International Journal of Business and Management Review
Vol.5, No.2, pp.36-48, March 2017
Published by European Centre for Research Training and Development UK (www.eajournals.org)

THE MANAGEMENT OF INFORMATION AND OPERATIONAL RISK IN BOTH THE PUBLIC AND PRIVATE SECTORS

Kenebara, Florence A.
Business Administration,
Niger Delta University,
Wilberforce Island, Bayelsa State, Nigeria

ABSTRACT*: Information technology is widely recognized as the engine that drives any growing economy, giving industries a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizationsin the public and private sectors are beginning to depend on technology-intensive information systemsto successfully carry out their missions and business functions. Information systems can include diverse entities ranging from high-end supercomputers, workstations, personal computers, cellular telephones, and personal digital assistants to very specialized systems (e.g., weapons systems, telecommunications systems, industrial/process control systems, and environmental control systems). Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation at large by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the nation. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.*

KEYWORDS: Management, Information, Operational Risk, Public and Private Sectors

INTRODUCTION

It is easy to find news reports of incidents where an organization's security has been compromised. For example, a laptop was lost or stolen, or a private server was accessed. These incidents are noteworthy because confidential data might have been lost. Modern society depends on the trusted storage, transmission, and consumption of information. Information is a valuable asset that is expected to be protected. Information security is often considered to consist of confidentiality, integrity, availability, andaccountability (Blakley, McDermott, and Geer, 2002). Confidentiality is the protection of informationagainst theft and eavesdropping. Integrity is the protection of information against unauthorized modification and masquerade. Availability refers to dependable access of users to authorized information, particularly in light of attacks such as denial of service against information systems. Accountability is the assignment of responsibilities and traceability of actions to all involved parties.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Naturally, any organization has limited resources to dedicate to information security. An organization's limited resources must be balanced against the value of its information assets and the possible threats against them. It is often said that information security is essentially a problem of risk management (Schneier, 2000). It is unreasonable to believe that all valuable information can be kept perfectly safe against all attacks (Decker, 2001). An attacker with unlimited determination and resources can accomplish anything. Given any defenses, there will always exist a possibility of successful compromise. Instead of eliminating all risks, a more practical approach is to strategically craft security defenses to mitigate or minimize risks to acceptable levels. In order to accomplish this goal, it is necessary to perform a methodical risk analysis (Peltier, 2005). This chapter gives an overview of the risk management process.

Organizational risk can include many types of risk (e.g., program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities. Effective risk management requires that organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems-systems that organizations depend on to accomplish their missions and to conduct important business-related functions. Leaders must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations—providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations.

Basic Concepts Associated With Risk Management

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization's missions/business functions. Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.

Risk management may be divided into three processes namely Risk Assessment, Risk Mitigation and Effectiveness Evaluation.(NIST, 2002; Farahmand, Navathe, Sharp, and Enslow, 2003; Alberts and Dorofee, 2002; Vorster and Labuschagne, 2005). It should be noted

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

that there is not universal agreement on these processes, but most views share the common elements of risk assessment and risk mitigation (Microsoft, 2004; Hoo, 2000). Risk assessment is generally done to understand the system storing and processing the valuable information, system vulnerabilities, possible threats, likely impact of those threats, and the risks posed to the system.

Risk assessment would be simply an academic exercise without the process of risk mitigation. Risk mitigation is a strategic plan to prioritize the risks identified in risk assessment and take steps to selectively reduce the highest priority risks under the constraints of an organization's limited resources.The third process is effectiveness assessment. The goal is to measure and verify that the objectives of risk mitigation have been met. If not, the steps in risk assessment and risk mitigation may have to be updated. Essentially, effectiveness assessment gives feedback to the first two processes to ensure correctness. Also, an organization's environment is not static. There should be a continual evaluation process to update the risk mitigation strategy with new information.

Risk Assessment

It is impossible to know for certain what attacks will happen. Risks are based on what might happen. Hence, risk depends on the likelihood of a threat. Also, a threat is not much of a risk if the protected system is not vulnerable to that threat or the potential loss is not significant. Risk is also a function of vulnerabilities and the expected impact of threats. Risk assessment involves a number of steps to understand the value of assets, system vulnerabilities, possible threats, threat likelihoods, and expected impacts. Here are the basic steps in risk assessment.

