Information Security Risk Assessment Methods, Frameworks and Guidelines

Michael Haythorn

East Carolina University

Abstract

Assessing risk is a fundamental responsibility of information security professionals. The basic need to provide products or services creates a requirement to have assets. With assets comes the need protect them from the potential for loss. Conducting a risk assessment is an essential step for organizations in order to ensure than proper controls are in place to protect assets that are critical to business functions. Risk assessment can be a very complex task, one that requires multiple methodologies and resources to perform quantitative and qualitative analysis based on factual evidence as well as subjective opinion. Ultimately the organization bears the responsibility for accurate analysis and control measures.

The need for an accurate risk assessment has created multiple entities for baseline frameworks that organizations can use to build upon to meet their needs. These frameworks are guidelines, but cannot replace the in depth knowledge that an organization must have to be successful in implementing controls based on a risk assessment. It is the responsibility of information security professionals within the organization analyze multiple frameworks and utilize the methods that are ideal in a case by case basis.

The following article presents details on risk, the assessment of risk including multiple industry frameworks and finally managing the risks that have been identified. Examples have been provided to show a broad scope explanation of how these principles may be applied to organizations.

Table of Contents

1 What is Risk?

Simply defined, risk is the potential for loss. In the information security world, risk can be seen as the measure of uncertainty in order to quantify probability. Risk needs to be quantifiable in order for an organization to evaluate the probability of exposure and thus be able to influence the outcome. A risk is made up of an event, the probability the event will occur, an asset that will be impacted and the impact of the outcome. The flow of risk can be seen in Figure 1.1 below.

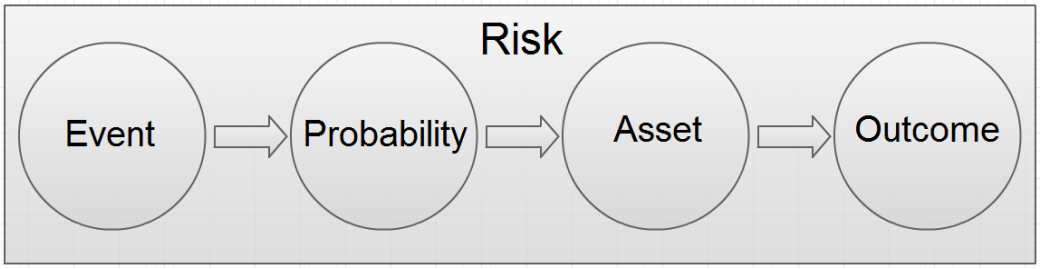

Figure 1.1 - Risk

1. 1 – Event

An event is described as a possible future situation that is undesirable or unwanted. Events are either known or unknown and can be natural or manmade. To the best ability of the evaluators, all events must be accounted for in order to have the best chance at influencing the impact of each event.

1.2 – Probability

The probability is the likelihood of a future event occurring. In order to determine probability, the exposure and frequency of events must be predictable. Probability is what makes risk assessment so difficult because it can vary greatly depending on the situation. Correctly determining the probability of an event can have a direct impact on the severity of the outcome.

1.3 – Asset

An asset is the direct or indirect target of an event. Assets are generally something of value including; applications, databases, software, hardware, buildings, people and infrastructures. The asset is what needs protection from the event.

1.4 – Outcome

The outcome is the impact that the event has on the asset. In the context of risk assessment the outcome is always negative or unwanted. The outcome impacts an asset in such a way that its value is affected through loss or harm of organizational assets.

2 Assessing Risk

In order to manage the impact of risk, organizations must conduct regular assessments of the risks that could potentially impact them. Risk assessment provides a mechanism for identifying which events and assets require the addition of controls to protect. Performing an assessment of risk is essential to order for an organization to understand how they might be impacted by future events. Assessing risk can be difficult depending on the knowledge a company has about their assets and the future events that threaten these assets. In order to properly assess risk organizations must be able to balance risks with rewards. Some risks are not worth the expense to attempt to prevent and some risks require a large amount of resources to defend against. The assessment of this risk is an essential part of information security in order to find a balance between risk and reward. The following figure 2.1 provides an example of the most common parts of the risk assessment process.

