Global Information Assurance Certification Paper

Modifying the OCTAVE® BIA/Risk Analysis Program to Accommodate a Small Business

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option A
Samuel A. Merrell, CISSP
09/19/2003

Abstract

Whether it is from a disaster recovery/business continuity, regulatory, defensive, or educational need, performing a risk analysis is the first step in the long journey of securing your company. Fortunately, the Software Engineering Institute (SEI [SM]), a Federally-Funded Research and Development Center (FFRDC) located at Carnegie Mellon University, has developed a methodology to make this process a little less daunting.

OCTAVE® (which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation [SM] is a methodology that involves knowledgeable people from each department, and uses them to identify critical assets, threats to those assets, and safeguards to protect the assets. This approach benefits from the institutional knowledge and expertise of those people who are closest to the assets that need to be protected. The OCTAVE methodology, as designed, is meant for large corporations (over 300 employees). It is possible, however, with some modification, to 'scale down' OCTAVE for use in much smaller companies. By forming a committee, using individuals rather than workgroups, and developing a risk scoring system, the small business can benefit from this thorough program and achieve the desired results. Additionally, although OCTAVE was designed as an information systems risk analysis tool, it is not difficult to expand the model to include any asset that a company should wish to protect. Developing asset profiles in OCTAVE gives the analyst a solid foundation on which to build recovery plans, compliance policies, or an in-depth understanding of the company. This document will not detail every step of the OCTAVE approach, as Christopher Alberts and Audrey Dorofee have written in the book "Managing Information Security Risks: the OCTAVE® Approach". It is my goal, however, to illustrate points in the approach that could be modified to scale down the OCTAVE approach to a smaller company.

The Business Need

As any manager can tell you, there has to be a business need before a company will begin a project. This ensures that what is being done fulfills, or works toward fulfilling, a business goal. Performing a risk analysis can be the first part of many different projects, which serve many different needs. These needs can be the development of a Disaster Recovery/Business Continuity plan, complying with regulations, or getting to know your systems so that you can effectively secure them.

Disaster Recovery/Business Continuity Planning

The foundation of a Disaster Recovery or Business Continuity plan is to know exactly what it is that you need to protect, and what you need to do to protect it. Without this basic information, plans would miss critical assets, or companies would be spending scarce resources on countermeasures that do not protect assets from the most dangerous threats.

The first element in developing a successful Disaster Recovery/Business Continuity Plan is the Risk Analysis, with a Business Impact Analysis.[1] This the most crucial part of Recovery planning, and is where risks to critical assets are identified.

Done properly, the BIA sets the stage for producing the enterprise-wide contingency plan. Because the BIA process is very analytical; it ensures that the BUSINESS—not you, not your manager, and certainly, not the political infrastructure of the organization - all focus directly on what the business would need in order to survive if, and when, disaster strikes.[2]

While a BIA asks, "what are the assets and the threats?" the risk analysis asks the question "How likely, and often, will these threats occur?"

Once the BIA and risk assessment are completed, the person or committee can be sure that they have a good starting point from which to develop a Recovery/Continuity Plan. The focus of this paper will be in performing OCTAVE as a part of a Disaster Recovery / Business Continuity Plan.

Regulations

Another important reason for conducting a Risk Analysis is the requirement from any number of regulations or regulatory bodies. Two notable examples of this are the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA) and the Health Information Portability and Accountability Act of 1996 (HIPAA).

The Gramm-Leach-Bliley Act, designed to govern financial institutions, and introduced the "Safeguarding Customer Information Rule," which stated:

> "You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue… *Objectives*…Insure the security and confidentiality of customer information; (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[3]"

[1] Ben Taylor and Ron Ginn, "The Big Picture" URL: http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='59' (Sept. 05, 2003).
[2] Fisher, Patricia A. P., "HOW TO CONDUCT A BUSINESS IMPACT ANALYSIS" *Disaster Recovery Journal*, URL: http://www.drj.com/articles/sum96/fish.html summer, 1996 (Free membership required).
[3] Federal Trade Commission, Vol. 67, No. 100 / 16 CFR Part 314, URL: http://www.ftc.gov/os/2002/05/67fr36585.pdf (May 23, 2002) .

