2011

An agile IT security model for project risk assessment

Damien Hutchinson
Deakin University

Heath Maddern
Deakin University

Jason Wells
Deakin University

DOI: 10.4225/75/57b53294cd8be
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

AN AGILE IT SECURITY MODEL FOR PROJECT RISK ASSESSMENT

Damien Hutchinson, Heath Maddern, Jason Wells
School of Information Technology, Deakin University
drh@deakin.edu.au, hmma@deakin.edu.au, wells@deakin.edu.au

Abstract

There are two fundamental challenges in effectively performing security risk assessment in today's IT projects. The first is the project manager's need to know what IT security risks face the project before the project begins. At this stage IT security staff are unable to answer this question without first knowing the system requirements for the project which are yet to be defined. Second organisations that deal with a large project throughput each year find the current IT security risk assessment process to be tedious and expensive, especially when the same process has to be repeated for each individual project. This also makes it difficult for an organisation to prioritise which projects require more investment in IT security in order to fit within budget constraints. This paper presents a conceptual model that is based on an agile approach to alleviate these challenges. We do this by first analysing two online database resources of vulnerabilities by comparing them to each other, and then compare them to the agile criteria of the conceptual model which we define. The conceptual model is then presented and an example is given of how it can be applied to an actual project. We then briefly discuss what further work needs to be done to implement the conceptual model and validate it against an existing IT project.

Keywords
Project Management, IT Security, Agile, Risk Assessment

INTRODUCTION

Effectively assessing IT security risk is an important part of today's IT projects to manage the increasing number of IT security risks to an organisations' production environment. Assessing the security risks involved in an IT project is time consuming and often relies on the expert knowledge of IT security specialists to identify the security risks.

Project managers often require IT security personnel to identify the IT security risks involved at the start of a project and recommend security controls to mitigate those risks, but IT security is unable to do so without knowing the project system requirements. IT security requirements may not be realised until after the analysis and design phase is complete.

Assessing IT security risks at this late stage can unexpectedly increase the projects budget and time until completion. This is also problematic for an organisation with a large yearly project throughput that is required to go through the process of performing IT security risk analysis and identify security control mechanisms for each project individually. This process becomes time consuming and costly when you consider a more agile IT security model could be employed that quickly identifies the IT risks to a project and recommends security controls to mitigate those risks. Such a model could then be used to compare the IT security threat level facing each project and allow the organisation to prioritise funding to projects with a greater level of IT security risk. The aim of this research is to develop an agile model for the assessment of security risk for IT projects.

When assessing IT security risks for IT projects we considered that IT projects can involve a broad range of information assets. To fit in with the agile model we defined four categories of information assets including application, network, system, and desktop. When referring to one of these within this paper, the intended meaning of each of these categories is as follows:

- Application projects: Projects that involve the building or maintaining of individual pieces of software
- Network projects: Projects that involve the building or maintaining of a network
- System projects: Projects that involve the building or maintaining of an operating system that applications run on
- Desktop projects: Projects that involves the building or maintaining of local client machines

Research Methodology

The following steps were used in the research and eventual design of an agile IT security assessment model:

Step 1: Literature survey.

A literature survey was undertaken to find out what IT security risk assessment methodologies and frameworks already existed for projects. The strengths and weaknesses identified were then compared to the current issues facing IT security risk assessment.

Step 2: Research into available vulnerability databases.

For an agile IT security risk assessment model to work it needs to identify the risks involved in an IT project. It would be particularly inefficient for these risks to be entered manually as there are thousands of potential risks involved in IT projects. Therefore an investigation was undertaken to determine whether any freely available vulnerability databases existed that could potentially be used in the model. Through this process two existing vulnerability databases were discovered. The features of each database were then compared to discover which is more suitable for the agile IT security risk assessment model.

Step 3: Design of an agile IT security risk assessment model.

The design of the agile IT security risk assessment model needed to take into account the agile criteria defined for the model, and the vulnerability database that would be used to populate the model. Considering these components as key inputs to the design, a database schema was developed to represent the initial design of the agile model. The design also included the process an organisation will go through using the model to assess IT security risks for a project.

Step 4: Validation of agile IT security risk assessment model.

The agile IT security risk assessment model then needs to be validated. Validation is performed by comparing the model against a real world test-case example. The test-case will test at least two of the four IT project types, such as application and network. The model will follow the test-case and attempt to identify the IT security risks involved in the project. The identified risks can then be compared with the actual risks found in the project/test-case. If the results from the agile model match the test-case solution then the model is a success.

Background

This literature review considered some of the IT Security Management methodologies and frameworks relevant to the development of our conceptual model. We looked at IT security risks, how they can be assessed, and discovered that mitigation is the preferred method for reducing the level of risk facing a project. We identified that currently IT security risk assessment can only be achieved during or after the systems analysis phase of a project and that a more flexible process is needed to identify the risks involved during the initialisation stage of a project.