System Characterization

It is obviously necessary to identify the information to protect, its value, and the elements of the system (hardware, software, networks, processes, people) that supports the storage, processing, and transmission of information. This is often referred to as the information technology (IT) system. In other words, the entire IT environment should be characterized in terms of assets, equipment, flow of information, and personnel responsibilities.

System characterization can be done through some combination of personnel interviews, questionnaires, reviews of documentation, on-site inspections, and automated scanning. A number of free and commercial scanning tools are available, such as Sam Spade, Cheops, CyberKit, NetScanTools, iNetTools, Nmap, Strobe, Netcat, and Winscan.

Threat Assessment

It is not possible to devise a defense strategy without first understanding what to defend against (Decker, 2001). A threat is the potential for some damage or trouble to the IT environment. It is useful to identify the possible causes or sources of threats. Although malicious attacks by human sources may come to mind first, the sources of threats are not necessarily human.Sources can also be natural, for example, bad weather, floods, earthquakes, tornadoes, landslides, avalanches, etc. Sources can also be factors in the environment, such as power failures. Of course, human threats are typically the most worrisome because malicious attacks will be driven by intelligence and strategy. Not all human threats have a malicious intention; for example, a threat might arise from negligence (such as forgetting to change a default

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

computer account) or accident (perhaps misconfiguring a firewall to allow unwanted traffic, or unknowingly downloading malicious software).

Malicious human attackers are hard to categorize because their motivations and actions couldvary widely (McClure, Scambray, and Kurtz, 2001). Broadly speaking, human attackers can beclassified as internal or external. The stereotypical internal attacker is a disgruntled employee seeking revenge against the organization or a dishonest employee snooping for proprietary information or personal information belonging to other employees. In a way, internal attackers are the most worrisome because they presumably have direct access to an organization's valuable assets and perhaps have computer accounts with high user privileges (e.g., Unix root or Windows admin). In contrast, external attackers must penetrate an organization's defenses (such as firewalls) to gain access, and then would likely have difficulty gaining access with root or admin privileges. External attackers might include amateur "hackers" motivated by curiosity or ego, professional criminals looking for profit or theft, terrorists seeking destruction or extortion, military agents motivated by national interests, or industrial spies attempting to steal proprietary information for profit. External threats might even include automated malicious software, namely viruses and worms that spread by themselves through theInternet. It might be feasible to identify major external threats, but a possibility always exists for a new unknown external threat.

Vulnerability Analysis

Threats should be viewed in the context of vulnerabilities. A vulnerability is a weakness that might be exploited. A threat is not practically important if the system is not vulnerable to that threat. For example, a threat to take advantage of a buffer overflow vulnerability unique to Windows95 would not be important to an organization without any Windows95 computers. Technical vulnerabilities are perhaps the easiest to identify. Vendors of computing and networking equipment usually publish bulletins of bugs and vulnerabilities, along with patches, for their products. In addition, several Web sites such as Bugtraq (http://www.securityfocus.com/archive/1) and CERT (http://www.cert.org/advisories) maintain lists of security advisories about known vulnerabilities. It is common practice to use automated vulnerability scanning tools to assess an operational system. Several free and commercial vulnerability scanners are available, such as Satan, SARA, SAINT, and Nessus. These scanners essentially contain a database of known vulnerabilities and test a system for these vulnerabilities by probing. Another method to discover vulnerabilities in a system is penetration testing which simulates the actions of an attacker (NIST, 2003). The presumption is that active attacks will help to reveal weaknesses in system defenses.

Not all vulnerabilities are necessarily technical and well defined. Vulnerabilities might arise from security management. For example, human resources might be insufficient to cover all important security responsibilities, or personnel might be insufficiently trained. Security policies may be incomplete, exposing the system to possible compromise. Other vulnerabilities might be related to system operations. For example, suppose old data CDs are disposed in trash that is publicly accessible. It would be easy for anyone to retrieve discarded data.

