop on Ubiquitous Knowledge Discovery for Users (UKDU'06).

Hillson D., and Murray-Webster, R. (2007) *Understanding and managing risk attitude*, 2nd ed., Gower Publishing.

Houmb, S., Islam, S., Knauss, E., Jürjens, J. and Schneider, K. (2010) Eliciting security requirements and tracing them to design: an integration of Common Criteria, heuristics and UMLsec, *Requirements Engineering*, 15, 63-93.

House of Lords (2007) *Fifth report of the House of Lords Science and Technology Select Committee* (10 August 2007), HL 165-II, 396 – 403.

Islam, S., Mouratidis, H. and Jürjens, J. (2011) A framework to support alignment of secure software engineering with legal regulations, *Software Systems Modelling*, 10, 369-394.

Jarke, M. and Pohl, K. (1993) *Establishing Visions in Context: Towards a Model of Requirements Processes,* In Proceedings of the 12th International Conference on Information Systems, Orlando, Florida, USA. 5-8 December 1993.

John, L.W. (2000) COBIT: A methodology for managing and controlling information and information technology risks and vulnerabilities, *Journal of Information Systems*, 14, 21-25.

Kauppinen, M. (2005) *Introducing requirements engineering into product development: towards systematic user requirements definition*. Ph.D. Department of Computer Science and Engineering. University of Technology. Espoo, Finland.

Krogstie, J. and Solvberg, A. (2003) *Information systems engineering: conceptual modelling in a quality perspective,* Trondheim, Norway: Kompendiumforlaget.

Kujala, S., Kauppinen, M., Lehtola, L. and Kojo, T. (2005) *The Role of User Involvement in Requirements Quality and Project Success*, In Proceedings of the 13th IEEE International Conference on Requirements Engineering, Paris, France, 29 August - 2 September 2005.

Liu, L. Yu, E. and Mylopoulos, J. (2003) *Security and Privacy Requirements Analysis within a Social Setting,* In Proceedings of 11th IEEE Requirements Engineering Conference, IEEE Press, 151-161.

Lopez-Carmona, M.A., Marsa-Maestre, I., de la Hoz, E. and Velasco, J.R. (2010) Using RFID to enhance security in off-site data storage, *Sensors*, 10, 8010-8027.

Mannan, M. and van Oorschot, P.C. (2007) *Security and Usability: The Gap in Real-World Online Banking,* In Proceedings of the 2007 Workshop on New Security Paradigms, 1-14.

Masscci, F. and Zannone, N. (2006) *Detecting conflicts between functional and security requirements with Secure Tropos*, John rusnam and the Allied Irish Bank.

McNulty, P. (2007) *AC Milan 2-1 Liverpool* [online] Available from: http://news.bbc.co.uk/sport1/hi/football/europe/6669039.stm [Date accessed: 28 January 2014].

Mead, N., Hough, E., Stehney, T. (2005) *Security Quality Requirements Engineering (SQUARE) Methodology*, Carnegie Mellon Software Engineering Institute, Technical Report CMU/SEI-2005-TR-009.

Mouratidis, H. and Giorgini,P. (2007) Secure Tropos: a security-oriented extension of the Tropos Methodology, *International Journal of Software Engineering Knowledge Engineering*, 17(2), 285-209.

Orr, K. (2004) Agile requirements: opportunities or oxymoron? *IEEE Software*, 21(3), 71-73.

O'Neill, M. (2014) The Internet of Things: do more devices mean more risks? *Computer Fraud & Security*, 2014(1).

OWASP (2001) *Application security attack components*. The Open Web Application Security Project [online] Available from: http://www.owasp.org/asac.

Pohl, K. (1994) The three dimensions of requirements engineering: a framework and its applications. *Information Systems*, 19(3), 243-258.

Ranum, M., (2005). The six dumbest ideas in computer security, *Information Security Bulletin*, 10, 285 – 290.

Riegelsberger, J., Sasse, M.A., McCarthy, J.D. (2005) The mechanics of trust: a framework for research and design, *International Journal of Human-Computer Studies*, 62(3), 381-422.

Rolland, C. and Prakash, N. (2000) From conceptual modelling to requirements engineering. *Annals of Software Engineering*, 10(2), 151-176.

Saffer, D. (2005) *Thinking about design thinking*. [online]. Available from: http://www.odannyboy.com/blog/new_archives/2005/03/thinking_about.html [Accessed 23 December 2008].

Sasse, M.A., Brostoff, S., and Weirich, D. (2002). *Transforming the 'weakest link' — a human-computer interaction approach to usable and effective security*. In R. Temple & J. Regnault (Eds.), Internet and wireless security, 243-258, London: IEEE.

Simon, H. (1969) *The sciences of the artificial*. Cambridge, Massachusetts, USA: MIT Press.

Sindre, G. and Opdahl, A.L. (2005) Eliciting security requirements with Misuse Cases, *Requirements Engineering*, 10, 34-44.

Townsend, K. (2000) Is poor security worse than no security? September 2000, *Computer Weekly* [online] Available at: http://www.computerweekly.com/feature/Is-poor-security-worse-than-no-security-at-all

van Lamsweerde, A. (2007) Engineering requirements for system reliability and security, In Broy, J.G.M., Hoare, C. (Eds.) *Software system reliability and security*, NATO Security through Science Series-D: Information and Communication Security, IOS Press, 9, 196-238.