The Safeguarding Customer Information Rule requires financial institutions to "Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures." [4]

HIPAA, which deals with the health-care industry, also has a requirement for risk analysis:

> We proposed the establishment of a formal security management process to involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This process would include implementation features consisting of a risk analysis, risk management, and sanction and security policies.[5]

It is apparent that risk assessment serves a purpose beyond that of disaster recovery, and it is a fundamental part of developing an environment of security, as well. These and other regulations demonstrate the fact that the government recognizes the need for organizations to understand the risks that they face, so that they can responsibly protect themselves.

Defense in Depth

If you do not know the risks that an asset faces, how can you protect the asset? Just as a risk analysis serves to provide information to the person developing a Disaster Recovery Plan, it is also an ideal way for the security professional to learn about the systems that they are charged with protecting. As SANS instructor Eric Cole advocates, "Know Thy System." The risk analysis is important in knowing a single system, or any asset, for that matter. Knowing the threats to a system will guide you in protecting the system.

Additionally, such an analysis can serve to educate the employees about the business, allowing business decisions to be made that account for the impact across the organization. The BIA/risk analysis can quickly define interdependencies among departments, identifying critical business processes. This could allow better decisions to be made about possible safeguards when these items are viewed as an aggregate, rather than granularly.

The risk assessment also serves to build a "Defense in Depth" strategy of protection of systems. If you know that the information that you are protecting is of vital national security, and threats are theft, fire, spies, and hackers, you will take more measures than to install a firewall. You will also physically secure the information, perhaps behind locked doors. You would install fire-suppression systems, and possibly encrypt the information, preserving its' confidentiality. While it would be possible to build a "Defense in Depth" model without the risk

[4] Federal Trade Commission, Vol. 67, No. 100 / 16 CFR Part 314, URL: http://www.ftc.gov/os/2002/05/67fr36585.pdf .

[5] DEPARTMENT OF HEALTH AND HUMAN SERVICES, "Health Insurance Reform: Security Standards; Final Rule" of the Health Information Portability and Accountability Act of 1996, From the Federal Register Online via GPO Access URL: wais.access.gpo.gov.

analysis, you would not be able to ensure that you are protecting against all threats, and missing a component could be catastrophic. If you installed firewalls, and fire extinguishers, but not physical locks on the door, anyone could access the information, and you are not protecting it. As you can see, it is only through being well educated in the risks to the assets that one can diligently protect it.

Enter the OCTAVE ® Methodology

The Software Engineering Institute (SEI(SM)), a Federally-Funded Research Center (FFRDC) located at Carnegie Mellon University, designed OCTAVE to assess information security risks by identifying critical assets to a company, defining the threats to those assets, and the vulnerabilities that can allow the threats to be realized. This methodology was designed to be performed by the company that needs the analysis, and therefore involves people who are the most familiar with the assets that need to be protected. CERT refers to this approach as "Self-Directed."[6]

"The OCTAVE framework consists of three phases:

- **Phase 1: Build Asset-Based Threat Profiles** - This is an organizational evaluation. Key areas of expertise within the organization are examined to identify important information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets (protection strategy practices), and weaknesses in organizational policies and practice (organizational vulnerabilities).

- **Phase 2: Identify Infrastructure Vulnerabilities** - This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action.

- **Phase 3: Develop Security Strategy and Plans** - Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) are analyzed to identify risks to the enterprise and to evaluate the risks based on their impact to the organization's mission. In addition, protection strategies for the organization and mitigation plans addressing the highest priority risks are developed."[7]

[6] OCTAVE Information Security Risk Evaluation URL www.cert.org/octave (August 19, 2003).
[7] Alberts, Christopher and Dorofee, Audrey Software Engineering Institute of Carnegie Mellon University "An Introduction to the OCTAVE[SM] Method" URL http://www.cert.org/octave/methodintro.html (August 19, 2003).