Impact Analysis

The impact of each threat on the organization depends on some uncertain factors: the likelihood of the threat occurring; the loss from a successful threat; and the frequency ofrecurrence of the

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

threat. In practice, these factors may be difficult to estimate, and there are various ways to estimate and combine them in an impact analysis. The impact analysis can range from completely qualitative (descriptive) to quantitative (mathematical) or anything between. It would be ideal to estimate the exact probability of occurrence of each threat, but a rough estimate is more feasible and credible. The likelihood depends on the nature of the threat. For human threats, one must consider the attacker's motivation, capabilities, and resources. A rough estimation might classify threats into three levels: highly likely, moderately likely, or unlikely (NIST, 2002).

The loss from a successful threat obviously depends on the particular threat. The result may include loss of data confidentiality (unauthorized disclosure), loss of data integrity (unauthorized modification), or loss of availability (decreased system functionality). In financial terms, there is direct cost of lost assets and indirect costs associated with lost revenue, repair, lost productivity, and diminished reputation or confidence. Some losses may be difficult to quantify. Qualitative impact analysis might attempt to classify impacts into broad categories, such as: high impact, medium impact, and low impact. Alternatively, quantitative analysis attempts to associate a financial cost to a successful threat event, called a single loss expectancy (SLE). If the frequency of the threat can be determined (e.g., based on historical data), the product called annualized loss expectancy (ALE) is the product of the SLE and frequency (Blakley, McDermott, and Geer, 2002; NBS, 1975):
ALE = SLE x (annual rate of occurrence).

Risk determination

For each threat, its likelihood can be multiplied by its impact to determine its risk level: Risk = likelihood x impact.
The most serious risks have both high likelihood and high impact. A high impact threat with a very low likelihood may not be worthy of attention, and likewise, a highly likely threat with low impact may also be viewed as less serious. Based on the product of likelihood and impact, each threat may beclassified into a number of threat levels. For example, a simple classification might be: high risk, medium risk, or low risk. Other classification approaches are obviously possible, such as a 0-10 scale (NIST, 2002).
The risk level reflects the priority of that risk. High risks should be given the most attention and most urgency in the next process of risk mitigation. Medium risks should also be addressed by risk mitigation but perhaps with less urgency. Finally, low risks might be acceptable without mitigation, or may be mitigated if there are sufficient resources.

Risk Mitigation

It may be safely assumed that any organization will have limited resources to devote to security. It is infeasible to defend against all possible threats. In addition, a certain level of risk may be acceptable. The process of risk mitigation is to strategically invest limited resources to change unacceptable risks into acceptable ones. Risk mitigation may be a combination of technical and nontechnical changes. Technical changes involve security equipment (e.g., access controls, cryptography, firewalls, intrusion detection systems, physical security, antivirus software, audit trails, backups) and management of that equipment. Non-technical changes could include policy changes, user training, and security awareness.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Given the output from the risk assessment process, risks can be assumed or mitigated. Risk assumption refers to risks that are chosen to be accepted. Acceptable risks are generally the low risks, but a careful cost-benefit analysis should be done to decide which risks to accept. When risk mitigation is chosen, there are a number of different options (NIST, 2002):

- Risk avoidance attempts to eliminate the cause of risk, for example, eliminating the vulnerability or the possibility of the threat. For example, common software vulnerabilities may be remedied by applying up-to-date patches. So-called deterrent controls seek to reduce the likelihood of a threat. Preventive controls try to eliminate vulnerabilities and thus prevent successful attacks.
- Risk limitation attempts to reduce the risk to an acceptable level, e.g., by implementing controls to reduce the impact or expected frequency. For example, firewalls and access controls can be hardened to make it more difficult for external attackers to gain access to an organization's private network. Corrective controls reduce the effect of an attack. Detective controls discover attacks and trigger corrective controls.
- Risk transference refers to reassigning the risk to another party. The most common method is insurance, which allows an organization to avoid the risk of potentially catastrophic loss in exchange for a fixed loss (payment of insurance premiums).

