IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5169

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

Information Security Risk Analysis: A Matrix-Based Approach

Sanjay Goel

University at Albany, School of Business, SUNY, BA310b, 1400 Washington Ave., Albany, NY 12222, USA, goel@albany.edu

Vicki Chen

General Electric Energy, 1 River Rd., Schenectady, NY 12345, USA, vicki.chen@ps.ge.com

ABSTRACT

This paper presents an information security risk analysis methodology that links the assets, vulnerabilities, threats and controls of an organization. The approach uses a sequence of matrices that correlate the different elements in the risk analysis. The data is aggregated and cascaded across the matrices to correlate the assets with the controls such that a prioritized ranking of the controls based on the assets of the organization is obtained. The approach does not obfuscate the intermediate data in the analysis, thereby providing transparency to the risk analysis process and allowing rationalization of the data. This approach allows organizations to start with sparse data with low fidelity and the analysis can be gradually refined as additional (and high quality) data is collected over time. A sample case study based on a study at a NY State agency is presented. This methodology was applied at General Electric and some preliminary results of the case study are presented in this paper.

INTRODUCTION

Computer networks and the Internet have enabled greater productivity in both government and private sector organizations. The Internet is also deeply integrated into our personal lives and becoming a driver of social behavior. Use of email and instant messaging has grown exponentially over the years and is becoming the preferred mode of communication. Despite the rise and fall of the dot-com industry, the Internet is changing the way consumers shop and the business models of companies. For example, the alternate business model of distribution of music through the Internet has changed the landscape of the music industry and driving innovation in peer-to-peer systems as well as in formats of digitization and compression of music files.

While the impact of the Internet on electronic commerce, communication, and dissemination of information is obvious, the major impact of computer networks has been on business process reengineering. Most routine corporate functions are now handled with automated processes anchored in databases. Networked information systems form the backbone of enterprises and are used in almost all aspects of business including: payroll, procurement, human resource management, as well as, analysis and design of engineering components. Information systems have significantly improved organizational productivity. However, total dependence on information systems for critical operations has left organizations vulnerable to anomalies and attacks on networks. Business-to-business (B2B) and business-to-consumer (B2C) commerce has fueled growth in the GDP over the last decade. In the government sector, several critical infrastructure elements such as dams, power grids, and emergency-response systems are dependent on networks and computers. As the dependence of the economy on information systems increases, the financial impact of information security failures also increases. This risk of financial loss due to a security breach is a cause for concern within corporations and government.

Most organizations do not have a complete understanding of their information security risk posture. Usually, ad hoc decisions are made on security implementation based on guidelines and alerts issued by government agencies and other trusted third parties. IT departments are responsible for keeping the security in check, but it is difficult for the organizations to get a clear picture of security posture without a formal risk analysis. While IT staff may be competent in implementing security tools, they often lack the expertise in financial modeling and risk analysis. Formal risk analysis methodology is mature in several fields (finance, engineering, nuclear plants and aviation). However, it is nascent in the information security discipline. Issues with risk analysis in information security are lack of standardized metrics and processes for valuation of assets, measuring impact of threats and estimating the benefit of controls and acute shortage of data that would enable reasonable statistical analysis to estimate risks. Another problem is the poor quality of data on threats and vulnerabilities that stems from organizations fear that revealing security incidents will attract other malicious hackers to exploit vulnerabilities and lead to increased frequency of attacks. Finally, the information security risk analysis process is very weak through basis on checklists and guidelines or very expensive requiring extensive internal data collection using penetration testing and honey pots. Most organizations often outsource risk assessment tasks and often conduct these assessments periodically (annually, or bi-annually) rather than continuously. Also, organizations do not have the ability to determine the quality of assessments and have to rely on consultants' verdicts.

We present a risk assessment methodology that can be used internally, which allows organizations to start with a small data set, as well as gradually refine and improve the analysis as high fidelity data becomes available. It also allows organizations to perform qualitative analysis on a broad scope, and then perform a more detailed analysis based on a critical subset of the problem. The rest of the paper is organized as follows: section 2 provides a brief review of the risk analysis literature, section 3 provides basic methodology, section 4 supplies a sample case study, and section 5 offers conclusions for the paper.