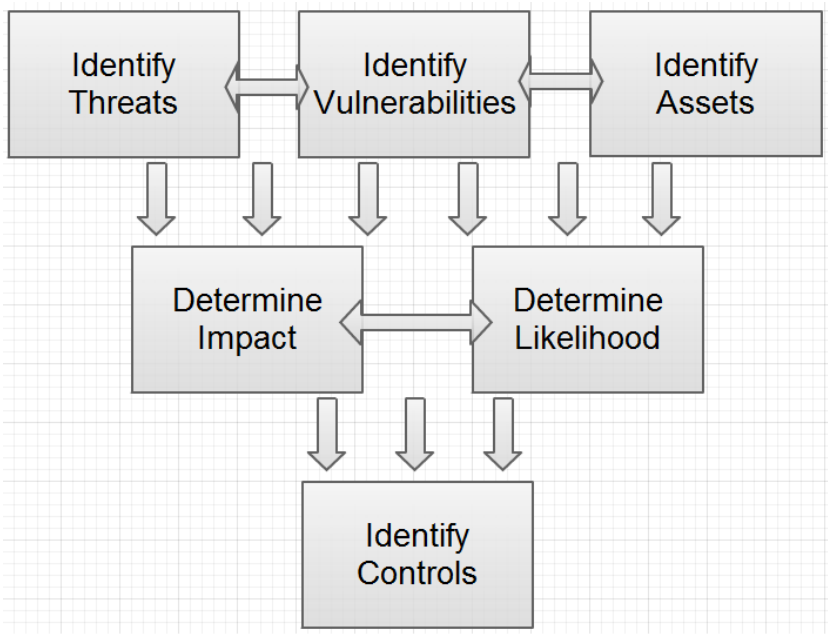

Figure 2.1 - Risk Assessment Process

2.1 – Threats

The risk assessment process requires organizations to compile a list of threats that could potentially have an impact on organizational assets. This activity requires that the organization have extensive industry knowledge and the assistance of trained professionals who are capable of accurate forecasting. Threats can be seen as events, sources, actions or inactions that could lead to the loss or harm of organization assets. It can be very difficult to identify all threats given the scope of assets, location, industry segment as well as the state of current events in the market. To aid in this process, there are many catalog resources available that can give a baseline of threats including the ISO 27005, NIST SP 800-30, OWASP and BITS frameworks. This baseline can be used by organizations to aid in the threat identification process but overall this action must be performed accurately for the organization itself. Some threats as identified in the frameworks may not apply and some threats faced by an organization may not be accounted for which is why it is essential for threats to be identified specifically for the organization itself.

On top of listing and describing threats it may also be beneficial for an organization to realize the relevance of each threat. For example a threat may be confirmed or seen before, it may be expected if seen by partner organizations or peers, it may be anticipated based on a report, it may be predicted based on research, and it may be possible as described by a source. This analysis can help to determine the impact likelihood later in the process. Table 2.1 provides a list of threats that can be included in this stage.

Threats
Perform reconnisance and gather information
Craft or create attack tools
Deliver/insert/install malicious capabilities
Exploit and compromise
Conduct an attack
Achieve results
Maintain a set of capabilities
Coordinate a campaign

Table 2.1 - Threat Assessment

2.2 – Vulnerabilities

Vulnerabilities are contributing factors that make assets capable of being leveraged by threat sources. The existence of a vulnerability is an essential piece of the measurement when calculating the probability of an event occurring. Vulnerability assessment can be even more difficult in some cases than threat identification because it requires that organizations know the specific weaknesses of their assets. In order to build a complete list of vulnerabilities, organizations can take into account the results of past risk assessments, penetration testing results, vulnerability assessments, security incident data, security metrics audit reports and third party industry events and research.

Vulnerability assessment can rely on quantitative and qualitative data to determine its severity. Vulnerabilities can be exposed and easily exploitable that could result in a severe impact while some is of no concern because there is no associated impact if the vulnerability is exploited. Organizations must use the information they have acquired to determine the severity of each. Table 2.2 provides a list of criteria for organizations when assessing vulnerabilities.