Steps in Risk Mitigation

1. ***Prioritize actions*:** The risks with their corresponding levels identified through the risk assessment process will suggest what actions should be taken. Obviously, the risks with unacceptably high levels should be addressed with the greatest urgency. This step should identify a ranked list of actions needed to address the identified risks.
2. ***Identify possible controls*:** This step examines all possible actions to mitigate risks. Some controls will be more feasible or cost effective than others, but that determination is left for later. The result from this step is a list of control options for further study.
3. ***Cost-benefit analysis*:** The heart of risk mitigation is an examination of trade-offs between costs and benefits related to every control option (Gordon and Loeb, 2002; Mercuri, 2003). This step recognizes that an organization's resources are limited and should be spent in the most cost effective manner to reduce risks. A control is worthwhile only if its cost can be justified by the reduction in the level of risk. Not every cost may be easy to identify. Hardware and software costs are obvious. In addition, there may be costs for personnel training, time, additional human resources, and policy implementation. A control might also affect the efficiency of the IT system. For example, audit trailsare valuable for monitoring system-level activities on clients and servers, but might slow down system performance. This would be an additional cost but difficult to quantify.
4. ***Select controls for implementation*:** The cost-benefit analysis from the previous step is used to decide which controls to implement to meet the organization's goals. Presumably, the recommended controls will require a budget, and the budget must be balanced against the organization's other budget demands. That is, the final selection of controls to implement depends not only on the action priorities (from step 1) but also on all competing priorities of the organization. It has been reported that companies spend only 0.047 percent of their revenue, on average, on security (Geer, Hoo, and Jaquith, 2003).

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

5. ***Assign responsibilities*:** Ultimately, implementation will depend on personnel with the appropriate skills. The personnel might be available within an organization, but for any number of reasons, an organization might decide to delegate responsibilities to a third party.
6. ***Implementation*:** In the final step, the selected controls must be implemented by the responsible personnel.

Trustworthiness of Information Systems

The concept of trustworthiness can also be applied to information systems and the information technology products and services that compose those systems. Trustworthiness expresses the degree to which information systems (including the information technology products from which the systems are built) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the systems across the full range of threats. Trustworthy information systems are systems that have been determined to have the level of trustworthiness necessary to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in their environments of operation. Two factors affecting the trustworthiness of information systems are:

- *Security functionality* (i.e., the security features/functions employed within the system); and
- *Security assurance* (i.e., the grounds for confidence that the security functionality is effective in its application).

Security functionality can be obtained by employing within organizational information systems and their environments of operation, a combination of management, operational, and technical security controls from NIST Special Publication 800-53.The development and implementation of needed security controls is guided by and informed by the enterprise architecture established by organizations.

Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. Assurance is obtained by: (i) the actions taken by developers and implementers with regard to the design, development, implementation, and operation of the security functionality (i.e., security controls); and (ii) the actions taken by assessors to determine the extent to which the functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for information systems and their environments of operation. Developers and implementers can increase the assurance in security functionality by employing well-defined security policies and policy models, structured and rigorous hardware and software development techniques, and sound system/security engineering principles.

Assurance for information technology products and systems is commonly based on the assessments conducted (and associated assessment evidence produced) during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

ongoing security control monitoring. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits of the implementation of the selected security functionality.

The concepts of assurance and trustworthiness are closely related. Assurance contributes to the trustworthiness determination relative to an information technology product or an information system. Developers/implementers of information technology products or systems may provide assurance evidence by generating appropriate artifacts (e.g., the results of independent testing and evaluation, design documentation, high-level or low-level specifications, source code analysis). Organizations using information technology products or systems may perform, or rely on others to perform, some form of assessment on the products or systems. Organizations may also have direct experience with the product or system, or may receive information about the performance of the product or system from third parties. Organizations typically evaluate all of the available assurance evidence, often applying different weighting factors as appropriate, to determine the trustworthiness of the product or system relative to the circumstances.

Information technology products and systems exhibiting a higher degree of trustworthiness (i.e., products/systems having appropriate functionality and assurance) are expected to exhibit a lower rate of latent design and implementation flaws and a higher degree of penetration resistance against a range of threats including sophisticated cyber-attacks, natural disasters, accidents, and intentional/unintentional errors. The susceptibility of missions/business functions of organizations to known threats, the environments of operation where information systems are deployed, and the maximum acceptable level of risk to organizational operations and assets, individuals, other organizations, or the nation, guide the degree of trustworthiness needed.

