Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 80 (2015) 30785-30790

ISSN: 2229-712X

IT Governance on security management decisions

Ioannis Koskosas

International Hellenic University, IHU-School of Economics, Business Administration and Legal Studies, 14th km Thessaloniki - Moudania, Thermi, 507001.

ARTICLE INFO

Article history:

Received: 21 September 2014;

Received in revised form:

19 February 2015;

Accepted: 28 February 2015;

Keywords

IT security,
Risk management,
Governance,
Case study, Interpretivism.

ABSTRACT

Implementation of this guidance, or indeed any IT best practice, should be consistent with your organization's management style and the way your organization deals with risk management and delivery of IT value. All analysts currently agree that probably the biggest risk and concern to top management today is failing to align IT to real business needs, and a failure to deliver, or be seen to be delivering, value to the business. Since IT can have such a dramatic effect on business performance and competitiveness and particularly in security management issues, a failure to manage IT effectively can have a very serious impact on the business as a whole. In this paper, the notion and impact of governance is analyzed in the context of IT security management decisions. In doing so, two case studies are used to identify possible factors that may affect managers in developing successful governance strategies.

Introduction

Governance is an abstract concept that applies to several scales of organization. It may refer to personal conduct or family units but more commonly refers to larger scale activities, i.e., professions, industry bodies, religions and political units (usually referred to as Local Government), up to and including autonomous regions and/or others within nation-states who enjoy some sovereign rights. It falls within the larger context of governance and principles such as consent of the governed, and may involve non-profit organizations and corporate governance. It can be used to describe people or group being able to exercise all of the necessary functions of power without intervention from any authority which they cannot themselves alter.

In the context of security management, governance describes the overall security management approach through which senior executives direct and control the entire security of the organization, using a combination of security management information and hierarchical management control structures. Governance activities ensure that critical security management information reaching the executive team is sufficiently complete, accurate and timely to enable appropriate security management decision making, and provide the control mechanisms to ensure that strategies, directions and instructions from management are carried out systematically and effectively.

However, IT governance covers the culture, organization, policies and practices that provide this kind of oversight and transparency of IT. IT governance is part of a wider management activity but with its own specific focus and in this case, security. The benefits of good IT risk management, oversight and clear communication not only reduce the cost and damage caused by IT failures – but also engenders greater trust, teamwork and confidence in the use of IT itself and the people trusted with the security of IT services.

However, in this paper an attempt is made to investigate the notion and impact of governance in the context of IT security management decisions. In doing so, two case studies are used to identify possible factors that affect managers' decisions in developing successful governance strategies. In the following, the chosen research approach is being discussed as well as its appropriateness for the research objectives. Then, risk management and information security governance are being discussed and then the research results from the two case studies are being presented. The paper ends with suggestions for further research.

Research Methodology Approach

In this paper, a qualitative research approach having philosophical foundations, mainly in interpretivism, was deemed the most appropriate. Miles and Huberman (1994) describe qualitative research as simply, research based upon words, rather than numbers. A more generalised, but appropriate definition is: "Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter" (Denzin, and Lincoln, 1998). This definition implies that qualitative researchers study things in their natural environment and understand events in terms of the meaning people assign to them and this is the strategy applied to this investigation.

Interpretivism was particularly useful when the results were being obtained. The respondents were providing their views from their interactions with the rest of the group in which goal setting was in process. For instance, when the respondents were asked questions regarding security goals, it was difficult for them to provide a response without having been involved in goal setting procedures.

The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method e.g. action research, case studies, field studies, application descriptions, it was decided that the advantages offered by case studies were deemed more appropriate to this research. Cavaye (1996) and Yin (1984) cite a benefit of a case study as "an investigation of a phenomenon within its real life context".

Two case studies were being chosen since they enable researchers to relate differences in context to constants in process and outcome (Cavaye, 1996). Also, since the issue of

Tele:
E-mail addresses: ioanniskoskosas@yahoo.com

governance on security management is a delicate and confident issue, the researcher while attempted to identify more organizations interested in the research, he identified only two of them due to difficulties mentioned above. However, according to Miles and Huberman (1994), multiple case studies can enhance generalisability, deeper understanding and explanation. Herriot and Firestone (1983) point out that the evidence from multiple case studies is often considered more convincing, with the overall study being considered more robust. This investigation further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases.

