Identification, Assessment, and Management of Risks in InfoSec

David McDaniel

mcdanielda15@students.ecu.edu

East Carolina University

Abstract

Since antiquity, humans have required the need to protect sensitive data. Whether for national security, financial, or a myriad of personal reasons, information security has been important. Threats of cipher-cracking, information theft, and physical damage have posed risks to this security. With the rise of the personal computer and the Internet, these issues have only been exacerbated, providing countless vectors through which information can be compromised. Due to this rise of risk in information technology, it is becoming increasingly important for an organization to practice thorough and methodical risk management for all information assets. This term paper provides an analysis of designing and implementing a risk management strategy for an organization. Focus is placed upon the identification of risks, the analysis of risks, the management (or treatment) of risks, and the importance of recurring monitoring. Also included is a brief overview of several popular risk management strategies and methodologies which can be utilized individually or collectively as a framework for a risk management strategy.

INTRODUCTION

Information Security, commonly referred to as "InfoSec", is defined by TechTarget as "a set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document and counter threats to digital and non-digital information" (Rouse, n.d.). In order to develop such a strategy to managing these threats, an organization needs to be able to properly identify, evaluate, and develop a plan to address each of the threats jeopardizing the security of their information assets. This process is known as risk management and is a vital aspect of information security. An information asset is defined as "an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an [organization] to perform its business functions" (Information Asset (Definition), n.d.). One could argue that it is impossible to defend against threats if you do not know what assets need to be protected and from what threats they should be protected. In this paper, the author will strive to put forth a thorough account of the processes, policies, and goals which comprise a risk management plan for an organization. Although the author endeavors to provide comprehensive information, it should be noted that countless methods and approaches can be used to accomplish similar goals. Risk management is comprised of a series of objectives including (1) risk identification, (2) risk assessment, (3) risk management (or treatment), and (4) risk monitoring (Webb, Ahmad, Maynard, & Shanks, 2014). An identification of several acknowledged methodologies, tools, and standards, these four objectives, and a brief dissection of some of the nuances of implementing a risk management program within an organization will serve a structural outline for this paper.

METHODOLOGIES AND STANDARDS

There have been many methods proposed for risk management process (including the identification, assessment, and review). Of these, many are based on the International Organization of Standardization (ISO) standards, such as ISO 31000 and ISO 31010 (Selvaseelan, 2018). Following is a listing of just a subset of the proposed methodologies for the risk management process. Inclusion or omission in this list, nor the order of inclusion should relay any bias, implied or otherwise as to the effectiveness and desirability of any given method. It is important to note that many of the approaches mentioned within this paper have originated in disciplines other than information security. This fact, however, is meaningless as the approaches can be adapted to focus on risks to information assets.

ISO 31000

The ISO 31000:2009 standard is often used as the basis upon which other standards and methodologies are based. (Olechowski, Oehmen, Seering, & Ben-Daya, 2016). Olechowski et al. (2016) explain that there are three four primary objectives and eleven principles (listed below) that are the focus of this standard, which provide directionality in the creation and implementation of a risk management plan for an organization.

Objectives:

1) Increased likelihood of achieving objectives
2) Establish a reliable basis for decision making and planning
3) Minimize losses
4) Be aware of the need to identify and treat risk throughout the organization

Principles:

1) Risk management creates value
2) Risk management is an integral part of organizational processes
3) Risk management is part of decision making
4) Risk management explicitly addresses uncertainty
5) Risk management is systematic, structured and timely
6) Risk management is based on the best available information
7) Risk management is tailored
8) Risk management takes human and cultural factors into account
9) Risk management is transparent and inclusive
10) Risk management is dynamic, iterative and responsive to change
11) Risk management facilitates continual improvement.

OCTAVE

Developed by the Department of Defense (DoD)-funded Software Engineering Institute (SEI), OCTAVE (an acronym for Operationally Critical, Threat, Asset, and Vulnerability Evaluations is comprised of the principle OCTAVE method and the OCTAVE-S method (tailored for smaller organizations) (Alberts, Dorofee, Stevens, & Woody, 2003). As explicated by Alberts et al (2003), OCTAVE is a methodology that is primarily self-directed by a small group of individuals from the organization that leverages their internal knowledge of the organization to evaluate the current security state and to guide its progression to identify, assess, and manage risks to the organization (as opposed to a more technological approach used by other methodologies).

