Type of submission: paper
Title: ROLE-BASED RISK ANALYSIS
Abstract:

At least two recent developments in information management warrant revisiting risk analysis methodologies. First, an explosive proliferation of networks and shared information has occurred. As a result, inefficiencies in the traditional risk analysis model have become magnified, and deficiencies become more pronounced. In addition, the selling of information and outsourcing of computer support have increased in recent years. Traditional risk analysis methodologies are not capable of adequately modeling the scenarios created by these recent developments.

This paper presents a role-based risk analysis model which addresses these scenarios, as well as traditional ones. By using the framework provided by this model, one can reduce the analysis effort required to identify appropriate countermeasures for new and old scenarios.

Authors: Lance J. Hoffman and Amit Yoran
Organizational Affiliation: George Washington University, Cyberspace Policy Institute
Phone numbers/E-mail Address:

Lance J. Hoffman	Amit Yoran
Voice: (202) 994-5513	Voice: (703) 379-0617
Fax: (202) 994-0227	Fax: (404) 685-0863
E-mail: hoffman@seas.gwu.edu	E-mail: amit@riptech.com

Point of Contact: Amit Yoran

ROLE-BASED RISK ANALYSIS

KEYWORDS: risk management, risk analysis, risk assessment, role-based modeling, liability, responsibility, role, actor, distributed risk environment, outsourcing

ABSTRACT

At least two recent developments in information management warrant revisiting risk analysis methodologies. First, an explosive proliferation of networks and shared information has occurred. As a result, inefficiencies in the traditional risk analysis model have become magnified, and deficiencies more pronounced. In addition, the recent increases in the activities of selling information and outsourcing computer support have caused the inefficiencies of traditional risk analysis methodologies to adequately model these scenarios.

This paper presents a role-based risk analysis model which addresses these scenarios as well as traditional ones. By using the framework provided by this model, one can reduce the analysis effort required to identify appropriate countermeasures for new and old scenarios.

1. INTRODUCTION

Risk analysis is “the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.” [1]

Principles of due care are “Just, proper, and sufficient care, so far as the circumstances demand it; the absence of negligence. That care which an ordinarily prudent person would have exercised under the same or similar circumstances.” [2]

According to a 1994 report by the U.S. Congress, Office of Technology Assessment,

> “Both *risk analysis* and *principles of due care* need further development. Neither approach is necessarily always appropriate and therefore neither is always sufficient to provide a strong defense against liability in the case of monetary loss related to loss, theft, or exposure of networked information. A combination of the two approaches will likely provide improved protection.” [3]

This paper presents a framework for improving current risk analysis methods. First a common risk analysis technique is given and shortcomings are identified. An alternative methodology is presented and an example is provided to illustrate its use. The new methodology’s advantages are enumerated and areas for future research are identified.

1.1 Background

Although information is an intangible asset, it is vulnerable to many kinds of threats ranging from natural disaster to corporate espionage. However, just as the number of threats is increasing, the number of information protection tools and capabilities is increasing. As a result, risk analysis has become an increasingly complex pursuit.

One method of managing risk is to apply a well-known risk analysis (RA) model to determine a cost effective and efficient method of reducing risk. Traditional risk analysis methodologies have existed for many years. [4, 5, 6]

We first briefly describe a common model of RA to ensure a common basis of understanding. From this, we will develop the role-based model.

Typical RAs require the following stages [7]:

1. Identify assets – These assets can be any part of the information "system". They can include hardware, software, data, people, documentation and supplies.
2. Determine vulnerabilities – Vulnerabilities are any person, threat, act or idea that may cause a loss in information secrecy, integrity, availability or any other defined information security goal.
3. Estimate likelihood of exploitation – This estimation is based on controls in place and probabilities that these controls are overcome.
4. Compute expected annual loss –the expected annual loss factors in loss of business opportunity, cost of data recovery and reconstruction, loss in sales and loss in public relations among others.
5. Survey new controls – Other controls and countermeasures are evaluated in relation to the defined vulnerabilities.
6. Project annual savings of control – This weighs the costs of implementing controls against possible associated losses.

