Proceedings of GLOGIFT 08
June 14-16, 2008
Stevens Institute of Technology
Hoboken, NJ, pp. 185-195

PREDICTING RISK FOR INFORMATION VALUE ASSET BASED ON ANNUALIZED LOSS EXPECTANCY

C S Atole[*] and R C Pathak[**]

ABSTRACT

Today the mankind is passing through the era of break through technological changes and fiercely competitive benchmarks in business scenario obtaining all over the world. To change and harness the intangible assets becomes an insurmountable mammoth task and it will be observed that we are standing, in this regards at the threshold of watershed. The manifestation of the product strategies ushers in the challenging task of managing explosive dimensions of data. Thus the management of the valuable database and information value asset in the network security system has become dire essential. At the same time the wealth of data and information security requires a full proof risk management system as well.

Risk relates primarily to the extent of ability of the people to predict a particular outcome with certainty. Risk management is the human activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. Thus risk management can be simply defined as systematic process of identifying, analyzing and responding to the probable risks in the projects. Software, systems, and information — the lifeblood of many businesses in the Information Age — are increasingly at risk, as the historical approaches to security and risk management become increasingly inadequate. Consequently, the evolution of methodologies focusing on software risk management at the enterprise level has been receiving increasing attention, and the need for a comprehensive risk management programs has become a necessity.

Efficient management is based on right information at right time, and today in the age of information technology, information security measures are taken by almost all the organizations. As information technology increases in importance, so do the number of threats directed against the critical infrastructure. The criticality of the infrastructure is centric around the pillars of information technologies. These pillars are Enterprise Resource management (ERP), Supply Chain Management (SCM), Customer Relationship Management (CRM), Knowledge Management (KM), Wireless Application Protocols (WAP), Data Warehouse and Data Mining. Risk factors may change or new ones appear at a space that might easily outdate protective safe guards that have already been implemented or recovery plans that had been previously developed and validated. In order to effectively calculate the chance of experiencing the undesirable outcome, as well as its magnitude, one must have awareness of the elements of risk and their relationship to each other.

In this paper attempt has been made to home down the risk management factors and its manifestation in information security system. Here we have concentrated on various risk metrics and with the help of case studies we have shown the qualitative and quantitative assessment of the risk identified, which in turn will help predict risk to information asset value based on annualized loss expectancy. This in turn will help managers to take timely action in the appropriate direction.

Keywords: *E- business, Information security, Risk management, Asset value, Threat, Single Loss Expectancy, Annualized Rate of Occurrence, Annualized Loss Expectancy*

Introduction

The Internet revolution began in North American in 1960 spreading all over the world and has

[*] Director, JSPM's Eniac Institute of Computer Application, Wagholi, Pune – 412207, (020)27051173 65101860, Fax: 020-27052590, chitrag_desai@yahoo.com

[**] Principal, JSPM's Imperial College of Engineering and Research, Wagholi, Pune – 412207 (020)27051170; 09822097724, Fax: 020-27052590, rcpathakindia@yahoo.com

become an essential tool for any business. Predictions were made [Kalakota, 1999][Dyson, 1997][Net Figures, 2001] regarding future indicating that Internet is not a fad nor it is a trend, but the beginning of next business revolution which will change the way we live and it has. Internet revolution exploded E-business and many companies are formulating Business-to-Business [LaFaire D, 2001] and Business-to-Customer. One good thing of E-Business is that it did not force to change the business but change the way to do the business. Businesses that accept transaction via web have gained a competitive edge by reaching a world wide audience at a very low cost.

Many successful e-businesses rely on a complex integration of IT support systems that can interact with many different channels. Databases, electronic email system, Internet web servers, personnel computer networks and mobile phones all are part of IT infrastructure for e-business. The world's biggest technology firms-Compaq, Computer Associates, Dell, Hewlett-Packard, IBM, Intel, Microsoft and SAP-formed a business internet consortium [Marketwatch, 2001], which is a non-profit making organization that has helped to generate technologies and practices for growing e-business market.