IT Security Risk

According to the NIST (National Institute of Standards and Technology) Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002) risk is defined as being a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation. Therefore to give an example of a realised IT security risk, a computer hacker (threat) is able to gain backdoor access to an organisation's internal network through an unprotected port (vulnerability) and is then able to collect highly sensitive information (reputational damage to the organisation).

To measure the level of risk the general consensus is you take into account the organisational asset being targeted, the system vulnerability, and the potential threat that can exploit that vulnerability (Cui & Zhang, 2008; Otuteye, 2003; Yazar, 2002). This can be written as a simple formula of Risk = Asset x Threat x Vulnerability (Yazar, 2002). Although the principle of determining risk is the same you can have slightly different formulas for working out risk depending on the IT field the organisation is working within.

In A Systematic Approach to E-Business Security (Otuteye, 2003) the IT field is E-Business where Otuteye suggests that the formula for determining the level of risk is Risk = (Threat x Vulnerability x cost of business disruption) / (cost of countermeasure). Here it can be argued that there is a greater emphasis for cost of business disruption for online business than in other IT environments. It is expected that e-businesses are online 24/7/365

days in a year so any disruption, even if the business is offline for a couple of hours, can cause significant harm to the business.

The Verizon process for measuring risk is called the Risk Exposure process where a numerical point based system is used to determine what category a potential risk should be catalogued in, either "high", "medium", or "low". The analysis uses five categories to help identify the threat level: the potential exploit threat, skill level required by the attacker, probability of attack occurring, level of risk to asset, and the value of asset(s) to the business (Gerschefske, 2006). An example of Verizon's complex risk analysis process is illustrated in figure 1.

The problem facing this process however is that identifying IT security risks becomes time consuming and the information required to perform the complex risk analysis process can only take place after system requirements analysis. This is not suitable for an organisation with a large project throughput that needs to know the IT security risks involved with a project before the project commences.

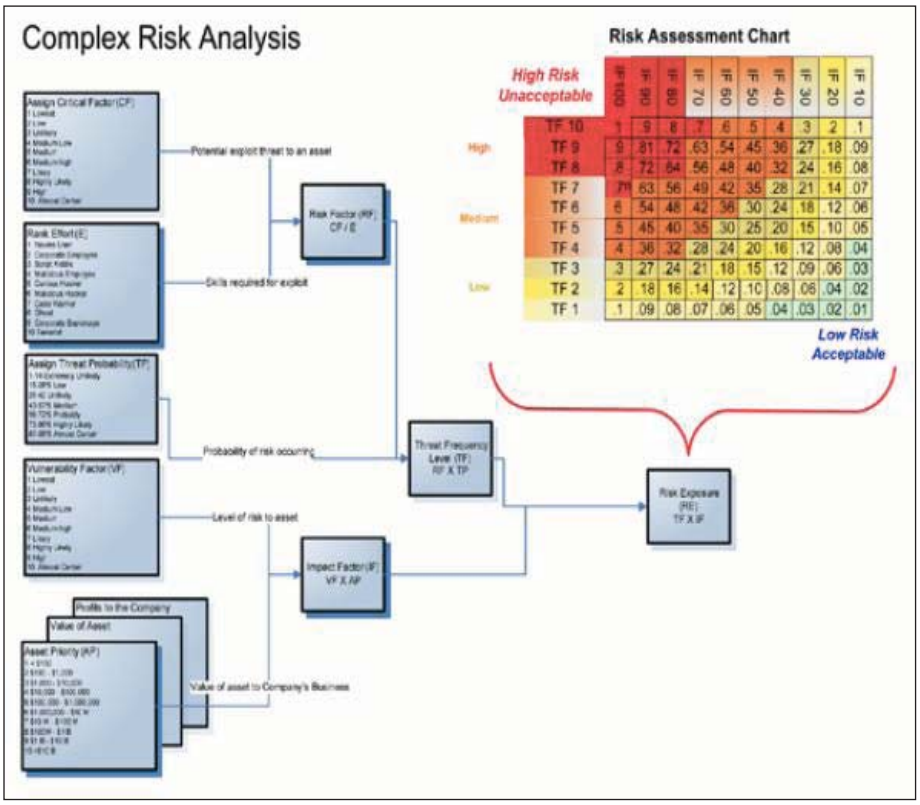

Figure 1. Complex Risk Analysis process used at Verizon (Gerschefske, 2006).

Information Security Management Frameworks and Methodologies

The work by Vermeulen & von Solms, (2002) proposes an information security management framework and accompanying information security management methodology. The framework, shown in figure 2, outlines the importance of "Top Management Commitment" and "Information Security Standards" being the initial elements that must be in place before an information systems project can commence. "Organisational Aspects" and "Security Vision and Strategy" are preparation elements that form the introductory stage to a project.

Figure 2. Vermeulen & von Solms proposal of an information security management framework (Vermeulen & von Solms, 2002).

