MIS Review Vol. 19, No. 2, March (2014), pp. 57-71
DOI: 10.6131/MISR.2014.1902.04

Modelling e-Health Systems Security Requirements: A Business Process Based Approach

Ahmed H. Alahmadi, Ben Soh, Azmat Ullah
Department of Computer Science and Computer Engineering, La Trobe University, Australia

ABSTRACT: *Today, health organisational executives agree that health systems can play an increasingly key role in the achievement of the e-health business. However, over the past many years, the achievement of health systems in public health organisations has been badly affected due to a lack of information regarding protecting health information systems and other health organisational resources from security threats. The aim of this paper is to link the security requirements and security goals in previously modelled health process at the early stages of system development that fulfil the health organisations' goals and objectives effectively and securely.*

KEYWORDS: *Security Requirements, Health Resources, Risk Management, Risk Analysis.*

1. Introduction

Dealing with security-related issues in information systems is a challenging task. However, security plays a vital role in the success of almost all components of the health organisation such as health decision making, health organisation strategy formulation, health organisation goal modelling, managing health organisational resources, structuring, and managing health organisational data (Stanley, 1997; von Solms & von Solms, 2009). Moreover, protecting running processes in health organization is important in the context of developing suitable health information system; therefore, handling information security within health organisations calls for a strong understanding of the viewpoint of e-health business and the architecture of the system that is being used in the health-related business organisations.

The evolution of e-health systems introduces a need for unique security, privacy and confidentiality that requires a fresh examination of the mainstream concepts of information security in relation to the e-health process. The e-health process is one of the most security and privacy sensitive elements in the health organisation that is managed electronically (Salini & Kanmani, 2012). The significance of security and privacy in e-health raises the issues of individual consent, confidentiality and privacy, which are considered the main factors in adopting a successful e-health system (Shoniregun, Dube & Mtenzi, 2010a). One way of developing a successful e-health system is the management of information security risk requirements within the health business organisation. Over the

last 25 years, security problems have adversely affected the employment and deployment of technology in both public and private health organisations (Ray & Biswas, 2014).

This paper proposes a technique to manage health security requirements in the early stages of health system development in relation to modelling health processes. The paper suggests how to model and map security goals that guarantee the protection of the health process and its resources from different threats. In this paper, we linked our previously published technique into managing e-health security requirements and protecting the e-health process (Ullah & Lai, 2011). The paper is structured as follows: in Section 2, we review the context of our paper, which includes the theoretical concept of information security in context of e-health. Section 3 presents the proposed methodological framework, which is further categorised into the identification of the e-health organisation environment, security goals and objectives selection, connecting security goals and objectives, derivation of security goals and objectives and health process analysis at the system planning stage. Finally, Section 4 presents the conclusion of the paper.

2. The context of the work

This paper aims to identify, model and analyse e-health security requirements into a previously modelled health process. Thus, it is important to describe security in the context of deriving system requirements from the health process.

It is undeniable that information technology has breached virtually all parts of business organisations in a diversity of ways and has had an uncountable effect on companies' achievements and performance. In another words, the increasing trend in the use of internet-based applications in business organisation infrastructure has shaped stunning opportunities for business organisations to attain effective supply chain management. This is because web-based applications have experienced important changes over the last few years; ten years ago, there were no web applications or interactive websites, but simply sites that were a collection of stationary pages. Business organisations that had customer facing websites were gifted to connect with customers via internet, and use their web applications as a stations to market and sell their products; business intranets were used mainly as spaces to post news and business organisation policies.

However, the advancement of information technology has increased security threats for organisations data. As organisation's data is a reserve like any other business resource and it can exist in many forms, including film, text, video and disc. Therefore, internet security is the process of defending business organisations resources. In other words, security can be defined as an activity that relates to the defence of organisational resources and resources infrastructure assets against the risk of loss, misuse and damage.

It designates controls that a business organisation needs to assure that it is realistically managing these risks (Ray & Biswas, 2014; von Solms & von Solms, 2009).

In e-health and e-market sectors, there could be several security threats such as: malicious e-health websites, in this threat the hateful URL discoveries are for e-health web applications that encompass exploits; malicious scripts in which internet hackers inject malicious scripts into the program of unaffected e-health web applications that have had their security cooperated; executable threats, these typically refer to the presentation and download of other detestable e-health web applications; trojans, which bring many malicious applications to e-health; and exploits, which target vulnerabilities and try to circumvent the courtesy of internet security applications (DeMarco & Lister, 2003). Moreover, advanced e-health systems are moved from organisation-centred to process-related architecture (Blobel, 2007). These facts have made the e-health business process the most important and initial part in modelling and analysing the e-health environment. This can be applied for complete understanding of e-health threats and risk and exploring the security requirements respectively.

The above-mentioned security threats can be encounter by analysing: Threats to e-health organisation, these are unwanted proceedings that could foundation the cautious or unintentional misappropriation of the health organisation recourses, loss and damage. Vulnerabilities, these are being deployed in handling security goals, which are categorised into availability, integrity and confidentiality. Impact, this states to the scale of the likely loss. Guaranteeing the security of health organisation elements particularly health process can be achieved finished the operation of a set of organisational (Agrawal & Johnson, 2007; Ray & Biswas, 2014).