E-commerce has waved all industries including finance industry also [Merkow, 1999]. However, despite all the hype of getting their products and services online, organizations have been faced with an even bigger problem, 'the threat of computer security', which is one of the main barriers to Internet commerce. The original Internet was designed research not electronic commerce. As such, it operated in a single domain of 'trust'. While provisions were made to allow remote users to globally access critical files on computers worldwide, security generally relied on users' mutual respect and honour, as well as their knowledge of conduct considering appropriate for interacting on the network. Like any other distribution channel, the web poses a unique set of security issues, which businesses must address at the outset to minimize risk.

Risk is an essential component of trust, but it is unclear whether risk is an antecedent of trust, or is an outcome of trust. Risk –taking behavior and trust behavior are really different sides of the coin; what really matters is that the connection between risk and trust depends on situation and the context of a specific, identifiable relationship. Spoofing, unauthorized disclosure, unauthorized action and data alteration are security risks on Internet transactions which are the burning issues of concern in the global platform.

Risk is closely associated with security [Kulloro, 1996] .Because risks are like those project entry points whose doors seem to be locked but are unsafe and any thing in any way can breech the system, which was thought to be secure [Atole, 2004]. And since last fifteen years as the information technology has formed the background of the entire business community. Network functionality has evolved steadily with the risk creeping along with it raising a big question mark on the security. When the risk is so related to security, it is important to know from where to start managing risk for handling security based problems. Risk management is built in to the process, so that risk to the success of the project are identified and attached early in the development process; where there is time to react. While there are number of ways to identify analyze and assess risk and considerable discussion on risk in media and among information security professionals, there little real understands of the process and metrics for analyzing and assessing risk.

In this paper attempt has been made to home down the risk management factors and its manifestation in information security system. Here we have concentrated on various risk metrics and with the help of case studies we have shown the qualitative and quantitative assessment of the risk identified, which in turn will help predict risk to information asset value based on annualized loss expectancy. This in turn will help managers to take timely action in the appropriate

direction.

Purpose of Information Security Management

Everyone has a different idea of what "security" is, and what levels of risk are acceptable. While it's often tempting to say "my data isn't interesting; nobody would want to hack me", you have no choice but to assume that if you're vulnerable to a certain kind of attack, some attacker eventually will probe for and exploit it, regardless of whether you're imaginative enough to understand why. It's considerably less important to understand attackers than it is to identify and mitigate the vulnerabilities that can feasibly be attacked.

The information security problem can be avoided or better handled by enforcing the policy [Harold, 2000]:

1. To achieve coherent security architecture, security must be considered from the outset and not as an after thought.
2. Competence in design for security policy enforcement, testing for security and assessment of security must be part of education of system implementers.

To handle security issue effectively it should be subject to proper management. The Information Security Management must establish and maintain a security program that ensures [Lidgoug, 1999]:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non repudiation

Availability

Availability ensures the survivability of network services despite denial of service attacks. Availability is a prime concern because in business information at right time means a lot and the same information after the time has gone means useless.

Confidentiality

It is the protection of information in the system so that unauthorized persons cannot access it. Confidentiality can be compromised in several ways. The following are some of the most commonly encountered threats to information confidentially.

- Hackers
- Masqueraders
- Unauthorized user activity
- Unprotected downloaded files
- Local area networks
- Trojan Horses

Integrity

Integrity guarantees that a massage being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

Non-repudiation

Non-repudiation ensures that the origin of a massage cannot deny having sent the massage.

In spite of taking care for disaster recovery and having contingency planning it is possible that the information system is subjected to some kind of risk. And as we know "taking a risk" means "taking a chance", but a risk or chance of what is not often so clear.

In the next section we will see how information security can be handled in risk management.

Handing Information Security in Risk Management

As we all know that today is the age of information technology, information security measures are taken by almost all the organizations. In spite of various measures taken there is a possibility that we night experience an undesirable outcome. In order to effectively calculate the chance of experiencing the undesirable outcome, as well as its magnitude, one must have an awareness of the elements of risk and their relationship to each other. Also we should be able to identity whether it is a high risk or low risk [Karolak, 1996].

The definition of high risk component varies depending on the context for example, a high risk component may be

1. One that contains faults found during testing.
2. One that contains faults found during operations.
3. One that is costly to correct when error has found.