To this end, a case study approach has been followed within the IT departments of two financial institutions in Greece due to the investigator's availability of access. The institutions range from medium (M-Bank[1]) to large (L-Bank) financial institutions accordingly, based on their market share in terms of loans. The IT department of M-Bank consisted of approximately 400 employees and in L-Bank 650 employees, respectively.

However, another issue to be resolved with the research approach used here concerns data collection. The design of this investigation employed multiple data collection methods as it is important in case research studies (Benbasat et al., 1987). In all cases data was collected through a variety of methods including interviews, documents, and observation and visits to the banks lasted for approximately 1 month. The total number of interviews within the case studies numbered approximately to 100 and each interview lasted about 1 to 2 hours. The interviewees ranged from IT managers, deputy managers, software programmers, and general staff. The interviews were face-to-face. In most cases, the conversations were tape-recorded. Tape recordings were used as they offer benefits that are not available with such other forms as the note taking of data collection.

Further, the use of multiple data collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989). Triangulation is not a tool or strategy, but rather an alternative to validation (Denzin and Lincoln, 1998; Flick, 1992). Thus, any finding or conclusion made from the cases is likely to be more convincing and accurate if it is based on several different sources of information (Yin, 1984). Five types of triangulation have been identified in the literature (Janesick, 2000): Data, Investigator, Theory, Methodological triangulation and Interdisciplinary. The present research used data triangulation, theory, methodological, and interdisciplinary.

Risk Management Governance

Risk management can be defined as a systematic process for the identification and evaluation of pure loss exposures faced by an organization or individual and for the selection and implementation of the most appropriate techniques for treating such exposures (Rejda and Mcnamara, 1998).

Risk management, however, encompasses disciplines from the natural, engineering, political, economic, and social sciences, and one of the key issues highlighted by the multidisciplinary of risk management is whether risk assessment as a scientific process can and should be separated from risk management.

Fundamental views of the role of science and society could actually provide the basis of the arguments for and against separation. At a certain point, the arguments of whether risk assessment should be isolated or integrated into risk management can be settled on the issue of whether science and the scientific process can be regarded as completely objective (Hester and Harrison, 1998).

With regard to science, there are two main schools of thought. Logical positivism suggests that science is objective and supports that scientific risk assessments should be kept separate from the social and political aspects of decision making. Conversely, cultural relativism argues that science and the scientific process are linked to subjective value judgements, that science is bound up with political and social institutions and therefore, is incomplete (Hester and Harrison, 1998). Nevertheless, between the two positions of complete isolation and total integration a variety of other positions exist that base their arguments to a greater or lesser extent on the two extremes.

However, to enable effective Governance, IT risks should always be expressed in the business context rather than in the technical language favoured by IT risk experts. The following generic structure for expressing IT risks in any organisation is suggested:

- Business specific risk (e.g. Operational risk of orders not being received)
- Generic common IT risk (e.g. IT availability risk)
- Specific IT risk (e.g. Denial of service attack on Internet customer order system)
- Business risks are affected by the business environment (management style, culture, risk appetite, industry sector factors such as competition, reputation etc., national and international regulations). IT risks can be similarly affected.

For IT to be effectively governed, top management must be able to recognise IT risks and ensure that significant risks are managed. Significance of an IT risk is based on the combination of impact (what effect the risk would have on the organization if it occurred) and likelihood (the probability of the risk occurring). Because of the complexity and fast changing nature of IT, education and awareness is essential to ensure risks are recognised – not just at the top management level but at all levels throughout the organisation. It is increasingly common for a dedicated risk management function to be established or for external advice to be obtained on a regular basis to ensure that risks are monitored and the rest of the organisation is kept informed. Maintenance of a risk catalogue or risk register can be helpful to ensure that a thorough review of all IT related risks takes place on a periodic basis and for providing assurance to management that risks are being addressed.