3. Methodology

Security and privacy difficulties arise when there is a need to protect health organisational resources (particularly e-health process) from security threats. However, defending health organisational resources is a serious task in this rapidly changing health environment because to succeed, organisations employ a complex structure. Information security in the context of e-health is a business problem in the sense that the entire health organisation's resources must be used to analyse and resolve security problems based on the organisation's strategic drivers, as the technical controls alone can only aim to mitigate one type of attack (Caballero, 2014). Therefore, in e-health domains, security- and privacy-related problems can be addressed by managing security in the form of identifying/modelling, mapping, and analysing the attacks for already modelled health process.

This paper presents an approach for modelling goals and objectives in previously modelled health process so that security requirements can be generated from the studied health process. The approach has been derived from our previously published work and propose a method of mapping security goals and objectives in the e-health processes that have been studied in previous published work (Alahmadi, Soh & Ullah, 2014). This approach describes the way to identify, model and analyse the attacks on health process and the overall health organisation, as shown in Figure 1, as security is the key concern of e-health businesses today. It defines the qualities estimated from e-health systems, for example, protection, usability and consistency. It also demonstrates how to model the health process using *i** language so that security requirements can be linked with the health process. Further, it illustrates the documentation of constraints and security requirements. Finally, it describes the method of risk analysis at the system architecture level in the form of impact, threat and vulnerability, as shown in Figure 1.

3.1 Identification of e-health organisation environment (Level 1)

To implement this proposed methodology, it is important to identify and analyse the e-health business processes prior to derive security requirements from the health process. A process of routine patient consultation has been used as a case study, which is an already published case study (Alahmadi et al., 2014). In this paper, security goals and objectives have been modelled and linked into that previously studied case study. To this aim, the *i** framework (Yu, 1993, 1997) is employed, as shown in Figure 2, which is a well-accepted framework in modelling and identifying security goals and objectives. The framework describes the business process in the sense of dependency relationships among organisational process actors. One of the main concepts of this framework is that actors have the right to act within their social environment. In other words, actors have their own goals and beliefs, and these goals are connected to each other. The

