Global Information Assurance Certification Paper

Simple Technique for Illustrating Risk (STIR)

Abstract

Risk Analysis (or Risk Assessment) is a vital part of any organisation's overall approach to Information Security. It is also a core requirement for the achievement of certification against the recogn ised standards for Information Security Management Systems, namely BS 7799/ISO 17799. There are three traditional approaches to risk analysis that have well-documented shortcomings that may lead to difficulties during implementation. This paper presents a review of these approaches along with a summary of some of the published methods and commercial tools that support them. This paper suggests a Simple Technique for Illustrating Risk (STIR) that has its roots in software development. STIR aids in the vi sualisation of the most important concepts of risk analysis and permits asset owners and security practitioners to discuss risk analysis issues using a common language. STIR may also be used in combination with the traditional approaches described.

Neil Martin

SANS Security Essentials (GSEC) Version 1.3

Table of Contents

Risk Analysis and Risk Management 3
Introduction 3
Assets, Threats and Vulnerabilities 3
Risk and Risk Analysis 3
Risk Management 3
Traditional Approaches to Risk Analysis 4
Quantitative 4
Qualitative 4
Knowledge-Based 4
Contemporary Approaches to Risk Analysis 4
Model-Based 4
Risk Analysis Methods 5
Commercial Tools 5
COBRA Risk Consultant 6
CRAMM V4 6
CSI IPAK 6
Due Care Database 6
RA Software Tool 6
Conclusions 6
Bridging the Gap 7
Introduction 7
Software Development and The UML 8
Risk Analysis and Software Development Parallels 8
Conclusions 9
Simple Technique for Illustrating Risk (STIR) 9
Introduction 9
Method 9
Step 1: Identifying Assets, Threats and Safeguards 10
Step 2: Discovering Patterns 10
Reporting 10
Examples of STIR ATS Diagrams 11
SANS Top Ten Vulnerabilities 11
IPAK Controls 12
Security Project 13
Example Report 14
Conclusions 14
Summary and Conclusions 14
Future Work 15
Theory 15
Named Associations 15
Additional Constructs 15
Practice 15
Usage Envelope 15
References 16

Risk Analysis and Risk Management

Introduction

Assets, Threats and Vulnerabilities

An organisation's value is maintained in its assets. Assets come in a variety of forms ranging from physical (such as buildings, fixtures and fittings) to intellectual (such as ideas, patents and software) to meta-physical (such as brand and reputation).

An asset may have a weakness that leaves it susceptible to damage or attack. This is known as the vulnerability of the asset.

A threat is an event that has the potential to cause harm to an asset. Threats may be natural (such as fire, earthquake and flood) or man-made (such as industrial espionage, theft and malicious damage).

Risk and Risk Analysis

When a threat takes advantage of an asset's vulnerability the asset is compromised. This compromise will affect the confidentiality, integrity or availability of the asset resulting in partial or total loss of value. The loss of value is known as the asset's exposure.

The term 'risk' is used to describe the possibility of this compromise occurring. The process of risk analysis involves identifying and measuring the risk that exists for damage to each individual asset in this complex landscape. Risk analysis has been used for many years in the health, insurance and finance industries. It has been applied to the Information Technology industry in general and the area of Information Security.

Risk Management

The process of risk management involves the definition of an overall strategy to address the risks discovered during risk analysis. A risk may be managed using a combination of three basic approaches: accepting the risk, minimising the risk, transferring the risk.

Accepting the risk involves documenting the fact that no additional effort will be applied to address the risk. Transferring the risk involves passing the responsibility for handling the risk to another party. This may include insuring the asset, or placing the asset under third party protection.

Much of the effort in a risk management strategy will involve minimising risk. In this case a safeguard (or countermeasure) may be employed to protect an asset by: addressing the vulnerability; addressing the threat; reducing the value of the asset.

Given that an asset may be at risk from any number of threat-vulnerability pairs and that there may be any number of safeguards capable of protecting the asset, the aim of risk management is to identify the 'most appropriate' safeguards. The 'most appropriate' safeguards will usually be a combination of the most cost-effective, the timeliest and the most practical. It is a certainty that it will not be possible to implement all of the possible safeguards.

