Journal of Advances and Scholarly Researches in Allied Education
Vol. 12, Issue No. 2, January-2017, ISSN 2230-7540

A Research Study of Risk Management in Information Security

Jhujhar Singh[1]* Dr. Om Parkash[2]

[1] Research Scholar, Department of Computer Science, OPJS University, Churu, Rajasthan

[2] Professor, Department of Computer Science, OPJS University, Churu, Rajasthan

Abstract – The risks associated with computer systems have been enormous for many years and still exist today. This article discusses several types of risks, including security, privacy, and judicial risks. Risk is usually defined as a function of event likelihood and impact and is divided into two categories: speculative and non-speculative. Speculative risk is the risk of taking risks to gain potential benefits. There are two main ways to assess risk: quantitative and qualitative. Risk management means consciously determining risk exposure. The starting point for the risk management process is to determine the risk acceptance criteria and reflect the risks that people are willing to accept.

Keywords: Software Risk Management, Network Risk Management, Secure Aggregation and Dissemination

----------X----------

I. INTRODUCTION

Risk is usually defined as a function of event likelihood and impact and is divided into two categories: speculative and non-speculative. Speculative risk is the risk of taking risks to gain potential benefits. An example is gambling. You may bet a certain amount and lose. There are still potential upsides and you can win bets and get more rewards. Non-speculative risks only have a negative impact. For example, natural disasters or computer system vulnerabilities that could negatively impact your business. There are two main ways to assess risk: quantitative and qualitative. Consider the risk that certain hardware components in the server will fail. The supplier may provide a number from the test lab indicating that the component can operate reliably for up to X hours. In addition, there may be historical data about the expected life of a component. Advanced assurance allows you to quantify the likelihood of failure. In addition, if the impact can be accurately quantified, that is, if the total cost of replacing a component can be quantified, the risk can be quantified. The problem with security risks is that it can be difficult to quantify the likelihood and impact of an attack. Qualitative methods can prove useful. There are many models for assessing risk. Here is a brief description of the model to illustrate the qualitative method. Microsoft created a DREAD (potential damage, repeatability, availability, affected user, discoverability) model to assess the risks associated with software vulnerabilities. The idea behind the model is simple: how difficult is it to find and exploit a vulnerability when faced with a skilled and aggressive attacker, and what are the potential impacts of exploiting the vulnerability? The five horror attributes of the vulnerability are rated high/medium/low and the sum of the three totals the total risk level. Microsoft has further improved its risk assessment methodology, but it still follows Dread's principles. This paper focuses on vulnerabilities. However, this vulnerability poses a risk if there are aggressive attackers. To fully understand the risks associated with a particular vulnerability, it is important to understand the context of the vulnerability. If there are no public documents on the system, researchers may find vulnerabilities in the system but cannot fully assess the associated risks. In addition, system owners believe that this vulnerability is unrealistic and cannot be exploited. Second, proof-of-concept attacks can play an important role in vulnerability verification and indicate the severity of the associated risk. At the very least, it brings uncontroversial evidence to the discussion and clarifies the context of the vulnerability.

II. RISK MANAGEMENT

Risk management means consciously determining risk exposure. The starting point for the risk management process is to determine the risk acceptance criteria and reflect the risks that people are willing to accept. Figure 1 outlines a qualitative risk management process that consists of two

phases: risk assessment and risk management. Because computer systems and their threats tend to change over time, this process should be performed regularly. The first activity in the risk assessment phase was to establish a good overview of the system. Second, identify threats and vulnerabilities. The combination of threats and vulnerabilities poses risks to the system. Finally, assess the risk by determining the potential and impact of each threat / vulnerability pair. A comprehensive assessment is critical to the success of the overall risk management process. In the second phase, for the identified risks, the risk is determined based on risk acceptance criteria. There are four ways to do this for each type of risk.

- **Accept —**This risk is acceptable and no action is required.
- **Control —**The risk is too high, measures are taken to reduce the possibility and impact of the risk and are acceptable.
- **Reject —**For example, the risk is too high to avoid the risk. Abandon dangerous functions or avoid risks.
- **Transfer —**Risk is transferred to other parties, for example through insurance.