OCTAVE was designed for large (over 300 employees) organizations[8], which build an analysis team, and involve members of all business units to use a collection of workshops and worksheets to collectively identify the critical assets, threats, and risks.

The OCTAVE methodology can, however, be used in a small company, with a slight modification to the original model.

Modifying OCTAVE to Fit a Small Company

A common rule of thumb in Information Security is that in order for an information security program to succeed, you must have the support of upper management. In a small company, this support is often easier to acquire, because executives of these companies are generally more accessible, and more 'hands-on' than in large companies. Implementing OCTAVE will be much easier if managers are aware of the executives' commitment to the program. Additionally a significant portion of Phase 1 of the OCTAVE methodology involves "identifying knowledge" of the people that are participating. In the small company that is going to perform its' own analysis, these steps often can be excluded, based on the simple fact that there might not be another person in the company who can cover the needed area. The work ahead can be time-consuming, so making the President's, or Vice President's support well known throughout the company is a valuable contribution.

The Committee

In the large corporation model, the first step after gaining management support is to create a team of people who act as coordinators for OCTAVE. This team is the set of people who ensure the OCTAVE program is followed, collect information produced by the departments, and analyze that information. OCTAVE recommends that this team consist of "3 to 5 members…. (who possess) the basic skills, such as good facilitation, communication, analytical, and problem-solving skills. However, attention to other factors can contribute to developing an effective analysis team."[9]

For the small company, one person can perform the task of coordinating OCTAVE projects; distributing worksheets and analyzing data, as long as they have the ability to clearly explain the activities, and the backing of senior management,. A solid understanding of risk analysis concepts will aid the facilitator in following OCTAVE, and guiding the company through the phases of the program.

According to the OCTAVE methodology, the preliminary steps in beginning the program are: (1.) set the appropriate scope of the OCTAVE methodology[10], and (2.) select participants[11]

---

[8] OCTAVE® Method Frequently Asked Questions (FAQ) URL: www.cert.og/octave/faq.html (August 19, 2003).
[9] OCTAVE® Method (FAQ) .
[10] Alberts, Christopher and Dorofee, Audrey Managing Information Security Risks, the OCTAVE℠ Approach Boston, Ma, Pearson Education, Inc., 2003, pp 45.
[11] Alberts and Dorofee, pp 45.