Risk Analysis and Risk Management are subjective processes. In order to successfully identify the risks and create an overall management strategy the security practitioners and the asset owners must communicate effectively.

Traditional Approaches to Risk Analysis

There are three traditional approaches to risk analysis.

Quantitative

Quantitative risk analysis involves taking a number of steps to measure the amount of damage done, ideally in financial terms, to an asset as a result of a compromise. This is repeated with designated safeguards in place to determine the reduction in exposure. The precise number of steps, the measurements required and the algorithms used, depend on the particular method employed and the tool used to support the method. Quantitative risk analysis requires hard facts and figures and is a time-consuming and expensive exercise. Problems with this approach are usually related to the uncertainty in the figures [C&A_1, Power, Schneier].

Qualitative

Qualitative risk analysis provides an easier route for measuring asset values and threat probabilities. These values may be described using simple phrases such as "High", "Medium" and "Low". This approach addresses the shortcomings of the quantitative approach by reducing the uncertainty inherent in the figures.

Knowledge-Based

Knowledge-based risk analysis involves reusing 'best practice' from similar organisations (where similar may relate to size, scope and/or market) and for the Information Security community in general. Some practitioners refer to this as 'good practice' or 'sound practice' since 'best' may not be measurable [Parker].

Contemporary Approaches to Risk Analysis

There is at least one up-and-coming contemporary approach to risk analysis.

Model-Based

In January 2001, the Business and Information Technology Department (BITD) of the Central Laboratory of the Research Councils (CLRC) commenced a project known as CORAS – A Platform for Risk Analysis of Security Critical Systems [BITD]. The aims of this project include the development of a framework for risk analysis based on objected-oriented modelling and the UML in particular. This project is scheduled for completion in June 2003.

Risk Analysis Methods

Some of the methods for risk analysis include:

The Aerospace Risk Evaluation System (ARiES) enhances the Livermore Risk Assessment Methodology (LRAM). Estimates of risk are based on assets, threats, controls (safeguards) and consequences (impacts). Controls may be preventative or mitigative [Summers].

Consultative, Objective and Bi-functional Risk Analysis (COBRA) is a range of risk analysis and review tools [C&A_2]. A major financial institution was involved in its development.

CCTA Risk Analysis and Management Method (CRAMM) is an internationally recognised method for information risk assessment. It is the preferred approach of the UK Government [Summers, Insight].

The Due Care Security Review Method developed by Donn Parker and his colleagues in the Information Security Consulting Group at SRI International, and later at Atomic Tangerine, defines a number of safeguards and control principles that are commonly recommended [Parker].

The Facilitated Risk Analysis Process (FRAP) is a qualitative process developed by Tom Peltier [Peltier_1, ISSA].

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE ^{sm}) is an approach for self-directed risk evaluations that measure against known or accepted good security practices [Carnegie].

The RA Methodology is a modular approach containing a collection of methods and processes that support risk assessment to the standards required by BS 7799/ISO 17799 [AEXIS_1].

Commercial Tools

The following table summarises some the of tool support that is commercially available for some of the risk analysis methods introduced:

Tool\Approach	Quantitative	Qualitative	Knowledge-based
COBRA Risk Consultant	Yes	Yes	Yes
CRAMM V4 CSI IPAK	Yes	Yes	 Yes
Due Care DB			Yes
RA Software Tool		Yes	

COBRA Risk Consultant

The COBRA Risk Consultant is a PC -based expert system that supports a combination of methods for risk analysis [C&A_3].

CRAMM V4

CRAMM, currently at version 4 is a software product that fully supports the CRAMM method [Hinton].

CSI IPAK

The Computer Security Institute (CSI) is the world's leading me mbership organisation dedicated to information security professionals. The CSI publishes an information security program assessment tool known as the Information Protection Assessment Kit (IPAK) [CSI] that provides a starting point for implementation of b est practice. This kit defines 11 critical areas of information security. Twenty important, widely acknowledged controls are defined within each of these areas.

Due Care Database

The Due Care Database is a proprietary checklist available from Atomic Tang erine and describes more than 350 commonly accepted safeguards [Parker].

RA Software Tool

The RA Tool is a Windows -based application that supports the RA Methodology [AEXIS_2].