Recent evidence suggests that most faults are found in only a few of the system components. If these few components can be identified early, then an organization can take mitigating action. Examples of mitigating actions include focusing defect detection activities on high risk components by optimally allocating testing resources, or redesigning components that are likely to cause field failure or be costly to maintain.

Early prediction is commonly cast as a binary classification problem. This is achieved through a quality model that classifies components into either a high or low risk category. As overview of quality model is shown in figure 1.

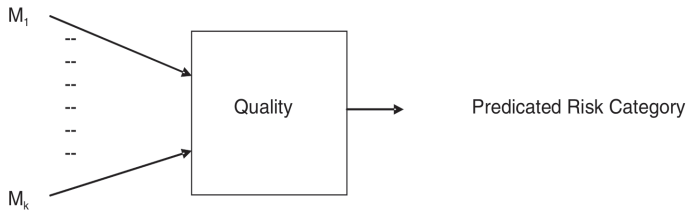

Figure 1. Definition of Quality Model

A quality model is developed using a statistical modeling or machine learning technique, or a combination of techniques. Thos is done using historical data. Once constructed such a model takes an input the values from a set of metrics (M1...Mk) for a particular component, and produce a predication of the risk category (say either high or low) for the component.

Once we know that there is a risk (high o low), one is better prepared to decide what to do about it-

1. Accept the risk
2. Do something to reduce the risk to an acceptable level.
3. To transfer the risk i.e., buy insurance.

This process of identifying, analyzing and assessing, mitigating, or transferring risk is generally characterized as risk management. There are thus a few key questions that are at the core or risk management process:

1. What could happen (threat)?
2. How much will it cost (annualized)?
3. How often could it happen (threat frequency, annualized)?
4. How certain are the answers to first three questions (recognition of uncertainty)?

Once we have identified and assessed risk, we need to answer the following questions:

1. What can be done (risk mitigation)?
2. How much will it cost (annualized)?
3. Is it cost effective (cost/benefit) analysis?

A comprehensive risk management approach to information security requires identification of vulnerabilities and threats that are most likely to occur, quantification of the potential harm to your business, and development of mitigation efforts to achieve an acceptable risk level [Cynthia, 1997]**.** This is not simply about managing a device, pushing a rule change or correcting a patch level. It requires determining which assets to patch first, what controls to implement, whether or not patching occurred, and what effect remediation efforts will have on overall risk exposure.

1. The risk management process begins with the development of a risk management narrative including a statement of acceptable risk tolerance used to determine policies and communicate decisions to stakeholders.
2. The risk identification process uses real-time data to identify vulnerabilities and threats related to security technology, people, and processes.
3. The application of standard assessment frameworks such as ISO 27002 and BSI 7799-2 to the risk management narrative and risk identification shows how company policies and implementation measure up to IT security best practices.
4. Through risk analysis, potential threats are identified and quantified according to the likelihood of attack, the asset value to the business, the location of the asset on the network, and any legal or compliance issues related to the risk. Risk analysis helps enterprises to prioritize risks and optimize available resources.
5. The response plan and risk mitigation road map prioritizes actions to reduce risk as quickly and cost effectively as possible.

Regular assessment and continuous monitoring helps ensure that mitigation has occurred, and helps identify new threats. Various risk elements, their relationship to each other and some form of metrics that can be used for predicting risk to the information security.

Elements of Risk Metric

There are six primitive elements of risk modeling

1. Asset Value
2. Threat Frequency
3. Threat Exposure Factor
4. Safegaurd Effectiveness
5. Safegaurd Cost
6. Uncertainty

Let us focus on the above risk elements and their associated parameters.