LITERATURE

Information security risk analysis has been investigated from an audit perspective (Cerullo & Cerullo, 1994) for a long time. Auditors generally use checklists to verify if different elements of security are in place and base their judgment on these checklists. Baskerville (1993) has been investigating information security risk analysis since the mid-1980s. He has identified risk analysis checklists for tools used for designing security measures for information systems. Parker (1981) and Fisher (1984) have used risk analysis as a fundamental basis for security design in information systems. They provide extensive checklists for considerations in the security assessment. The problem with specific tools and checklists is that they become obsolete quickly and need to be constantly updated. Applications of such tools do not lead to scientific knowledge

advancement for information security design. Backhouse and Dhillon (1996) attempt to create a logical model for information security as a structure of responsibility and duty rather than standard checklists. Anderson, Longley and Kwok (1994) propose a model based on the identification and evaluation of threats originating from the operational environment and systems that assets under protection encounter. Suh and Han (2003) present an approach for information security risk analysis that incorporates operational continuity. They determine the value of assets based on the importance of business functions and the criticality of assets to operations. Several methodologies are used in the analysis: paired comparison, asset-function assignment tables, and asset dependency diagrams. Other models for information security design additionally focus on identification and evaluation of system vulnerabilities and specification of countermeasures (Weiss, 1991).

Various attempts have been made to develop complex tools for information security risk analysis. CRAMM (Barber & Davey, 1992) is a generic risk assessment tool. The basic premise behind the approach is that risk is dependent on asset values, threats, and vulnerabilities. The data for CRAMM is obtained via interviews with asset owners, the system users, and other technical support staff. CORAS (Stolen, 2002) uses a combination of Unified Modeling Language (UML) and Unified Process (UP) to support a model-based risk assessment on security-critical systems. It integrates several existing methodologies such as Fault Tree Analysis, Failure Mode and Effect Criticality Analysis, and Markov analysis into a single platform for facilitating risk analysis. OCTAVE (Alberts and Dorofee, 2003) is a more recent risk analysis tool developed at Carnegie Mellon Software Engineering Institute, which provides an extensive set of worksheets and checklists for implementing information security.

METHODOLOGY

This methodology correlates the assets, vulnerabilities, threats, and controls of the organization and determines the importance of different controls corresponding to the assets of the organization. The organization's assets are defined as things of value that it needs to protect. Assets can be tangible such as data and networks and intangible such as reputation and trust. Vulnerabilities are weaknesses in an information asset that can be exploited by threats such as a database or a web server. Threats are potential causes of unwanted events that can result in harm to the assets of the organization. Threats can be accidental or malicious. Controls are defined as measures that the organization can take to minimize the impact of threats on one or more assets of the organization.

The methodology proposed in the paper uses three separate matrices, i.e. vulnerability matrix, threat matrix and control matrix to collect the data that is required for risk analysis. The vulnerability matrix (Table 1) contains the associations between the assets and vulnerabilities in the organization, the threat matrix (Table 2) similarly contains the relationships between the vulnerabilities and threats, and the control matrix (Table 3) contains the links between the threats and controls. Each cell in a table contains the value of the relationship between the row and the column element of the table (e.g. asset and vulnerability). It uses one of the three values, i.e. low, medium or high.

When the risk analysis is initially conducted, lists of assets, vulnerabilities, threats, and controls are generated and added to the respective tables. The matrices are then populated by adding data that correlates the row of the matrix with the column of the matrix. Finally, the data from the vulnerability matrix is aggregated using Equation 1 and then cascaded on to Table 2. Similarly, data in the threat matrix is aggregated using equation 2 and cascaded on to Table 3. The data from the Control matrix is then aggregated to obtain the relative importance of the different controls.