Qualitative	Quantitative		Description
Very High	96-100	10	The vulnerability is exposed and exploitable
High	80-95	8	The vulnerability is of high concern
Moderate	21-79	5	The vulnerability is of moderate concern
Low	5-20	2	The vilnerability is of minor concern
Very Low	0-4	0	The vulnerability is not a concern

Table 2.2 - Vulnerability Assessment

2.3 – Assets

Organizations must identify critical assets in this phase of the process. Identifying which assets are critical can be subjective based on the individual or group conducting the assessment. It is the responsibility of the information security professional to evaluate assets based on their criticality when compared to the overall list of assets. Assets can include applications, databases, software, hardware, buildings, people and/or infrastructures. In order to create a list of critical assets the organization can take into account business impact analysis documents, asset inventory reports,

internal and external audits, surveys of assets from various groups and any existing criticality data.

2.4 – Impact

Impact must be measureable, but can be based on quantitative data and qualitative data depending on the threat and the asset. Quantitative risk assessments deal with estimating the loss from a monetary perspective using calculations such as the Single Loss Expectancy, Annualized Rate of Occurrence and Annualized Loss Expectancy. In order to use this method, there must be numbers associated with loss. For example by not complying with a specific regulation the result would be a fine of $10,000. In this case it is simple to see if controls are not put in place to comply with this regulation that the monetary loss would be set at $10,000. Qualitative risk assessment on the other hand is not as easy to calculate therefore organizations must use relative values to assign to the potential impact of an event. Levels typical range from low or non-existent to high or critical and even though it is not quantitative using real numbers an event of critical impact could still result in a significant financial loss.

Like the vulnerability assessment, impact assessment can be assigned a quantitative or qualitative rating based on the comparison of impacts. Some impact has the potential to cause multiple sever or catastrophic events such as the loss of life while other impacts may have negligible effect on an organization. Table 2.3 provides a list of criteria for organizations when assessing impact.

Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 2.3 - Impact Assessment

2.5 – Likelihood

The likelihood of an event exploiting vulnerability is an essential measurement during the risk assessment process as well. This stage is the primary component in order to produce a rating for each asset. Determining the likelihood of an event occurring, like much of the risk assessment process, can be very subjective. Completing it relies in historical data in conjunction with the experience of industry professionals to be accurate. The outcome of this process will create a risk rating which will eventually lead to the amount of time, energy and money is used to control the assets identified from the threats.

In general, the approach at this stage is to assign qualitative values or quantitative values to each threat in order to compare one event to another. A range of likelihood of threat events can range from very low to very high, or from 0-100 on a scale. Whatever the measurement method is the methodology should be applied across the board in order to have accurate and measureable data to analyze. Table 2.4 provides an example qualitative rating system that an organization can use to analyze the likelihood of an event.

Qualitative	Quantitative		Description
Very High	96-100	10	The threat event could have multiple severe or catastrophic adverse effects on an organization
High	80-95	8	The threat event could have sever or catastrophic adverse effects on an organization
Moderate	21-79	5	The threat event could have serious adverse effects on an organization
Low	5-20	2	The threat event could have limited adverse effects on an organization
Very Low	0-4	0	The threat event could have negligible adverse effects on an organization

Table 2.4 - Impact Assessment

2.6 – Controls

The objective in this stage of the process is to identify existing controls already in place to reduce the impact of a future event on an asset. This information is critical in order to avoid implementing controls that may already exist, or to evaluate the effectiveness of the controls

over the period between risk assessments. Historical information can be leveraged in this stage to see if a control that was put into place based on another risk assessment has been effective in reducing the impact of the threat as well as identifying weakness is the current approach to make the control more effective.