STRIDE

STRIDE (an acronym for Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) is a threat-modeling tool developed by Microsoft which provides a way of classifying threats against an organization to better develop pointed questions involved in the risk assessment (Microsoft Corporation, 2009)

RISK IDENTIFICATION

Any organization is ill-fitted to combat threats against information assets unless and until the organization knows which threat(s) it faces, which means that the risk identification portion of the risk management process is, arguably, the most important. Identification of such risks involves the identification of (1) the information assets of the organization in question and (2) the known and unknown threats to the confidentiality, integrity, and availability of these resources.

During the identification of the organization's resources, it is important that one recognizes the full spectrum of possibilities. Not only are computer hardware and software potentially considered information assets, but the information (e.g., design documents and databases), services (e.g., electrical and internet/telecommunication services), and even people (e.g., management and users) can be considered information assets for an organization (Wei, Wu, & Chu, 2018). Identification of information assets should be completed during the development of an initial business impact analysis (BIA). When performing the business impact analysis, the risk management team should focus on those assets that are critical to the business processes and pose risk to interrupting the successful realization of the organization's mission (Taubenberger, Jurjens, Yu, & Nuseibeh, 2013). The probing nature of the BIA will provide the risk

management team a list of critical information assets (both technical and non-technical) that can, in turn, be used in the risk identification process.

Once all necessary information assets have been enumerated, the risk management team should proceed using a preferred technique to list all conceivable risks to each of the information assets identified. Although countless methods can be derived to craft such a list, three of the most well-known methods are that of brainstorming, premortem, and layered analysis. A broad overview of each approach is given below. It is important that the team in charge of risk identification use any available approach to be thorough and identify all foreseeable risks to information assets as "risks that remain unidentified are implicitly assumed (and unmanaged)" (Gallop, Willy, & Bischoff, 2016).

Brainstorming

One of the most simplistic and widely used methods of identifying items for countless processes in addition to risks, brainstorming is defined by the Oxford Dictionary (Brainstorming, n.d.) as "Group discussion to produce ideas or solve problems." A group of individuals familiar with the organization, its objectives, and its information assets would implement this approach by gathering in a physical or virtual setting to generate a listing of all foreseeable threats to the information assets identified.

Premortem

A explained by Gallop, Willy, and Bischoff (2016), is essentially the opposite of a postmortem (or an event occurring after a disaster). Using this method, Gallop, Willly, and Bischoff (2016) explain, the investigators, or risk management team would envision that a

system has failed and to imagine the causes that could have potentially precede such an event. They also concluded in their research that teams using this approach identified risks of higher quality and quantity than those using a different approach. These findings seem to indicate the importance of having a structured plan in order to better identify potential risks.

Layered

Focused more on information technology and software risks, Raspotnig and Opdahl (2013) described the potential usage of a layered approach to risk identification. Using such a risk identification approach Raspotnig and Opdahl (2013) explain, involves thinking of each information asset as a series of concentric circles beginning with the software and extending outwards through the computer-based system, the total system, and finally the environment in which the system exists. An analysis of how each of the layers within a system could be exploited allows for a systematic and thorough approach to the identification process.

RISK ASSESSMENT

The key point for an organization to keep in mind during the selection and execution of a risk assessment process is to gauge the probability of a threat becoming a reality as well as the magnitude of the damage that would be incurred by the event upon the information asset(s) impacted. As numerous of methods as exists for risk identification, there exist at least as many methods for the assessment of the identified risks. In general, risk assessment methodologies are classified as either being qualitative, quantitative, or a hybrid of the two. A majority of organizations opt for a more qualitative approach, due to its flexibility, however, there exists a need for quantitative methods to put a monetary value upon the risk that an organization faces.

(Saljua & Idris, 2012). A brief description of the types along with some of the more popular methods for both qualitative and quantitative approaches are provided below. Those who opt for a hybrid approach often choose features of multiple plans to mesh into one, customized approach to their organization.

Qualitative

Method Description

Qualitative assessments are distinguished from quantitative assessments due to a non-monetary valuation of the likelihood of occurrence and significance of the impact that the risk poses to the information asset. Often, an organization using a qualitative risk assessment approach will create a risk matrix which comprises a measure of an asset's vulnerability and a likelihood of the risk occurring (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). For each risk, the same matrix is used, providing a numerical or symbolic (e.g., "Low", "Medium", "High") valuation for prioritizing the risks. Figure 1 represents a sample risk assessment matrix. The individual columns indicate the probability/likelihood of the particular event occurring along with a numerical value. The columns indicate how severe the damage will be if the risk becomes a reality. The cell where a given probability and severity meet contains a calculated value based upon the numerical values set for each row and column. Therefore, if the risk has a moderate likelihood and a relatively low severity, it will be assigned a valuation of "6".