Conclusions

Quantitative methods for risk analysis demand that particular atten tion be applied to the valuation of assets and the quantification of a number of aspects of the perceived threats. This may be time -consuming and difficult. In practice it may be difficult to place a monetary value on an asset, or to gauge the impact or likelihood of a threat.

Qualitative methods allow the measures to be approximated, thereby reducing the complexity. This approach to risk analysis is most prevalent [Brooke, C&A_1, Synder].

One of the major problems with risk analysis methods is uncertain ty. "Risk is a probability. Security is a probability" [1]. The value of an asset is difficult to quantify, the likelihood of a threat exploiting an asset's vulnerability is difficult to estimate, single or annualised loss expectancy is difficult to calcul ate. People are not good at estimating these values.

Some experienced practitioners have more extreme views. Donn Parker, formerly with Atomic Tangerine, is quoted as follows: "I can assure you that risk analysis or assessment does not work and is mostly a waste of time."[2].

[1] Schneier, p.257.
[2] Power, p.283.

The strength of knowledge -based risk analysis is that it is based upon experience. The experience gained by security practitioners and organisations trying to solve similar problems.

This evidence suggests that a simple technique for risk analysis combining the strengths of knowledge -based and quantitative/qualitative methods will be useful. This technique should support the practical, common sense approach of knowledge -based analysis and also allow the numeric/subjective approach of both quantitative and qualitative analysis to be utilised where appropriate.

Bridging the Gap

Introduction

A risk analysis exercise requires input from many individuals and groups. Management, asset owners, security managers and practitioners will all be involved in the process. These individuals must work together as a team to develop a winning risk management strategy.

Tom Peltier of Netigy Corporation identifies the close working relationship between the risk management team and the business team as one of the factors of a successful risk analysis [Power]. He also states: "To be successful, the needs of the customer must be identified and met. Every time a risk analysis is to be conducted, the risk management professional must meet with the client to determine what is to be reviewed, what kinds of risks are to be examined and what the client needs as a deliverable or results from the process." [3].

Dan Erwin of Dow Chemical agrees: "To perform a risk assessment, the facilitator assembles experts on all elements of the system or process being analysed. It is critical to have the right people involved because they will understand the risks and be able to delineate and document the issues." [4].

It follows from these observations that effective communication of concepts and ideas within the risk management team will be crucial to the success of the exercise.

The basic approaches and many of the methods described earlier require tables of asset, threat, vulnerability and safeguard ratings to be created and cross -referenced. A number of examples of this technique and applications of it are readily available [Bayne, Mina, Rajasingham]. Whilst this does result in documentation of sorts it is difficult to distil these completed tables into a clear picture.

[3] Peltier_2, p.1.
[4] Erwin, p.1.

Software Development and The UML

One of the most fundamental issues in software development projects is the documentation of requirements. Traditionally it was the job of the analyst to discuss the requirements of the system with the business representative and d efine them using a formal method. This would usually result in the creation of a Business or System Requirements document. The developers would design and build the system using this English description of its expected capabilities. Unfortunately, this approach was, and still is, prone to misunderstanding and error. A damning criticism of many software projects is that the delivered system was not fit for purpose [Helms].

The Unified Modelling Language (the UML) is a standard language for writing software blueprints. It may be used to visualise, specify, construct and document software intensive systems [Booch]. One of the basic building blocks of the UML is the Diagram.

A particular type of diagram is the Use Case Diagram. This diagram permits visualisation of the high level functional requirements of the system and is often used as a catalyst for discussion between the business representative and the software architect. The requirements of a system can be described in terms of Use Cases and Use Case Scenarios using a common language understood by both business and technical personnel.

Risk Analysis and Software Development Parallels

There are a number of parallels between the risk analysis and software development landscapes:

Risk Analysis	Software Development
The asset owner has the domain knowledge and experience.	The business representative has the domain knowledge and experience.
The security practitioner has the technical knowledge and experience.	The architect/developer has the technical knowledge and experience.
Each party has their own language for expressing knowledge.	Each party has their own language for expressing knowledge.
Effective communication is key to the process of risk analysis.	Effective communication is key to the process of requirements definition.
Risks must be prioritised.	Requirements must be prioritised.
Risks may be interdependent.	Requirements may be interdependent.