Let us assume that there are m assets where the relative cost of asset a_j is C_j $(j = 1,\ldots, n)$. Also let c_{ij} be the impact of vulnerability v_i on asset a_j. Then the relative cumulative impact of vulnerability v_i on the assets of the organizations is:

$$V_i = \sum_{j=1}^{j=n} v_{ij} * C_j \qquad (1)$$

Let us assume that there are p threats that impact the n vulnerabilities and d_{ki} is the potential of damage from threat t_k to vulnerability v_i. Then the relative cumulative impact of the threat T_k is:

$$T_k = \sum_{i=1}^{i=m} d_{ki} * V_i \qquad (2)$$

Let us assume that there are q controls that can mitigate the p threats and e_{lk} is the impact of control z_o on threat t_k. Then the relative cumulative impact of the Control Z_o is:

$$Z_o = \sum_{l=1}^{l=p} e_{ol} * T_l \qquad (3)$$

CASE STUDY

A risk analysis study was conducted using the proposed approach at General Electric Energy, Wind Division, which is a new division for GE. The Wind business, recently acquired from Enron, has a fragmented organizational structure. Its facilities are scattered across several countries, including, Spain, Germany, US, Denmark and China. There is very little uniformity in its processes and operations. In addition, their engineering divisions do not share a common network. This is a highly competitive business where new technology is being constantly developed and manufacturers constantly try to leapfrog each other, information security is thus critical to protect their assets and to prevent disruption of their operations.

Table 1. Asset Worksheet (correlation between assets and vulnerabilities)

Scale 0 – No Impact 1 – Weak Impact 3 – Moderate Impact 9 – Strong Impact **Vulnerabilities**	**Assets & Costs** Trade Secrets (IP)	Client Secrets	Reputation (Trust)	Lost Sales/Revenue	Cleanup Costs	Information	Hardware	Software	Services	Communication	Relative Vulnerability Impact ↓
Web Servers											Relative Asset Value ←
Compute Servers											
Firewalls											
Routers											
Client Nodes											
Databases											

Table 2. Vulnerability Worksheet (correlation between threats and vulnerabilities)

Scale 0 – No Impact 1 – Weak Impact 3 – Moderate Impact 9 – Strong Impact **Threats**	**Vulnerabilities** Web Servers	Compute Servers	Routers	Client	Databases	Firewalls	Software	Power	Transmission	Relative Importance of Threats ↓
Denial of Service Attacks										←
Spoofing & Masquerading										Relative Vulnerability Impact
Malicious Code (Viruses, etc.)										
Human Errors (Accidental)										
Insider Attacks (Malicious)										
Intrusion										
Spamming										
Physical Damage to Hardware										

Table 3. Threats worksheet (correlation between controls and threats)

Scale 0 – No Impact 1 – Weak Impact 3 – Moderate Impact 9 – Strong Impact **Controls**	**Threats** Denial of Service	Spoofing &	Malicious Code	Human Errors	Insider Attacks	Intrusion (Hackers)	Spamming	Physical Damage	Relative usefulness of controls ↓
Firewalls									←
IDS									Relative Importance of Threats
Single Sign-on									
DMZ									
Security Policy									
Employee Training									
Configuration of Architecture									
Hardening of Environment									

In order to protect the new technology, increase revenue, as well as enhance communication and productivity, a uniform informational infrastructure is necessary. This involves integrating business processes across different divisions into a single monolithic process shared by all the organizations. In order to be able to build security into the processes at the inception, an analysis of the security posture of the organization was conducted using the proposed methodology. This case study presents a comprehensive risk analysis of its assets, vulnerabilities, and threats inherent in the business processes. The three matrices that relate the assets with the vulnerabilities, threats and controls in the organizations are presented in Tables 4, 5 & 6 respectively.

Table 4 presents the vulnerability matrix that associates the system vulnerabilities with the impacts/assets of the organization. To construct the matrix, relative importance of assets/impacts to the business was computed. For instance, the survival of the business depends on its ability to develop and protect new technology; therefore, new technology is ranked high. Based on the assets, key vulnerabilities related to each asset/ impact were determined and the impact of the vulnerabilities on assets/ impacts was added to the table.

The data in the vulnerability matrix was aggregated and sorted to determine the relative importance of vulnerabilities. Since external hackers need to penetrate the firewall in order to access confidential information, firewall ranks high in the vulnerability matrix. Also, since GE Wind's subsidiaries are globally distributed, data transmission ranked high. The aggregate vulnerability data was added to the threat matrix along with the threats corresponding to the vulnerabilities. Based on the perceived ability of the threats to exploit vulnerabilities the threat matrix was populated as shown in Table 5.