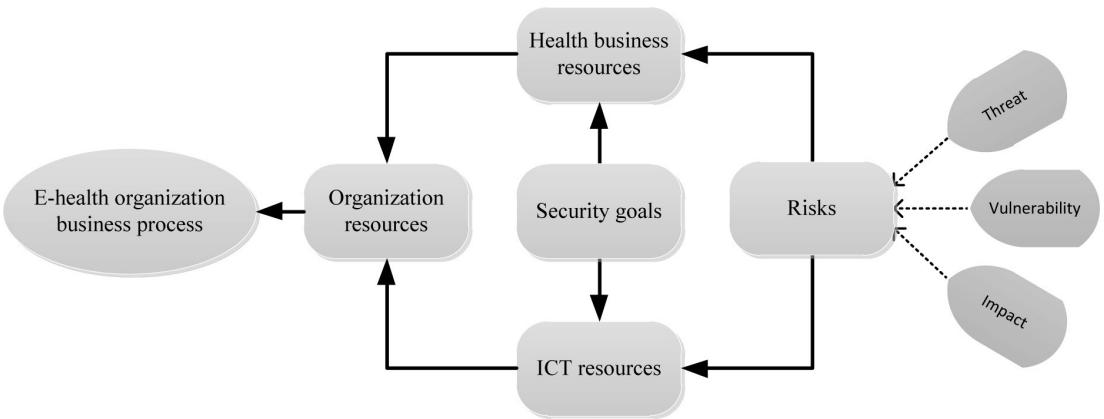

Figure 1 The Proposed Methodology Framework

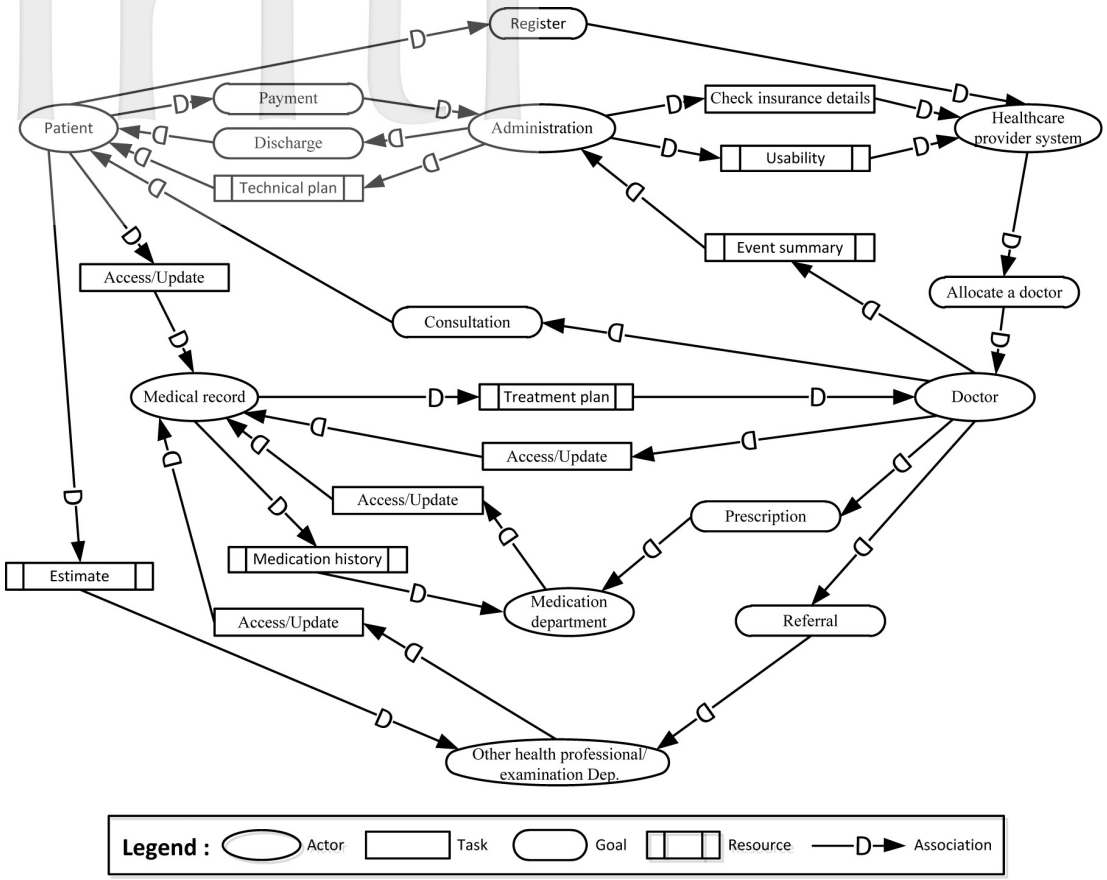

Figure 2 Process Model of Routine Patient Consultation Visit

framework specifically embeds intentional relationships into the dependencies between process actors, where actors aim to achieve goals, accomplish tasks, produce resources and satisfy soft goals. The *i** framework distinguishes two types of dependencies: the strategic dependency model that is employed to describe the dependency relations among the organisational processes actors; and the strategic rationale model that is employed to define the stakeholder's safeties in terms of what they require, what is their main concern, and how these concerns might be considered in the organisational and health system environments. The framework is well-accepted for the purpose of modelling and reasoning the organisational business process and the environment of the related information system as indicated by Ullah and Lai (2011).

The main goal of the case study in this paper is to show the possibility of managing a routine consultation visit to a healthcare centre and its associated gaols electronically. The process is categorised into seven actors: *patient*, *healthcare provider system*, *doctor*, *medication department*, *other health professional/examination department*, *medical*

record database, and *administration*. These actors are the main members of the health organisation process that are used to describe how the work is organised among them. In view of that, all *i** dependencies are described in the framework as relationships between those actors. Moreover, the *business goal* dependency in this case study is divided into six goals, as shown in Figure 2. The seven goals are as follows: *Registration* -- retrieves the patient's data if the patient is already registered in the health care provider system or registers the patient as a new patient. *Allocate doctor* -- allocates a doctor based on availability and the situation of the patient. *Consultation* -- undertakes the clinical examination according to the treatment plan if any. *Referral* -- patient referrals are given where further examination is required by another health professional or examination department. *Prescription* -- prescribe drugs to medication departments if necessary according to the patient medication history. *Discharge* -- discharges the patient after organising a follow up visit if required. Finally, *Payment* -- administration finalise the payment with patient after checking insurance information.

Moreover, *task* dependencies in our case can be applied when one of the actors performs any activity of the studied process. For instance, in this case study, all of the *patient*, *doctor*, and *medication department* do "Access/update" the medical record database, and the *administration* actor does "*check insurance details*" for the health care provider system. Moreover, the *resources* dependency is used to describe the organisational actor's dependency. For example, doctor should provide *event summary* to the administration to discharge the patient. Also, the health medical record actor should provide *treatment plan* to the doctor to manage the consultation, and *medication history* to the medication department. Lastly, the *soft goal* dependency is dissimilar from health goal dependency, as soft goals only discuss the goals for which there are no straightforward standards to identify whether the condition is satisfied.