2.7 – Risk Assessment Case Study

Using the risk assessment process that has been established, the following example provides detail about a specific event and how it can be measured during this process. The threat in this example is a hacker, which is a common threat facing organizations with assets available on the internet. The vulnerability identified by the risk assessment team is a security misconfiguration. Misconfigurations are a common vulnerability among organizations and it must be accounted for on a risk assessment. Security misconfiguration can include out of date software or hardware, the installation of unnecessary features like ports, services or privileges and the improper use of default settings. These vulnerabilities are typically unknown because they would be less likely to exist if they were known by the organization. Security misconfigurations can have an impact on assets such as applications, databases, software, hardware and infrastructures. The likelihood of impact from a hacker using a security misconfiguration is high due to the amount of tools available that can scan for these weaknesses and number of hackers using these tools.

In this example the existing controls are to patch systems regularly and change default passwords. Figure 2.2 provides a diagram of the process flow. The controls that had been implemented previously successfully stopped an attack from a hacker based on default passwords, but it was not successful in blocking an open vulnerable port from creating a medium level impact on an infrastructure asset. Based on this example the organization will need to reevaluate their practices with ports and firewall configurations to close this hole. Additionally the organization should utilize third party software to perform analysis on their network, both internally and externally to locate these vulnerabilities before the hackers do.

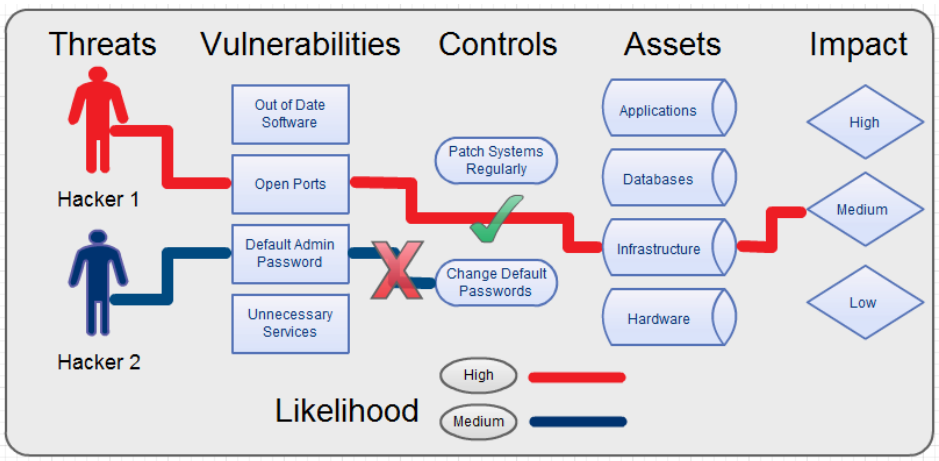

Figure 2.2 - Risk Assessment Example

3 Industry Risk Assessment Frameworks

3.1 – ISO 27005

The ISO 27005 is a standard published by the International Organization for Standardization (ISO) and provides guidelines for information security risk management. The standard was defined to assist organizations in implementing information security based on a risk management approach. The process outlined by the methodology is to identify the information assets that are at risk, the potential threats or threat sources, the potential vulnerabilities and the potential consequences if the risks materialize. The ISO 27005 standard provides some examples of each category but is not designed to be an exhaustive list; instead it is intended to provide organizations with enough information to build on. The ISO 27005 standard does not include information about quantitative versus qualitative risk assessment methods, noting that both are appropriate methods of estimating risks instead of defining them.

3.2 – NIST SP800-30

The Federal Information Security Management Act (FISMA) that was passed in 2002 added a statutory provision to ensure that agencies comply with mandatory processing standards. The National Institute of Standards (NIST) is the technology measurement and standards department was asked to develop standards and guidelines for the federal government. The NIST handbook is similar in information covered to the ISO/IEC 27002 but since it is tied to the governmental practices is goes into significantly more detail related to security controls and assessing the adequacy of the controls.

The NIST SP800-30 standard defines risk as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. The purpose is to provide guidance for conducting risk assessments of federal information systems and organizations as well as documentation providing guidance to prepare for assessments, conduct assessment and maintain assessments.

3.3 – FAIR

Factor Analysis of Information Risk (FAIR) is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events. This framework provides risk analysis as well as creating an understanding of what risk is and the factors that drive risk. The FAIR system is proprietary and requires a license from RMI. The FAIR framework attempts to focus on events that are possible providing a probabilistic approach that is applied to assets and threats. FAIR defines six kinds of loss; productivity, response, replacement, fires and judgments, competitive advantage and reputation. Value and liability are defined as the criticality of the impact, the cost of the asset and the sensitivity associated with the disclosure of the information. Threats can be grouped into access, misuse, disclose, modify and deny access.

