Health IT Security Journal

Volume 1, No. 2

A publication of the HITSF

Does securing healthcare's Big Data require Big solutions or just Big thinking?

Security requirements elicitation process for hospital information system using SQURE methodology

Health IT Security Journal

Volume 1, No. 2

HITSF

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Letter from the editor

Dear readers,

This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

www.healthitsecurity.org

IN THIS ISSUE

Does Securing Healthcare's Big Data Requires Big Solutions or Just Big Thinking?

by Eric Vanderburg

Many recent innovations both in healthcare and other industries have been geared around the concept of big data. Big data is a collection of data that is so vast that it cannot be managed using traditional data management tools such as mainstream Database Management Systems (DBMS). Big data solutions try to find meaning in this vast and seemingly unmanageable collection of data. In healthcare, this information can be analyzed to identify ways to improve patient care, employee morale, operational efficiency or to provide new healthcare services.

Healthcare organizations are collecting more and more information in the course of doing business and this continues to grow. In fact, IBM estimates that 90% of the data that currently exists was created in the last two years. Much of this data would be created with or without big data solutions and this vast amount of data must be managed.

However, big data solutions interface with much of this data meaning that the system itself has a level of access to a wide variety of data sets. This presents a central place where a data breach would potentially have the greatest data breach impact. Big data security cannot be optional for the risks of a data breach are too great. However, some wonder if the cost of adequate security might negate the positive aspects of big data solutions? After all, it would be simple to conclude that big data requires big security but this is not necessarily the case.

These five strategies can help you secure big data without exorbitant expense. The strategies are designed to be implemented along with the big data solution to take advantage of tasks that would already be required and to avoid modifying a big data solution after it has already been put in place. It is much easier to build security in from the beginning than to add it on later.

1. Work with knowledgeable experts to understand your company's obligation to protect Protected Health Information (PHI). This will differ based on the country you do business in. Establish data protection standards and policies to control access and use of PHI.

2. Big data projects must interface with many different data sources such as log files, relational databases, flat files, loose files and binary data. The first step in securing this data is to understand what data the organization has. This will be required to implement the big data project so security professionals should work with big data implementers to collect this data. Inventory data sources, especially those that contain PHI then determine who is responsible for that data and then ensure that standard security controls as outlined in the first step are implemented for the data. Don't try to do it all yourself. Rather, let the policy and standard guide the data owner's implementation of controls for specific data sources or applications. Often, big data implementations require changes to be made to data sources so this is the perfect time to implement security controls since the systems are already being modified.

3. Establish incident response plans or breach response plans for handling types of data breaches. Consider who would need to be contacted in a breach and how the breach would be contained.

4. Consider implementing Data Loss Prevention (DLP) solutions to track and restrict the flow of PHI. Both open source and enterprise DLP solutions are available depending on your skill set and budget.

5. Encrypt communications between data sources and the big data system and data that is stored by the big data system. Analyzing big data will require significant effort with or without security. However, if just a little more time is given to the project, security can be built into the implementation. Use these five steps to implement a secure big data solution today and realize the benefits big data has for healthcare.

About the Author:
Eric Vanderburg

Director, Information Systems and Security,
JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