3.2 Security goals and objectives selection

Identifying the goals and objectives of securing both health and ICT resources associated with an e-health business process is critical in extracting the security requirements of an e-health system. This section aims to identify the security goals and objectives of the already modelled e-health business process. Although, there are several e-health business process security goals, the literature highlighted the most fundamental: confidentiality, integrity and availability (CIA) (Alemán et al., 2013, Shoniregun, Dube & Mtenzi, 2010b). Researchers note the ever-growing necessity for confidentiality and integrity objectives in e-health information systems, while at the same time ensuring the availability of these systems to authorised parties (Smith & Eloff, 1999). These security goals clearly match the concept of soft goals in the *i** framework where there are no clear measurements indicate the fulfilment of their conditions. In Figure 3, these "soft goals"

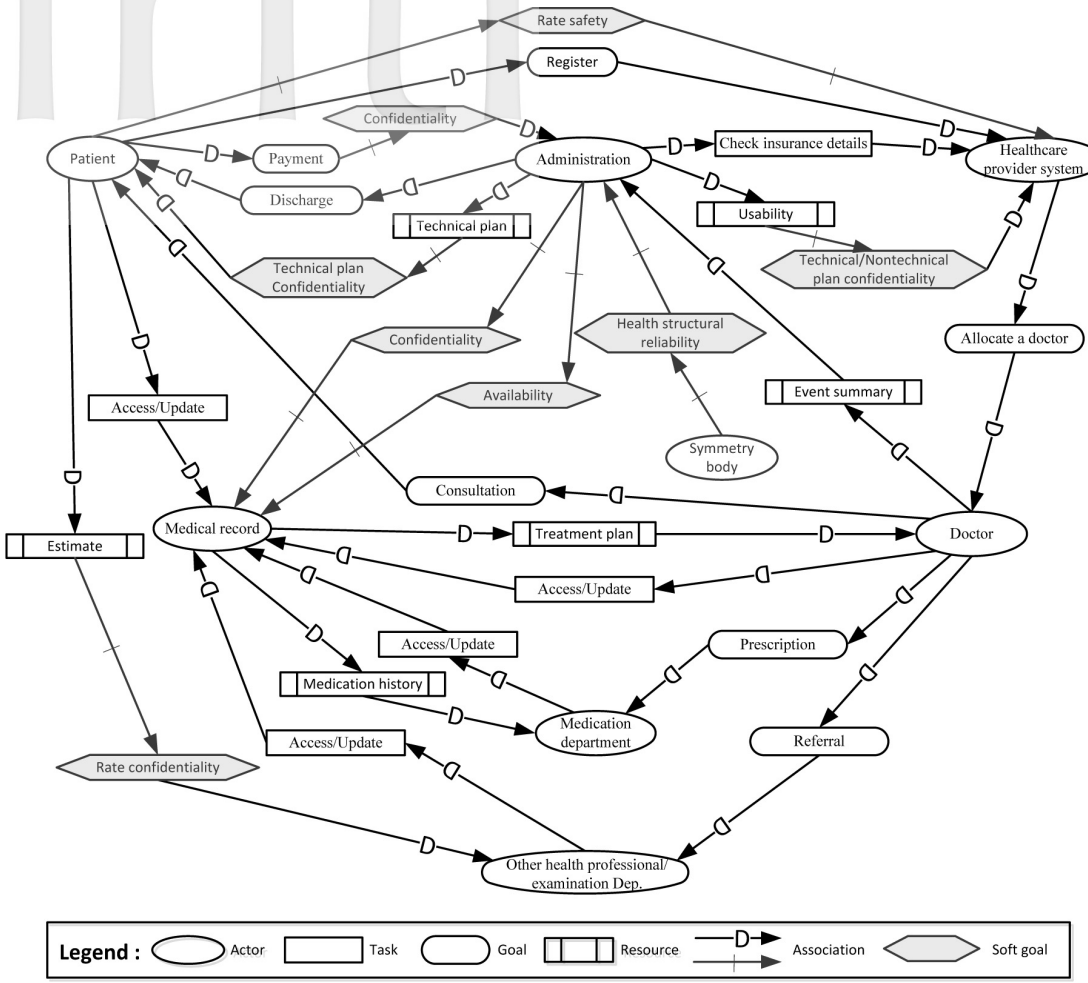

Figure 3 Selection of Security Goals and Objectives

are presented in relation to our case study resources. Discussion of the above-mentioned security goals in relation to our case study are given hereafter.

Confidentiality refers to the issue of disclosure and communication of information. According to the ISO EN13606 standard (Muñoz et al., 2011), it is defined as the process that ensures the accessibility of the information only to those authorised authorities and entities. In context of our case study, it is a soft goal in all data exchanging tasks between patient, administration, and medical records. Similarly, resources such as technical plans and usability must have a level of confidentiality as security goals to ensure the authorised communication and access between parties in the e-health organisation, which contributes to the organisation's confidence.

The second main e-health business process security goal is integrity, which refers to the duty to guarantee that information is accurate and is not modified in an unauthorised

manner. The integrity of the e-health business process must therefore be protected to ensure patient safety. In relation to our case study, "rate safety" is applied as a soft goal in the relationship between patient and health provider system. This goal aims to ensure that the related information's entire life cycle is fully auditable, which is one of the important components of patient safety protection. Moreover, integrity of both software and hardware health resources is a prerequisite for health information integrity. Information integrity can be intentional or unintentional changes to information that occur in transit (Savola & Abie, 2010). As a result, integrity is intimately linked to reliability dimension of software and system quality. From this perspective, a new actor is introduced into the case study called "symmetry body" to satisfy the "health structural reliability" of the modelled e-health business process.