Organizational Culture

Organizational culture refers to the values, beliefs, and norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations. Culture describes the way things are done in organizations and can explain why certain things occur. There is a direct relationship between organizational culture and how organizations respond to uncertainties and the potential for near-term benefits to be the source for longer-term losses. The organization's culture informs and even, to perhaps a large degree, defines that organization's risk management strategy. At a minimum, when an expressed risk management strategy is not consistent with that organization's culture, then it is likely that the strategy will be difficult if not impossible to implement. Recognizing and addressing the significant influence culture has on risk-related decisions of senior leaders/executives within organizations can therefore, be key to achieving effective management of risk.

Recognizing the impact from organizational culture on the implementation of an organization-wide risk management program is important as this can reflect a major organizational change. This change must be effectively managed and understanding the culture of an organization plays an important part in achieving such organization-wide change. Implementing an effective risk management program may well represent a significant organization-wide change aligning the people, processes, and culture within the organization with the new or revised

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

organizational goals and objectives, the risk management strategy, and communication mechanisms for sharing risk-related information among entities. To effectively manage such change, organizations include cultural considerations as a fundamental component in their strategic-level thinking and decision-making processes (e.g., developing the risk management strategy). If the senior leaders/executives understand the importance of culture, they have a better chance of achieving the organization's strategic goals and objectives by successfully managing risk.

Culture also impacts the degree of risk being incurred. Culture is reflected in an organization's willingness to adopt new and leading edge information technologies. For example, organizations that are engaged in research and development activities may be more likely to push technological boundaries. Such organizations are more prone to be early adopters of new technologies and therefore, more likely to view the new technologies from the standpoint of the potential benefits achieved versus potential harm from use. In contrast, organizations that are engaged in security-related activities may be more conservative by nature and less likely to push technological boundaries—being more suspicious of the new technologies, especially if provided by some entity with which the organization lacks familiarity and trust. These types of organizations are also less likely to be early adopters of new technologies and would be more inclined to look at the potential harm caused by the adoption of the new technologies. Another example is that some organizations have a history of developing proprietary software applications and services, or procuring software applications and services solely for their use. These organizations may be reluctant to use externally-provided software applications and services and this reluctance may result in lower risk being incurred. Other organizations may, on the other hand, seek to maximize advantages achieved by modern net-centric architectures (e.g., service-oriented architectures, cloud computing), where hardware, software, and services are typically provided by external organizations. Since organizations typically do not have direct control over assessment, auditing, and oversight activities of external providers, a greater risk might be incurred.

In addition to the cultural impacts on organizational risk management perspectives, there can also be cultural issues between organizations. Where two or more organizations are operating together toward a common purpose, there is a possibility that cultural differences in each of the respective organizations may result in different risk management strategies, propensity to incur risk, and willingness to accept risk. For example, assume two organizations are working together to create a common security service intended to address the advanced persistent threat. The culture of one of the organizations may result in a focus on preventing unauthorized disclosure of information, while the nature of the other organization may result in an emphasis on mission continuity. The differences in focus and emphasis resulting from organizational culture can generate different priorities and expectations regarding what security services to procure, because the organizations perceive the nature of the threat differently. Such culture-related disconnects do not occur solely between organizations but can also occur within organizations, where different organizational components (e.g., information technology components, operational components) have different values and perhaps risk tolerances. An example of an internal disconnect can be observed in a hospital that emphasizes different cultures between protecting the personal privacy of patients and the availability of medical information to medical professionals for treatment purposes.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Culture both shapes and is shaped by the people within organizations. Cultural influences and impacts can be felt across all three tiers in the multitier risk management approach. Senior leaders/executives both directly and indirectly in Tier 1 governance structures set the stage for how organizations respond to various approaches to managing risk. Senior leaders/executives establish the risk tolerance for organizations both formally (e.g., through publication of strategy and guidance documents) and informally (e.g., through actions that get rewarded and penalized, the degree of consistency in actions, and the degree of accountability enforced). The direction set by senior leaders/executives and the understanding of existing organizational values and priorities are major factors determining how risk is managed within organizations.

Effectiveness Evaluation

Effectiveness assessment is the process of measuring and verifying that the objectives of risk mitigation have been met. While risk assessment and risk mitigation are done at certain discrete times, the process of effectiveness evaluation should be continuously ongoing. As mentioned earlier, there are two practical reasons for this process in risk management.