They are all important elements for an information security management framework but the critical element is having a set of information security standards. Having these will help speed the process of identifying the set of security controls that need to be implemented from the beginning of a project. It also provides improved consistency of security for baselining production environments for current and future projects undertaken by the organisation.

In addition the information security management methodology proposed by Vermeulen & von Solms, (2002) shown in figure 3, outlines the need of having security specific tasks throughout the development lifecycle of a project including the Introductory, Initial, Analysis, Development, Implementation, and Continuation phases. As depicted in figure 3, determining the information security requirements task is performed during the analysis phase once the overall project requirements can be scoped out. This however introduces the same problem where IT security risks need to be identified before the project commences and not during the analysis and design phase.

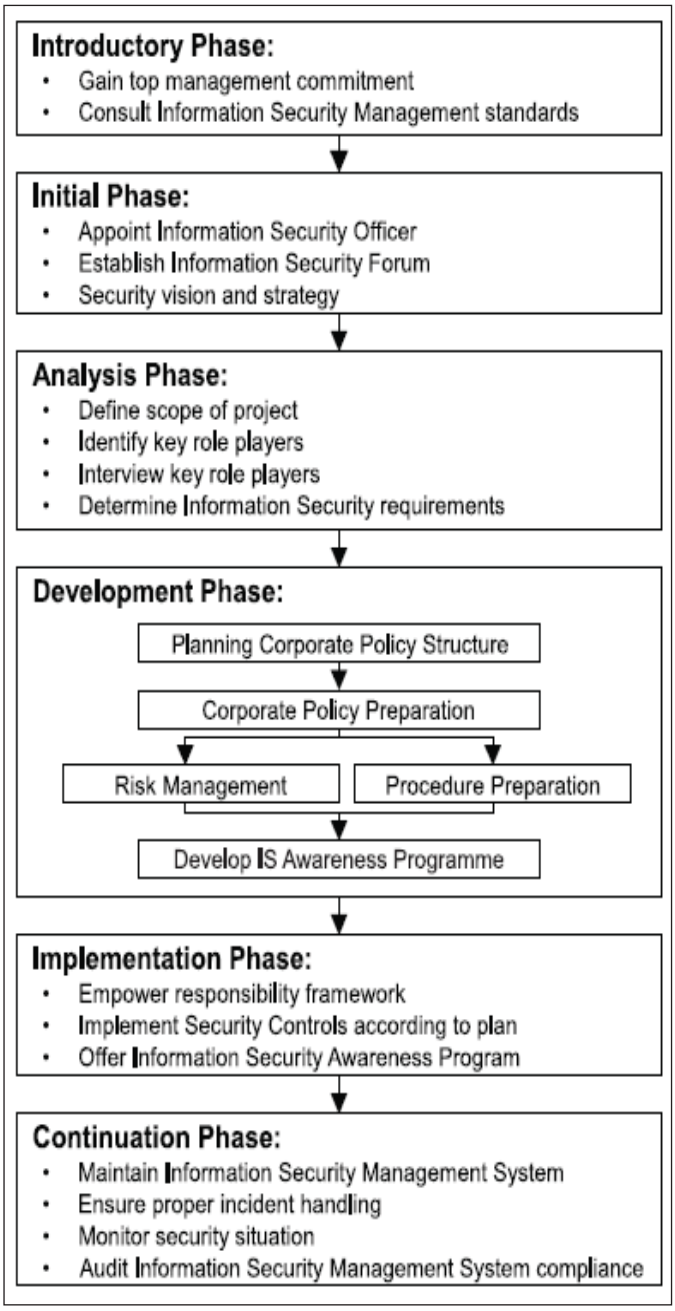

Figure 3. Vermeulen & von Solms proposal of an information security management methodology (Vermeulen & von Solms, 2002).

An assessment framework for enterprise level IT risks is discussed in Azizi & Hashim, (2010). The framework is called the Enterprise IT Risk Management (EIRM) framework and is structured into five risk components based on the enterprise level including "Infrastructure Development and Support", "Operations and Maintenance of Business Process Related Software & Hardware", "Office Level Support", "Software Development", and "Outsourcing Management", as illustrated in figure 4. Although some of the elements of this framework are beyond the scope of this research the way the framework is structured has the potential to group IT security risks based on the type of project, such as application, system, network, or desktop. This would then allow the project manager to focus solely on the IT security risks facing their project. For example the manager of a project for developing a new application would only need to look at the security risks associated with application based projects.