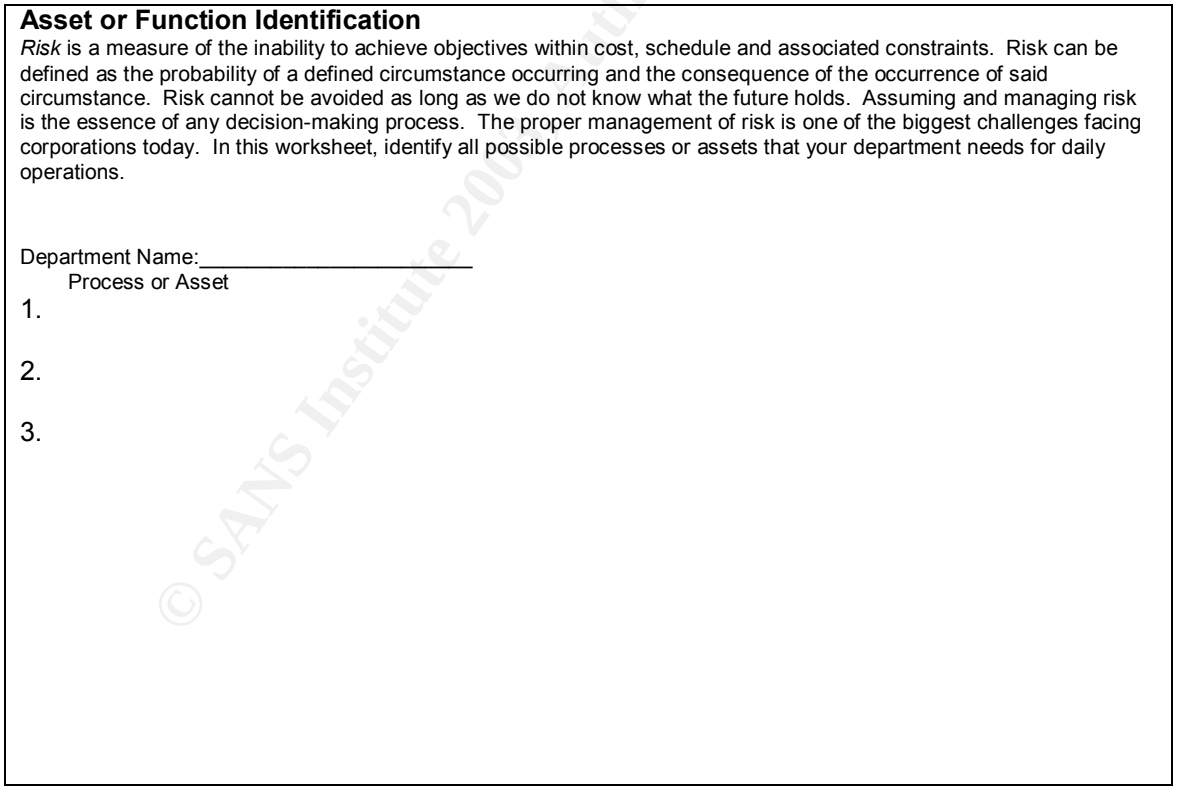
The OCTAVE methodology suggests that the large company begin a process of determining who might be best suited to participate in the program, based on their knowledge of the business, and their involvement in the areas that are being examined.

In the small company, this process is significantly easier; select one member of management from each department or business unit, preferably the most senior manager. This accomplishes a few things: it ensures that no part of the company is left out of the process, allowing for a thorough analysis, and it increases the likelihood of identifying all critical assets for analysis. Ideally, this person would be the most knowledgeable about his/her business unit. In addition, your OCTAVE committee becomes self-defining.

Phase 1

The OCTAVE methodology uses Phase 1 to accomplish many different tasks, including the identification of the knowledge of the people who are on your team. The auto-selection process of picking the senior managers of all departments assumes that you have the most knowledgeable people in the company in the various departments as the managers.

Next, the task is to identify the critical assets to the company. This is accomplished through a series of worksheets. (Fig. 1)



Asset or Function Identification

Risk is a measure of the inability to achieve objectives within cost, schedule and associated constraints. Risk can be defined as the probability of a defined circumstance occurring and the consequence of the occurrence of said circumstance. Risk cannot be avoided as long as we do not know what the future holds. Assuming and managing risk is the essence of any decision-making process. The proper management of risk is one of the biggest challenges facing corporations today. In this worksheet, identify all possible processes or assets that your department needs for daily operations.

Department Name:_____

Process or Asset

1.

2.

3.

Figure 1 – Sample Asset Identification Worksheet

The simple worksheet above allows the committee to identify the various assets within their department. What is important to understand in this process is

that it is not crucial to make sure that all assets are identified, as it would become a very difficult task to do so; those items that are missing will make themselves apparent when you test your Recovery Plan. Treating the plan as a living document at its inception will remind you of the need to update it down the road. Obviously, all participants should be identifying as many critical assets or processes as possible, but it is not necessary to spend too much time making an exhaustive search of forgotten items.

Once the assets have been identified, the committee members develop "Areas of Concern"[12] for each asset, which is where specific threats to assets are listed with the outcome of that threat. For example, if the threat was "fire," the outcome may be "destruction of confidential information."
These Areas of Concern are then matched with an "impact." Therefore, the threat of, "Fire" could cause the outcome of "destruction of confidential information," which would affect the company by "possible regulatory penalties," "loss of customer confidence," and "damaged reputation."