Availability as an e-health business process security goal refers to the accessibility and usability of the resource upon demand by an authorised entity. In e-health organisation, the availability concern is also critical to effective healthcare delivery. All resources in an e-health organisation must remain operational even in difficult situations such as the face of system failures and denial-of-service attacks. Availability appears as a security goal between administration and medical records; both need to be accessible and usable upon request to ensure the availability of healthcare delivery. Medical records need to protect the sharing of patient data in order to ensure the availability of accurate and timely information to all authorised communicating partners.

3.3 Connecting security goals and objectives

Once the health process and security goals have been identified, it is important to link and map security goals and objectives into the health process. As in the above sections we described how information security objectives can be mapped with business requirements. In this section, we identify the security objectives to defend the resources in the planned health process (Aware, 2006). The literature shows that many approaches have appeared in order to protect health processes. The key approaches are integrity, availability and confidentiality, which have been described in the previous section. Security goals at this phase authorise the definition of soft goal of security using *i** framework. Requirements engineering literature demonstrates that it is likely to map security goals into the health business organisational requirements (Liu, Yu & Mylopoulos, 2003; Mouratidis, Giorgini & Manson, 2003; Van Lamsweerde & Letier, 2000). Figure 3 shows security soft goals in our case study where the way of identifying security soft goals is dissimilar from health business resources, for example, confidentiality/privacy is the soft goal for the estimations, constructing recognised health goals into the health organisational hierarchy that defines the stipulations of all involved goals, and their influence to the higher level components of the health business, which are either part of the health organisation strategy or associated to the organisational external security factors.

Moreover, Figure 3 shows the information security belonging goals displaying how to protect the health process and significant information about consumers. For instance, the measurement of confidentiality goal subsidises to consumer belief and self-confidence, the technical plans confidentiality goals subsidise to corporation confidence. However, in some cases, information security goals can be characterised as safety dependencies, where process actors designate security questions rather than the soft goals of the health organisation. In the process of routine patient consultation, we present a new process actor called regularity body in order to fulfil the structural reliability of the health organisation.

3.4 Derivation of security goals and objectives

To implement security goals and objectives and to derive security requirements from proposed health process of routine patient consultation, we only deliver detailed information on the "Management" actor and its relations with the "process manager" as shown in Figure 4. The e-health system plan proposes cooperative sustenance for a set of health services employed by several health organisation departments and also maintains the structure calculations bustle in the health organisation. The first structure calculations process task dependency recognised at the health organisational level is among the "process manager" and the "management." But the second structure calculations in the process are defined at the health system level, where two mediators, the "system manager" and "administration," accomplish this task. A "system manager" uses the "e-health system" plan structure calculations examination on the basis of technical plan history and technical plan estimations. However, for empowering structure calculations are that essential to be transported to the "management," a process manager authenticates the consequences that the control tool generates.

Once authentication has been provided, the "e-health system" manager gives feedback on medicine package availability and payment confirmation to the "management" by using the goal called feedback in the "administration" actor. This frame of implementation and modelling security requirements at the health system level also presents a new actor known as "health system manager," which is knowledgeable in estimating structure tools, and in apprising technical plans according to the demands of the health organisation and its system. At this stage, it is understood that the framework clearly defines how security goals and objectives can be labelled at the health process level and how goals can be transported into constraints at the level of health system development.

At this stage, our framework also shows that the protection from unauthorised entry constraint can be achieved by using this proposed framework. It showed that pattern of three security requirements is demarcated in this proposed case study in health sector, this pattern donates to the reengineering of the security constraint: inner access measure,