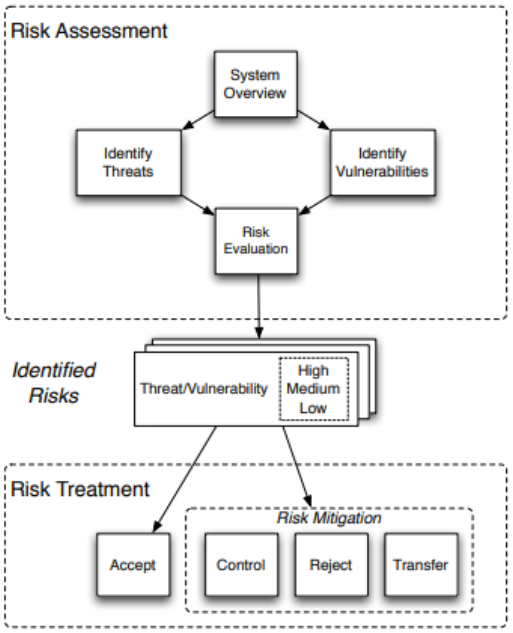

Figure 1: Risk Management Process

After the risk processing phase, there is a residual risk (called residual risk) that meets the risk acceptance criteria.

a. Software risk management

Over the years, the use of risk management as a tool to ensure the success of software projects has been advocated. This has advantages in project completion and software quality. To manage software security, Verdon and McGraw consider risk management an integral part of the software development lifecycle. After Bill Gates proposed a "trusted computing" program, Microsoft changed the software development methodology and brought the Trustworthy Computing Security Development Lifecycle (SDL). Microsoft gave an overview of SDL and concluded from previous results that SDL significantly improved software security. Another interesting discovery is that it focuses on risk management (called threat modeling in this article) during the design phase and is the most effective sub-process in SDL.

Risk management is always part of ensuring business security. Prior to the Internet era, risk management focused on protecting property and other assets from accidents and natural disasters. Today, however, companies need to consider how an increasingly digital connection extends the definition of risk management and how it applies to network security.

b. Network Risk Management

Network risk management seeks to identify, assess, and control threats to an organization's digital assets, such as information stored on internal and external servers or public cloud services, and digital information in transit. As technology evolves to create new ways to connect people, places, and things, cybercriminals will follow and become more sophisticated, using many access points available to legitimate users to access sensitive information. Developed a new method in Just one year (2012 to 2013)

c. Network Risk Management Optimizes Network for Productivity and Security

Because customer trust is essential to build a solid customer base and growth, organizations must take all possible steps to protect the business and the tools used to do business. This includes managing network security by maximizing the use of the Internet and cloud computing while minimizing the threats associated with doing business in a space vulnerable to cyber-attacks, viruses, malware, and hackers.

Who Performs Network Risk Management

The responsibility for cyber risk management rests with the hiring of the company's chief risk officer (CRO), sometimes referred to as the chief risk manager (CRMO) or risk manager (RMO), or a managed service provider. To help these administrators maintain cybersecurity and stay alert, some organizations have established risk management standards, including the National Institute of Standards and Technology and ISO.

These standards help identify threats and vulnerabilities, identify ways to mitigate these risks, and implement risk mitigation efforts.

III. RISKS TO ORGANIZATIONAL NETWORKS

Many senior managers are concerned about the threat of hackers and cyber criminals, but do not know what to do. Because danger comes from multiple directions, the cost is high and it seems difficult to control the threat. However, treating these threats as random attacks that can only be prevented after they occur is an expensive view. Each organization has about 1.4 cyber-attacks per week. Depending on the type of attack, it may take 2.6-53 days to mitigate the damage. The amount of work and cost to resolve an attack can be very large. However, most attacks are tuned and predictable to some extent. Cyber criminals often use the same input methods and similar attacks to steal data and money. The most common input methods are through employee access (15% of attacks), theft devices (13%), and systems from other organizations in the supply chain (14%). More and more cybercrime is being implemented by large organizations using spear phishing strategies. This is the act of gaining access through an employee's account, impersonating the employee, and then entering the company. A variation on this type of attack is to impersonate a manager or authorized agency member before transferring funds or data to an external account. The third type of attack is when a hacker accesses and retains data or a website and requests funds in return. A denial of service (DOS) attack can shut down a website for hours or days.As the attack progresses, you can track and discover all of these attacks. Cybercrime can be monitored to meet this challenge.

How to Approach Risk Management

As a result, many organizations are considering stop loss measures to protect their assets. However, risk management needs to take a more detailed approach. If you are at risk, your organization can choose:

1. Avoid risk by eliminating the possibility of attack
2. Reduce the risk of potential attacks
3. Spread the risk across other departments and organizations
4. Store and manage risks whenever they occur

There are multiple risks associated with cybercrime. Risk management should start from a broader perspective and strive to reduce inventory to a reasonable level of risk. But for many organizations and government groups, cybercrime spends a lot of time and money, which seems overwhelming. Therefore, you should consider identifying and identifying priorities and effective ways to mitigate risk. The National Institute of Standards and Technology (ISO) helps organizations develop their own risk management standards. It is recommended that each company consider the following management methods:

- Integrated into the entire organization architecture
- Comprehensive and transparent
- Integrate risk into all major decisions
- Systematic and structured, but can cause human error
- Continuous monitoring

For the most companies, the key to success is to look at various risk factors and rank them based on the risk factors that are the most risky and worth controlling. Risk factors include hackers who break into money transfer systems and employees who lose their mobile devices. The next step is to establish a way to address the priority risk. Some methods require specialized knowledge and technical intervention, while others can be handled through training. Staff training is an excellent way to ensure the security of entry points (such as mobile devices and WiFi) and to draw attention to more eyes.