These parallels suggest that it should be possible to borrow the UML Use Case Diagram approach used in software development to express risk analysis findings.

Conclusions

The UML Use Case Diagram is viable as the basis of a common language to aid discussion between security practitioners and management representatives.

Simple Technique for Illustrating R isk (STIR)

Introduction

The purpose of the Simple Technique for Illustrating Risk (STIR) is to provide a technique to support the visualisation and documentation of assets, threats and safeguards. STIR is a two -step process.

The first step involves illust rating the assets, threats and safeguards in a diagrammatic form known as a STIR Asset -Threat-Safeguard (ATS) Diagram. This diagram extends the standard UML Use Case Diagram by adding custom tags to define assets, threats and safeguards. This representat ion aids discussion between asset owners and security practitioners and allows the assets, possible threats and potential safeguards to be easily confirmed. Furthermore, the use of UML software tools for this purpose facilitates flexible reporting.

The second step involves reviewing the completed illustration to look for any unusual or unexpected patterns. These patterns can then be the focus of further, detailed discussions and focussed risk analysis.

The principal benefits of this illustration are:

- Unprotected assets may be easily identified.
- Common safeguards that protect several assets may be easily identified.

This technique can be used to combine knowledge -based risk analysis with quantitative/qualitative risk analysis. Both of these steps are optio nal.

In summary, the ATS Diagram becomes a ‘design document’ for a subsequent risk analysis.

Method

The STIR technique in context is illustrated in Figure 1.

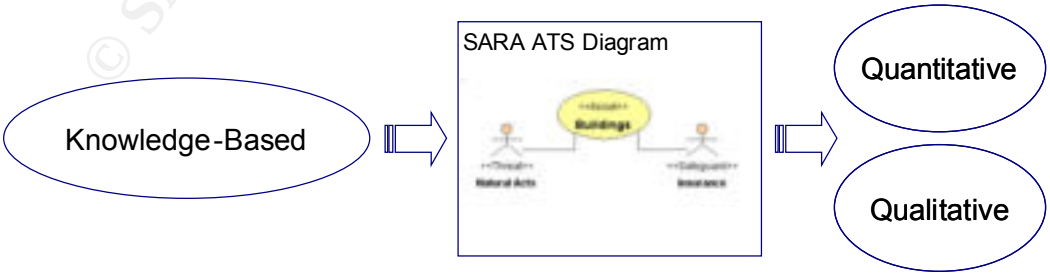

Figure 1. STIR technique in context.

Step 1: Identifying Assets, Threats and Safeguards

Potentially, the assets, threats and safeguards will have been identified using Knowledge-Based risk analysis. In this case, the first step simply involves illustrating these on the ATS Diagram. Otherwise these elements must first be identified. Note that at this stage the only requirement is that we document these elements. No effort need be applied to estimating asset value or quantifying threat probability.

Assets are added as Use Cases with the Asset tag (also known as a stereotype). Threats are added as Actors with the Threat tag. Safeguards are added as Actors with the Safeguard tag. Threats and safeguards are associated with assets using Associations. These associations indicate that the threat is capable of compromising the asset and the safeguard is capable of protecting the asset.

Step 2: Discovering Patterns

A quick glance at an ATS Diagram can reveal much information about the overall landscape.

Viewing assets it is easy to identify those assets that are subject to multiple threats (especially where the threats are diverse in nature) and also those that are protected by multiple safeguards.

Viewing threats it is easy to identify those threats that are capable of compromising multiple assets.

Viewing safeguards it is easy to identify those safeguards that are capable of protecting multiple assets.

The key to this step, however, is to identify:

- Assets that have no associated threats or safeguards.
- Assets that have associated threats but have no associated safeguards.
- Assets that have no associated threats but have associated safeguards.

These patterns indicate areas requiring further examination and are prime candidates for a detailed subsequent risk analysis.

Reporting

Use of an UML-capable software tool for drawing ATS Diagrams results in the capability to produce detailed reports in flexible formats such as HTML.

