Global Information Assurance Certification Paper

Aligning an information risk management approach to BS 7799-3:2005

G7799 Gold Certification

Author: Ken Biery Jr., kenbiery@earthlink.net

Adviser: Lori Homsher

Accepted: October 20th, 2006

© SANS Institute 2006, Author retains full rights.

Table of Contents

© SANS Institute 2006, Author retains full rights.

Abstract

This paper discusses the need and importance of information risk management in terms of business and organizational priorities. In the most basic sense, risk management is understanding and protecting those assets identified as most important to the business. Based on this, the reduction and ongoing management of identified risk can be addressed by business priority.

There are a variety of information security risk management approaches. This paper presents a risk management method that is aligned with *BS 7799-3:2005, Part 3: Guidelines for information security risk management*[1]. This approach helps provide guidance for companies seeking to meet the numerous requirements of ISO 27001 that are related to risk treatment and management activities.

[1] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management*. London, U.K.: Author

Part 1 - Business Risk Management – Overview

Security professionals are frequently challenged to demonstrate how their security programs provide tangible benefits to business operations. The main issue is providing a framework of understanding so everyone in the organization can identify how critical business operations are being protected. To be effective, this approach should have alignment among security and business goals. It enables a common understanding of how security adds value to business operations.

Business management has the tendency to regard security as a necessary expense. While security organizations may not like that they are considered a *necessary expense*, this typically leads to limited funding and/or expense reduction efforts. Security management often compounds the problem by using security *geek-speak* in their discussions with management. This may result in limited security understanding at the business management level. It is important for the security team to help management understand how security adds value to, or protects, business operations. Without a better way of presenting the value that security provides, security organizations will continue to be marginalized.

On the other side, management has only a limited amount of time to focus on security issues. Also, management may not have taken the opportunity to communicate what the business' most critical operations are to the security team. This is the information the security team needs to better prioritize and focus their efforts.

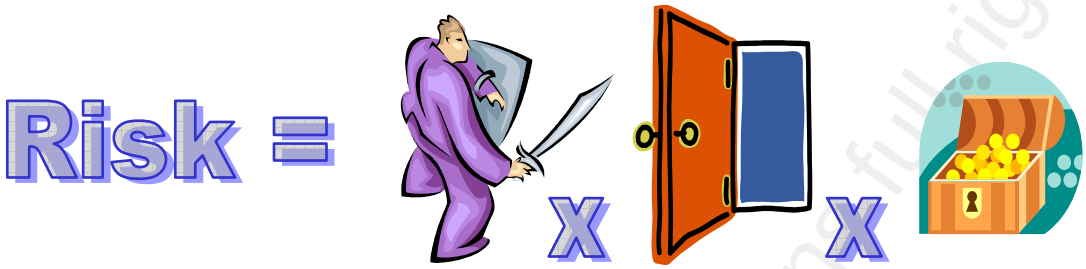
Without this guidance, the security effort may not focus on the most important resources. Ideally, an organization needs to develop a business-centric, or critical operations, approach to security risk measurement and mitigation.

1.1 - Defining Risk Management

Business risk management (BRM) is designed to address the issue of how business and security management can have a detailed understanding of the value security provides to the business operations. BRM is the process of aligning critical business function protection with security effort prioritization. The focus should be on protecting the most valuable business resources rather than just looking at security risk has high, medium, or low vulnerabilities. This is the difference of looking at vulnerabilities versus risk.

Before moving forward in the discussion of business risk management, it is important to distinguish between vulnerabilities, threats, and risk. The typical definition of risk (R) is that it is a composite of a threat (T) exploiting a vulnerability (V) to cause a negative impact on an asset (A). Therefore, threats, vulnerabilities and assets are elements of risk. Using this formula of R=TxVxA, if one of the elements is missing, then risk is probably not present. In reality, most risk can never be fully mitigated, but is usually reduced to an acceptable level.