Risk professionals are divided on what is the best approach to managing this aspect of their organization's operations, a new survey has revealed. Research conducted by security and compliance management solutions providers, questions experts from the US and the UK on areas including enterprise risk management, compliance and internal audit processes, business operations and IT operations.

They were asked to determine whether risk management is an 'art' or a 'science' For this question, 'art' was defined as decision-making based on intuition, expertise and a holistic view of their organisation, while 'science' involved using objective, quantitative measures to guide strategy.

It found that responses were split fairly in the US, with 49 per cent of individuals in the country calling risk management

[1] The names used do not represent actual banks' names since confidentiality was required.

an art. In the UK, professionals leaned slightly more towards science, with 58 per cent of people agreeing with this approach.

The research also found there were differences in opinion based on respondents' roles within their organisation. As a chief technology officer, observed: "*Business operations and risk managers tend to view risk management as more of an art because they don't feel a precise answer is needed to be able to make a decision*". However, those from IT operations and security were more likely to view risk assessments as a "*maths problem*" that has a clearly defined answer than can be identified with the right information.

Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Dependent on the type of risk and its significance to the business, management and the board may choose to:

- Mitigate, by implementing controls
- Transfer, by sharing risk
- Accept, by formally acknowledging that the risk exists and monitoring it

The analysis of IT risks can be very time-consuming and there is a danger of "analysis paralysis". To ensure effective and timely identification of risk, management workshops involving knowledgeable and interested representatives from the business, IT, audit and, if necessary external advisors, can help to rapidly pinpoint key risks requiring attention, as well as prioritizing risk management actions. It is also important to identify the benefits of managing a risk as they can help to justify the business case for taking action. Benefits can include financial savings such as reduced losses and improved efficiencies as well as intangibles such as improved reputation and image.

Risk management checklists are useful for raising awareness and reminding everyone of typical risk related issues. Regular self-assessments, internal audits and external audits/assessments are also helpful to ensure objectivity, and a thorough approach. For technical areas such as Internet security, the advice of an expert is likely to be required to ensure any technical vulnerabilities have been identified.

Information Security Governance

Executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment. Sound security is fundamental to achieving this assurance. Over the years, a number of security approaches have been developed that help in managing IS security and in limiting the chances of an IS security breach. According to Siponen (2001) the majority of these approaches fall into four different generations.

First and second generation methods aim at finding out what can be done and actually dominate the principles, checklists, and most standards for secure systems development. Third generation approaches include modelling and fourth generation emphasize socio-technical design. Siponen (2001) supports the view that there have been only a few isolated (less-well known) approaches to consider the socio-technical aspects of information systems security management. The majority of IS security methods entails checklists, risk analysis, and evaluation methods. Although these approaches help in managing security, Siponen (2001) supports the need for IS security approaches to provide a holistic modelling support which can be integrated into modern IS development approaches, and the lack of approaches which focus on socio-organizational roles of IS security.

Hirschheim et al., (1995), Backhouse and Dhillon (1996), Hitchings (1996) and James (1996), suggest that although the value of most IS security methods, tools, and techniques is evident, their focus is on narrow, technically oriented solutions and they ignore the social aspects of risks and the informal structures of organizations (see also the arguments proposed by Baskerville, 1991; Willcocks and Margetts, 1994; Straub and Welke, 1998; Siponen, 2000). Dhillon and Backhouse (2001) have also analyzed existing approaches within the socio-philosophical framework of Burrell and Morgan (1979) and in so doing, they suggest that a socio-organizational perspective is the way forward if information systems security is to be achieved.

Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the degree of protection applied.

Although awareness of these security issues has increased significantly at board levels, most senior business managers are uncertain about actions they should take and rely heavily on technical advisors. Proper governance of security, like any other aspect of IT, requires top management to be more involved in setting direction and overseeing the management of risk. Faced with the fear of unknown risks, and uncertainty regarding the effectiveness of existing controls, top management naturally wonder where to focus attention and set priorities. A risk assessment is usually the best place to start. A complimentary approach is to focus on establishing a security baseline irrespective of the risks – i.e. ensure that all the basic measures are in place.