Information Assets

A specific information asset may consist of any subset of the complete body of information, i.e., accounts payable, inventory control, payroll, etc. Information is regarded as intangible assets separate from the media on which it resides. There are several elements of value to be considered: first is the simple cost of replacing the information, second is the cost of replacing supporting software and third the values that reflect the costs associated with loss of the information's confidentiality, availability and integrity. Some consider the supporting hardware and NetWare to be information assets as well .However, these are distinctly tangible assets. Therefore using tangibility as the distinguishing characteristic, it is logical to characterize hardware differently than the information itself. Software , on the other hand , is often regarded as information .These five elements of value of an information assets often dwarf all other values relevant to an assessment of risk .Let us have a look at the definition of five levels of information value:

- V1: Negligible adverse effects
- V2: Minimal Damage
- V3: Some damage
- V4: Serious damage
- V5: Exceptionlly grave damage

Threats

This term defines an event the outcome of which could have an undesirable impact. Depending upon the severity of the threats seven levels of threats have been defined;

- T1: Inadvertent or accidental
- T2: Casual adversary, minimal resources, little risk
- T3: Adversary minimal resources significant risk
- T4: Sophisticated, moderate resources, little risk
- T5: Sophisticated, moderate resources, significant risk
- T6: Very sophisticated, abundant resources, little risk
- T7: Very sophisticated, abundant resources, significant risk

Any of the threat level will incur asset value loss from a threat event; this can be represented by using the metric exposure factor, which is defined as below:

Exposure Factor (EF)

This factor represents a measure of magnitude of loss or impact on the value of an asset. It is expressed as a percent, ranging from 0% to 100%, of asset value loss arising from a threat

event. This factor is used in the calculation of single loss expectancy (SLE), which is defined below.

Single Loss Expectancy (SLE)

This factor is used to determine the monetary loss (impact) for each occurrence of a threat event.

Asset value * exposure factor = Single Loss Expectancy

The SLE is usually an end result of a Business Impact Analysis.

To effectively identify risk and to plan budgets for information risk management and related risk reduction activity, it is helpful to express loss expectancy in annualized terms. Annualized loss expectancy (ALE) is defined as below:

SLE * ARO = ALE

The ALE for a threat with an SLE of $10000 that is expected to occur only once in 100 years is $100. Where, ARO is Annualized Rate of Occurrence.

Annualized Rate of Occurrence (ARO)

This term characterizes, on an annualized basis, the frequency with which the threat is expected to occur. For example, a threat occurring once in a 10 year has an ARO of 1/10 or 0.1; a threat occurring 50 times in a given year has an ARO of 50.0

When an ARO is fractioned in the equation, the significance of this risk factor is addressed and integrated in to the information risk management process. Thus, risk is more accurately portrayed, and the basis for meaningful; cost/benefit analysis of risk reduction measures is established.

Safeguard

This term represents a risk-reducing measure that acts to detect, prevent or minimize loss associated with the occurrence of a specified threat or category of threats .Safeguards are also often described as controls of countermeasures. Safeguard effectiveness represents the degree, expressed as a percent from 0 to 100 % to which a safeguard may be characterized as effectively mitigating vulnerability and reducing associated loss risk .Here characterizes the absence or weakness of a risk reducing safeguard .It is a condition that has the potential to allow a threat to occur with greater frequency ,greater impact or both .For example, not having a fire suppression system could allow an otherwise minor ,easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased a consequence of not having a fire suppression system.

Uncertainty

This term characterizes the degree, expressed as a percent from 0.0 to 100% to which there is a less than complete confidence in the value of any element of risk assessment uncertainty is typically measured inversely, with respect to confidence i.e., if confidence is low, uncertainty is high.

Attackers

Attackers, also sometimes called “actors”, can range from the predictable (disgruntled ex-employees, mischievous youths) to the strange-but-true (drug cartels, government agencies, industrial spies). When you consider possible attackers, almost any type is possible; the challenge

is to gauge which attackers are the most likely.

A good rule of thumb in identifying probable attackers is to consider the same suspects your physical security controls are designed to keep out, minus geographical limitations. This is a useful parallel: if you install an expensive lock on the door to your computer room, nobody will ask, “Do you really think the maintenance staff will steal these machines when we go home?”

Risk Analysis: A Case Study

Risk analysis is to combine the estimates of the value of potential loss and probability of loss to develop an estimate of annual loss expectancy. The purpose is to pinpoint the significant threats as a guide to the selection of security measures and to develop a yardstick for determining the amount of money that is reasonable to spend on each of them. In other words, the cost of a given security measure should relate to the loss (es) against which it provides protection

Once you’ve compiled lists of assets and vulnerabilities (and considered likely attackers), the next step is to correlate and quantify them. One simple way to quantify risk is by calculating annualized loss expectancies (ALEs).

