Global Information Assurance Certification Paper

Matt Jacobs
Version 1.4b

ABSTRACT

Risk analysis is used by enterprises in many different ways. In today's environment it is imperative that companies take all possible precautions to protect themselves from these risks. A risk analysis is a good tool to help companies identify and define possible risks in a new project or undertaking. A formal risk analysis is made up of three sections, risk assessment, risk communication, and risk management. The goal of a risk analysis is to find ways to reduce risk in a specific application/project to an acceptable level, since it is impossible to ever completely eliminate risk.

Risk Analysis: Tying it All Together

RISK ANALYSIS

Everything you do has an element of risk. Whether it is considered to be a high risk such as jumping out of an airplane or a low risk such as tying your shoes, there is an element of risk involved. In the jumping out of the plane scenario one runs the risk of his or her parachute not opening. While tying your shoe there is a risk that you may pull too hard and break your laces. Each decision made is a choice to either accept the risk and move on or to not accept the risk and choose a different course of action. Some decisions are simple and can be made on the fly. In the business world however, and the security industry in particular, these decisions are not always that easy and need to be thought through and analyzed to make sure the correct decision is being made.

Risk analysis allows an enterprise the ability to define, control, and accept risk as it sees fit. The term risk has many definitions, two of which are: 1) the possibility of loss or injury, and 2) someone or something that creates or suggests a hazard. Some examples of risk in the information security field include natural disasters, disgruntled employees, hackers, and unsecured systems/networks. There are three main phases to a risk analysis. These include a risk assessment, risk management, and the communication of risk (Belveze, p.3). The three phases of risk analysis should not be looked upon as three separate processes but as one single interactive process.

A risk analysis should be performed whenever a company is close to deciding to undertake a new project in which money, time, and company resources are going to be used. The amount of time and depth of the risk analysis will very greatly based upon the project at hand. Something important to keep in mind however is that the risk analysis must be completed in a reasonable amount of time so that it does not impact the continuity of business. Those involved in the analysis should include experts from any and all areas that the

project will touch but should be headed by a designated risk assessment specialist whose main duties fall under either the information security group or its auditing counterpart. When the risk analysis is complete the enterprise should have a clear picture of whether or not to proceed with the project. If the decision is to proceed with the project those directly involved as well as management will have a clearly defined and prioritized list of risks as well as possible controls to help mitigate those risks. At this point is important to state that risk can never be fully eliminated but provided that acceptable controls exist, risk should be able to be reduced to an acceptable level.

RISK ASSESSMENT

Information security risk has become a major factor in the cost of doing business over the last decade. Everyday hackers, vendors, and security professionals find new holes in software, systems, and other technologies that they exploit while at the same time developing new techniques to bypass and dismantle security precautions placed by enterprises in order to protect themselves from these individuals as well as the known holes (accepted risk) within the aforementioned systems, software and technologies. The risk assessment is a process to measure risks to an asset and identify controls in hopes of mitigating these risks to a level that can be managed and secured by the enterprise. The risk assessment portion of a risk analysis is traditionally managed out of the information security department to help ensure a non-biased opinion as well as a safeguard of the information obtained throughout the assessment.

Risk assessments are important to an enterprise because unknown and unmanaged risks can lead to major security incidents. Once an incident takes place the response and recovery can become extremely expensive so it is highly beneficial for an enterprise to protect themselves from as many of these risks as possible beforehand. Besides the expense incurred by unknown risks that end up becoming exploited there are several other reasons that make a formal risk assessment make sense. Over the last several years' two very important pieces of legislature have been passed that put an enterprise at risk if certain types of information are exploited. The Gramm-Leach Bliley act signed into law by then President Clinton on November 12, 1999 places regulations on financial institutions as to their use and responsibility in protection of non-public personal customer information. The Health Insurance Portability and Accountability Act of 1996 (also known as HIPPA) among other things provided a standard for the privacy of individually identifiable healthcare information in order to help guarantee the privacy and confidentiality of individual's medical records. Liability can arise for a company found to be negligent in the administration of these laws.

Other types of enterprise liability also exist. Internal liabilities such as employees accessing pornographic sites can not only cause the individual embarrassment but also pose a liability to the enterprise if other employees see these images and videos and become offended by them to the point where they

sue the organization. Opportunities for external liability can also present themselves. For example if a company does not perform good due diligence (by performing a risk assessment or something similar in nature) and allows their network or systems to be hacked and used for the purpose of causing another enterprise or individual to sustain damage through attacks such as denial of service the company used by the hacker to launch said attacks can be found liable. These types of liabilities cannot only be expensive for an organization but can also be public relation nightmares.