This traditional methodology provides rational decision-making in information protection, but lacks efficiency, as we will show later. Also note that this process describes risk analysis and not risk management. Risk management is "the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review." [1]

1.2 Developments in Assessment Methodologies

Over time, several modifications to the traditional risk analysis methodology have been made. Osgood traces developments in risk assessment. Each development in RA's evolution has refined its application to a specific environment and increased the capabilities of risk analysis. He also develops a risk analysis model for multiple-system multiple-sites environments. [8]

Jaworski presents an approach to risk assessment which analyzes a perpetration of successions of threats at multiple vulnerability points. [9] Drake and Morse develop an new approach to measuring security breaches and controls. “The driving principle of this model is that not all of the losses caused by a security breach occur at the time of the security breach itself, but most of the losses occur later when the consequences of the breach are enacted.” Drake and Morse use this principle to develop a methodology which can model a security breach over time and determine how to best limit the losses incurred. [10]

2. NEED FOR METHODOLOGY DEVELOPMENT

The standard risk analysis model requires significant modifications when applied to different environments. We will demonstrate through this paper that commercial needs differ significantly from military and other government needs, and that the RA model in its present stage of development is not particularly well suited to address business requirements or model distributed business environments.

2.1 Business Requirements Differ from Military Requirements

Historically, much of the work done in risk analysis methodologies and techniques has been done by the military. For obvious reasons, the military has always been concerned with security and mitigating risk exposure, and techniques developed and decision analyses used often were geared toward military needs. Business requirements in the areas of risk analysis and management differ from the military requirements: they may share a common thread for cost efficiencies, whereas military requirements can also carry the onerous burden of human lives. Military risk analysis, therefore, usually focuses on collateral worst case scenarios.

The traditional model does not adequately address business requirements. One area which needs further development is the assessment of legal liability in instances of information compromise. The RA model in its present state does not address these issues. For example, when information is compromised in a commercial situation, attribution of blame and/or liability in accordance with the RA model is difficult at best. The attribution of blame and/or liability is important in determining legal and/or fiscal liabilities.

For an individual or an organization that is filling a specific role in the business process, performing a standard risk analysis in order to determine what their specific liabilities are, is not an easily understood or intuitive process. The standard RA model is both convoluted and inadequate for determining a role or agent based assessment of risk (as discussed below).

2.2 Emphasis Must Shift From Automation to Efficiency

To date, much of the work done in RA development has focused on automating existing analyses techniques. Significant resources have been dedicated to developing software programs to automate the time-intensive processes. As the RA model is applied to new situations, especially those involving complex networks over which organizations do not have complete control, the need to expand the model, enhance its flexibility, and increase its efficiency has become apparent. Continuing with brute force automation of inefficient processes will not address emerging analyses requirements.

2.3 Outsourced Distributed Risk Analysis is Not Often Addressed

The use of outsourced computer support is increasing in many areas such as LAN administration, helpdesk support, contract programming, application development, and Internet site maintenance. Although these external organizations provide valuable services, they complicate the risk analysis environment. As outsourced organizations do not have ultimate ownership of the information with which they deal, the value they place on information may differ from the owner's assessment of value.

The idea that one organization is responsible for another organization's information leads us to introduce the concept of "information bailment." Bailment is defined as, "a delivery of goods or personal property, by one person to another, in trust for the execution of a special object upon or in a relation to such goods, beneficial either to the bailor or bailee or both, and upon a contract, express or implied, to perform the trust and carry out such object," [2]. Assuming information is a "good" and has value, then an information bailment is enacted when one party "transfers" digitally stored information to another for a purpose, such as storage or processing. While the concept of information bailment is new, instances of information bailment are readily apparent; such as a local Internet Service Provider (ISP) hosting a website for customer who requires that the information be available for public access on a continuous basis. This and similar scenarios do not lend themselves to be readily analyzed with existing RA models because the company and the ISP place different values on the information asset and its availability. They also face different threats to that information and have different countermeasures at their disposal.