Level (Probability)	Severity				
	1 (minor)	2	3	4	5 (devastating)
A (nearly guaranteed) [Value = 5]	5	10	15	20	25
B [Value = 4]	4	8	12	16	20
C [Value = 3]	3	6	9	12	15
D [Value = 2]	2	4	6	8	10
E (very uncommon) [Value = 1]	1	2	3	4	5
Low Priority [1-5]					
Medium Priority [6-10]					
High Priority [11+]					

Figure 1

Failure Mode and Effects Analysis (FMEA) and Failure Mode and Effects criticality Analysis (FMECA)

A long-existing risk analysis method, this approach has often been utilized as an engineering analysis method (Saljua & Idris, 2012). The FMEA approach uses a Risk Priority Number (RPN) which is a product of three factors of a given failure mode: occurrence (O), severity (S), and non-detection (D) (Renjith, Jose kalathil, Kumar, & Madhavan, 2018). Renjith et al. (2018) continue to explain that there is a downfall into using the RPN supplied by a FMEA/FMECA methodology: interpretation. The author of this paper argues that this is not simply a limitation of the FMEA/FMECA methodology, but a limitation of qualitative approaches in general as it involves a subjective interpretation of facts and experiences and is likely to vary from one person to another (and even from time to time for a given individual).

NIST SP 800-30 Revision 1

Widely used as a guideline alone and as part of other risk assessment strategies, the National Institute of Standards and Technology (NIST) SP 800-30 Revision 1 publication provides a general framework for risk assessment along with step-by-step methodology (Lim &

Suparman, 2012). Located in the text of the special publication, NIST even provides samples of tables that can be used to qualitatively evaluate the probability and effect of a risk upon an organization (NIST, 2012). In addition to the assessment framework and charts, the text of the NIST publication also provides a thorough method of risk assessment reporting for executive management to garner support for the risk management team's findings and seek further direction on addressing the risks (NIST, 2012).

Quantitative

Method Description

Unlike qualitative methods, quantitative approaches attempt to assign a monetary or other measureable value to a risk. While management decisions can be more easily swayed based upon a monetary assessment, quantitative appraisals pose their own difficulties, such as an imprecise evaluation of the damage to an information asset and the research and calculations for each risk can be very time consuming (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). Although many methods exist for quantitatively assessing a given risk, most all approaches utilize a derivative of the Annualized Loss Expectancy (ALE) method.

Annualized Loss Expectancy (ALE)

Potentially the most widely known quantitative appraisement (also known as an "expected value analysis" (EV) of risk is the ALE approach (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). To use the ALE approach, an organization uses a structured approach (as shown below) to calculate, as a monetary value, the significance of a particular risk to a given information asset.

*Single Loss Expectancy (SLE) = Exposure Factor (EF) * Asset Value Before (AVB)*

*EF = (AVB – Asset Value After) / (AVB * 100)*

Annualized Rate of Occurrence (ARO) = Number of Times (NT) / Number of Years Observed (NYO)

*Annualized Loss Expectancy (ALE) = SLE * ARO*

(Dzarma & Jibasen, 2015)

Once the valuations have been calculated for each information asset risk in the organization, the risk management team can proceed to prioritize the risks based on these values. Risk with a higher value require more immediate and intense scrutiny in comparison to lower values. Approaches to identified and assessed risks are covered in the following section.

RISK MANAGEMENT (TREATMENT)

Also known as "Risk Control," the treatment of risks that have been identified and assessed to be of significant concern is where the organization takes an actionable stance to address these risks. As mentioned previously, it is important that the organization appropriately and objectively assess the risks that could potentially impact the successful execution of the organization's mission. Whitman & Mattord (2017) indicate that there are five possible techniques that can be used to approach each of the risks:

1) Defense
2) Transference
3) Mitigation
4) Acceptance
5) Termination

Defense

Utilizing a defense strategy for a given threat indicates that the organization has acknowledged the threat poses enough of a risk to the organization to act to either eliminate or reduce the risk posed by threat (Whitman & Mattord, 2017). This approach generally entails the organization putting in a technological or policy-based control. An example of such a technique would be for the organization to implement a new firewall when threats are identified that cannot be controlled by their existing equipment. Policy-based controls could be used in the event of a threat involving the potential removal of hard copies of intellectual property from the premises. Management could implement a new policy that states there are no external bags or containers allowed into the building or, if so, they are subject to search upon employees' departure. Implementing these potential items could either completely or partially eliminate the risk that the named threats pose.