Examples of STIR ATS Diagrams

SANS Top Ten Vulnerabilities

The following example illustrates a sample control drawn from the SANS Top Ten list of vulnerabilities [SANS].

> *SANS Top Ten Vulner ability: G2 Accounts with No Passwords or Weak Passwords*[5]
>
> Most systems are configured to use passwords as the first, and only, line of defence. User Ids are fairly easy to acquire, and most companies have dial -up access that bypasses the firewall. Theref ore, if an attacker can determine an account name and password, he or she can log on to the network. Easy to guess passwords and default passwords are a big problem; but an even bigger one is accounts with no passwords at all. In practice all accounts wi th weak passwords, default passwords, and no passwords should be removed from your system.
>
> In addition, many systems have built -in or default accounts. These accounts usually have the same password across installations of the software. Attackers commonly look for these accounts, because they are well known to the attacker community. Therefore, any default or built -in accounts also need to be identified and removed from the system.

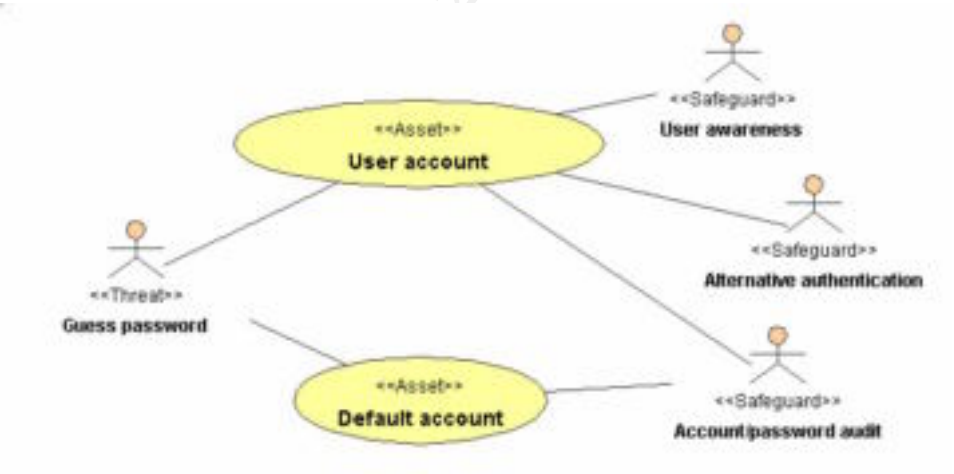

Figure 2. ATS Diagram for SANS Top Ten description.

[5] SANS

IPAK Controls

The following examples illustrate two sample controls drawn from the IPAK.

Personnel Policies and Practices [6]

Exit interviews are conducted with terminating employees to recover portable computers, telephones, smart cards, company equipment, keys and identification badges and to identify morale problems if they exist.

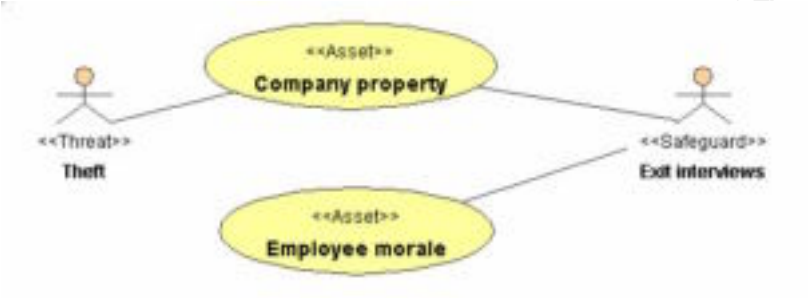

Figure 3. ATS Diagram for Personnel Policies statement.

Physical Security [7]

Documents containing sensitive information are not discarded in whole, readable form; they are shredded, burned or otherw ise mutilated.

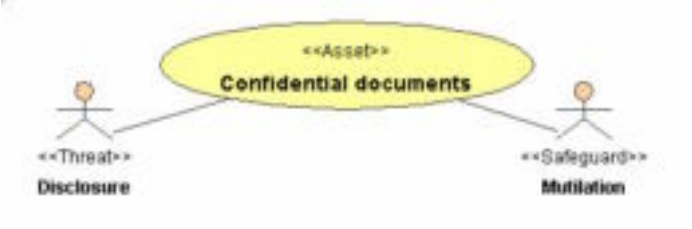

Figure 4. ATS Diagram for Physical Security statement.

