INTEGRATING TECHNICAL APPROACHES, ORGANISATIONAL ISSUES, AND HUMAN FACTORS IN SECURITY RISK ASSESSMENT BY ORGANISING SECURITY RELATED QUESTIONS

Lili Yang[1], Malcolm King[1] and Shuang Hua Yang[2]
[1]*Business School, Loughborough University, Loughborough, Leicestershire, U.K.*

[2]*Computer Science Department, Loughborough University, Loughborough, Leicestershire, U.K.*

Keywords: Computer network, employee security risk assessment, organisational issue, human factors.

Abstract: This paper aims to develop a multiple perspective framework for employee security risk assessment by simultaneously, not sequentially, addressing three distinct perspectives: technical, organisational, and human factor perspectives. Interactions between technical approaches and human factors, and between organisational issues and human factors are investigated. A security related question library that integrates organisational culture and human factors with network security risk assessment in a BS ISO/IEC 27001 compliant environment is established in order to identify security vulnerabilities.

1 INTRODUCTION

Performing employee security risk assessment is a big challenge for any security engineer as human factors are critical elements that represent both safeguards and major threats (McCumber, 2004). DTI Survey (2006) reports that 65% UK large businesses in 2006 have suffered from staff misuse of information systems. There are a number of the existing security risk assessment tools. Most, if not all of them, however are technical focused without any consideration of organisational and human issues. The definition of information security provided by Tsujii (2004) illustrates the multi-perspective nature of information security. Dhillon and Backhouse (2001) mentioned that traditional approaches to information security have not considered impacts of organisational and human issues adequately. In this article we aim to integrate technical issues, organisational culture and human factors for employee risk assessment in a BS ISO/IEC 27001 compliant environment by organising security related questions. A structured question library for this integration is established and applied in the multiple perspective integrated approach for the employee security risk assessment.

The rest of the paper is organised as follows. Section 2 reviews the multiple perspective concept. Section 3 presents the interaction between technical, organisational and human factor perspectives. A structured question library is established in Section 4 for the multiple perspective vulnerability identification. Section 5 provides an illustration of the approach through a case study analysis and from this conlusions are drawn in Section 6.

2 MULTIPLE PERSPECTIVE CONCEPT

The multiple perspective concept was initially proposed in the 80's for technology assessment by Linstone et al. (1981) and was considered appropriate for the design and management of complex systems which are sociotechnological in nature. Linstone proposed a techncal perspective (T), an organisational perspective (O), and a personal perspective (P). The word perspective is used to distinguish how we are looking from what we are looking at. We believe that the T, O, P perspective concept here is suitable for security risk assessment as well.

Yang L., King M. and Hua Yang S. (2008).
INTEGRATING TECHNICAL APPROACHES, ORGANISATIONAL ISSUES, AND HUMAN FACTORS IN SECURITY RISK ASSESSMENT BY ORGANISING SECURITY RELATED QUESTIONS.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - ISAS*, pages 311-315
DOI: 10.5220/0001711603110315

Any element can be viewed from the technical perspective, or the organisational perspective, or the personal perspective and may appear differently depending on how it is viewed. As indicated by Linstone et al. (1981), the use of the T perspective to study the technical elements, the use of the O perspective to study the organisation elements, and the use of the P perspective to study the individual elements are vital but by no means adquate. Any perspective may illuminate any element. It is inconceivable that a technical element can be understood without use of the T perspective. But the O and P perspectives may add important insights. Similarly, appreciation of an organisation requires an O perspective, but much can be gained by use of the T and P perspectives. Linstone et al. concluded that "most importantly, the different perspectives are mutually supportive, not mutually exclusive".

Even though the multiple perspective concept has been widely appreciated in the inforamtion security community, for example the McCumber Cube model of information systems security (1991) presents security measures in three layers: technical, policy and practice, and huamn factors. However it is rare to see any approach or a real application that has implemented the multiple perspective concept in security risk assessment. Most of the existing secuity risk assessment tools are technical focused with little or no consideration of organisational and personal factors in literature.