3.4 – OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) is a collection of tools, techniques and methods for risk assessments. The framework for this tool was developed by the Software Engineering Institute of Carnegie Mellon and is highly regarded by the information security profession. The OCTAVE framework is extremely detailed containing three methods; the original OCTAVE method which forms the basis for the OCTAVE body of knowledge, OCTAVE-S for smaller organizations and OCTAVE-Allegro which is a streamlined approach to the risk assessment process. Each method can be assembled by a team of individuals within an organization; they can be tailored to fit different organizational environment, security, resiliency objectives and skill levels.

The framework is a process-driven methodology to identify, prioritize and manage information security risks. OCTAVE has three phases, build asset-based threat policies, identify infrastructure vulnerabilities and develop security strategies and plans. Analysis of risk impact is based on rankings assigned to assets such as reputation, financial and productivity.

3.5 – ENISA

ENISA is the European Union Agency for Network and Information Security has outlined a framework with basic parameters within which risks must be managed can be defined. In order to define an efficient framework, organizations must understand their background, evaluate risk management activities that exist as well as develop a structure for initiatives and controls. The ENISA approach helps organizations clarify and gain a common understanding of objectives, identify environments, identify the main scope of the objectives, develop criteria to measure risks against and define key elements for structuring risk identification and assessment.

3.6 – CRAMM

The CCTA Risk Analysis and Management Method (CRAMM) was developed by the Central Computing and Telecommunications Agency (CCTA). CRAM is currently in use by NATO and the Dutch armed forces. The framework is composed of three stages; establishment of the objectives, assessment of the risks and identification and selection of countermeasures. The CRAMM method uses the CRAMM tool and is appropriate for large organizations such as military, government organizations or large industry bodies. CRAMM assists organizations in calculating risks from asset values and vulnerabilities. The framework also helps to decide how to manage the risks that are identified.

4 Managing Risk

Once risks have been identified and their potential for impact has been evaluated, organizations must decide what they plan to do with this information. It is not possible to completely avoid all risks in every situation, financially this does not work. Instead organizations must use the data they have collected to decide on the appropriate next steps in order to provide the most protection for the highest likelihood threats that have the potential for the highest impact to the organization. This is the most important part of the process as deciding to do something versus not do anything could have major impacts on the organization.

Based on the information provided in the risk assessment organizations must evaluate the frequency and the severity of an event to help the decide if they should take steps to avoid or reduce the risk, accept responsibility for retaining the risk or transfer all or part of it to a third

party. Figure 3.1 below shows an example mitigating risk chart where the dots represent threats identified and how they will be handled based on their frequency and probability of impact.

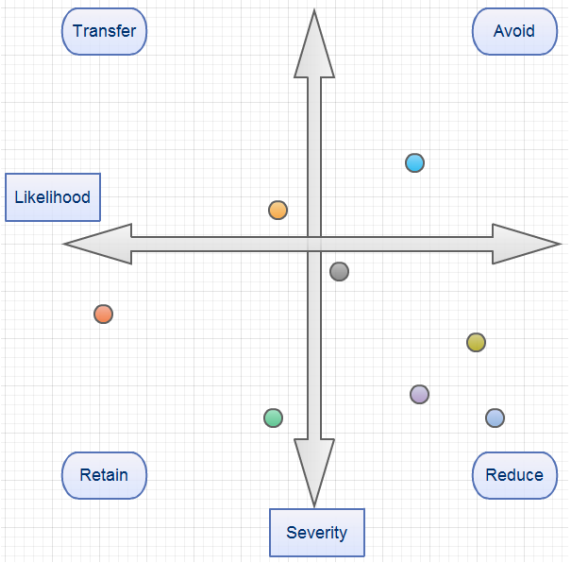

Figure 3.1 - Managing Risk

4.1 – Reduce

Reduction is one of the most common responses based on a threat identified during a risk assessment. In order to reduce risks, organizations can take a range of steps based on the severity of the threat and criticality of the asset. For example, an organization identifies weak passwords as a threat that could have high impact if a password is stolen. Steps can be taken to reduce the risk of weak passwords by implementing a password policy that requires strong passwords.