First, risk assessment is not an exact science. There are uncertainties related to the real range of threats, likelihood of threats, impacts, and expected frequency. Similarly, in the risk mitigation process, there are uncertainties in the estimation of costs and benefits for each control option. The uncertainties may result in misjudgments in the risk mitigation plan. Hence, an assessment of the success or failure of the risk mitigation plan is necessary. It provides useful feedback into the process to ensure correctness.

Second, an organization's environment cannot be expected to remain static. Over time, an organization's network, computers, software, personnel, policies, and priorities will all change. Risk assessment and risk mitigation should be repeated or updated periodically to keep current.

Future Trends

Today risk management is more of an art than a science due to the need in current methods to factor in quantities that are inherently uncertain or difficult to estimate. Also, there is more than one way to combine the factors to form a risk mitigation strategy. Consequently, there are several different methods used today, and none are demonstrably better than others. Organizations choose a risk management approach to suit their particular needs.

There is room to improve the estimation accuracy in current methods and increase the scientific basis for risk management. Also, it would be useful to have a way to compare different methods in an equitable manner.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

CONCLUSION

Risk management is a critical component of any information security program. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Risk assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Federal and State mandates require routine assessments to identify risk and ensure appropriate controls. Risk assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and considering control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident.Information security is an ongoing process to manage risks. One could say that risk management is essentially a decision making process. The risk assessment stage is the collection of information that is input into the decision. The risk mitigation stage is the actual decision making and implementation of the resulting strategy. The effectiveness evaluation is the continual feedback into the decision making.

Although current methods have room for improvement, risk management undoubtedly serves avaluable and practical function for organizations. Organizations are faced with many pressing needs, including security, and risk management provides a method to determine and justify allocation of limited resources to security needs.

REFERENCES

Alberts, C., and Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Reading, MA: Addison Wesley.

Blakley, B., McDermott, E., and Geer, D. (2002). Information security is information risk management. In proc. of *ACM Workshop on New Security Paradigms (NSPW'01)*, 97-104.

Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.

Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2010.

Decker, R. (2001). *Key elements of a risk management approach*. GAO-02-150T, U.S. General Accounting Office.

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

Farahmand, F., Navathe, S., Sharp, G., and Enslow, P. (2003). Managing vulnerabilities of information systems to security incidents. In proc. of *ACM 2nd International Conf. on EntertainmentComputing (ICEC 2003)*, 348-354.

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

Geer, D., Hoo, K., and Jaquith, A. (2003). Information security: why the future belongs to the quants. *IEEE Security and Privacy*, 1(4), 24-32.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Gordon, L, and Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5, 438-457.

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, June 2010.

Hoo, K. S. (2000). *How much is enough? A risk management approach to computer security*.

ISO/IEC 15408:2005, *Common Criteria for Information Technology Security Evaluation*, 2005.

McClure, S., Scambray, J., and Kurtz, G. (2001). *Hacking Exposed: Network Security Secrets and Solutions*, 3rd ed. New York, NY: Osborne/McGraw-Hill.

Mercuri, R. (2003). Analyzing security costs. *Communications of the ACM*, 46, 15-18.

Microsoft. (2004). *The security risk management guide*. Retrieved October 25, 2006, from http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx.

National Bureau of Standards. (1975). *Guidelines for Automatic Data Processing Risk Analysis*. FIPS PUB 65, U.S. General Printing Office.

National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).

National Institute of Standards and Technology Special Publication 800-37, Revision 1,

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1,

National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003

National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems*, special publication 800-30.

National Institute of Standards and Technology. (2003). *Guideline on Network Security Testing*, special publication 800-42.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

Peltier, T. (2005). *Information Security Risk Analysis*, 2nd ed. New York, NY: AuerbachPublications.

Retrieved October 25, 2006, from http://iisdb.stanford.edu/pubs/11900/soohoo.pdf.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York, NY: John Wiley & Sons.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Vorster, A., and Labuschagne, L. (2005). A framework for comparing different informationsecurity risk analysis methodologies. In proc. of *ACM Annual Research Conf. of the South AfricanInstitute of Computer Scientists and Information Technologists (SAICSIT 2005)*, 95-103.

ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)