3. METHODOLOGY

We have modified the traditional risk analysis model by introducing and applying a role-based approach to perform the analysis. To better understand the role-based RA model, we will define some terms.

A *role* refers to a specific function that an entity plays in the model. It is defined by the responsibilities and expectations of any scenario. By defining roles within each scenario the model is customized to represent the situation it depicts. These roles enable the model to better simulate the real situation faced by each entity. An information owner, as defined in Section 3.1, is an example of a role.

An *actor* is a term we use to refer to an entity that fills a defined role within the model. A example of an actor is a corporation with financial statements as the information. In this example, the corporation is the actor and the role being filled is that of information owner.

The Role-Based Risk Analysis (RBRA) Model, which defines roles and actors, enables analysis in scenarios that the traditional RA model is not capable of addressing well. Example scenarios include environments with outsourced information services and situations which require a legal analysis of liability. These issues are further detailed below.

Role-Based Risk Analysis introduces two additional stages, role and actor definition, ahead of the traditional RA stages. Thus, the RA process now has eight stages.

1. *Define the roles.*
2. *Identify the actors.*
3. Identify assets from actor’s perspective.
4. Determine vulnerabilities.
5. Estimate likelihood of exploitation.
6. Compute expected annual loss.
7. Survey applicable controls and their costs.
8. Project annual savings of controls.

3.1 Role-Based Risk Analysis Stages

1. Define the Roles

The first step in performing a role-based risk analysis is to understand the roles involved. If accurate results are to be obtained, the roles must be properly identified and defined. Although roles are situation-dependent, in many instances, the roles defined will be very similar to the roles we will present in this document. It is important to note that the RBRA model is sufficiently flexible to allow each assessor to evaluate and define the roles of interest specific to their particular scenario.

For the purposes of developing and illustrating the RBRA methodology, we will define five roles which can be thought of as functional areas. These roles may or may not be independent and the role/actor pairs are not mutually exclusive. In other words, an actor can fill multiple roles, and multiple actors can also fill any given role. In our example model the following roles are defined: the Information Owner (IO), the Information Holder (IH), the Protecting Agent (PA), the Acting Agent (AA) and the Sponsor (SP).

Information Owner (IO) – The term Information Owner represents that party who owns the information. A very simple example of an IO is a corporation with financial statements as the information.

Information Holder (IH) – The term Information Holder represents those parties that maintain direct control of the information. An example of an IH is an accounting firm which maintains direct control of another company's financial statements. In this case the IH and IO are two different parties. In another example, an IH might be a corporation which stores its financial statements on a corporate network. In that scenario, the IH and IO are one and the same.

Protecting Agent (PA) – The term Protecting Agent represents those parties entrusted with protecting information. This role can be filled by either a third party, the IH, the IO, or both. An example of a clearly defined PA is a company that actively maintains the firewall to a corporate network. Less obvious Protecting Agents may be harder to identify, but are accounted for in the RBRA model. For instance, if a company implements a firewall, the developer of that firewall product is an indirect PA even though they were not involved in each installation of their firewall.

Acting Agent (AA) – The term Acting Agent refers to any realized threat (person, thing, event or idea) acting upon an information asset. One example of an AA is a hacker attempting to gain unauthorized access to data. Other examples of AAs include fires, floods and other natural disasters.

Sponsor (SP) – The term Sponsor refers to any entity promoting an Acting Agent's activity. This role need not always be filled. An example of a Sponsor is an individual that hires a hacker to obtain access a competitor's data. Another less obvious example is an employee who disposes of a lit cigarette by tossing it down the trash disposal, which leads to a destructive fire that destroys the computer center.