After the Areas of Concern have been fully explored, the next step in OCTAVE would be to have the committee identify and select the most critical of the identified items. This is done because it is not impossible that dozens, if not hundreds, of assets could be identified. Analysts should use their own judgment on this matter. The amount that you eliminate from the list of assets should depend on the reason for performing the risk analysis. If you have a fully tested Disaster Recovery Plan in place, and are trying to determine the capability of that plan to protect your critical assets, then perhaps such a reduction would be appropriate. On the other hand, if your company does not have a plan in place, and they are using OCTAVE to build such a plan, then it would be in their interests to work with a larger list at first, and reduce items upon subsequent reviews in the future.

When the list of assets has been completed, and threats to those assets have been identified, along with the impact that those threats can have, we next develop a definition of the asset. This definition describes the asset, how it is used, who uses it, and why it is critical to the company.[13]

The last step of Phase 1 is to develop what is called a 'Threat Profile'. This is a "structured way of presenting a range of threats to a critical asset,"[14], and involves developing "Threat Trees." These trees have the following elements:

- Asset – something of value to the enterprise
- Actor – who or what may violate the security requirements (confidentiality, Availability) of an asset
- Motive (or objective) – whether the actor's intentions are deliberate or accidental (applies only to human actors)

[12] Alberts and Dorofee, pp 93.
[13] Alberts and Dorofee, pp 125.
[14] Alberts and Dorofee, pp 112.

- Access – how the asset will be accessed by the actor, e.g., network access, physical access (applies only to human actors)
- Outcome – the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset.[15]

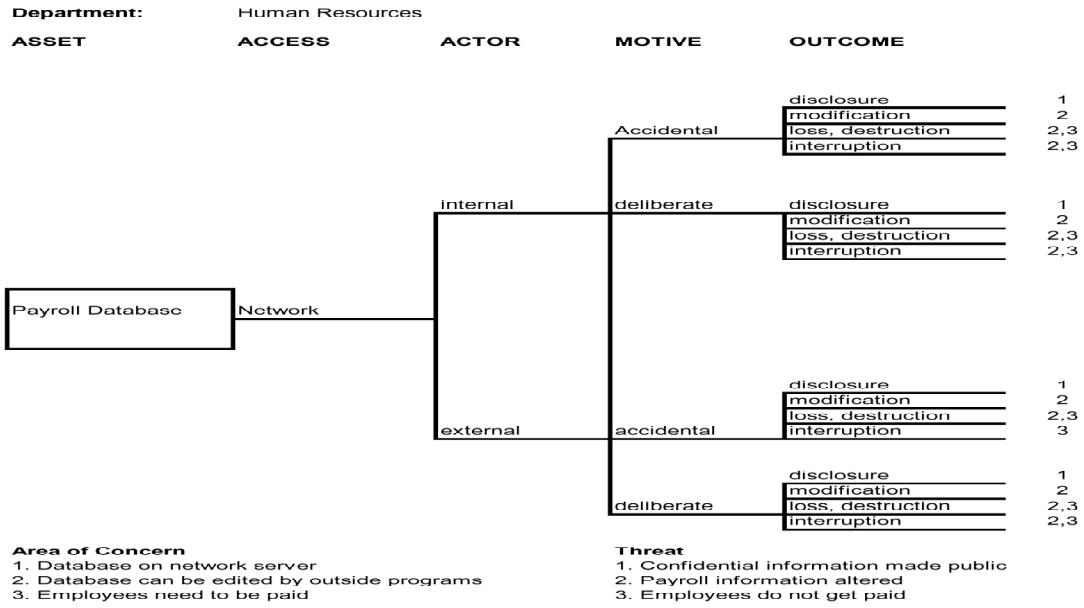


Figure 2 -- A sample threat tree with Areas of Concern[16]

Phase 2

There are parts of Phase 2 that apply to both small and large companies, so this section does not go into much detail.