Managing investments in the implementation and operation of controls is critical, since security can be an expensive and time-consuming task, and experience has shown that large sums of money can be wasted on ineffective or inadequately implemented technical solutions. However, proving security ROI can be difficult since actual reductions in losses or incidents must be shown, and it is sometimes impossible to know if a risk has been prevented.

There is no doubt though, that the easiest way to demonstrate cash return, is by showing the cost of incidents and wherever possible this should be done even if the examples are based on assumptions rather than actual figures. Increasingly, the benefits of good security are being recognized by management who understand that security is needed to enable e-business and that a reputation for good security can enhance customer loyalty, sales and ultimately share price. These benefits should be considered when building the business case for security investments. Given that IT security is a specialized topic and there is a shortage of skills, organizations will often seek support from third parties. Information security specialists can play a key role although governance and final decision-making must remain in-house.

Empirical Study

One of the causes of poor information security and ineffective governance of information security is a misunderstanding of what it actually covers and how it should be addressed. One of the main IT executive officers at M-Bank stated: "*Security relates to the protection of valuable assets including information, against loss, misuse, disclosure or damage. The objective of information security is protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity*". Although awareness of security issues has increased significantly at board levels, most senior business managers are

uncertain about actions they should take and rely heavily on technical advisors. Proper governance of security, like any other aspect of IT, requires top management to be more involved in setting direction and overseeing the management of risk. One IT security employee from L-Bank said: "*Most of the top management executives oversee the IT security necessities and the importance of having clear security goals in respect of the business goals only*". A possible interpretation of that sentence is that the ownership and responsibility for information security in L-Bank was not accepted by senior management in IT as well as in business.

Moreover, one of the IT security issues within both financial institutions was the establishment of a unit responsible for maintaining and renewing on a monthly basis as disaster recovery plan and post-evaluation of possible security breaches. That denotes that regardless of the top management, IT management understood its role and the importance of IT security was communicated to all and that a policy existed to underpin activities in a changing environment. Such a policy existed in both institutions with a few differences though in the evaluation and implementation process. For example, in M-Bank the risk monitoring phase was assumed as an independent final step from that of execution, while in L-Bank there was an additional step of controlling the security issues reactively and based purely on checklists of previous security incidents. From the interviews analysis, an understanding is made that in M-Bank some of the security activities planned are considered as a proactive phase to that of monitoring and reactive to that of execution.

Similarly, 90% of the IT staff in L-Bank (including managers, IT employees, IT security officers, etc) supported that any shortage of skilled resource in the area of security must be addressed, as it may be difficult or even impossible to retain all the necessary skills and functions in-house. L-Bank however was one of the largest financial institutions in Greece, whereas the IT software and hardware were developed mainly in-house. In the case of M-Bank, as smaller financial institution, IT solutions were developed in cooperation and coordination with external IT solutions collaborators; that is the M-Bank was partly based on outsourcing main IT security project activities. As an IT project manager specifically said: "*Outsourcing helps more easily ownership and responsibility of information security to be accepted and understood better by business executives and recognize better any weaknesses in security*".

Similarly, management concerns in both financial institutions were focused on gaps between security development stages because there were many possible security weaknesses involved that had to be addressed before final implementation. So, the main question for both institutions was, "*are such possible weaknesses addressed*"? Second, another question that was always considered with regard to security governance was of the type, "*are resources and money being wisely invested*"? or "*are the right controls being implemented in the areas most vulnerable to attacks*"?

One of the causes of poor information security and ineffective governance of information security is a misunderstanding of what it actually covers and how it should be addressed. That is why, when financial institutions and any organization involved with IT security governance, if they want effective security results should have procedures about policy development, roles and responsibilities, design, implementation and monitoring as well as awareness, education and training of human resources. These are basic categories within which IT security governance is developed safely and becomes stronger throughout time.

Discussion

As previously said, IT information security can be governed more properly if it can be dealt not only from its operational and technical aspect but also from its human and organizational side of IT security itself. If managers and executives can maintain the balance between these aspects of IT security, then the outcome will be beneficial for any organization with the winner being the overall success of IT security implementation and governance.