3 INTERACTIONS BETWEEN TECHNICAL APPROACHES, ORGANISATIONAL ISSUES AND HUMAN FACTORS

It is not surprising that the main features of computer network security practices adopted by an organisation are technical. Any tangible and intangible assets must be protected by technical controls that depend on technical approaches. The typical technial approaches include: (a) Identification and authentication. These controls prevent unauthorized personnel from entering the computer system. Security controls include passwords and firewalls. (b) Logical access control. These controls ensure that sensitive information assets and information systems are only accessed by authorized individuals. Security controls include access policy and technical mechanisms such as encryption and access control lists. (c) Audit trails. These controls ensure the users are accountable for their actions and that indications of system instability or security problems are identified and tracked. Security controls include audit events and review of audit trails. However, these technical mechanisms do not offer much protection when employees have a right of access but use it for malicious pruposes or make human errors because of 'carelessness' or 'lack of awareness'. There are many inidcations that the technical secuirty measures are not very successful. Most analyses suggest technical solutions are not enough, and 'the human factor' is often the cause of the downfall, beacause organisational structures and cultures allow the human errors or malicious actions happen. Many organisations are exploring organisational policies that are limited to training staff in the security procedures they are expected to follow. These appear to focus on what not do, i.e. how to avoid creating a security risk. Very little is available about how to create a security culture in which employees take positive responsibility for creating a climate of security and trust.

Many problems can occur if a balance among the three perspectives can not be achieved. Employees may work around the existing security system to meet their work demands because of the poor usability of the technical system such as too rigid or inappropriate in an emerging situation, or a poor match to their skills and organisational cultures. All these inappropriate interactions may put the need for security in jeopardy. In one particular example, the staff of an Accident and Emergency Department in a UK hospital (Collins, 2007) found that putting their smart card and their password into a computer every time when they wanted a patient record was taking precious minutes away from treating patients. So they decided that the leader of the shift would put his card into a computer at the beginning of the shift and leave it there for everybody to use. They also decided to make public what they are doing to challenge what they regard as a time consuming and inappropriate way of protecting patient security. The feature of this example was that the actions of employees are creating the potential for security breaches that may be serious for patients and in turn for the NHS Trust. However, they are doing this not out of malice or ignorance; they are doing it because the constraints of the security procedures are getting in the way of what they regard as legitimate ways of undertaking their work. In this case, and potentially in many others, the need is for security policies, procedures, and technical approaches that are accepted by employees and are found to be workable.

4 INTEGRATION BY ORGANISING SECURITY RELATED QUESTIONS

Checklist approach is one way to prompt people to check for some aspects of security that may be overlooked. The IT security professional must ensure they are answering the questions from the checklists. When these questions are written down, the job becomes much easier. However, checklists are hard to compile and easy to misuse. The available questions in the checklist are normally limited as it does not deal with the complex nature of security risk assessment and does not cover the technical, organisational, and human factor perspectives.

In this section a structured question library is proposed for the multiple perspective vulnerability identification in terms of BS ISO/IEC 27001, an international standard about 'Information technology – security techniques – information security management - systems requirements' (ISO/IEC 27001, 2007). The focus is on why an incident occurred and what should be done in the first place to prevent it. The structure of the knowledge base/questions library is also considered. BS ISO/IEC 27001 adopts a process approach, called PDCA (Plan-Do-Check-Act), for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organisation's ISMS (Information Security management System). Process approaches are based on the assumption that important properties of a system, e.g. security properties, can be inferred indirectly from documentary evidence showing how the system was constructed and analysed. A precondition of a process-based security assessment is that the interactions between construction and analysis processes are validated and documented, and documentary evidence is accurate, i.e. shows whether the processes have been applied correctly. The scope of the standard is broad. Its requirements are "intended to be applicable to all organizations, regardless of type, size, and nature." One of the key outcomes in the plan phase of PDCA is a series of the identified risks including the assets within the scope of the ISMS, the owners of these assets, the threats to those assets, the vulnerabilities that might be exploited by the threats, and the impacts that losses of confidentiality, integrity and availability may have on the assets.