Phase 2 of The OCTAVE methodology begins by identifying technological vulnerabilities within the critical assets identified in Phase 1. These technological vulnerabilities are mapped using technical tools such as topology diagrams,

[15] Alberts and Dorofee, pp 112.
[16] Alberts and Dorofee, pp 114.

diagramming tools, etc. The purpose of this exercise is to identify "Systems of Interest,"[17] which are systems that act as a vector for threats to exploit vulnerabilities. Once again, here it is possible to include all identified assets as "systems of interest," for the fact that it is not likely that there is an asset that cannot be exploited in some way.

Step 2 of Phase 2 is to classify components of assets. If you are analyzing technological items, such classifications may include Servers, Routers, Firewalls, etc. The purpose of this exercise is to define the methods and materials needed to access the asset. For example, if your asset is "payroll database", it may be classified as "software" that includes the components "Server", "PC", "Network" and "Modem". This offers a global view of all of the items that can have an impact upon the asset through vulnerabilities. This step is useful for ensuring that all possible vectors are accounted for in the analysis.

The last part of Phase 2 is to run automated vulnerability tools that are commercially available, in order to search for technical problems in your computing infrastructure. This is useful, and scales to small companies, but it is important to perform this analysis in light of the access vectors that were identified earlier. If there is a known vulnerability identified in an operating system, and your company is not using the software that can be exploited, then it is not essential that you include that risk (although, Defense-in-Depth principals suggest that you make sure that any non-essential software is either disabled or removed for all systems).

Phase 3

In Phase 3, we define the likely impact an identified threat can have on our asset. This is done using questionnaires and trees. The trees extend those done in earlier exercises, adding an "impact" column. OCTAVE suggests that this impact rating should be "High, Medium, and Low." As you will see in the next section, for symmetry this has been modified to a scale of 1 – 9, with nine being the maximum possible impact.

Additionally, one of the steps that OCTAVE does not use that I have added is the idea of "Likelihood" of the risk having the impact. This is useful in determining if a countermeasure is appropriate. For example, if the risk is "Being hit by falling meteor" but the annual likelihood is "one time in 1000 years (.001)", then perhaps buying the meteor-proof roof for our building is not that practical. This is useful when beginning the Business Impact Analysis for the Disaster Recovery Plan.

[17] Alberts and Dorofee, pp 144.

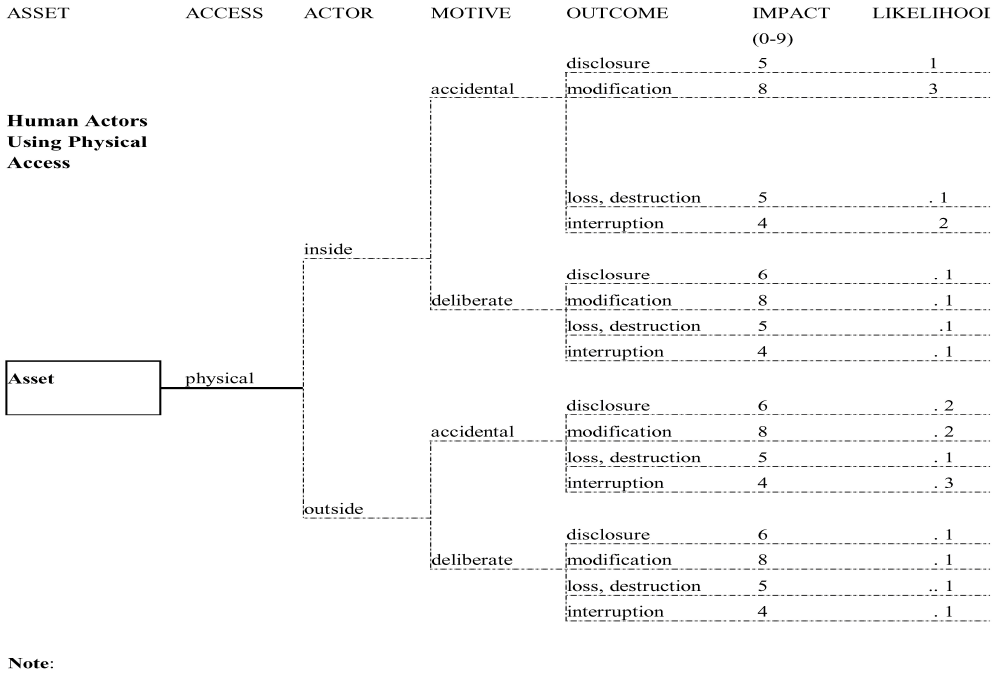


Figure 3 --A sample threat tree[18]

