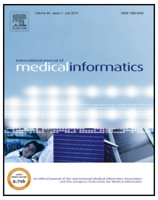
International Journal of Medical Informatics 84 (2015) 941–949

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com



Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template

Ying He[a,*], Chris Johnson[b]

[a] School of Computer Science and Informatics, De Montfort University, UK
[b] School of Computing Science, University of Glasgow, UK

ARTICLE INFO

Article history:
Received 30 December 2014
Received in revised form 18 August 2015
Accepted 19 August 2015

Keywords:
Generic Security Template
Lessons learned
Security incident
Knowledge redistribution
Healthcare

ABSTRACT

Context: The recurrence of past security breaches in healthcare showed that lessons had not been effectively learned across different healthcare organisations. Recent studies have identified the need to improve learning from incidents and to share security knowledge to prevent future attacks. Generic Security Templates (GSTs) have been proposed to facilitate this knowledge transfer. The objective of this paper is to evaluate whether potential users in healthcare organisations can exploit the GST technique to share lessons learned from security incidents.
Methodology: We conducted a series of case studies to evaluate GSTs. In particular, we used a GST for a security incident in the US Veterans' Affairs Administration to explore whether security lessons could be applied in a very different Chinese healthcare organisation.
Results: The results showed that Chinese security professional accepted the use of GSTs and that cyber security lessons could be transferred to a Chinese healthcare organisation using this approach. The users also identified the weaknesses and strengths of GSTs, providing suggestions for future improvements.
Conclusion: Generic Security Templates can be used to redistribute lessons learned from security incidents. Sharing cyber security lessons helps organisations consider their own practices and assess whether applicable security standards address concerns raised in previous breaches in other countries. The experience gained from this study provides the basis for future work in conducting similar studies in other healthcare organisations.

1. Introduction

Security incidents have affected healthcare organisations across the world. For example there are strong similarities between the US Veterans' Affairs Administration (VA) 2007 data loss incident [1], the Shenzhen 2008, the Chinese data loss incident [2] and the UK National Health Service (NHS) Surrey security Asset disposal incident [3]. However, these examples are just the tip of the iceberg. Symantec reported that the healthcare industry accounted for 36% of all security incident breaches in 2013 [4]. At 44%, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industries in 2014 [5]. Such incidents can result in the loss of company/organisational reputation and customer confidence, legal issues, a loss of productivity and direct financial losses [6]. The focus in Healthcare 'lessons learned' and information exchange has been on safety [7–13] rather than security [14–16].

Governments have realised the importance of learning from security incidents. A number of initiatives support the exchange of information about previous breaches. For example, the UK government has launched the Cyber Security Information Sharing Partnership (CISP). This is intended to help government and industry share and redistribute intelligence on cyber security threats. The partnership includes the introduction of a secure virtual 'collaboration environment' where stakeholders can exchange information on threats and vulnerabilities in real time [17]. There is a need to foster an environment where different parties can speak the same language while redistributing this information.

The recommendations and insights derived from previous security incidents are usually disseminated through a series of formal and informal reports, meetings and presentations to management [18,19]. For example, NHS disseminates lessons learned from security incidents using team meetings, notice boards, incident reporting and investigation training courses (e.g. use of case studies), email, newsletter, internal alert systems and so on [20].

[*] Corresponding author.
E-mail address: ying.he@dmu.ac.uk (Y. He).

http://dx.doi.org/10.1016/j.ijmedinf.2015.08.010
1386-5056/© 2015 Elsevier Ireland Ltd. All rights reserved.

Meetings are held and notes are gathered to document responses, disagreements, suggestions and additions to security policies and incident procedures [18]. Issues to document include the effects of the damage, actions taken during the incident, policies and procedures that require a change and evidence that can be used for pursuing the responsible person(s) [21]. It is expected that healthcare organisations will act on these lessons, for instance by changes in procedures or training processes and incident response policies. However, previous case studies show that security lessons have not been effectively redistributed within many organisations [22–24].

Generic Security Templates [25] have been developed to represent lessons learned from security incidents. They extend the application of the existing Goal Structuring Notation (GSN) [26] to support the exchange of lessons learned in the aftermath of data breaches. GSTs represent the links between particular findings and the requirements of security standards and policies at a level of abstraction that is intended to support reuse. In this paper, we conducted a series of studies to evaluate whether users can exploit GSTs to redistribute lessons learned from a specific security incident from the US Veterans' Affairs Administration into a healthcare organisation in China.