4.2 – Avoid

Organizations can also choose to avoid some risks. This is not always possible because risks generally cannot be completely avoided. In order to avoid risks organizations typically will avoid certain activities, for example an organization will choose not to build its data center near the coast to avoid the possibility of hurricane damage. Another example of avoiding risk would be to eliminate an organizations online presence to avoid the potential to be impacted by a hacker. It is not always feasible for a company to avoid risk completely.

4.3 – Retain

When an organization retains the risk identified typically they are doing this for financial reasons. Organizations will assume or retain risks when the cost to reduce or avoid it is greater than the value of the asset. For example, a company may choose to retain the risk of a tornado striking a building. This decision is based on the evaluation of the likelihood that a tornado has to come in contact with the building and the financial cost to protect the building from the impact of a tornado.

4.4 – Transfer

An organization can also choose to transfer all or some of the risk. This is typically done through insurance policies or vendor agreements. This method is typically a last resort because the transference of risk generally comes at a higher cost than reduction or retention when avoidance is not possible. An example of risk transference is an organization takes out an insurance policy against water damage on all servers. They will pay a fee monthly to the insurance company so they can accept the responsibility of replacing the assets that were damaged.

4.5 – Managing Risk Case Study

In order to provide an example of how organizations will manage risk based on the risk assessment of several different threats including hackers, theft, and fire. This is not an exhaustive list of threats, but will provide enough detail to examine the steps organizations might to manage the risk for each. In this example, a large internet sales company has performed a risk assessment and has identified the above risks. Based on their results the following can be concluded from their analysis. Figure 4.1 displays the graphical view of these results.

Hackers introduce threats that most internet companies must deal with, vulnerabilities that could potentially allow hackers to impact assets range based on the infrastructure in place. This type of threat has a high likelihood and the potential for a high impact. This can be reduced by implementing controls to lessen the chances of a successful attack. The threat can also be transferred by outsourcing security operations to a third party company, but the organization will still bear responsibility for a successful attack based on reputation. It is not possible to completely avoid this threat because of the nature of the organization. It is also not feasable to retain this threat because the organization would not be able to absorb the damage done by

attackers if nothing is done. In this case the organization will take the necessary steps to reduce the impact from the hacker threat.

The threat of theft is present in most companies, from both internal and external sources. Vulnerabilities include the lack of security system, inadequate locks and improper storage procedures. The likelihood of theft to the organization is low and the impact is medium. This type of threat cannot be avoided because organizations are required to have assets that can be stolen. The threat can be reduced, but because of the likelihood and potential for impact it may not be necessary to add additional controls. The threat in this case will likely be transferred to an insurance company who will replace what is stolen if a theft occurs.

The threat of fire is one that all organizations with a brick and mortar building must face. Vulnerabilities include improper ventilation, storage practices, training, and the provision of equipment. Fire is unlikely but the potential for impact is very high including the catastrophic destruction of buildings and the loss of life. This type of threat cannot be avoided provided that a building is required for operations. The threat can be transferred to third party through insurance policies but the damage may still affect the organization itself. The threat can be retained, but the potential impact associated greatly outweighs the cost of providing controls to reduce the impact of a fire. In this case reduction through proper practices and following fire codes is the best option.