2. Identify the Actors

The second step in the RBRA methodology is to identify the actors. An assessor using this model needs to properly identify role/actor pairs. For each role/actor pair the assessor has a unique set of threats, losses and countermeasures to evaluate. As stated above, role/actor pairs are not mutually exclusive. For example, an actor serving as an Information Holder may also serve as a Protecting Agent. Once the roles and actors have been identified, the remaining stages of risk assessment will be more intuitive to implement.

3. Identify the Assets from Actor's Perspective

Various actors value the same information asset differently. For example, an Information Owner may place a higher value on proprietary information than an Information Holder.

This is a critical concept that the RBRA model encompasses which traditional models omit.

4. Determine Vulnerabilities.

The assessor then determines vulnerabilities facing each role/actor pair. Again, these vulnerabilities are specifically defined for each role/actor pair based upon their unique circumstance. In a traditional RA an exhaustive search is performed and all potential vulnerabilities are identified and then have to be analyzed for applicability. When properly implemented RBRA yields the same results as the traditional RA exhaustive search, but is more efficient since the role filters the domain of all possible vulnerabilities to only the appropriate ones.

For example, an actor that is exclusively an Information Owner (not filling any other roles in the RBRA model) only needs to evaluate those vulnerabilities associated with an IO role. One of these vulnerabilities might include accidental disclosure of the information to a competitor organization. Some vulnerabilities are not in the subset of vulnerabilities specific to an IO and need not be evaluated. These might include hacker break-ins or fire. These vulnerabilities are appropriately addressed when performing an analysis of the Information Holder or Protecting Agent roles.

5. Estimate Likelihood of Exploitation.

For each vulnerability determined in Stage 4, a likelihood of exploitation is determined.

6. Compute Expected Annual Loss.

For each vulnerability determined in Stage 4, a computation of expected annual loss is also performed.

7. Survey Applicable Controls and Their Costs.

Based on the vulnerabilities determined in Stage 4 of the RBRA model, the set of applicable controls and their costs is determined. Just as in Stage 4 when the RBRA reduced the domain of appropriate vulnerabilities to some subset of all vulnerabilities, in Stage 7, the domain of all controls is also pared down to those appropriate to the role/actor pair. By applying a role-based analysis, the set of applicable controls is reduced to some subset of the controls evaluated in traditional risk analysis models. At the same time, the results of the control survey are the same as the exhaustive search results required by the traditional RA.

8. Project Annual Savings of Control.

Based upon the results of the previous stages of analysis, the projected annual savings of implementing each control is determined.

Role-Based Risk Analysis introduces the two additional stages of role and actor definition ahead of the traditional RA model. The initial stages allow the assessor to reduce the set of vulnerabilities and controls to those appropriate to a given role. This set reduction does not decrease the power of the model. All of the elements which are obtained in the exhaustive technique used in traditional RA are included in the RBRA results. This is the case because only those vulnerabilities and/or controls which are inappropriate to a given role are filtered out during the initial stages of the RBRA. At the same time, significantly less analysis is required to obtain these results because the assessor is able to filter out the non-relevant vulnerabilities and/or countermeasures.

As an example, consider the following figures. The first illustrates the subset of total threats faced by IO, IH and PA roles. The second presents the subset of total countermeasures available to the IO, IH and PA roles. These are not intended to be complete, but instead aid to the understanding of the model. Even in the worst case, only 29 of the 36 items need be considered while in a given role. Thus, clearly defining roles to prevent ambiguity of responsibilities saves considerable work in the long run