[6] Power, p.288.
[7] Power, p.288.

Security Project

The following example illustrates a sample control drawn from an actual security project from Q1 2000.

Security Project Example

The loss of an individual through resi gnation or personal injury can be partially addressed by effective management policies. Succession planning, task sharing and management reporting/review demand effective communication of all aspects of the role and responsibilities of any individual. In addition, specific insurance can be used to cover the cost of recruiting and training a replacement. Finally, use of employment contracts to better manage working conditions provide another means of raising awareness of this issue.

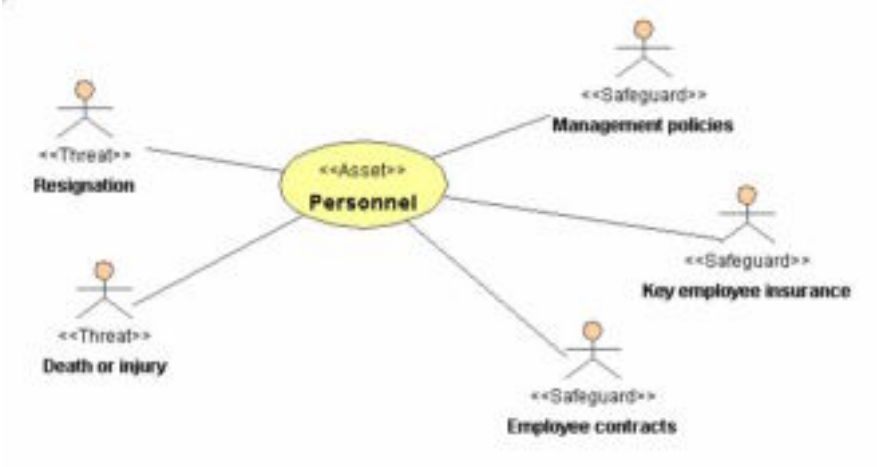

Figure 5. ATS Diagra m forSecurity Project statement.

Example Report

The following screenshot illustrates a sample report for the defined examples:

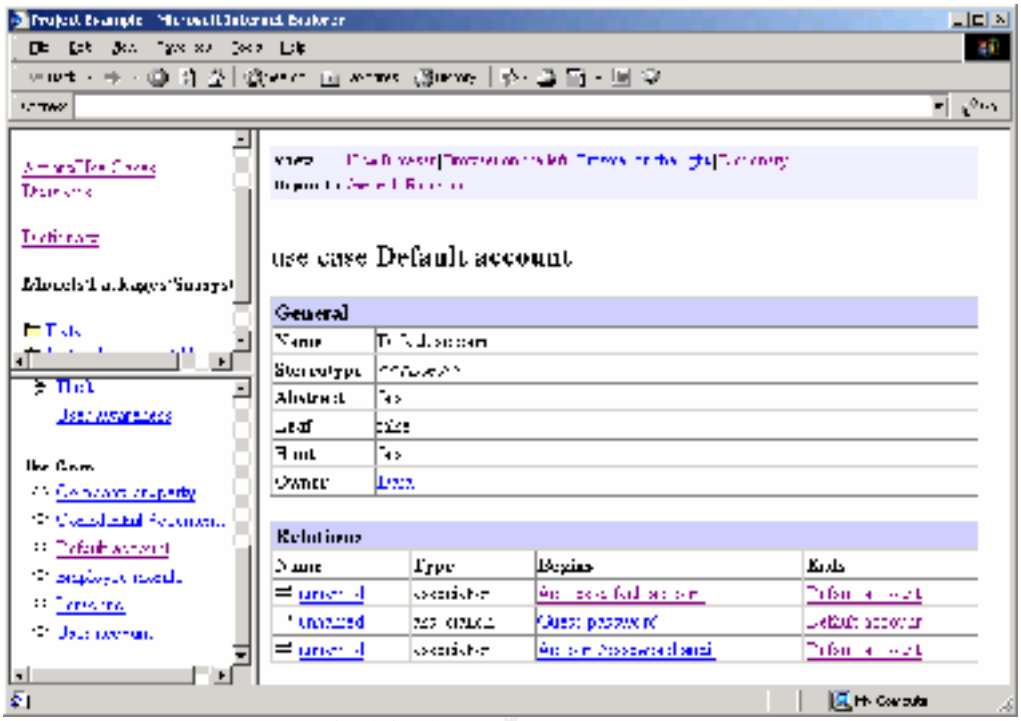

Figure 6. Example HTML report for defined ATS Diagrams.