Once the threat trees have been completed, the OCTAVE risk analysis is complete. The results are to be used by the organization to determine the best ways to either reduce or accept the risk. Countermeasures can be identified and implemented, insurance can be purchased, or the risk can be formally accepted by the organization.

Which is 'More Critical'?

One important question that remains after the modifications suggested here to OCTAVE is "which of these are more important than the others?" Since the

[18]Alberts, Christopher J., Dorofee, AudreyJ. "OCTAVE[SM] Method Implementation Guide Version 2.0 Volume 9: Process 7 – Conduct Risk Analysis" pp. E7-14 (June, 2001).

original request of the committee was to identify what is important to the business, now a priority of recovery must be developed.

There are two different routes you can take to perform a risk analysis; one is a **quantitative approach**, where the analyst identifies the dollar value associated with an asset. This endeavor can be quite daunting, due to the need to include such things as the cost to develop and maintain the asset, as well as the costs that would be incurred to replace the asset if lost. A purely quantitative approach to risk analysis has a significant benefit; once you know how much an asset costs, it is a straightforward task to determine how much money to spend protecting the asset. This Asset Value is then plugged into an equation, along with what is known as the *exposure factor* (the measure of impact that a threat can have on a specific asset), to arrive at the *Single Loss Expectancy* (SLE). The SLE can then be multiplied by the number times a year that a threat can happen, to arrive at the *Annual Loss Expectancy* (ALE), which will tell the company how much money it should invest in protecting that asset. For example, if an Oracle database has an asset value of $10,000, and the threat of an employee accidentally deleting records would do 5% damage, the SLE for this threat would be $500. If the employee makes this type of mistake once a month, then the ALE would be $6,000. Therefore, the company should not spend over $6000 a year on protecting the database from employees' accidents.

This cut-and-dry approach is convenient, direct, and easily understood. One of the significant problems with the quantitative approach, however, is that it is often quite difficult to determine all of the costs involved. How do you determine the cost of a database of a small business's customers that has been in development for 25 years, and has existed on three different computing platforms? If you have a small I.T. staff, which typically is required to perform many different tasks, including database administration, how do you add their costs to the equation? Departmental managers concern themselves with the use of the asset, generally not with its' value. These and other questions must be answered to arrive at an accurate Asset Value, but it can be very challenging to identify all costs that make up the 'real' value.

OCTAVE follows a different path, however, which is generally called the **qualitative approach**. As we have seen, this approach relies on the knowledge and experience of the employees participating in the program, and does not need to account for monetary costs, and thus can be easier on the analyst.

We can build on this approach when we need to prioritize the identified items that we need to protect. We accomplish this through another worksheet (figure 4). This worksheet, designed using evaluation criteria taken from the OCTAVE method, and serves to track the impact of the unavailability of an asset over time. It uses a rating system of zero – nine, where '0' is no impact and '9' is the maximum impact that the asset could possibly have on the organization. The worksheet gauges impact over time, using increments of one hour, two hours, one day, one week, and two weeks. This time should be adjusted to fit the needs of your organization, but the assumption made is that any incident should be on its way to recovery within 2 weeks. The analyst should expect to see a global increase of impact as time goes by, but the rate at which individual assets'

impact increases will identify which items should have priority over others. By adding the assigned values for each asset, you can develop an 'impact score' that can also identify which assets have overall critical impact. Those assets that score the highest must have an overall higher criticality to the organization, and, therefore are a good place to start when developing a protection plan.