The risk assessment is composed of many parts. The first step is to identify the asset or project in question. Next the object is to find a way to reduce the risks to an acceptable level. The risk assessment must be swift and efficient enough to be viewed by the enterprise as a business enabler, not an inhibitor. If the assessment drags out and prevents the normal workflow, employees and participants in the risk assessment are going to be less likely to do a thorough job and have the chance at being resented by others in the organization. Deciding to perform a risk assessment is not enough. It is important to have an executive business sponsor for the assessment. This individual should be the same individual who will be responsible for signing off on the approval of the project. By having this individual on board it provides an essence of approval for those being asked to participate that their endeavors are needed and important, not just a formality being instituted by the security department. As stated before the risk assessment team needs to include not just security personnel but employees from the business side that are experts in the subject matter. Once the assessment is complete it is important that the results are kept confidential so that corporate politics do not come in to play. Finally a recommendation on the project itself should be made to the individual or group that is ultimately responsible for making a decision on the projects future making sure to include a prioritized list of risks discovered and any applicable controls that can help to mitigate them.

There are three main models used by organizations in performing a risk assessment. The quantitative model is a mathematical model that assigns a value to a potential risk. The qualitative model that is more of a subjective assessment used to determine potential incidents, and a hybrid model that is a combination of the two.

Quantitative risk assessment attempts to place a value on the loss that could occur if a specific event happens. Quantitative risk assessment is a mathematically structured approach that attempts to remove all subjective determinations. The quantitative value is determined by multiplying the potential loss by the probability of that event taking place. This value is called the annual loss expectancy (ALE) or is also referred to as the estimated annual cost (EAC). By using this method it is possible to rank the associated risks in order as to those that are most likely occur down through those that are most unlikely to occur. One of the biggest benefits of the quantitative approach is that the results are expressed as values, percentages, and probabilities that tend to be most easily understood by management. This way they have a clear-cut answer and an accounting based presentation to support it. There are many weaknesses

associated with this approach. The biggest problem tends to be that the data used is often times unreliable and inaccurate since the probability of the specific event occurring is rarely precise. Other problems associated with quantitative risk assessment are that the computations are complex and require a large amount of background research to assign probabilities to the events. Also, it is difficult to address issues that are not in the scope of the project such as risk and impacts on employees, shareholders, customers, suppliers, etc. While not the most used option, quantitative risk assessments do provide benefit to the enterprise. It is important to remember when dealing with the results of this type of assessment that even though the calculations produced exact numbers, the values used to arrive at these numbers were not precise. Therefore the results of this type of analysis need to be reviewed thoroughly to ensure that a potential risk that garnered a low value is not overlooked as being insignificant.

Qualitative risk assessments tend to be favored among organizations due to the fact that they are easier and quicker to accomplish. The calculations are simple. There is not a need to determine the monetary value of the asset as well as it is not necessary to quantify the frequency of the threat. The qualitative approach also provides for greater flexibility in the way the assessments are ran and then reported. Qualitative risk assessments also make it easier to utilize business experts outside of security and technical staff since their expertise is used subjectively to help determine risks (Peltier, p.20).

The process involved in a qualitative assessment involves evaluating risk based on scenarios and then determining the supposed impact of that incident. The risk analysis team will comprise several lists. These lists include threats, vulnerabilities, and controls. Threats are the things that can go wrong such as fire, hackers, and fraud. Vulnerabilities are things that make a system or application more open to an attack. For example mismanaged policies on a firewall are vulnerability for a hacker the same way flammable materials such as paper or gasoline would be a vulnerability to a fire. Controls are the means to keep vulnerabilities in check. Types of controls include; Deterrent controls that reduce the chance of a deliberate attack. Preventative controls that protect vulnerabilities or reduce their potential impact. Corrective controls reduce the effect of an attack, and detective controls seek out attacks and initiate preventative and corrective controls (SRA directory, p.2). The risk assessment team will then rank these lists using their knowledge of the business environment and the severity of each incident. The assigned rankings are then used in an algorithm to assign a subjectively concluded risk factor. For example one commonly used algorithm is: *Threat * Vulnerability = Risk*. This formula would be used for each risk possibility that the assessment team composed. After this is complete the team would then assess the controls available and determine if the risks were acceptable. There are many different variations of this algorithm used in qualitative assessment. There is not one right or wrong one to use, but is best left up to the enterprise to determine a standard so that all assessments are done using the same process. One variation I have not encountered in my research includes factoring in the controls initially. The algorithm that I have been developing is: *Threat * (Vulnerability - Control for that vulnerability) = Risk*.

The benefit I derive from this algorithm is that once I apply it the subjective number I am left has already taken the controls into consideration. Therefore if the values that I am left with are still outside the acceptable risk threshold I know right then that the project is too risky to undertake.