For each vulnerability associated with each asset, you estimate first the cost of replacing or restoring that asset (its single loss expectancy) and then the vulnerability’s expected annual rate of occurrence. You then multiply these to obtain the vulnerability’s annualized loss expectancy.

In other words, for each vulnerability we calculate: single loss expectancy (cost) × (expected) annual rate of occurrences = annualized loss expectancy.

For example, suppose Mommenpop, Inc., a small business, wishes to calculate the ALE for denial-of-service (DOS) attacks against their SMTP gateway. Suppose further that e-mail is a critical application for their business; their ten employees use e-mail to bill clients, provide work estimates to prospective customers and facilitate other critical business communications. However, networking is not their core business, so they depend on a local consulting firm for e-mail-server support.

Past outages, averaging one day in length, have tended to reduce productivity by about one-fourth, which translates to two hours per day per employee. Their fallback mechanism is a fax machine, but since they’re located in a small town, this entails long-distance telephone calls and is expensive.

All this probably sounds more complicated than it is; it’s much less imposing expressed in spreadsheet form (Table 1).

Table 1: Itemized Single Loss Expectancy

Item Description	Estimated Cost
Recovery: consulting time from 3rd–party firm (4 hrs @ $150)	$600.00
Lost productivity (2 hours per 10 workers @ avg. $17.50/hr)	$350.00
FAX paper, thermal (1 roll @ $16.00)	$16.00
long–distance FAX transmissions (20 @ avg. 2 min @ $.25 /min)	$10.00
Total SLE for 1–day DOS attack against SMTP svr.	$950.00

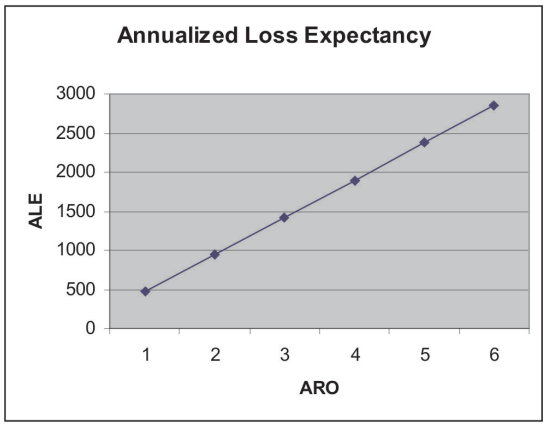

Figure 2: Increase in ALE with Increased Frequency of ARO

One thing to remember when using the ALE value is that, when the Annualized Rate of Occurrences is of the order of one loss per year, there can be considerable variance in the actual loss. For example, suppose the ARO is 0.5 and the SLE is $10,000. The Annualized Loss Expectancy is then $5,000, a figure we may be comfortable with. Using the Poisson Distribution we can calculate the probability of a specific number of losses occurring in a given year:

Table 2: Poisson Distribution for ALE

Number of Losses in Year	Probability	Annual Loss
0	0.6065	$0
1	0.3033	$10,000
2	0.0758	$20,000
?3	0.0144	?$30,000

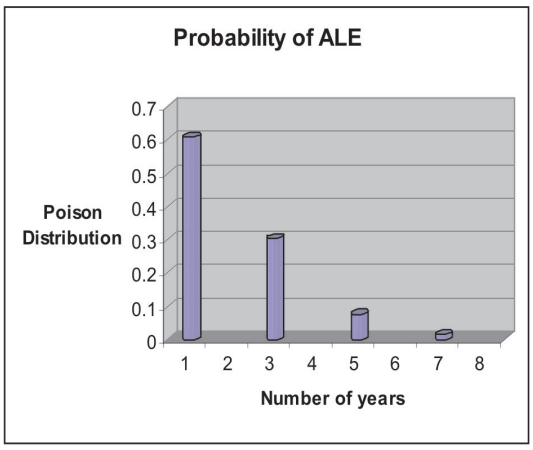

Figure 3: Poisson Distribution for ALE

We can see from this table that the probability of a loss of $20,000 is 0.0758, and that the probability of losses being $30,000 or more is approximately 0.0144. Depending upon our tolerance to risk and our organization's ability to withstand higher value losses, we may consider that a security measure which costs $10,000 per year to implement is worthwhile, *even though it is more than the expected losses due to the threat.*