Transference

If an organization has acknowledged that a threat poses significant risk to the organization, but they are unable, either due to economic, skill, or other reasons, the organization could choose to transfer the risk to an external entity. This risk transference could come in the form of an outsourcing of service or by purchasing insurance to cover the financial impact of the threat, should it actually occur (Pandey & Snekkenes, 2016). This approach is generally reserved for threats that are impossible for the organization to control, or would prove too costly to control using a defense or mitigation approach. For instance, if an organization has facilities located in a flood plain, it may be economically feasible for the firm to purchase flood insurance to cover the financial losses of the organization should a flood occur and damage or destroy the

facilities. Within the past decade, cybersecurity insurance has become a realistic and useful solution for risk transference for organizations who face severe economic fallout should they become the victim of a data breach (Pal & Golubchik, 2010).

Mitigation

Mitigation techniques are used to reduce the impact of a threat if an attacker successfully exploits a vulnerability (Whitman & Mattord, 2017). This differs from the "defense" strategy due to its focus. Whereas the defense method aims to minimize or eliminate the possibility of a possible occurrence of a threat, the mitigation approach assumes that the threat has already been exploited. A possible example of such a mitigation strategy can be represented by a threat of an attacker gaining unauthorized access to a web portal for an organization. A defense strategy may address this threat by reducing the attack surface of the web server (e.g., using a hardware- or software-based firewall to block specific ports and/or using an Intrusion Detection and Prevention System (IDPS) to detect and shut down malicious acts. However, using a mitigation strategy, the organization would aim to reduce the impacts to the information assets it maintains by possibly segregating the web server from other portions of the network and removing any other data/services from the system. This would minimize the amount of damage that would be caused to the information asset should it be exploited.

Acceptance

Part of the risk management process is to determine an organization's "risk appetite". The risk appetite for an organization is the amount of risk that it is willing to accept, where a lower risk appetite correlates to a higher desired security level (Sveen, Torres, & Sarriegi, 2009).

Commonly used if a threat is of low risk (due to low impact, low probability, or both, the organization may elect to accept the possible consequences and take no action (Keskin, Tatar, Poyraz, Pinto, & Gheorghe, 2010). To demonstrate an example of a risk acceptance strategy being implemented, one could imagine an organization which operates facilities within North Carolina. Although not unheard of, the region experiences very low quantities of seismic activity, so the organization may opt to accept the consequence of any damage posed by an earthquake event rather than to use another approach such as transference (purchase earthquake coverage through an insurance agency) or defense (upgrade the facilities structure to support seismic events).

Termination

If an organization determines that the cost or effort to control the risks associated with a threat, the choice can be made to terminate the risk altogether (Whitman & Mattord, 2017). Although one could be led to believe that this simply means to cease using an information asset, this could also mean the removal of a system or process that is introducing the threat in the first place. For instance, if an organization faces a risk posed by the availability of a guest wireless network in the facility, it may opt to remove the guest network completely instead of incorporating physical and virtual controls to segregate guest and internal network traffic to minimize or eliminate the threat.

RISK MONITORING

A risk management strategy can never be considered a one-time project to undertake. Organizations should routinely monitor (1) the effectiveness of their risk management strategy to

address risks (2) the risk environment to determine if there are new risks, risks that have changed in priority or probability, or risks that are no longer existent to the organization. Just as the technology and business landscapes are constantly changing, so do the risks that organizations face. Many risk management models exist, such as the ones presented by ISO/IEC 27005:2011 and NIST SP 800-39 (Wangen & Snekkenes, 2014). However, van Deursen, Buchanan, and Duff (2013) introduced their own method which utilizes an organizationally-designed database to house a listing of the threats posed to the organization and security incidents that occur and used the data to track the effectiveness of the organization's risk management strategy in minimizing risks in a healthcare information environment. Although this was a specific implementation of a database-style approach, such implementations could be used by other methods to monitor the performance of any risk control by analyzing trends in incidents.

SUMMARY

Every organization maintains a number of information assets that are critical the execution of its mission. At any time, each information is posed by a number of foreseen and unforeseen risks of varying probabilities and impacts. It is imperative for an organization to develop, execute, and repeat a risk management strategy that includes the identification, assessment, treatment, and ongoing monitoring of these risks. Failure to perform these actions could have dire impacts on the organization such as economic penalties, loss of intellectual property, reputational damage, harm to personnel or the public, and even punishments in civil or criminal court (Yildirim, 2016). Depending on the size and experience of the organization, it may choose to perform risk management strategies internally, or by hiring external consultants to aid. As stated by Yildirim (2016), "To provide high level information security in enterprises,

understanding and applying information security standards as well as knowing current threats is important." It is the author's wish that the content contained within this publication provide a useful base of knowledge to begin the development and execution of a risk management strategy.