There are several weaknesses to the qualitative method. The most obvious is the loss of the ability to do a cost vs. benefit analysis to determine the viability of purchasing controls or in updating and developing new policy and procedures to mitigate the risk. Qualitative assessments are often times seen as being too subjective and imprecise for senior management. Also the quality of the assessment is only as good as the team that puts it together.

The Hybrid assessment approach is a combination of qualitative and quantitative risk assessment. Many companies use the qualitative approach to identify the possible areas of impact and use the quantitative approach to put a value on the asset as well as an estimated dollar value on the impact the risk could have. This approach is beneficial because it is flexible and can be customized to meet the particular management, audit, and security needs of a particular organization.

COMMUNICATION OF RISKS

Once the risk assessment has been carried out, the results need to be communicated with senior management, and more specifically with those in charge of making the decision as to whether or not to take on the project. The risk assessment team has spent considerable time in gathering, defining, and analyzing the data so it is important that their hard work is organized professionally and presented in a way so that someone unfamiliar with the project can read the risk assessment from cover to cover and be informed enough about the project and the risk assessment process itself that he or she can make a judgment as to whether or not to move ahead with the project.

There is no incorrect way to construct the risk analysis report; however it is important that this be a formal document that can be used as reference in the future. That being said, this report should be typed, free of grammatical errors, well laid out, and protected by a cover of some sort. There are many sets of guidelines in constructing the report itself, but the information contained in the analysis should be fairly consistent.

The analysis report should contain an introductory section that gives an overview of the scope of the project being analyzed. This portion of the analysis should discuss what the system or project hopes to accomplish, why it was chosen, where it came from, how much it costs, etc. Secondly it is important that those reading the analysis know who created it. Earlier I mentioned that a risk assessment was only as good as the people that ran it. This is the section to list those individuals, their areas of expertise, and how they contributed to the analysis.

The next section that is important to have in your risk analysis could be labeled as a disclaimer or as I like to refer to it, the small print. This section

should provide information as to any circumstances that may have impeded the analysis, such as time or resources. This section can also be used to direct the readers to past risk analysis reports that used the same assessment models and methods so that the results can be benchmarked against each other if need be.

Now that some of the background and formalities are out of the way the next section is the heart of the report itself, the risk analysis findings. This section will be the bulk of your report and should cover several things. First the analysis should list the threats and vulnerabilities determined by the team. These threats and vulnerabilities should be layed out in order from those that pose the most risk to those that have been determined to have the least amount of risk. This way those reading the report will be able to easily determine those threats and vulnerabilities that pose the greatest risk to the organization. The next part of the analysis portion should contain a summary of the risks, their probabilities (if using a quantitative analysis method), the potential loss in dollars that the risks could pose (rough dollar values will be used here if using a qualitative model for risk assessment). Finally give the groups findings as to the risks that are the most probable to take place. Make sure that this portion of your report does not include in depth analysis including charts, graphs, and calculations. This type of supporting documentation can be saved and attached to the end of the report as an appendix. The purpose of this portion of the report is strictly to give an overview of what the findings of the assessment were. This section of the report should conclude with a description of the controls that are suggested in order to mitigate each of the risks listed previously. This is a good area to list the costs associated with these controls as well as explain exactly what this control can accomplish (Can it completely control the risk, or to what degree can the control mitigate the risk?).

Now is the time in the report for the risk analysis team to make their recommendations concerning the project or system in question. This section may start off with an opinion formulated by the group that contains what they would do if the situation was theirs to determine. It might also start with a single statement either in support or against the subject of the report. After this initial recommendation it is important for the team to discuss the implications of proceeding with this project whether or not they are in favor of it. This portion should discuss the controls needed to mitigate as much of the risk as possible, the costs and benefits of these controls, as well as what it would take in terms of resources to purchase, develop, test, implement, and maintain these controls if the project were to be approved. It is important that each control be discussed individually so that those making the decision can pick and choose which controls they are willing to spend money on, and which risks they are willing to accept.

The risk analysis report should briefly touch on the other areas of the report. It should restate what the analysis covers, the team that was involved, any factors that got in the way or had influence over the analysis, the process used to do the assessment, the recommendation derived by the group from the analysis, and the controls proposed by the risk analysis team that can help to mitigate the risks of the project. At this point the risk analysis is relatively

complete. It is important to attach all documentation; graphs, charts, calculations, and a reference list (if any outside publications or research was used) before presenting your risk analysis to senior management or the risk management team.