Department	Function					
Audit	**Compliance**					
		An hour	A day	Two days	1 week	2 weeks
If this function were not performed following a disaster, what would be the impact to the company, on a scale of 0-9, with 9 being the highest possible impact.	Human life	0	0	0	0	0
	Customer service	0	0	0	0	0
	Ill will	0	0	0	0	5
	Operating efficiency	0	2	3	4	5
	Laws broken	0	0	0	0	9
	Impact on environment	0	0	0	0	0
	Contracts violated	0	0	0	0	0
	[optional spaces for your own factors…]					
	Score:	0	2	3	4	19
				Total Score		28

Figure 4 – a sample of prioritizing the impact of unavailable assets.

Beyond I.T.

Although OCTAVE was designed primarily for an Information Technology Risk Assessment, I do not feel that a company is limited to this use. The model works just as well for any asset of the company, large or small, that requires a security risk analysis. Therefore, OCTAVE serves as an excellent whole-company Risk

Analysis/Disaster Recovery-planning tool, and does not have to be limited to technological areas.

OCTAVE®-S

At the end of the summer, 2003, the Software Engineering Institute released a preliminary version of OCTAVE®-S, which is the 'official' program that accomplishes the same task as this document, i.e., making OCTAVE accessible for a small company (less than 100 people)[19]. Information about OCTAVE®-S can be obtained on OCTAVE web site http://www.cert.org/octave/osig.html.

Summary

Performing a Risk Analysis can be a daunting task for the small company, with often the same disaster recovery, regulatory, business, and technical needs as large business, but less resources available to it. The small business benefits from publicly available methods. One such methodology is OCTAVE, which was designed with large businesses in mind, but can, with slight modification, be used by the small company to perform the same task. These modifications include scaling down the size of the task force, and eliminating a portion of the method that identifies the knowledge of the respondents. It is also important to think of the methodologyas ongoing, and always changing. This is because of the fact that no matter what size they are, companies are always installing new technologies, taking on new projects, or expanding their business. This change in business continuously introduces new sources of risk, which must be accounted for through a thorough Risk Analysis.

[19] Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody "OCTAVE®-S Implementation Guide, Version 0.9 Volume 1: Introduction to OCTAVE-S" pp 1

List of References

1. Ben Taylor and Ron Ginn, "The Big Picture" URL: http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='59' (Sept. 05, 2003)

2. Fisher, Patricia A. P., "HOW TO CONDUCT A BUSINESS IMPACT ANALYSIS" *Disaster Recovery Journal*, URL: http://www.drj.com/articles/sum96/fish.html summer, 1996 (Free membership required)

3. Federal Trade Commission, Vol. 67, No. 100 / 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule, URL: http://www.ftc.gov/os/2002/05/67fr36585.pdf (May 23, 2002)

4. DEPARTMENT OF HEALTH AND HUMAN SERVICES, "Health Insurance Reform: Security Standards; Final Rule" of the Health Information Portability and Accountability Act of 1996, From the Federal Register Online via GPO Access URL:http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-3877.htm

5. OCTAVE Information Security Risk Evaluation URL www.cert.org/octave (August 19, 2003)

6. Alberts, Christopher and Dorofee, Audrey, Software Engineering Institute Carnegie Mellon University "An Introduction to the OCTAVE[SM] Method" URL http://www.cert.org/octave/methodintro.html (August 19, 2003)

7. OCTAVE® Method Frequently Asked Questions (FAQ) URL: www.cert.org/octave/faq.html (August 19, 2003)

8. Alberts, Christopher and Dorofee, Audrey Managing Information Security Risks, the OCTAVE[SM] Approach Boston, Ma, Pearson Education, Inc., 2003

9. Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody "OCTAVE®-S Implementation Guide, Version 0.9 Volume 1: Introduction to OCTAVE-S" pp 1

10. Alberts, Christopher, and Dorofee, Audrey, "OCTAVE[SM] Method Implementation Guide Version 2.0 Volume 9: Process 7 – Conduct Risk Analysis" pp. E7-14.

® - OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

SM – Operationally Critical Threat, Asset, and Vulnerability Evaluation and Software Engineering Institute are service marks of Carnegie Mellon University.