Figure 1. Typical Threats and Associated Roles

Threat		IO	IH	PA
<u>Information leakage</u>				
Disclosure		✓		✓
Malicious programs (trapdoor, Trojan horse)				✓
Dysfunctional system controls			✓	✓
Physical intrusion			✓	
Eavesdropping		✓		✓
Traffic analysis		✓		✓
Emanations analysis		✓		✓
Masquerade		✓		✓
Scavenging			✓	✓
<u>Integrity violation</u>				
Malicious programs (trapdoor, Trojan horse)				✓
Dysfunctional system controls		✓	✓	✓
Modification		✓	✓	✓
<u>Denial of service</u>				
Malicious programs (trapdoor, Trojan horse)				✓
Natural disaster		✓	✓	✓
Accidental destruction		✓	✓	
Resource flooding			✓	
Communications flooding				✓
Theft			✓	✓
Malicious destruction		✓		✓
Totals	19	10	9	16

Figure 2. Typical Countermeasures and Associated Roles

Countermeasure		IO	IH	PA
Statement of non-disclosure		✓		
Encryption		✓		✓
Authentication		✓		✓
Non-repudiation		✓		✓
Digest				✓
Time stamping		✓	✓	✓
Outsourced security consulting		✓	✓	
Documented Trusted Computing Base		✓	✓	✓
Defined and enforced security policy			✓	✓
Audit			✓	✓
Access controls				✓
Firewalls				✓
Intrusion detection systems		✓	✓	✓
Personnel controls			✓	✓
System verification procedures			✓	✓
Redundancy/fault tolerance		✓		
Archives				
Totals	17	9	8	13

3.2 Applying the Role-Based Risk Analysis Model

For greater intuitive understanding of the RBRA methodology, we apply a few key stages of the model to the following simple scenario:

> A computer software engineering firm (Company A) provides and investment banking company (Company B) copies of its financial information. It also maintains this financial information on its own network for periodic updating. Company B retains this information on their corporate network. Company B also hires an information security consulting firm (Company C) to protect the information on their network. Company C implements a firewall to protect Company B's network. The firewall used is developed by Company D. Company A's in-house data automation department provides protection for the information on its network. Finally, an individual F, that works for a competitor, hires Company E to retrieve information on Company A's finances.

In Stage 1 of the RBRA methodology, roles are defined as appropriate. For the scenario described above, the pre-defined roles are easy to apply. Once the correct roles are defined, the actors are assigned to the relevant roles.
The role/actor pairings are presented in the following table.

ROLE	ACTOR
Information Owner	Company A
Information Holder	Company B and Company A
Protecting Agent	Company C, Company D and Company A
Acting Agent	Company E
Sponsor	Individual F

Once roles and actor pairs are determined, the remainder of the RBRA methodology is applied to individual role/actor groups. Each actor needs to evaluate only those vulnerabilities and countermeasures for each information asset which apply to his/her role(s). In our example, Company A must evaluate all vulnerabilities and countermeasures which apply to the IO, IH and PA. These threats vary widely and can range from insider disclosure to hacker penetration and from power failure to destruction by fire. In addition, Company A must evaluate all countermeasures which correspond with the threats and vulnerabilities faced.

Company B's process is similar, however, it acts under different constraints. By outsourcing its entire information technology support or even just the information protection aspect of its network, Company B can attempt to decrease its direct responsibility for the security of Company A's financial information.

Analysis for the other actors in this scenario is not presented here. Although the analysis for other role/actor pairs is similar to the analysis above, the combinatorial complexity is significantly greater due to the number of vulnerabilities and countermeasures faced by the IH and PA roles. This analysis will be presented in a subsequent paper. Results of risk analysis performed using the RBRA methodology, such as the amount of savings gained by implementing a particular control, yields similar results to an analysis of fiscal results obtained by standard risk analysis models.

4. BENEFITS OF A ROLE-BASED METHODOLOGY

In scenarios where a Role-Based Risk Analysis is appropriate, several advantages can be gained. Although the shift from traditional analysis to role-based analysis is not necessarily a complex one, it is significant for at least three reasons.