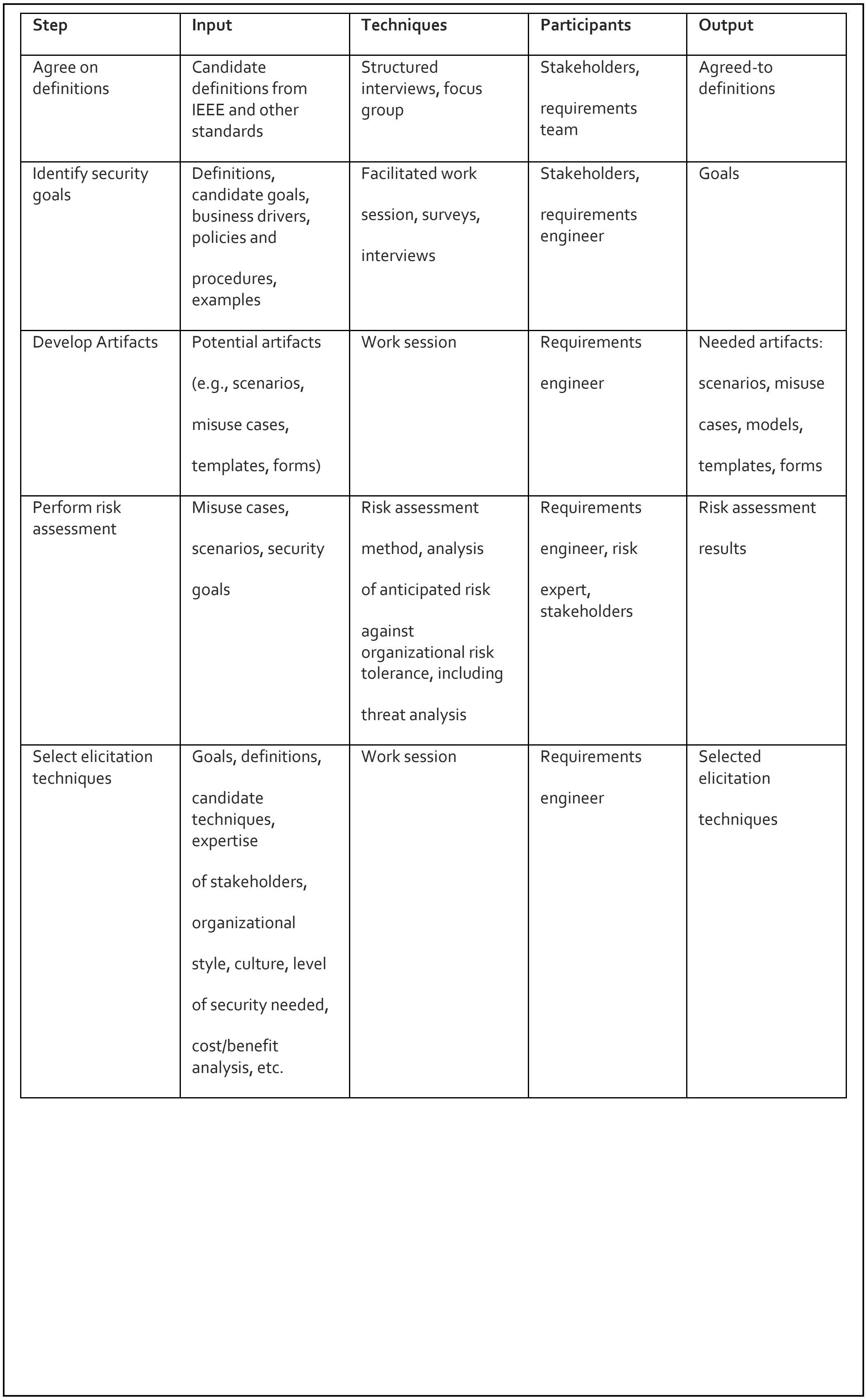
Security Requirements Elicitation Process for Hospital Information System Using SQUARE Methodology

by Hadi Syahrial

Complexity of hospital information systems leads to security vulnerabilities. Security requirements elicitation is important during the early stages of the hospital information system development life cycle because it determines whether the system is vulnerable to future attacks when it is exposed to the real world. Instead, security requirements are usually prepared after a product is finished. SQUARE methodology is an approach to elicit security requirements at the early stages of the system development.

Security Quality Requirements Engineering (SQUARE) is a process aimed specifically at security requirements engineering. The SQUARE methodology was developed by cyber security lab in Carnegie Mellon University to support the nine-step Security Quality Requirement Engineering process. This process includes sub-processes and techniques to improve requirement identification, analysis, and specification. It also focuses on management issues associated with the development of good security requirements.

SQUARE steps:
1. Agree on definitions
2. Identify security goals
3. Develop artifacts to support security requirements definition
4. Perform risk assessment
5. Select elicitation techniques
6. Elicit security requirements
7. Categorize requirements
8. Prioritize requirements
9. Requirements inspection



Step	**Input**	**Techniques**	**Participants**	**Output**
Agree on definitions	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Stakeholders, requirements team	Agreed-to definitions
Identify security goals	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Stakeholders, requirements engineer	Goals
Develop Artifacts	Potential artifacts (e.g., scenarios, misuse cases, templates, forms)	Work session	Requirements engineer	Needed artifacts: scenarios, misuse cases, models, templates, forms
Perform risk assessment	Misuse cases, scenarios, security goals	Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis	Requirements engineer, risk expert, stakeholders	Risk assessment results
Select elicitation techniques	Goals, definitions, candidate techniques, expertise of stakeholders, organizational style, culture, level of security needed, cost/benefit analysis, etc.	Work session	Requirements engineer	Selected elicitation techniques

At present, there is no consensus on a single best approach to security requirements engineering. However, many organizations intuitively feel that attention to this area will pay off in supporting their business goals.

Step	Input	Techniques	Participants	Output
Elicit security requirements	Artifacts, risk assessment results, selected techniques	Accelerated Requirements Method (ARM), Joint Application Development (JAD), interviews, surveys, model-based analysis, checklists, lists of reusable requirements types, document reviews	Stakeholders facilitated by requirements engineer	Initial cut at security requirements
Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints	Initial requirements, architecture	Work session using a standard set of categories	Requirements engineer, other specialists as needed	Categorized requirements
Prioritize requirements	Categorized requirements and risk assessment results	Prioritization methods such as AHP, Triage, WinWin, etc	Stakeholders facilitated by requirements engineer	Prioritized requirements
Requirements inspection	Prioritized requirements, candidate formal inspection technique	Inspection method such as Fagan, peer reviews, etc.	Inspection team	Initial selected requirements, documentation of decision-making process and rationale

About the Author:

Dr. Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.