However, in the two case studies there were times that top management naturally wonder where to focus the attention of IT security and set priorities accordingly. Particularly, as one top management member of L-Bank said: "*A risk analysis and assessment might be the best place to start if you really want to address threats, vulnerability and impact of security risks*". Thus, even business management should always be aware of security threats in the context of IT security governance and should ultimately sign-off acceptance of the security risk plan. This is indeed an area where the business part of any organization needs to be more involved. In that way, the effectiveness of existing or new controls will be properly estimated by top management.

Another approach to IT security is to focus on establishing a security baseline so that the security measures will be in place according to the security policies. For example, the security standards such as the ISO17799, ISO38500 or COBIT, can be used to establish key security functions within the infrastructure. To remind, the term "standard" is sometimes used within the context of information security policies to distinguish between written policies, standards and procedures. Organizations should maintain all three levels of documentation to help secure their IT environment.

However, for information security to be properly addressed, there should be more involvement of executive management, board directors, etc., while information security to be properly implemented, skills resources need to be utilized such as information systems auditors, security professionals and technology providers.

Given that IT security is a specialized area and there are specific skills requirements, organizations will often cooperate with third parties in developing, maintaining and controlling security. That was the case with M-Bank where outside information security specialists played an important role in its IT security decision making although governance and final decision making was inside the house. In the case of M-bank, IT key security resources on which external help was provided included areas of: systems vulnerability and testing, incidents management, data monitoring or availability of rapid attack response. L-Bank on the contrary, was developing and controlling most of its IT security resources in-house since its larger size allowed for doing so.

Limitations and Further Research

There are opportunities to undertake further intensive research to identify more critical factors and their relation in IT security governance. Although an effective IT security governance seems to depend on Investors, Providers and Controllers, there are Key Security Responsibilities that need to be determined and action planning to be always in place in case of security incidents.

Another issue interesting to investigate would be the role and type of feedback in communication between in-sourcing and outsourcing, e.g., whether the type of feedback (outcome or

process feedback) provided by both parties, is effectively managed and used or whether there are traps in decision making.

The relationship between theory and practice may be considered weak and unstructured, as qualitative approaches have been criticised for not infusing theoretical factors. To this end, in this research an attempt was made to analyze and address this issue by investigating factors which may affect IT security governance. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, this research was conducted in a structured methodology guided by specific aim based on the literature review.

Moreover, the research findings may be influenced by political games that different banking units wish to play. As the participation in a research study can help organizational members to voice their concerns and express their views they can use this opportunity to put forward those views that they wish to present to other members of the organization. To this end, in order to mitigate or record the effect of "suspicion" for interpretive research as suggested by Klein and Myers, this investigation used a collection of various perspectives and an interpretation of how the interviewees react to the opinion expressed by other members.

Conclusions

Governance is an abstract concept that applies to several scales of organization. In the context of IT security management, governance describes the overall security management approach through which senior executives direct and control the entire security of the organization, using a combination of security management hierarchical management control structures.

In this paper, the notion and impact of IT security governance was studied and analyzed through two single case studies, specifically M-Bank and L-Bank. In doing so, the research was focused on possible factors that may affect managers in developing governance strategies. Some of the conclusions are that there is a need for organizations and institutions to protect against the inherent risks in the use of information technology/information systems while at the same time, recognizing the benefits that emanate from having security information systems. In this respect, as dependence on information technology increases, security is globally recognized as an omnipresent quality.

However, as new technology emerges and offers the possibility to enhance business performance, a more improved approach to information security can accrue real value to organizations by contributing to relations with customers, trading partners, improved competitive advantage and protected reputation.

In L-Bank, the process of controlling IT security governance a security baseline that consists of effective security policies and cover key vulnerabilities, satisfies the business requirements to take advantage of available and emerging technology to drive and make feasible the business strategy. In M-Bank, is was more difficult to balance the differences among business and technology units, reminding us the still existent business-technology gap. Although, awareness of these security issues had increased significantly at board levels, most senior business managers were uncertain about actions they should take and rely heavily on technical advisors. Proper governance of security, like any other aspect of IT, requires top management to be more involved in setting direction and overseeing the management of risk.