4.1 Appropriateness to Distributed Business Environments

In scenarios where information and responsibilities are distributed among different entities, a role-based methodology is more intuitive and lends itself toward a more accurate depiction of the business process. This model enables the actors to more easily and efficiently address the different responsibilities, threats and countermeasures for each role as required. Standard risk analysis methods are not capable of accurately modeling the modern distributed business process, whereas the RBRA model provides greater comprehension and a clearer depiction of the scenario.

4.2 Reduction in Analysis Complexity

Since only a subset of threats apply to each role/actor pair, a role-based methodology yields a smaller analysis requirement than traditional models. As a consequence of the smaller threat set, the set of appropriate countermeasures will be smaller as well. Thus, there is improvement in model efficiency. For instance, an Information Holder that is not also serving in the capacity of Protecting Agent need not consider threats specific to that role unless they also apply to the Information Holder role. In determining and evaluating the appropriate countermeasures, the Information Holder needs to consider only a subset of choices available in the traditional model.

4.3 Non-Traditional Fields of Analysis

The role-based risk analysis can be applied to non-traditional fields of risk analysis. One such area is in determining legal liability for compromised information assets. Through defining roles and identifying actors, legal standards of care can be established and liabilities assessed for a given scenario. A standard of care can be defined as that which an ordinarily prudent person would exercise under the same or similar circumstances when charged with like duty (an ordinarily prudent actor in that given role). [11]

5. SHORTCOMINGS OF ROLE-BASED MODELS

Although the RBRA model is very flexible, like any other model it is not appropriate in every situation, and it must be continuously revisited as scenarios evolve over time. For example, relationships between actors and roles are dynamic. An Information Holder may become an Information Owner. Another shortcoming of the RBRA model is the parochial view it is capable of presenting when a universal understanding would be preferred. Because a role-based analysis identifies and delineates specific responsibilities people may be reluctant to implement it in situations where avoidance of responsibility is a goal.

6. FUTURE RESEARCH

While this paper establishes a framework for Role-Based Risk Analysis there remains several key areas where future research is necessary. These include the development of a vulnerabilities/countermeasures matrix for each role identified in the RBRA model, developing legal standards of care for each role, and techniques for preventing the model from providing the assessor with a parochial view of risk. While no formal method for determining the relevance or appropriateness of threats and counter measures to any given actor has yet been established, our initial taxonomy provide a framework for this analysis to be done.

REFERENCES

[1] National Computer Security Center, Glossary of Computer Security Terms – NCSC-TG-004, Government Printing Office, October 1988, pp. 39.

[2] Henry C. Black, M.A., Black's Law Dictionary, West Publishing, 1979.

[3] U.S. Congress, Office for Technology Assessment, Information Security and Privacy in Networked Environments, Government Printing Office, September 1994.

[4] Hoffman, Lance J., Smoking Out the Bad Actors: Risk Analysis in the Age of the Microcomputer, Institute for Information Science and Technology, March 1988.

[5] Hoffman, Lance J. Risk Analysis and Computer Security: Bridging the cultural gaps, Presented at the 9th National Computer Security Conference, National Bureau of Standards, Gaithersburg, MD, Septermber 1986.

[6] Henrion, Max and Morgan, Granger, M. A computer aid for risk and other policy analysis, Ris*k Analysis*, Vol. 5, No. 3 (September 1985).

[7] Charles P. Pfleeger, Security in Computing, Prentice-Hall, 1997, pp. 462-471.

[8] Thomas W. Osgood, “A Risk Analysis Model for the Military Environment,” Proceedings of the 11th National Computer Security Conference, October 1988.

[9] Lisa M. Jawarski, “Tandem Threat Scenarios: A Risk Assessment Approach,” Proceedings of the 16th National Computer Security Conference, September 1993.

[10] David L. Drake and Katherine L. Morse, "The Security Specific Eight Stage Risk Assessment Methodology," Proceedings of the 17th National Computer Security Conference, 1994.

[11] Tharp v. Brewer, 7 N.C. App 432,438,172 S.E.2nd 1919, 1924 (1970).