Conclusions

STIR is a simple, but effective, technique for illustratin g assets, threats and safeguards. It results in the generation of high -level documentation in the form of useful designs and reports. The illustrations bridge the communication gap between asset owners and/or management and security practitioners.

The technique can be used in conjunction with the quantitative, qualitative and knowledge-based approaches to risk analysis and can identify specific areas on which to focus.

Summary and Conclusions

Risk analysis is a vital part of an information security strateg y and is a mandatory part of BS 7799/ISO 17799 certification.

The recognised approaches to risk analysis have accepted shortcomings. Comprehensive quantitative risk analysis can be time -consuming and expensive. Adopting a qualitative approach can reduce the overall complexity of the problem and potentially the effort required. Knowledge -based risk analysis, involving the adoption of best, sound or good practices, can provide a solid starting point for many organisations and security practitioners.

However, the Information Security industry is not in 100% agreement that these traditional approaches can always be successfully implemented, despite the fact that there are a vast array of methods and commercial tools that support these approaches singly or in combination.

Uncertainty and doubt abound in risk analysis. It is not an exact science and there are no silver bullets or cure-alls. A successful implementation requires hard work from a committed multidisciplinary team. Any simple tools and/or techniques that derive real practical benefits will always be useful.

Future Work

There are two distinct areas for future work. The first relates to the theory of this approach and involves the implementation of additional UML mechanisms. The second relates to the approach in practice and involves using it on additional real projects.

Theory

Named Associations

In addition to use cases (assets) and actors (threats and safeguards), the UML Use Case Diagrams permit stereotypes to be applied to associations. This mechanism could be used to name the asset vulnerability that the threat will attack. This can be considered as an illustration of the threat vector. The association between a safeguard and an asset could also be named to illustrate how the safeguard protects the asset. Future work would describe the possible techniques for naming associations and make recommendations as to the most appropriate method.

Additional Constructs

UML Use Case Diagrams support the use of special keyword: extend and include. The keyword 'extend' is used to illustrate that a new use case is a specialised extension of a previously documented case. This mechanism supports variant behaviour. The keyword 'include' is used to illustrate that a new use case includes a previously documented case in its entirety. This mechanism supports common behaviour. Future work would describe the possibilities for adopting these techniques within ATS Diagrams and make recommendations as to the most appropriate method.

Practice

Usage Envelope

"In theory, there is no difference between theory and practice. In practice, there is." Chuck Reid.[8] The real usefulness of this approach will only become apparent through practical experience. This experience must be gained on a variety of risk analysis projects of varying size and scope in order to determine the 'usage envelope'. Future work would describe the effects of using this approach on a number of projects, draw conclusions both for and against the approach and make recommendations as to its general suitability.

[8] Moncur

References

AEXIS_1 AEXIS. "RA Methodology". RA Software Tool. 15 January 2002 URL: http://www.aexis.de/RA%20Tool.htm#Methodology (27 March 2002).

AEXIS_2 AEXIS. "RA Software Tool for BS 7799 Risk Assessment". RA Software Tool. 15 January 2002. URL: http://www.aexis.de/RA%20ToolPage.htm (27 March 2002).

Bayne Bayne, James. "An Overview of Threat and Risk Assessment". 2 2 January 2002. URL: http://rr.sans.org/audit/overview.php (27 March 2002).

BITD Business and Information Technology Department. "CORAS A Platform for Risk Analysis of Security Critical Systems". 26 March 2001. URL: http://www.bitd.clrc.ac.uk/Activity/CORAS (27 March 2002).

Booch Booch, Grady; Rumbaugh, James; Jacobson, Ivar. The Unified Modeling Language User Guide. Reading: Addison Wesley Longman, Inc, 1999. 14-16.