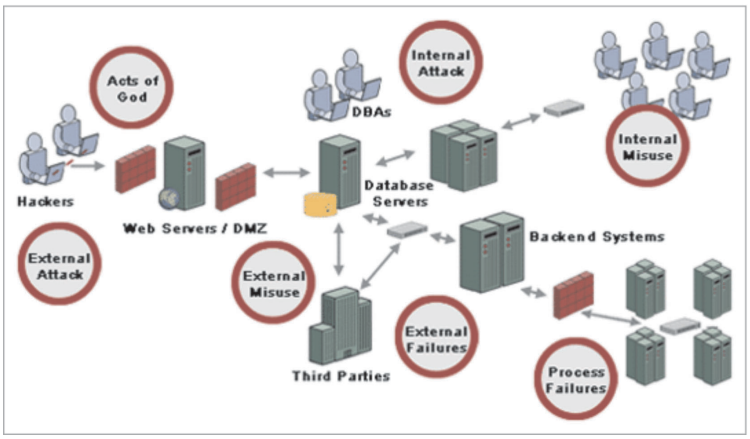

Figure 4: Effective Risk Management in Information Security System

Once the annualized loss expectancy is identified, security professional's can make tradeoffs to achieve an acceptable level of risk without compromising data availability, confidentiality, and integrity. An effective risk management program gives c-level executives a way to manage the evolution of their information security systems.

Conclusion

Security is a major concern for Internet users and system administrators. Whether to protect confidential data and information in individual files, lock a computer system to unauthorized users, control access to an intranet or an extranet, or conduct business on Internet, one need to determine an appropriate level of security and the effective means to achieve the objectives. The threat to Internet security is one of the main barriers to electronic transaction via the Internet medium. With the current popularity and the potential profits of electronic business, many executives face a conflict situation. That is Connecting to the Internet and expanding their business would lead to risks and threats of intrusion. On the other hand remaining disconnected from the Internet would sacrifice their customer contact and services to their competitors.

In this paper we have focused on information security problem and the purpose of information security management. Here we have discussed how security issues if handled in early software development process in risk management phase can help risk managers to take timely actions. Also managing risk means identifying, assessing, mitigating and transferring risk. This requires proper identification of risk elements applicable to information security. Various risk elements have been identified and risk metrics are concentrated that will help in giving the quantitative and qualitative assessment of risk identification.

Acknowledgement

We are thankful to Honorable Founder Secretary, Prof. T J Sawant and Campus Director Prof. V A Bugade of Jayawant Shikshan Prasarak Mandal, Pune for their kind support and motivation.

References

- Atole, Chitra and Kale K V, (2004), "Handling Information Security in Risk Management", *National Level Conference on Computer Communication and Security*, India, 240-248.
- Cynthia E Irvine, (1997)," Challenges in Computer Security Education", *IEEE Software pages* 110-111
- Dyson., S. (1997) *Release 2.0: A Design for living in the Digital Age*, Broadway Books, Newyork
- Harold F, Tipton, (2000), *Handbook of Information Security Management: Access Control*, McGraw Hill
- Kalakota, R and Whinston, A.B (1999) *Electronic Commerce, A Managers Guide,* Addison Wesley
- Karolak, D W., *Software Engineering Risk Management,* IEEE Computer Society Press
- Kolluru, R., Bartell, S., Pitblado, R., and Stricoff, S., (1996), "*Risk Assessment and Management Handbook for Environmental, Health, and Safety Professionals*", Boston: McGraw-Hill.
- Lidguou Zhou, Zygmont, (1999), "*Securing Ad-hoc Networks*", DARPA and Air Force Research Laboratory, Air Force martial Command, USAF Project Activity.
- LaFaire, D (2001) "Are you Ready to B2B?", *EAI Journal*
- Marketwatch(2001), "Consortium to address e-business Challenges", *Finance on Windows*, Spring
- Merkow, M. (1999) "E-commerce Security Technologies" *ec-outlook*
- Net Figures (2001) "E-business at a Glance" *Finacial Time*, - Connectis, 9 March.