Annex A in BS ISO/IEC 27001 gives the lists of the control objectives and controls for information security that are "directly derived from and aligned with those listed in BS ISO/IEC 1799:2005". These cover:

- Security Policy,
- Organisation (of internal organisation and external parties)
- Asset Management
- Human Resources Security before during & after employment
- Physical & Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development & Maintenance
- Correct Processing In Applications (cryptography & reliability issues)
- Information Security Incident Management
- Business Continuity Management (risk assessment & recovery planning)
- Compliance with Legal Requirements

The lists are not exhaustive but cover most aspects in the information security domain from technical, organisational and human factor perspectives.

From A.5.1.1 and A5.1.2 of BS ISO/IEC 27001 two vulnerability related questions can be derived as follows.

Question Q.5.1.1: Has an information security policy been approved by management, published, and communicated to all employees and relevant external parties?

If the answer is 'Yes' to the question Q.5.1.1 there will be no weak point in the production, dissemination, and communication of the information security policy. Otherwise, a vulnerable point has been identified.

Question Q.5.1.2: Has the information security policy been reviewed at planned intervals or when significant changes occur?

If the answer is 'Yes' to the question Q.5.1.2 there will be no weak point in the updating of the information security policy. Otherwise, a vulnerable point has been identified.

Questions Q.5.1.1 and **Q.5.1.2** identify the vulnerability from the organisational aspect. Similarly, a set of comprehensive questions can be derived from BS ISO/IEC 27001 from technical, organisational, and human factor perspectives.

For the questions to be efficiently used in security vulnerability identification they must be structured in a logical fashion. It is reasonable to classify the questions into three categories:

technical, organisational, and human factor and ask 'how', 'where', and 'who' related questions separately. The technical category covers all the questions concerning the technical approaches adopted, facilities employed including software packages and hardware equipments. These questions ask how the security will be enhanced or degraded. The organisational category covers all the questions concerning management, security policy, and physical environment. This type of questions asks where the security will be enhanced or degraded, i.e. at what soft and hard environments. The human factor category covers those questions concerning employee vulnerabilities and asks who will take actions to enhance or degrade the security.

In principle, each question should only belong to one category. In practice, it might be the case that some questions belong to several categories. In these cases, the questions are defined into different version with a different description and an emphasis on a single perspective. Thereby any overlap between questions and categories can be removed.

5 CASE STUDY

A well known example (Koumpis et al. 2007), the theft of a laptop computer from a UK building society in 2006 underlines how the technical, organisational, and human factors are all critical influences on the security risks imposed by employees. A long-standing employee downloaded a customer database to his laptop computer so he could work at home. This laptop computer was subsequently stolen, and the employee did not inform the company until returning from a three week holiday. The building society did not inform their customers for a further three months. The Financial Services Authority (FSA), the regulator of all providers of financial services in the UK, imposed a fine of just under £1 million on the building society, concluding that the company had failed to assess the risks, and had not implemented proper procedures and training to manage the risk. A combination of factors have clearly led to this security breach: technical factors enabled data transfer to the laptop computer, lack of logging of such actions, and access to the data by the public through the absence of encryption or 'kill' technology; human factors include the lack of appreciation of the risks involved by the individual; organisational factors include the lack of policies regarding safe working practices.

The action that took place in this accident is 'a customer database was downloaded to an employee's laptop computer and brought outside a working place'. If the following questions have been asked in a regular security risk assessment, this accident may have been prevented from happening in the first place.

Technical perspective – how to take the action:

Q.9.2.1: Has equipment been sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access?