C&A_1 C & A Systems Security. "Introduction to COBRA". Introduction to Security Risk Analysis and the COBRA Approach. URL: http://www.securitypolicy.co.uk/riskanalysis/introcob.htm (27 March 2002).

C&A_2 C & A Systems Security. "COBRA Risk Consultant". Introduction to Security Risk Analysis and the COBRA Approach. URL: http://www.securitypolicy.co.uk/riskanalysis/riskcon.htm (27 March 2002).

C&A_3 C & A Security Risk Analysis Group. "Introduction to Risk Analysis". URL: http://www.security-risk-analysis.com/introduction.htm (27 March 2002).

Carnegie Carnegie Mellon Software Engineering Institute. "OCTAVE sm Information Security Risk Evaluation". Information Security Risk Evaluation. 7 January 2002 URL: http://www.cert.org/octave/ (27 March 2002).

CSI Computer Security Institute. "CSI Information Protection Assessment Kit (IPAK)" URL: https://wow.mfi.com/csi/order/publications.html (27 March 2002).

Erwin — Erwin, Dan. "e-risk, Liabilities in a Wired World". CSI ALERT Newsletter, Number 209. August 2000.
URL: http://www.gocsi.com/pdfs/erisk.pdf (27 March 2002).

Helms — Helms, Hal. "Why Projects Fail – and What You Can Do About It". WebReference Newsletter. 3 January 2002.
URL: http://www.webreference.com/new/020103.html (27 March 2002).

Hinton — Hinton, Craig. "CRAMM". SC Magazine, December 2001.
URL: http://www.scmagazine.com/scmagazine/sc-online/2001/review/059/product.html (27 March 2002).

ISSA — Information Systems Security Association, Inc. "ISSA Hall of Fame Award Recipient Thomas R. Peltier". 16 April 2000.
URL: http://www.issa.org/tompeltier.htm (27 March 2002).

Insight — Insight Consulting. "About CRAMM".
URL: http://www.crammusergroup.org.uk/cramm.htm (27 March 2002).

Mina — Mina, Ted. "Application Security, Information Assurance's Neglected Stepchild – A Blueprint for Risk Assessment". SANS Institute Reading Room. 26 July 2001.
URL: http://rr.sans.org/audit/stepchild.php (27 March 2002)

Moncur — Moncur, Michael. The Quotations Page.
URL: http://www.quotationspage.com/search.php3?homesearch=chuck+reid (27 March 2002).

Parker — Parker, Donn. "Why the Due Care security review method is superior to Risk Assessment". CSI ALERT Newsletter, Number 212. November 2000.
URL: http://www.gocsi.com/duecare.pdf (27 March 2002).

Paul — Paul, Brooke. "Risk-Assessment Strategies". Network Computing. 30 October 2000.
URL: http://www.networkcomputing.com/1121/1121f32.html (27 March 2002).

Peltier_1 — Peltier, Tom. "Facilitated Risk Analysis for Business and Security"
URL: http://www.gocsi.com/facilitated.htm (27 March 2002).

Peltier_2 — Peltier, Tom. "Risk analysis in business process". CSI ALERT Newsletter, Number 211. October 2000.
URL: http://www.gocsi.com/risk.pdf (27 March 2002).

Power — Power, Richard. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Indianapolis: QUE Corporation, 2000. 280 - 290.

Rajasingham — Rajasingham, Prabhacker. "Threat and Risk Assessments: SOME Issues". SANS Institute Reading Room. 10 April 2001. URL: http://rr.sans.org/audit/risk.php (27 March 2002).

SANS — SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated)". SANS Institute Resources. Version 2.502. 30 January 2002. URL: http://www.sans.org/top20.htm (27 March 2002).

Schneier — Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000. 255 -258.

Snyder — Snyder Jr., John S. "Business Impact Analysis for the Security Professional". SANS Institute Reading Room. 16 May 2001. URL: http://rr.sans.org/securitybasics/impact.php (27 March 2002).

Summers — Summers, Rita C. Secure Computing: Threats an d Safeguards. New York: McGraw-Hill Companies, Inc, 1997. 624 -627.