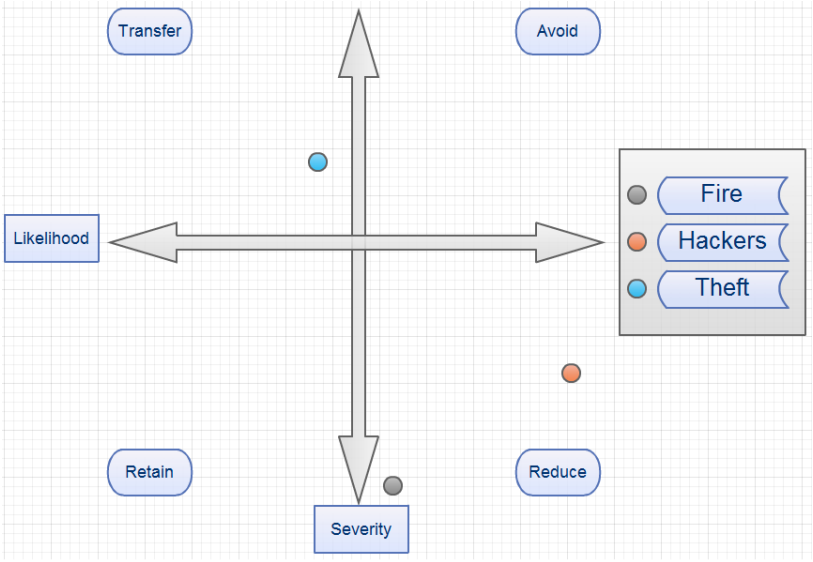

Figure 4.2 - Managing Risk Example

6 Closing

Performing risk assessments can be approached in different ways. In the end, in order for organizations to adequately assess the threats, vulnerabilities, likelihood and impact they must have acquired an extensive knowledge of how their company functions. Without this knowledge the organization will be unable to provide adequate analysis of risk and therefore be exposed to loss. Risk analysis is extremely complex and requires qualitative, quantitative and subjective analysis based on the factors that are present.

Every risk assessment is different and there is not one answer for two organizations. With the use of frameworks available from professional organizations and standards bodies organizations can create a baseline to build upon for their specific circumstances. Organizations must properly assess risk and then decide what should be done with this knowledge. They can then choose to avoid, retain, transfer or reduce the risk based on the factors discovered during the assessment process. Ultimately the results of this process will be based on the potential for financial impact versus the cost to implement a solution. If the solution is more expensive than the impact the money is not likely to be spent. Organizations must properly assess their assets and the threats they face regularly in order to maintain the most relevant security controls.

7 References

(1) Alberts, Christopher. "OCTAVE Criteria, Version 2.0.". N.p., n.d. Web. 20 Nov. 2013. http://www.cert.org/archive/pdf/01tr016.pdf.

(2) Chou, Te-Shun. "Risk Assessment and Real Time Vulnerability Identification in IT Environments." *Information Assurance and Security Technologies for Risk Assessment and Threat Management*. Hershey: IGI Global, 2011. 229-253. Print.

(3) Hopkin, Paul. "Analzsing Potential Impact." *Risk Management*. London: Kogan Page, 2013. Print.

(4) Marquis, Mark. "10 Steps to Do It Yourself CRAMM." *DITY Weekly Newsletter*. N.p., n.d. Web. 21 Nov. 2013. http://itsmsolutions.com/wp-content/uploads/2013/01/DITYvol4iss50.pdf.

(5) Rausand, Marvin. "How to Measure and Evaluate Risk." *Risk assessment theory, methods, and applications*. Hoboken, N.J.: J. Wiley & Sons, 2011. Print.

(6) Talabis, Mark, and Jason Martin. *Information Security Risk Assessment Toolkit*. Waltham: Syngress, 2012. Print.

(7) "FAIR (Factor Analysis of Information Risk)." *Basic Risk Assessment Guide*. N.p., n.d. Web. 21 Nov. 2013. http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf.

(8) "European Union Agency for Network and Information Security." *Risk Assessment — ENISA*. N.p., n.d. Web. 24 Nov. 2013. http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment.

(9) "Guide for Conducting Risk Assessments." *Information Security* 1 (2012): n. pag. *NIST Special Publication*. Web. 21 Nov. 2013.

(10) "ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)." *ISO/IEC 27005 risk management standard*. N.p., n.d. Web. 24 Nov. 2013. http://www.iso27001security.com/html/27005.html.

(11) "Top 10 2013-Top 10." - *OWASP*. N.p., n.d. Web. 24 Nov. 2013. https://www.owasp.org/index.php/Top_10_2013-Top_10.