Table 6 shows the control matrix in which aggregate data of threats from the threat matrix and the corresponding controls were added. The relative impact of different controls on the threats was also determined using subjective judgment and the data was aggregated to determine the prioritized list of controls. This information, coupled with the cost of controls is used for security planning. The results of this analysis and the aggregate data in the matrices will be used during process integration and for selection of software and hardware.

CONCLUSION

The paper presents an easy to use methodology for information security risk analysis that the organizations can easily adapt. The methodology provides easy to use templates that can be gradually refined as more information becomes available. The methodology provides transparency to the analysis process. The case study at GE Wind highlights important security issues that the organization faces. Since the assets, threats and vulnerabilities are constantly changing an adaptive easy to use methodology is valuable to companies for conducting risk assessments internally. This simple methodology will promote a risk analysis by more companies that are often daunted by the expensive, elaborate and cumbersome methodologies proposed by auditing firms.

REFERENCES

Alberts, C., and Dorofee, A., *Managing Information Security Risks: The Octave Approach*, Pearson Education Inc., 2003.

Backhouse, J. and Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5(1), 2-9.

Table 4. Vulnerability Matrix for GE Energy, Wind Division

Vulnerabilities Matrix Strong 9 Moderate 3 Weak 1 Not Related 0 Priority Ranking 1&2 not important 3 Important, not a Key Driver 4 Important, but impacted by Key Drivers 5 Key Driver	**Assets/Impacts**	Export Control info.	Reputation (Trust)	IP control/management	Confidential Client Secrets	Lost Sales/Revenue	Information Integrity	Services Availability	Communication	Cleanup Costs-old & new system	Software-new & old system	Hardware-new& old	Total Score	Rank (Higher more significant)
Vulnerabilities	**Priority**	11	10	9	8	7	6	5	4	3	2	1		
Firewalls	5	9	9	9	9	3	9	3	9	3	9	9	504	13
Data Transmission	5	9	9	9	3	3	9	9	9	9	9	3	498	12
Databases	4	9	3	9	9	9	9	3	3	9	9	3	474	11
Application architecture	4	9	9	9	3	3	3	3	1	9	9	9	406	10
Physical security	3	9	3	3	9	9	3	3	3	9	1	9	374	9
Intranet Computer Servers – Configuration Errors	2	9	1	9	9	1	3	9	3	3	9	1	372	8
Extranet Servers (internet facing) – Configuration Errors	4	1	9	9	9	1	3	9	3	3	9	1	364	7
Password Strength (Password attack)	3	9	9	3	9	1	3	1	3	1	9	1	352	6
Client Nodes (User PCs & Laptops)	3	9	3	9	9	1	3	3	1	3	3	9	350	5
Hardware – Web server, Router…	5	1	9	3	9	3	3	9	3	9	3	9	338	4
Insecure wireless	2	9	3	9	9	1	3	3	1	3	1	1	338	4
Internet base service (Like VPN)	1	9	1	3	3	1	1	3	1	3	3	1	208	2
Power outage	1	0	1	0	0	3	1	9	3	3	1	1	106	1

Table 5. Threat Matrix for GE Energy, Wind Division

Threat Matrix

Strong 9 | Moderate 3 | Weak 1 | Not Related 0

Priority Ranking
1&2 Not important
3 Important, not a Key Driver
4 Important, but impacted by 5s
5 Key Driver