REFERENCES

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003, August). Introduction to the OCTAVE Approach. Pittsburgh, PA.

Brainstorming. (n.d.). Retrieved from OxfordDictionaries: https://en.oxforddictionaries.com/definition/brainstorming

Dzarma, D. E., & Jibasen, D. (2015, July). Threat Analysis of Some Information Seucirty Assets in Ibrahim Babangida Library of Modibbo Adama University of Technology, Yola. *International Journal of Pure and Applied Sciences and Technology, 29*(1), 1-9.

Gallop, D., Willy, C., & Bischoff, J. (2016, April). How to catch a black swan: Measuring the benefits of the premortem technique for risk identification. *Journal of Enterprise Transformation, 6*(2), 87-106. doi:10.1080/19488289.2016.1240118.

Information Asset (Definition). (n.d.). Retrieved from Queensland Government Chief Information Office: https://www.qgcio.qld.gov.au/publications/qgcio-glossary/information-asset-definition

Keskin, O., Tatar, U., Poyraz, O., Pinto, A., & Gheorghe, A. (2010, January). Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study. *International Conference on Cyber Warfare and Security*.

Lim, C., & Suparman, A. (2012). Risk analysis and comparative study of different cloud computing providers in Indonesia. 10.1109/ICCCSN.2012.6215714. .

Microsoft Corporation. (2009, November 12). *The STRIDE Threat Model*. Retrieved from Microsoft: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

National Institute of Standards and Technology. (2012, September). Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Management, 34*(8), 1568-1578. doi:10.1016/j.ijproman.2016.08.002.

Pal, R., & Golubchik, L. (2010). On the economics of information security: The problem of designing optimal cyber-insurance contracts. *ACM SIGMETRICS Performance Evaluation Review, 38*(2), 51-53. doi:10.1145/1870178.1870196.

Pandey, P., & Snekkenes, E. (2016, May). Using financial instruments to transfer the information security risks. *Future Internet, 8*(4), 20. doi:10.3390/fi8020020.

Raspotnig, C., & Opdal, A. (2013, April). Comparing risk identification techniues for safety and security requirements. *The Journal of Systems & Software, 86*(4), 1124-1151.

Renjith, V. R., Jose kalathil, M., Kumar, P. H., & Madhavan, D. (2018, 01). Fuzzy FMECA (failure mode effect and criticalicy analysis) of LNG storage facility. *Journal of Loss Prevention in the Process Industries*, doi:10.1016/j.jlp.2018.01.002.

Rouse, M. (n.d.). *What is information security (infosec)?* Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/information-security-infosec

Saljua, U., & Idris, N. B. (2012, 06). Information risk managament: Quantitative or qualitative? Cross industry lessons from medical and finanicial fields. *Journal of Systemics, 10*(3), 54-59.

Selvaseelan, J. (2018). Development and Introduction of the Risk-Sentience Auxiliary Framework (RSAF) as an Enabler to the ISO 31000 and ISO 31010 for High-Risk Environments. *Administrative Sciences, 8*(2), 22. doi:10.3390/admsci8020022.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14-30. doi:10.1016/j.cose.2015.11.001.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection, 2*(3), 95-109. doi:10.1016/j.ijcip.2009.07.003.

Taubenberger, S., Jurjens, J., Yu, Y., & Nuseibeh, B. (2013). Resolving vulnerability identification errors using security requirements on business process models. *Information Management & Computer Security, 21*(3), 202-223 https://doi-org.jproxy.lib.ecu.edu/10.1108/IMCS-09-2012-0054.

van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitorign information security risks within health care. *Computers & Security, 37*, 31-45. doi:10.1016/j.cose.2013.04.005.

Wangen, G., & Snekkenes, E. A. (2014). A comparison between business process management and information security management. *2014 Federated Conference on Computer Science and Information Systems*, (pp. 901-910). Warsaw.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014, July). A situation awareness model for information security risk management. *Computers and Security, 44*, 1-15. doi:10.1016/j.cose.2014.04.005.

Wei, Y.-C., Wu, W.-C., & Chu, Y.-C. (2018). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing, 279*, 48-53. doi:10.1016/j.neucom.2017.05.106.

Whitman, M. E., & Mattord, H. J. (2017). *Management of Information Security, Fifth Edition.* Boston, MA: Cengage Learning.

Yildirim, E. Y. (2016). The Importance of Risk Management in Information Security. *Proceedings of The IIER International Conference*, (pp. 5-8). Rio de Janeiro, Brazil.