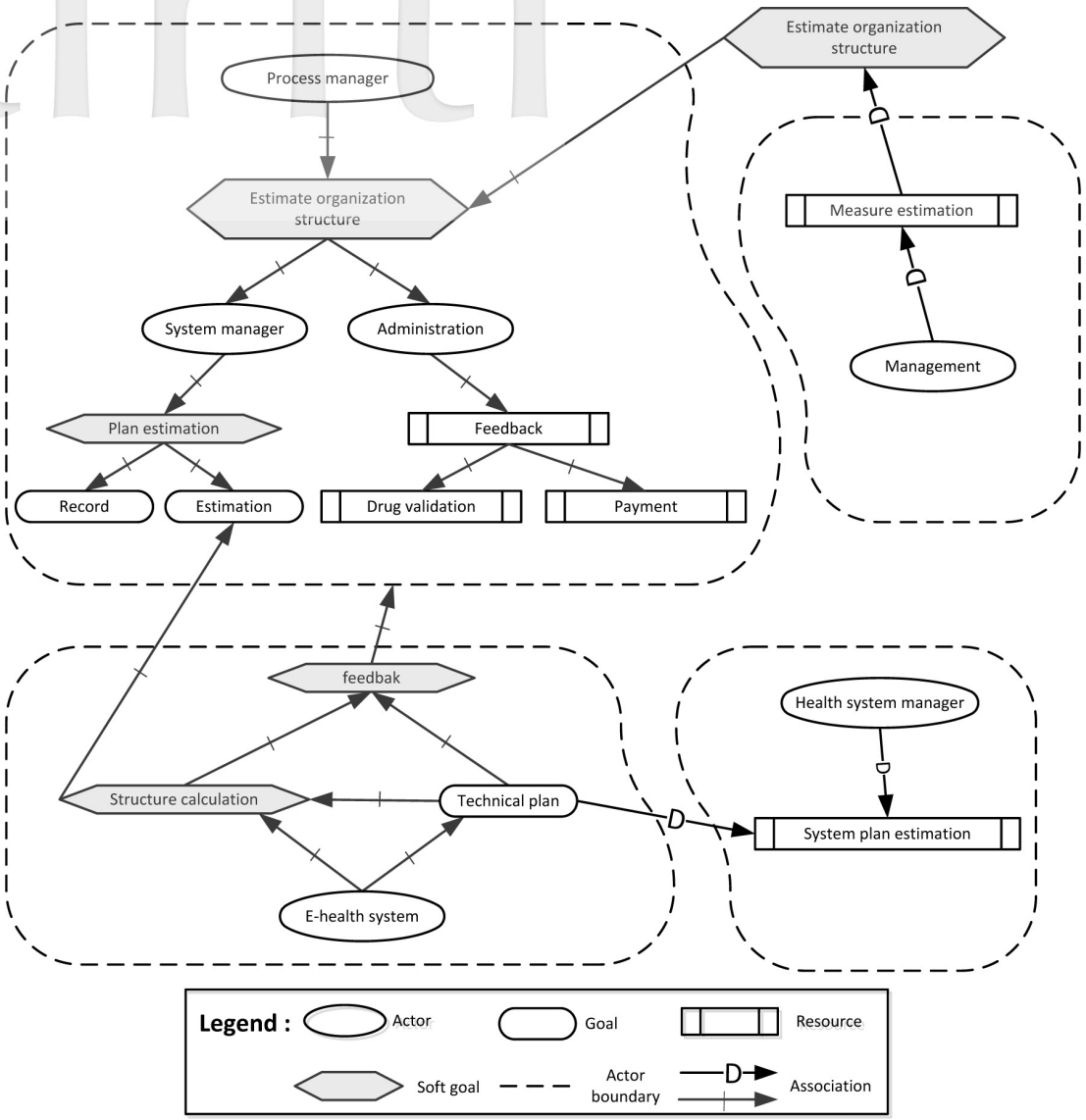

Figure 4 Derivation of Security Goals and Objectives

which defends the inner mechanisms of the health business process such as regulatory access and modifications; outdoor access measure, which is a protect measure to guarantee that outside mechanisms are not able to access the health system database; access authorisation, which is protect measure that acts on the health system customers, which are patients and other users from the health organisation administration authentication mechanism.

3.5 Health process analysis at system planning stage

Risk management is a process that involves frequently classifying, analysing, treating, and monitoring risk throughout the software product life cycle. In this section, we emphasise a technique of examining risk at the system planning stage. At this level of our discussion, several system planning-related components are recognised, for instance, the security measures that can be employed to accomplish the security requirements and the security measures that can be employed to classify the most satisfactory security requirements that are fundamental to the technique of security risk supervision. At this stage, we are concerned with the precise "risk history" security requirement recognised in the discovery of constraints and security requirement phases. In our case, Figure 5 demonstrates that the security requirements could be accomplished with the solution based on "monitoring threats" as well as with technology-based clarifications connected in the company system and network platform.

Moreover, every control in the risk examination framework presented in Figure 5 can further be characterised into sub-levels, for example, control for health software