The remainder of the paper is structured as the following. Section 2 reviews related work. Section 3 introduces GSTs. Section 4 presents our first evaluation of this approach, GST acceptance testing. Section 5 presents a second evaluation, the implementation of the approach within a Chinese healthcare organisation. Section 6 discusses the findings, and Section 7 summarises conclusions and future work.

2. Related work

2.1. Incident learning

A key activity in Security Incident Response and Handling (SIRH) is to learn from errors or mistakes made during previous incidents. It is important to identify policies and processes that undermine existing defences. It is also important to identify any weaknesses in staff competency. These insights must then be fed-back into security management processes [18,19]. Recent studies have provided rich controls for preventing information security threats and vulnerabilities, including technical countermeasures (e.g., anti-virus software tools), and organisational defences (e.g. security standards). However, reflection on security incident response is typically limited to the technical process and does not leverage opportunities to learn about the security threat environment and the effectiveness of internal procedures, controls, training and policies in order to strengthen the organisation's information security management systems [27,28]. There is relatively little research into effective means of disseminating security recommendations and best practices between organisations. The lessons from previous security incidents contain rich information about the causes of previous breaches. Failure to learn from previous incidents seems to be a common trait across many different kinds of security incidents [23].

2.2. Incident learning in healthcare

The loss of patient data can affect both the individuals' concerned and healthcare organisations responsible for securing that data. If a patient's information is disclosed accidentally or unintentionally, it may constitute an infringement of privacy. Disclosure can cause embarrassment. It may also have an impact on an individual's career. The loss of patient data can have other long-term financial implications, including the loss of health insurance [29]. Data can also be sold on to other criminals, for example to support identity theft. From the perspective of healthcare organisations, security incidents can cause significant damage to reputation. They may also lead to fines, for instance under the new European Commissioners' Data Privacy Directive (Directive 95/46/EC) [30]. Therefore it is imperative for healthcare organisations to learn the lessons that have been identified following previous incidents and take actions to prevent any recurrence.

In Europe and North America, there are legislative requirements to report security incidents [20,31,32]. A key aim of incident reporting is to prevent any future recurrence of previous incidents not only in the organisation where the incident occurred but in other healthcare institutions [20]. In China, there have not been legislative requirements for healthcare organisations to report or exchange security incidents. Partly in consequence, information security has not attracted significant attention from healthcare providers [33,34], although some attempts have been made to protect patient data [35–38]. Gao suggests two main reasons for the lack of motivation: (1) the Chinese traditional culture does not address the importance of personal privacy; and (2) healthcare systems in China are still in their infancy and there has not been large-scale health data exchange that can potentially trigger large amounts of privacy violations [39]. However, the implementation of healthcare information systems can hardly be successful if information privacy cannot be ensured [40]. There is a need to learn successful practices from international experience to improve healthcare security management systems [39].

3. Generic Security Templates (GST)

This section introduces GSTs and related work. GSTs build on previous research into safety assurance cases [41]. Instead of collecting evidence to argue that the design and operation of an existing application is acceptably safe, GSTs collect the insights that have been derived when a system has proven NOT to be acceptably secure. They represent security lessons (i.e. information about the causes of a breach and subsequent recommendations) from previous incidents and map them to the requirements of healthcare information security management systems.

3.1. Definition of the Generic Security Template

A *Generic Security Template* is "a documented body of lessons identified from a security incident that is intended to provide feedback about the implementation of specific security standards or guidelines" [25]. The GST links the analysis of an incident to specific security standards or guidelines that help to implement particular recommendations. Fig. 1 provides a customised Goal Structuring Notation from the domain of safety analysis for our cyber security GSTs. There are four principal syntactic components, A *Goal* is a claim, the statements that the goal structure is designed to support. *Lessons learned* exist to support different levels of goals. It refers to the security issues (causes of a security incident); and the security recommendations that are intended to avoid any recurrence of a data breach [25]. *Strategy* is inserted between goals at two levels of abstraction, to explain how the top-level goal is addressed by the aggregation of sub-goals. *Context* is used to declare supplementary information and provide adequate understanding of the context surrounding the claim/strategy. Usually it presents concepts clarification introduced in the claim/strategy [42]. Examples of the application of GSTs can be found in [25,43–45].

3.2. Represent security lessons using the GST

GSTs provide a graphical overview of the mapping between the causes/recommendations derived from security incidents and the guidelines/policies/standards/regulations that are intended to