It is essential therefore for executive management to understand why an effective IT information security governance is important and take action to ensure that:

1. Classify objectives and actions into technical and non-technical areas
2. Ensure that effective security policies are in place
3. Establish a security baseline
4. Cover key vulnerabilities
5. Communicate management concerns for IT security to ensure staff awareness
6. Focus on changes – evaluate and test for security exposures
7. Ensure that Board presentations emphasize security as an enabler and not as a disabler
8. Responsibility for any security aspects of corporate compliance is accepted by the Board
9. Any shortage of skilled resources in any area possible is addressed, as it may be impossible to retain all the necessary skills and functions in-house
10. Monitoring technology developments, future trends and regulations.

References

Backhouse, J. and Dhillon, G. (1996) Structures of Responsibility and Security of Information Systems, *European Journal of Information Systems*, **5**(1), pp.2-9.

Baskerville, R. (1991) Risk analysis: an interpretive feasibility tool in justifying information systems security, *European Journal of Information Systems*, **1**(2), pp. 121-130.

Benbasat, I., Goldstein, D.K., and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, **11**(3), pp. 369-386.

Bureau Van Dijk (2013) Professionals split on best approach to risk management, *Company Information and Business Intelligence*, News letter – June 11th.

Burrell, G. and Morgan. G., (1979) *Sociological paradigms and organizational analysis: elements of the sociology of corporate life*, London: Heinemann Educational Books.

Cavaye, A.L. (1996) Case Study Research: A Multi-Faceted Research Approach for IS, *Information Systems Journal*, **6**(3), pp.227-242.

Denzin, N. and Lincoln, Y. (1998) Major Paradigms and Perspectives, In*: Strategies of Qualitative Inquiry*, N.Y.K. Denzin and Y.S. Lincoln, (eds.) Sage Publication, Thousand Oaks.

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

Eisenhardt, K. M. (1989) Building Theories from Case Study Research, *Academy of Management Review*, **14**(4), pp.532-550.

Flick, U. (1992) Triangulation Revisited: Strategy of Validation or Alternative? *Journal for the Theory of Social Behaviour*, **22**(2), pp. 175-198.

Herriot, R. E., and Firestone, W. A. (1983) Multisite Qualitative Policy Research: Optimizing Description and Generalizability, *Educational Researcher*, **12**(3), pp. 14-19.

Hester, R.E. and Harrison, R.M. (1998) *Risk Assessment and Risk Management, Issues in Environmental Science and Technology*, The Royal Society of Chemistry, UK.

Hirschheim, R., H.K. Klein, K. Lyytinen, (1995) *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*. Cambridge University Press, Cambridge. Iivari, J., R. Hirschheim.

Hitchings, J. (1996) *A Practical Solution to the Complex Human Issues of Information Security Design, In: Information Systems*

Security: Facing the Information Society of the 21st Century. Gritzalis, D. (eds), pp. 3-12, London: Chapman and Hall.

James, H. (1996) Managing Information Systems Security: A Soft Approach, *Proceedings of the Information Systems Conference in New Zealand*, Editor: Phillip Sallis, October 30-31, Palmerston North, New Zealand.

Janesick, V. (2000) The Choreography of Qualitative Research Design. In: Denzin, N.K. and Lincoln, Y.S. (eds.) *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage.

Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis: An Expanded Sourcebook*, Sage publications, Newbury Park, CA.

Rejda, G.E. and Mcnamara, M. (2013) *Principles of Risk Management and Insurance*, 12th Edition, Prentice Hall.

Siponen, M.T. (2000) A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, **8**(1), pp. 31-41.

Straub, D.W. and Welke, R.J. (1998) Coping with systems risks: Security Planning Models for Management Decision Making, *MIS Quarterly*, **22**(4), pp.441-469.

Willcocks, L. and H. Margetts (1994) Risk assessment and information systems, *European Journal of Information Systems*, **3**(2), pp.127-138.

Yin, R.K. (1984) *Case Study Research, Design and Methods*, Sage Publications, Newbury Park, CA.