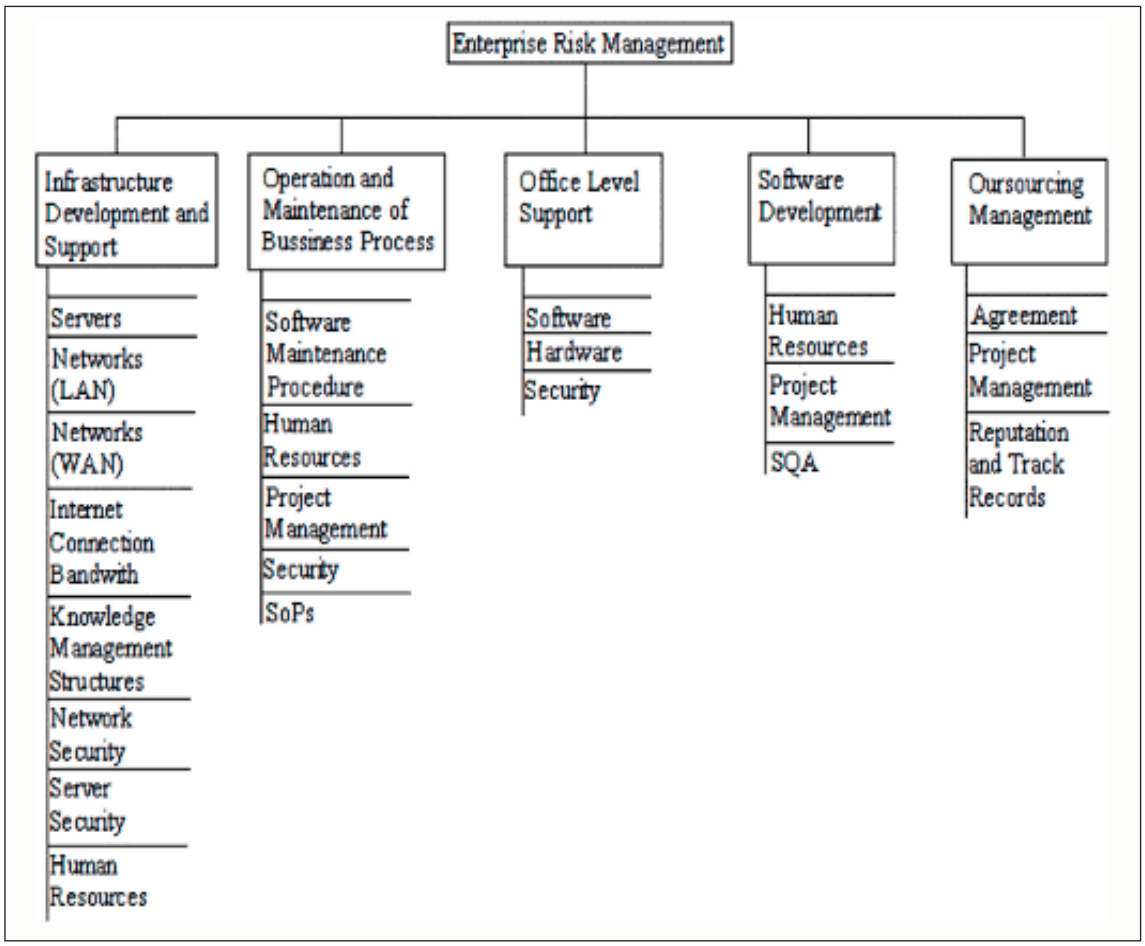

Figure 4. Azizi & Hashim proposal of an assessment framework for enterprise level IT risks (Azizi & Hashim. 2010).

There are two security requirements analysis methodologies proposed by Cui & Zhang, (2008). The first methodology is called Modeling System Requirements, and focuses on the use of graphical models to represent the vulnerabilities and threats that face a system. Their method for modelling the system allows them to identify the people involved in the system as well as the key components of the system and how they all communicate, relate, and depend on each other. The Goals (such as backup data), Resources, Soft Goals (security requirements such as integrity), and Tasks can be connected to each of the major components of the system.

After all dependencies and related tasks are identified, a hypothetical "what if" scenario can be drawn for each individual asset of the system. A "what if" scenario could be if an information asset was compromised and became the attacker. For instance figure 5 shows that if the "Storage Server" became the attacker they could steal data, modify data, leak out data and security requirements such as data security, consistency of data, confidentiality of data and data integrity would be compromised. Such a visual presentation has the benefit for non-technical stakeholders such as project managers to understand the importance of IT security and the potential risks that are faced within their project. However the same problem still arises in that system requirements need to be known first before IT Security staff can identify the risks involved and propose appropriate security controls to mitigate those risks.