RISK MANAGEMENT

The group charged with making determinations as to whether or not a project or request for a new system is approved is commonly referred to as the risk management group or in the case of an individual with this power, the risk manager. It is imperative that this individual or group be comprised of individuals who are not part of the risk analysis team. This is to ensure impartiality to the risk analysis itself. This group or individual has many responsibilities both before a risk analysis takes place and after it has been completed.

Before a risk analysis ever begins the risk management is responsible for creating the enterprises risk policy and profile. This profile will provide a framework as to the companies' tolerance for risk, and the policy will help to set guidelines as to when a full blown risk analysis is required. Once a project or request comes to the attention of risk management that meets the guidelines set forth in the risk policy to constitute a risk analysis management will assign a lead from within the information security group to get the ball rolling. It is important at this point that those involved with risk management now take a step back away from the process and let the risk assessment commence without any further discussion that may influence or discount the validity or independence of the risk assessment.

Once the risk assessment has been completed and the risks have been communicated back to the risk management team through the risk analysis report/presentation discussed earlier, it is now the decision of the risk management team as how to proceed. They have several options available to them. They can choose to accept the recommendation of the risk assessment team. In the case that the risk assessment team chose to not recommend the project this would then be the close of that situation. If the risk assessment team recommended that the project be implemented than the approval of the risk management team would not only sign off on the project taking place but would be required to determine which risks to accept and which risks to purchase or develop controls for. At this point the risk management team is not only signing off on accepting the project, but because a thourough risk analysis was done and presented, the risk management team is now also signing off on the risks associated with the project.

If the risk management team decides to go against the recommendation of the risk analysis group several things may happen. If the risk analysis had not recommended the project and the management team wants to accept it, they are doing so with the full knowledge and documentation from the risk analysis that supports the opinion that there is too much risk involved to proceed. Depending on company policy it is often times mandated that if the risk management team

still wants to accept a project that has not been recommended by a thourough risk analysis that the risk management team must then gain the approval of a higher authority such as a CEO or board of directors. This ensures that someone of great authority within the institution is aware that a project that has a high potential of risk for the company is being willfully instituted. Rarely does a situation like this occur unless the project in question has the potential to bring in so much money that the risk is accepted. The other alternative is that the risk analysis team recommends the project but the risk management team chooses to deny the request anyway. This can be done for many reasons such as business need. Just because a project or system is found to have low or moderate risk does not necessarily mean it is right for the business to accept. Budgets may be tight, the strategies may have changed, any number of reasons can be used to determine a project should not be undertaken. The important thing is that in the event that the company thinks about pursuing this project down the road a solid framework has been laid that will make the updated risk analysis a more streamlined task.

CONCLUSION

It is important to remember that the three parts of a risk analysis are one integrated task that need each other to produce the best and most efficient risk analysis. Risk assessment determines the threats, vulnerabilities, probabilities, and controls associated with the request. Risks are then communicated through compiling and presenting the risk analysis report to the risk management team. The risk management team not only makes a determination as to the outcome of the project request but is also responsible for developing and standardizing the companies risk profile. This ultimately determines the acceptable level of risk for that company. Remember that it is impossible to eliminate risk in an organization but it is essential to minimize that risk to the greatest extent possible.

LIST OF REFERENCES

ABS Consulting. URL: http://www.jbfa.com

Belveze, Henry. "Risk Assessment and Risk Management in the Food Chain." URL: http://www.fedesa.be/Events/ForumV/hnrblvz.htm

Bier, Vicki and Zimmerman, Rae. "Risk Assessment of Extreme Events." URL: http://www.ldeo.columbia.edu/CHRR/Roundtable/Zimmerman_WP.pdf

Krause, Mickey and Tipton, Harold. Information Security Management. New York. Auerbach Publications. 2002.

Krause, Mickey and Tipton, Harold. "Risk Management and Business Continuity Planning." Handbook of Information Security Management. URL: http://www.cccure.org/Documents/HISM/223-228.html

Peltier, Tom. Information Security Risk Analysis. New York. Auerbach Publications. 2001.

Peltier, Tom. "Risk Analysis in Business Process." URL: http://www.gocsi.com/pdfs/risk.pdf

Security-risk-analysis.com. "Introduction to Risk Analysis." URL: http://www.security-risk-analysis.com/

Texas Department of Information Services. "Information Resources Security and Risk Management Policy, Standards, and Guidelines." 1994. URL: http://www.dir.state.tx.us/oops/infosec/

Texas Department of Information Services. "Practices for Protecting Information Resources Assets." Mar 2000. URL: http://www.dir.state.tx.us/IRAPC/practices/

United States General Accounting Office. "Information Security Risk Assessment: Practices of Leading Organizations." Accounting and Information Management Division. Nov 1999. URL: http://www.gao.gov/special.pubs/ai00033.pdf