IV. SOLUTIONS FOR RISK MANAGEMENT

Cybercrime is not an unstoppable force. There is no need to place a small dam in front of the water wall to develop a risk management plan. Despite the price, governments and large organizations are benefiting. Some of these benefits are:

- Learn how to successfully analyze and evaluate risk factors
- Learn how to avoid or mitigate risk
- Resolve issues to prevent or resolve cybercrime
- Collaborate with other organizations to identify, prioritize, and prevent threats

Cybercrime experience shows that there are several effective ways. Most organizations have resources such as ISO guidelines, statistics, and

risk management software. Solar Winds MSP (formerly LOGIC now) develops risk management software that helps MSP to develop cyber-crime and proactive IT strategies.

V. KEYS TO SUCCESSFUL RISK MANAGEMENT

- **Continuous internal checks**: Cyber criminals can attack vulnerable areas at any time, continuous monitoring within the organization's network reduces the chances of criminals penetrating deep into the system.
- **Segmentation of networks from data and other business functions**: When cybercriminals enter the system, they search for data nodes and transfer funds from the hands of companies. Separation systems make it easier to detect and contain criminals.
- **Collaboration with other organizations**: Cyber criminals target all types of businesses and organizations, communication with others helps build a community to check for intrusions, report attacks, and find the source of those attacks.

VI. 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.

VII. CONCLUSION

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 a valuable 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

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002). “A survey on sensor networks,” *IEEE Communications Magazine,* vol. 40, no. 8, pp.102-114.
2. D. W. Carman, P. S. Krus, and B. J. Matt (2000). “Constraints and approaches for distributed sensor network security,” Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD.
3. Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia (2013). “Threat Models and Security Issues in Wireless Sensor Networks”, *International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013*
4. I.F. Akyildiz, E.P. Stuntebeck (2006). “Wireless underground sensor networks: research challenges”, *Ad-Hoc Networks* 4, pp. 669–686
5. Kriti Jain, Upasana Bahuguna (2012). “Survey on Wireless Sensor Network”, *IJSTM,* Vol. 3 Issue 2, pp. 83-90.
6. Shio Kumar Singh, M. P. Singh, D. K. Singh (2011). “A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks”, *International Journal of Computer Trends and Technology*-, May to June Issue 2011, ISSN: 2231-2803
7. Dr. Manoj Kumar Jain (2011). “Wireless Sensor Networks: Security Issues and Challenges”, *IJCIT,* vol. 2, issue 1, pp. 62-67.
8. Snehlata Yadav, Kamlesh Gupta, Sanjay Silakari (2010). “Security issues in wireless sensor networks”, *Journal of Information Systems and Communication,* vol. 1, issue 2, 2010, pp. 01-06
9. Pooja, Manisha, Dr. Yudhvir Singh (2013). “Security Issues and Sybil Attack in Wireless Sensor Networks”, *International Journal of P2P Network Trends and Technology,* vol. 3, issue 1, pp. 7-13.
10. A.D. Wood, J.A. Stankovic (2002). “Denial of service in sensor networks”, *IEEE Computer*, Vol. 35, Issue 10, pp. 54-62.

11. Chapter in Encyclopedia of Multimedia Technology and Networking, 2nd ed., M. Pagani (ed.), Idea Group Publishing, to appear 2009., http://engweb.swan.ac.uk/~tmchen/papers/info-sec-risks.pdf

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

13. 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), pp. 97-104.

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

15. 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 Entertainment Computing (ICEC 2003), pp. 348-354.

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

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

18. Hoo, K. S. (2000). How much is enough? A risk management approach to computer security. Retrieved October 25, 2006, from http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.

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

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

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

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

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

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

25. Peltier, T. (2005). Information Security Risk Analysis, 2nd ed. New York, NY: Auerbach Publications.

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

27. Vorster, A., and Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. In proc. of ACM Annual Research Conf. of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2005), pp. 95-103.

Corresponding Author

Jhujhar Singh*

Research Scholar, Department of Computer Science, OPJS University, Churu, Rajasthan

jujharsingh13@gmail.com