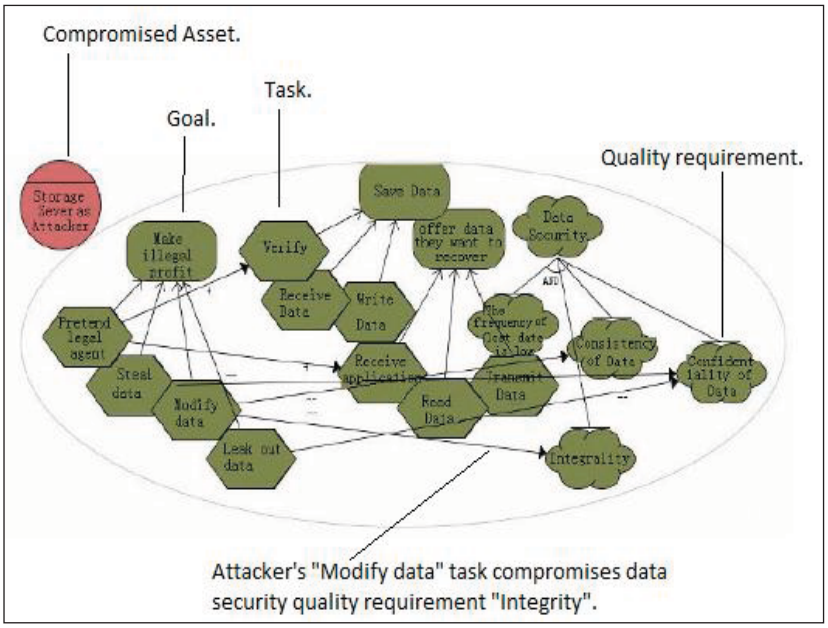

Figure 5. Storage server as attacker (Cui & Zhang, 2008).

The second methodology proposed by Cui & Zhang, (2008) is called Engineering Security Requirements and uses written documentation to represent the vulnerabilities and threats that face the system. It comprises eight individual steps including, Agree on Definitions, Identify Security Goals, Develop Artifacts (such as system architecture diagrams, use/misuse cases, attack trees), Perform Risk Assessment, Select Elicitation Techniques, Elicit Security Requirements, Categorise and Prioritise Requirements, and finally Repository Improvement.

The advantage of this methodology is that it encourages input by all stakeholders not just necessarily those involved directly with implementing IT security. For example in step two "Identify Security Goals" stakeholders are encouraged to list 6-10 security goals that they feel are most important to their role in the business, then requirement engineers give their suggestions to the security goals, and finally an agreed upon list of prioritised security goals is made.

However the process is tedious, involves onerous documentation, eight steps to complete, and relies on the cooperation and availability of numerous stakeholders. With an organisation that has a large IT project throughput, such a methodology becomes too costly and time consuming to implement.

IT security risk methodologies such as the ISO 27005 and OCTAVE standards were also considered (Alberts & Dorofee, 2008; ISO, 2011). However these well-established security risk standards still introduce the same limitations presented throughout the literature review. In particular, IT security risks can only be identified once the analysis and design phase of a project takes place. This prevents the organisation and project manager from knowing the IT security risks involved with a project before project commencement. The IT security risk analysis process is also time consuming and costly for an organisation with a large project throughput.

Tool/toolbox Prototypes

Information security management tool/toolbox prototypes were proposed by both Azizi & Hashim, (2010) and Vermeulen & von Solms, (2002). Although the prototype by Azizi & Hashim, (2010) is a working piece of software and the one by Vermeulen & von Solms, (2002) is a conceptual model, they both share similarities in providing the use of a questionnaire to complete in order for the tool to produce an outcome. The outcome produced in the prototype by Azizi & Hashim, (2010), shown in figure 6, is a graphical representation of the level of risks present for different components of the project and allows the user to select the most "at risk" components to assign appropriate mitigation steps. A graphical representation of the level of risk present in each project would be beneficial for our future research as it gives a clearer picture to non-technical stakeholders of which projects present a greater risk and therefore would require greater awareness, mitigation or funding. However this is something to consider in the future and is beyond the scope of the current research.

Figure 6. Risk levels representation (Azizi & Hashim, 2010).

The conceptual model by Vermeulen & von Solms, (2002) produces a list of recommended "Information Security Policy Statements", "Safeguards", and "Security Procedures" based on the user input into the questionnaire. A similar questionnaire based system, like the ones used in both prototypes, could potentially be employed to help organisations identify and prioritise which security risks are most important to their project. This could be achieved by having the project manager answer a series of project risk and IT security related questions which could then be processed to determine the vulnerabilities that relate to the project.

Through analysis of the literature, our proposed model will need to align with the initialisation stage of the project so IT security risks and risk mitigation options can be identified at the beginning of the projects' development lifecycle. This model will also need to allow for easier understanding by both technical and business staff so all stakeholders involved with the IT project have a clear view of the IT security requirements at the beginning of the project.