Taking a company laptop computer to home obviously gives a 'No' answer to this question.

Q.10.10.4: Have system administrator and system operator activities been logged?

If the answer to Q.10.10.4 is 'Yes', any database downloading activities should be logged and the system administrator should be alerted when the downloading activity is happening.

Q.11.5.3: Have systems for managing passwords been interactive and ensured quality passwords?

If the database and the laptop computer are password protected any unauthorised access may be stopped.

Organisational perspective – where to take the action:

Q.9.2.5: Has security been applied to off-site equipment by taking into account the different risks of working outside the organisation's premises?

This question is directly related with taking the laptop computer to home. The positive answer to Q.9.2.5 may introduce more security protection measures into the laptop computer.

Q.9.2.7: Has equipment, information, or software not been taken off-site without prior authorization?

Positive answer to Q.9.2.7 will alert management with possible risks of losing their sensitive customer database.

Q.12.3.1: Has a policy on the use of cryptographic controls for protection of information been developed and implemented?

Any encryption on the database will further stop the information breach.

Human perspective – who to take the action:

Q.8.2.2: Have all employees of the organisation received appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function?

Lack of security training should have been avoided if the answer to Q.8.2.2 is 'Yes'.

6 CONCLUSIONS

The UK government departments such as the Technology Strategy Board responded proactively to the growth in network security failures through its technology programme and the network security innovation platform. This article is part of the outcome of the research on the human vulnerabilities in network security initiative with its focus on employee risk assessment. The proposed multi-perspective approach has addressed employee security risk in all its aspects, particularly in: organisational issues, technical approaches, and human factors, and that any perspective may illuminate any issue, the different perspectives are mutually supportive, not mutually exclusive. Interactions between these three perspectives have been identified. Employees may work around the existing security system to meet their work demands because of the inappropriate interactions among these three perspectives such as poor usability of the technical system or a poor match to their skills and organisational cultures. All these inappropriate interactions may put the need for security in jeopardy. Employee risk assessment can be carried out simultaneously from human factors (who), technical approach (how), and organisational issue (where) perspectives. A library of vulnerability related questions derived from BS ISO/IEC27001 is structured and applied in the employee security risk assessment. A case study has been used for the application and explanation.

ACKNOWLEDGEMENTS

This research was financially funded by the Technology Strategy Board (TSB) and BAE Systems in the UK. Project number TP/7/NSP/6/S/P0013L.

REFERENCES

Collins, T., 2007. NHS security dilemma as smartcards shared, *Computer Weekly*, 20th January.

Dhillon, G and Backhouse, J., 2001. Current direction in IS security research: towards socio-organisational perspectives, *Information System Journal*, 11, pp. 127 -153.

Douglas J. Landoll, The security risk assessment handbook: a complete guide for performing security risk ncis, 2005assessments, Boca Raton, Fla: Taylor & Francis, 2005

DTI, 2006. Information security breaches survey, Available at http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf, accessed in 2007.

ISO/IEC 27001, http://www.iso.org/iso/catalogue_detail?csnumber=42103, accessed in 2007.

Koumpis C, Farrell G, May A, Mailley J, Maguire M, Sdralia V., 2007.To err is human, to design-out divine; reducing human error as a cause of cyber security breaches, *A Human factors Working Group Complementary White Paper, Cyber Security Knowledge Transfer Network,* Vodera Ltd & Loughborough University.

Linstone, H., 1981. The multiple perspective concept with applications to technology assessment and other decision areas, *Technological Forecasting and Social Change*, 20, pp. 275-325.

McCumber, J, 1991. Information systems security: a comprehensive model, *Proceedings of the 14th National Computer Security Conference*, Washington, D.C., October.

McCumber, J., 2004. Assessing and managing security risk in IT systems.

Tsujii, S., 2004. Paradigm of information security as interdisciplinary comprehensive science, *Proceedings of the International Conference on Cyberworlds*.