Threats	Priority	Vulnerabilities: Firewalls	Data Transmission	Databases	Application architecture	Physical security	Hardware – Web server, Router…	Password strength (Password attack)	Intranet Computer Servers – Configuration Errors	Client Nodes (User PCs & Laptops)	Extranet Servers (internet facing) – Configuration Errors)	Insecure wireless	Internet base service (Like VPN)	Power outage	Total Score	Rank (Higher more significant)
		13	13	11	10	9	9	7	6	5	4	3	2	1		
Intrusion (Hacking, Password attacks)	5	9	3	3	9	9	1	9	3	9	9	9	3	1	170	12
Server Failures	3	9	9	9	3	9	9	1	9	1	9	1	1	9	158	11
Physical Damage to hardware	1	1	9	9	9	9	9	0	3	3	3	1	1	3	132	10
Extortion	4	1	3	3	3	9	3	3	3	9	9	3	3	1	122	9
Insider Attacks (Malicious)	4	3	3	3	3	9	1	3	9	9	1	3	1	1	114	8
Spoofing & masquerading	3	1	9	1	3	1	1	1	9	9	9	9	1	1	110	7
Denial of Service	2	9	1	0	9	1	3	1	9	1	9	3	3	1	100	6
Human error (Accidents)	3	3	9	3	3	3	1	3	9	3	3	1	1	1	90	5
Theft of computers (laptops/servers)	2	1	0	1	1	9	1	1	1	9	1	3	1	1	76	4
Violation Export Control compliance	1	1	1	1	1	9	1	1	1	9	1	1	1	1	74	3
Malicious Code(Viruses, Worms, etc)	4	1	1	1	3	1	1	1	3	9	3	3	3	1	62	2
Buffer Overflow attacks	5	0	9	0	1	1	1	1	3	1	3	1	1	1	46	1

Table 6. Control Matrix for GE Energy, Wind Division

Control Matrix

Strong 9 | Moderate 3 | Weak 1 | Not Related 0

Priority Ranking
1&2 not important
3 Important, not a Key Driver
4 Important, but impacted by 5s
5 Key Drive

Controls	Priority	Threats: Intrusion (Hacking, Password attacks)	Server Failures	Physical Damage to hardware	Extortion	Insider Attacks (Malicious)	Spoofing & masquerading	Denial of Service	Human error (Accidents)	Theft of computers (laptops/servers)	Violation Export Control compliance	Malicious Code (Viruses, Worms, etc)	Buffer Overflow attacks	Total Score	Rank (Higher more significant)
		12	11	10	9	8	7	6	5	4	3	2	1		
Security Policy	5	9	1	1	9	9	9	3	3	3	9	9	1	436	12
Hardening of Environment (physical)	5	9	3	9	1	9	1	3	3	9	9	3	1	422	11
Firewalls	5	9	9	3	3	1	9	1	3	1	1	1	1	366	10
Configuration of Architecture	4	1	9	9	1	3	1	9	1	1	1	0	9	316	9
Employee Training	2	9	1	0	3	3	3	1	9	3	9	9	9	308	8
Auditing & Monitoring (logs, spybot, etc) -IDS	4	3	9	3	1	3	9	1	3	3	1	3	3	306	7
System Administrative Due diligence	4	3	1	1	3	3	3	3	9	3	9	3	3	240	6
DMZ	3	3	9	3	3	0	3	1	3	0	0	0	0	234	5
Single Sign-on	3	1	1	0	9	3	9	1	1	1	3	0	0	215	4
User disclosure of credentials, passwords, etc	3	3	1	0	3	9	3	0	0	1	9	1	1	201	3
Spyware (prevent external spyware load in our system)	2	1	1	1	1	3	9	1	0	1	1	1	1	145	2
GPS tracking system (Asset Tracking System)	1	0	0	0	1	1	1	0	1	9	9	1	0	94	1

Barber, B. and Davey, J. (1992). The use of the CCTA risk analysis and management methodology CRAMM. *Proc. MEDINFO92*, North Holland, 1589 –1593.

Baskerville, R. (1993). An Analytical Survey of Information System Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*, 375-414.

Cerullo, M.J., and Cerullo, V. (1994). EDP risk analysis. *Computer Audit Journal*, (2), 9-30.

Fisher, R. (1984). *Information Systems Security*. Prentice-Hall.

Parker, D.B. (1981). *Managers Guide to Computer Security*. Prentice-Hall, Inc, Reston, VA, USA.

Stolen, K., den Braber, F. & Dimitrakos T. (2002). *Model-based Risk Assessment – The CORAS Approach.*

Suh, B. and Han, I. (December 2003). The IS Risk Analysis Based on a Business Model, *Information and Management*, 41(2), 149-158.

Weiss, J.D. (1991). A System Security Engineering Process. *In Proceedings of the 14th National Computer Security Conference*, Washington, DC.