DEVELOPMENT OF CONCEPTUAL MODEL

To be agile the model needs to be accommodating to a variety of IT organisations. These organisations may differ in the types of IT projects they develop and project methodologies they use. In collaboration with an IT security manager of an organisation with an annual throughput of 40-50 projects, the challenges of IT security risk identification and management for projects were discussed. Through these discussions and background literature that reinforced these challenges in practice, a set of agile criteria was identified for inclusion in the design of an agile model. The agile criteria are as follows:

- The conceptual model can be used in a variety of industry standard project methodologies such as Prince2 (ILX Group, 2011).
- IT security risks can be identified:
  - At the start of a project before system requirements analysis takes place.
  - When new features are added later in the project's development lifecycle.
  - For application, network, system, and desktop based projects.
  - For new, upgrade, and infrastructure related projects.
  - Based on how risk determination and development questions are answered.
- IT security risks can be measured based on their likelihood and impact to the project.
- Security controls can be recommended immediately after IT security risks have been identified.
- The conceptual model can be understood by both technical and business personnel.

The development of the agile model requires several components including the design of a database schema to represent the data structure, the discovery and selection of an appropriate vulnerabilities database which can be used to populate the agile model, and the design of risk determination and development questions, so it is possible to identify potential risks based on the questions answered. In this section we first identify two vulnerability databases to determine which provides the best match to meet the defined agile criteria. Second we determine the relationship between the two databases and the agile criteria we have defined, and third we give an illustration of the initial design of the agile model in the form of a database schema. Finally we demonstrate the process of how the agile model can be applied to perform IT security risk assessment.

Identification of Vulnerability Databases

An online search was performed to discover existing threat and vulnerability data that is publicly available, currently being maintained, and could be used in the design and future implementation of the conceptual model. Two online sources were found and are presented briefly in this section. The first online resource is called CVE (Common Vulnerabilities and Exposures) and currently has a total CVE listing of 47,422 vulnerabilities. The CVE is available for download in several file formats including XML, HTML, Text and Comma-Separated (CVE, 2011). An online search engine for the CVE list is also available on NIST's National Vulnerabilities Database website (NVD, 2011).

The second online resource is called OSVDB (The Open Source Vulnerability Database) and currently has a total vulnerability listing of 74,627. It provides users with a database schema of how the database is structured and allows users to freely download the database in either CSV (comma-separated values), MySQL or SQLite file formats (OSVDB, 2011). If CSV is selected an SQL script is also provided to import the data directly into a MySQL database. An online vulnerability search of the database is also provided on their website.

Relationship Between Databases and Defined Agile Criteria

From comparing the two databases we discovered that both were equal in how they met the agile criteria we defined, however only two of the agile criteria were met by the resources. These included: 'IT security risks can be measured based on their probability and impact values'; and 'a solution or security control recommendations can be made immediately after IT security risks have been identified'. This further demonstrated the need for the design of an agile IT security model in order to meet all of the defined criteria.

Initial Design of the Agile Model

The first iteration of the conceptual model design is illustrated as a database schema in figure 7.

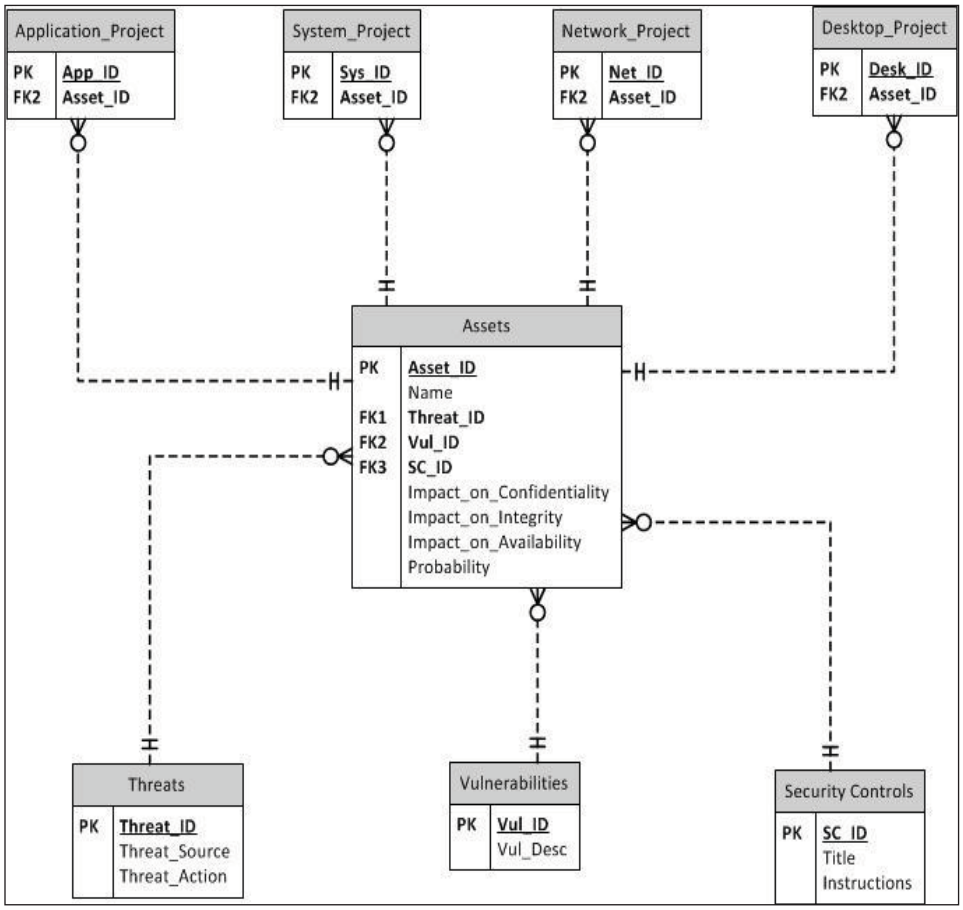

Figure 7. First iteration of conceptual model.