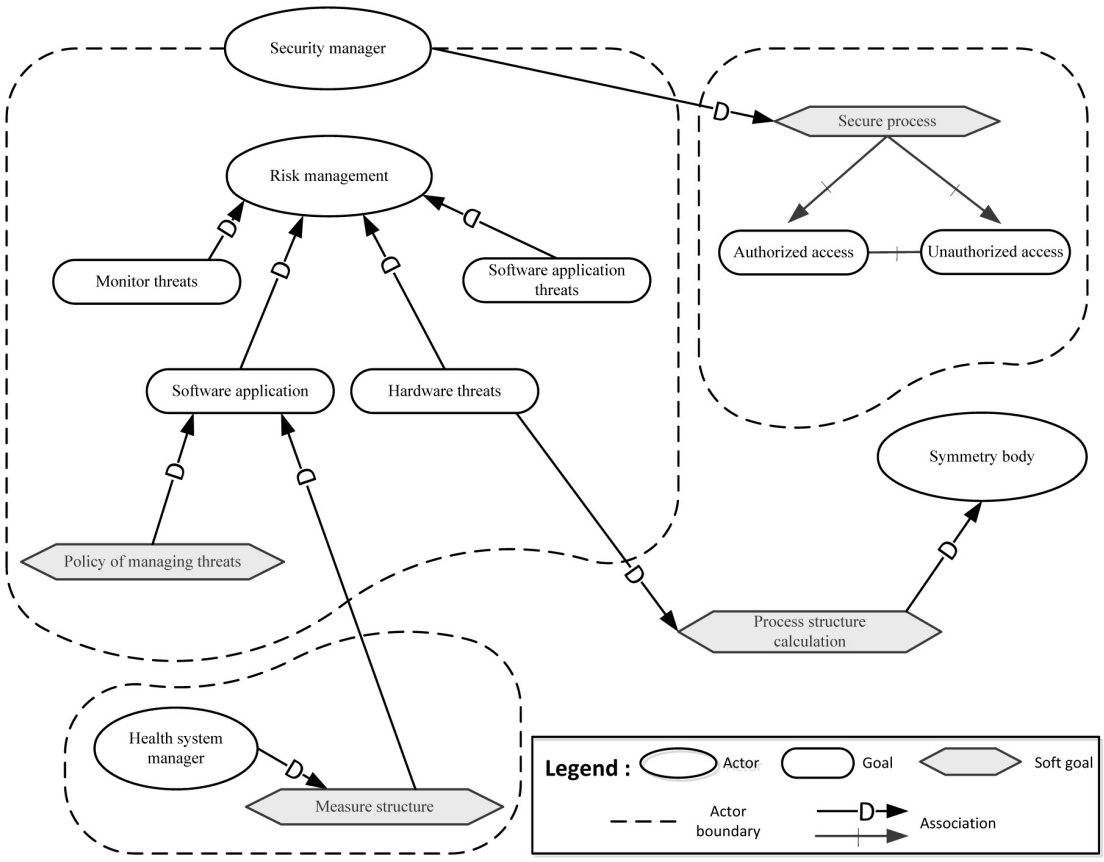

Figure 5 Derivation of Security Goals and Objectives

applications, which is made up of two tasks: examine the policy of managing threats and mapping structure calculation. These tasks define the guidelines and regulations to examine the inspected events according to likely security violations; and preserve the data analysis database after the examined event. Every control in this health case study has worth and cost in terms of operation, placement and maintenance activities. Therefore, the safety of every goal is important. The "secure process" soft goal in Figure 5 is employed to ensure that the system activities in this proposed health process are only being employed by the authorised entries and to guarantee the activities are protected from unauthorised access. At this stage the health process is secure and ready for the next phase which is risk analysis at the health system planning level.

4. Conclusion

Rapid developments in the field of e-health have led to the requirement for more research to be conducted in this field. In the last few years, several e-health projects have been carried out in different patterns. Notably, among this research is the study of telemedicine, EMR, mobile-health, and health monitoring systems, which aim to provide an enabling environment that enhance the ability of providing better healthcare services and overcome problematic geographical barriers in providing healthcare delivery. However, not many researchers have discussed the issue of e-health in context of protecting health process. It is widely accepted that security for technology resources and managing risk is a critical task in the development of secure health systems and in order to protect health business organisational resources in the context of developing electronic health system.

Our aim in this paper is to challenge the issue of information security at the earliest stage of e-health development. The case study on the process of routine patient consultation in a health sector has been used to validate this proposed approach. The results indicate the following: first, security requirements and constraints must be derived from the health processes, as processes are the firm key element where the accomplishment of all others health organisational components are based. Second, requirements engineering is appropriate to model the security goals and objectives within the health organisation. Third, it is best to model and map the security requirements at the early stage of the development of health systems that could guarantee a fulfilment of health organisational goals.

References

Agrawal, R. and Johnson, C. (2007), 'Securing electronic health records without impeding the flow of information', *International Journal of Medical Informatics*, Vol. 76, No. 5-6, pp. 471-479.

Alahmadi, A.H., Soh, B. and Ullah, A. (2014), 'Improving e-Health services and system requirements by modelling the health environment', *Journal of Software*, Vol. 9, No. 5, pp. 1189-1201.

Aware, W.T.A. (2006), 'Unapproved DRAFT standard for systems and software engineering-life cycle processes-risk management (Revision of ISO/IEC 16085 IEEE Std 1540-2001 First edition 2004-10-01),' IEEE Std P16085/D3.

Blobel, B. (2007), 'Comparing approaches for advanced e-health security infrastructures', *International Journal of Medical Informatics*, Vol. 76, No. 5-6, pp. 454-459.

Caballero, A. (2014), 'Information security essentials for IT managers: protecting mission-critical systems', in Vacca, J.R. (Ed.), *Managing Information Security* (2nd ed.), Syngress, Waltham, MA, pp. 10-16.

Demarco, T. and Lister, T. (2003), 'Risk management during requirements', *IEEE Software*, Vol. 20, No. 5, pp. 99-101.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á. and Toval, A. (2013), 'Security and privacy in electronic health records: a systematic literature review', *Journal of Biomedical Informatics*, Vol. 46, No. 3, pp. 541-562.