Agile IT Security Model Process

This example demonstrates how the agile IT security model process will work for the proposed development of a new application project. This process occurs during the initialisation stage of a project. At this stage the database OSVDB (Open Source Vulnerabilities Database) is used to populate the Assets, Threats, Vulnerabilities, and Security Control tables. The project manager will have already made a database entry in the Project table giving the project a name, a description of what the project is, if its success depends on the completion of other projects, and listing the project as "new". Once this is complete the following steps take place in order to identify the vulnerabilities and level of IT security risks facing the project. These steps are also illustrated in figure 8.

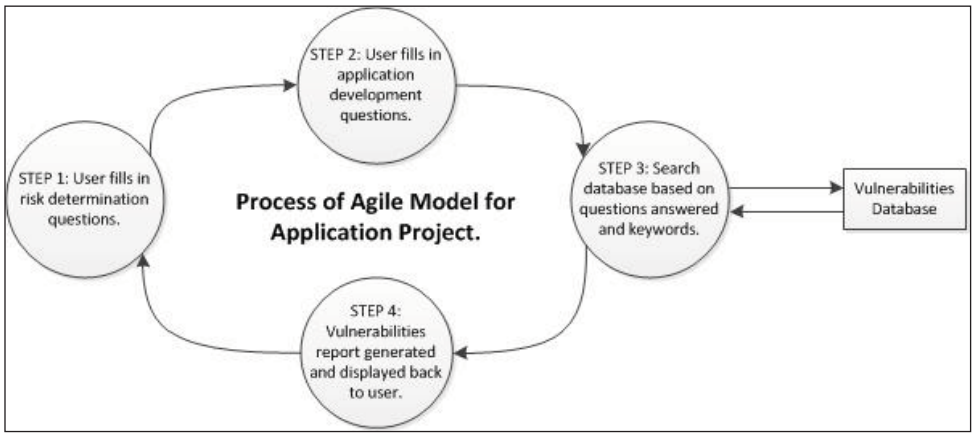

Figure 8. Process for an Application Project.

Step 1: User fills in risk determination questions.

The project manager is asked to fill in a series of project risk determination questions. The answers to these questions will help determine the level of risk facing the project. An example of project risk determination questions is shown in Table 1.

Table 1. Example of risk determination questions.

Technology Scope	Risk Level
What is the scope of your project? (Select One only)	
i) No System Technology change	L
ii) Removing/retiring an existing system	L
iii) Small change required to 1 or 2 systems	L
v) Introduce a new system requiring no changes to existing systems / interfaces	M
vii) Introduce new system and / or make substantial changes to one existing system	H
vii) Introduce new system and remove/retire an existing system	H
Innovation	
What degree of technology innovation does the project require? (Select One only)	
i) No technology	L
ii) Existing technology	L
iii) New technology	M
iv) Developing technology "Leading Edge"	H
v) New technology, "Bleeding Edge"	H

After all questions have been answered the risk level of the project can be determined. A project is considered to be of "high" risk if one or more answers have the Risk Level - H. A "low" risk project will have all answers with a Risk Level - L, and a "medium" risk project is one where the answers do not warrant the label "high" or "low" risk.

Step 2: User fills in application development questions.

The project technical lead is then responsible for answering a series of application development questions. If it was a Network Project then the questions would be network specific. Each question can be answered with a simple "Yes", "No", or "N/A". An example of these questions is shown in Table 2.

Table 2. Example of application development questions (The Santa Fe Group, 2009).

Item	Question/Request	Response
I.2.2	Does the application development process explicitly guard against the following:	
I.2.2.1	Invalidated input?	
I.2.2.2	Broken access control?	
I.2.2.3	Broken authentication?	
I.2.2.4	Replay attacks?	
I.2.2.5	Cross site scripting?	
I.2.2.6	Buffer overflow?	
I.2.2.7	Injection flaws (e.g., SQL injection)?	
I.2.2.8	Improper error handling?	

I.2.2.9	Data under-run / overrun?	
I.2.2.10	Insecure storage?	
I.2.2.11	Application denial of service?	

Step 3: Search database based on questions answered and keywords.

With the questions from Steps 1 and 2 answered, a search of the vulnerabilities database can then take place. This can be done using a keyword search based system where keywords from questions such as (denial of service, authentication, buffer overflow, cross site scripting etc.) can be used to query the database which then returns a list of relevant vulnerabilities to the project. Only keywords from questions that warrant a response will be used. For example if the response to the question "Does the application development process explicitly guard against the following: Cross site scripting?", is No, then a keyword search for "Cross-site scripting", or "XSS attack" is performed. Otherwise no keyword search is made for that question.

Step 4: Vulnerabilities report generated and displayed back to user.

This is the final step of performing IT security risk assessment for a project. Here the resulting list of vulnerabilities from Step 3 is generated into a report and displayed back to the project manager for assessment. The project manager can now measure the overall level of IT security risks facing the project, comparing the results to other projects, and can then prioritise funding to projects with a higher IT security risk level.

The results of the database search can be stored in the Application_Project table, with all discovered vulnerabilities being referenced back to the proposed project. This provides a permanent history of past projects, allowing a project manager to quickly review the IT security risks associated with a similar project, as well as the measures taken to mitigate those risks. Over time the conceptual model grows with the organisation as more projects are entered into the database. This in turn will develop a set of IT security standards that the organisation follows for particular types of projects undertaken.

FUTURE WORK

The next step is to implement and validate the conceptual model. Implementation will involve developing an interface for users to answer the project risk questions, constructing a database based on the conceptual model design and populating it with the OSVDB records. Validating the agile model will require the use of an existing IT project as a test-case, running the agile model against the test-case, and comparing the results to identify if all the IT security risks associated with the project were discovered.

CONCLUSION

There are two fundamental problems in IT security risk assessment for projects today that we try to solve with the proposed conceptual model. The first problem involves the need to know what IT security risks face the project before the project begins, but current methods do not allow for this. The second problem is the tedious and expensive IT security risk analysis process that organisations with a large project throughput have to perform for each individual project. This in turn makes it difficult for organisations with a limited budget to decide which projects to invest more funds into based on their IT security risk level. To help alleviate these issues we proposed an agile IT security model. We identified through a literature survey that currently no agile IT security model exists that allows stakeholders of an IT project to identify the risks involved during the project initialisation stage. The model we present allows for this as well as achieving all the agile criteria we have defined. Finally we presented the next steps that need to be undertaken to realise the benefits of this agile conceptual model to perform risk assessment for IT projects.

REFERENCES

Alberts, C. Dorofee, A. 30 Jan 2001, “An Introduction to the OCTAVE(sm) Method”, Software Engineering Institute – Carnegie Mellon University, Retrieved September 28, 2011, from source http://www.cert.org/octave/methodintro.html#procs

Azizi, N. Hashim, K. 9-11 July 2010 , "Enterprise level IT risks: An assessment framework and tool," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on , vol.3, no., pp.333-336.

CVE, 2011, 'Common Vulnerabilities and Exposures', Retrieved September 12, 2011, from source http://cve.mitre.org/data/downloads/index.html

Gerschefske, M. 2006, 'IT Security Risk Management', Verizon Business, Retrieved September 02, 2011, from source http://www.verizonbusiness.com/resources/whitepapers/wp_it-security-risk-management_en_xg.pdf

ILX Group, 2011, 'Prince2 Process Model', Retrieved September 28, 2011, from source http://www.prince2.com/prince2-process-model.asp

ISO, 2011, "ISO/IEC 27005:2011", International Organization for Standardization, Retrieved September 28, 2011

Jing-Song Cui, Da Zhang, 20-23 Aug. 2008, "The research and application of security requirements analysis methodology of information systems," Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on , vol., no., pp.30-36.

NVD, 2011, 'National Vulnerability Database', NIST, Retrieved September 12, 2011, from source http://web.nvd.nist.gov/view/vuln/search

OSVDB, 2011, 'The Open Source Vulnerability Database', Retrieved September 13, 2011, from source http://osvdb.org/

Otuteye, E. 2003, 'A Systematic Approach To E-Business Security', University of New Brunswick, Canada, Retrieved September 06, 2011, from source http://ausweb.scu.edu.au/aw03/papers/otuteye/paper.html

Stoneburner, G. Goguen, A. & Feringa A. 2002, 'Risk Management Guide for Information Technology Systems', Recommendations of the National Institute of Standards and Technology, Retrieved September 07, 2011, from source http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

The Santa Fe Group, 31 Oct 2009, "Standardized Information Gathering (SIG) Questionnaire v5.0", Shared Assessments Program, Retrieved September 25, 2011, from source http://www.sharedassessments.org

Vermeulen, C. von Solms, R.V. 2002, 'The information security management toolbox – taking the pain out of security management', Information Management & Computer Security, Vol. 10 Iss: 3, pp.119 - 125.

Yazar, Z. 2002, 'A Qualitative Risk Analysis and Management Tool - CRAMM', SANS Institute InfoSec Reading Room, Retrieved September 07, 2011, from source http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83