Liu, L., Yu, E. and Mylopoulos, J. (2003), 'Security and privacy requirements analysis within a social setting', *Proceedings of the 11th IEEE International Requirements Engineering Conference*, Monterey, CA, pp. 151-161.

Mouratidis, H., Giorgini, P. and Manson, G. (2003), 'Integrating security and systems engineering: towards the modelling of secure information systems', *Proceedings of the 15th Conference on Advanced Information Systems Engineering*, Velden, Austria, pp. 63-78.

Muñoz, P., Trigo, J.D., Martínez, I., Muñoz, A., Escayola, J. and García, J. (2011), 'The ISO/EN 13606 standard for the interoperable exchange of electronic health records', *Journal of Healthcare Engineering*, Vol. 2, No. 1, pp. 1-24.

Ray, S. and Biswas, G.P. (2014), 'A Certificate Authority (CA),-based cryptographic solution for HIPAA privacy/security regulations', *Journal of King Saud University -- Computer and Information Sciences*, Vol. 26, No. 2, pp. 170-180.

Salini, P. and Kanmani, S. (2012), 'Elicitation of security requirements for e-health system by applying model oriented security requirements engineering (MOSRE) framework', *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*, Coimbatore, India.

Savola, R.M. and Abie, H. (2010), 'Development of measurable security for a distributed messaging system', *International Journal on Advances in Security*, Vol. 2, No. 4, pp. 358-380.

Shoniregun, C.A., Dube, K. and Mtenzi, F. (2010a), 'Introduction to e-healthcare information security', in Shoniregun, C.A., Dube, K. and Mtenzi, F. (Eds.), *Electronic Healthcare Information Security*, Springer, New York, NY, pp. 1-27.

Shoniregun, C.A., Dube, K. and Mtenzi, F. (2010b), 'Towards a comprehensive framework for secure e-healthcare information', in Shoniregun, C.A., Dube, K. and Mtenzi, F. (Eds.), *Electronic Healthcare Information Security*, Springer, New York, NY, pp. 123-150.

Smith, E. and Eloff, J.H. (1999), 'Security in health-care information systems -- current trends', *International Journal of Medical Informatics*, Vol. 54, No. 1, pp. 39-54.

Stanley, A. K. (1997), 'Information security -- challenges for the next millennium', in Yngström, L. and Carlsen, J. (Eds.), *Information Security in Research and Business*, Chapman & Hall, London, UK, pp. 3-8.

Ullah, A. and Lai, R. (2011), 'Managing security requirements: towards better alignment between information systems and business', *Proceedings of The Pacific Asia Conference on Information Systems (PACIS)*, Brisbane, Australia, Paper 195.

Van Lamsweerde, A. and Letier, E. (2000), 'Handling obstacles in goal-oriented requirements engineering', *IEEE Transactions on Software Engineering*, Vol. 26, No. 10, pp. 978-1005.

von Solms, S.H. and von Solms, R. (2009), 'Information security management and information security governance', *Information Security Governance*, Springer, New York, NY, pp. 25-26.

Yu, E.S.K. (1993), 'An organisational modelling framework for multi-perspective information system design', Technical Report DKBS-TR93-2, University of Toronto, Toronto, Canada.

Yu, E.S.K. (1997), 'Towards modelling and reasoning support for early-phase requirements engineering', *Proceedings of the Third IEEE International Symposium on Requirements Engineering*, Annapolis, MD, pp. 226-235.

About the authors

Ahmed H. Alahmadi is a lecturer in the Department of Computer Science at Al-baha University, Saudi Arabia. Currently he is a PhD candidate in the Department of Computer Science and Computer Engineering at La Trobe University, Melbourne, Australia. His PhD research is in e-health business requirements engineering. He has achieved his Bachelor degree in Computer Science from Taibah University, Saudi Arabia, and then achieved his Master's degree in Computer Science from La Trobe University. His research interests include E-health, software engineering, business process modelling, requirements engineering, and process Mining.

Corresponding author. Department of Computer Science and Computer Engineering, La Trobe University, Bundoora, 3086, Australia. Tel: +61-431-678-641. E-mail address: a.alahmadi@latrobe.edu.au

Ben Soh is an Associate Professor in the Department of Computer Science and Computer Engineering at La Trobe University, Melbourne, Australia and a Senior Member of IEEE. He in 1995 obtained his PhD in Computer Science and Engineering at La Trobe. Since then, he has had numerous successful PhD graduates and published more than 150 peer-reviewed research papers. He has made significant contributions in various research areas, including fault-tolerant and secure computing, and web services. E-mail address: b.soh@latrobe.edu.au

Azmat Ullah is with the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne Australia. He received his PhD degree in computer science and computer engineering, from La Trobe University, Melbourne Australia and MSc degree in advanced software engineering, from The University of Sheffield, England, United Kingdom. He has made significant contributions in various research area including E-health, Business-IT alignment, business process management, green computing, software engineering, software processes, requirements engineering, and information system development. E-mail address: a.ullah@latrobe.edu.au