Figure 1 – Typical Risk Formula



1.1.1 - Threats

Threats are usually identified as two types, human and natural. A human threat is someone taking some sort of action. The action is defined as intentional (like writing a virus) or accidental (mistakenly deleting a data backup). A natural threat is something like floods, tornados, or earthquakes, which are beyond the scope of this discussion. Human threats typically have wide-range of skills from minimal to highly proficient. In the information security realm, a *script-kiddie* is an attacker that only has minimal skills to use hacking programs written by others. At the other end of the spectrum is the super, or uber, hacker who writes various programs that script kiddies can use in most automated attacks. For most organizations, threats cannot be mitigated since attackers are always trying to exploit vulnerabilities regardless of what the organization has done to protect itself. However, the successes of attacks are usually determined by the vulnerabilities the attacker can exploit.

1.1.2 - Vulnerabilities

Vulnerabilities must be present in order for a threat to be successful. Additionally, the vulnerability must affect an asset. So if there is no vulnerability for a threat to exploit and there is no damage to an asset, then there is minimal risk. For example, suppose there is an attacker trying to gain access to 5,000 customer credit cards. The attacker is taking advantage of a vulnerability in a web application to access this information. If the attack is successful, it costs the company responsible for protecting the information over $500,000 in direct costs associated to the charges to put a credit watch on each of the 5,000 customer accounts that were exposed. There would also be some indirect costs of losing customer's confidence. However, if the company was more proactive and the web application was patched, then the threat could not have successfully attacked the site.

1.1.3 - Assets

The final element of the risk formula is an asset. An asset is any item, process, or resource that is valued by the organization. It is critical to identify an asset's value and which part of the organization owns it. If an asset has a very low value, then it is does not make sense to spend a lot of money to protect it. If a company does not have this type of measurement system, it may have a difficult time making this kind of decision. It is also important to remember that an asset's value can be much different than its cost.

Assets generally have two types of value. The first is a monetary value that represents the purchase price or net present value, if applicable. The second type is more value add or intangible, but arguably more important. This type is the value it provides to business operations. For example, an e-commerce application and server may only have hardware and software cost of $50,000, but it is responsible for millions in revenue every month.

An important intangible asset for a business is its reputation and the trust consumers place in it. Although a hacking incident itself may not create any direct losses, the business customers may start to leave in droves due to lack of confidence in the company, especially if there are strong competitors. Losing customers definitely qualifies as a direct loss from decreased revenue. For publicly traded companies, this usually brings swift punishment from Wall Street in the form of falling stock prices.

While this discussion is not going to focus on intangible asset values, it is important to understand how they can be determined. In a publicly traded company, intangible assets represent the difference between the tangible assets as recorded in the financials and the company's market capitalization value. For example, a company with a $5 billion market capitalization may have $1 billion in tangible assets and $4 billion in intangible assets. Therefore, 80% of the company's value ($4 billion) is made up of intangible assets. Intangibles assets are usually comprised of intellectual property, knowledge management, brand reputation, corporate culture, customer loyalty, and innovation to name the most commonly cited ones.

A number of the key intangible assets are information based and require significant protection. This is why having an information security program that embraces BRM is crucial. A security team that understands the basics of intangible assets and can articulate how their efforts protect them enables a further quantification of their value to the organization.

Part 2 - Risk Management Lifecycle

BRM needs to be structured to be effective. It follows an ongoing process of assessing risks, addressing risks, monitoring risks, and enhancement. This is known as the risk management lifecycle[2].

Due to the dynamic nature of business and changing security exposures, risk management should be structured to stay current with both of these elements. It should be aligned with, and driven by, business priorities. Therefore, a consistent and repeatable process for risk management is required. The risk management lifecycle should include the following elements:

- **Risk management scope** – It is important to recognize that risk management should not be limited to just IT. Information systems are dependant on the physical locations they are placed in, and the people that use and manage them. To be representative of the environment, it needs to be inclusive of people, processes, and technologies.

In recognition of this, the ISO 17799/27001 standards include requirements for operational, physical and business continuance areas as well. A complete overview of all of the required areas is contained in BS ISO/IEC 270001:2005[3]. Additional guidance for these requirements is contained in BS ISO/IEC 17799:2005. This comprehensive approach is necessary to satisfy the requirements of the Information Security Management System (ISMS).

[2] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* 4.2 - Risk approach/philosophy (pg.8). London, U.K.: Author

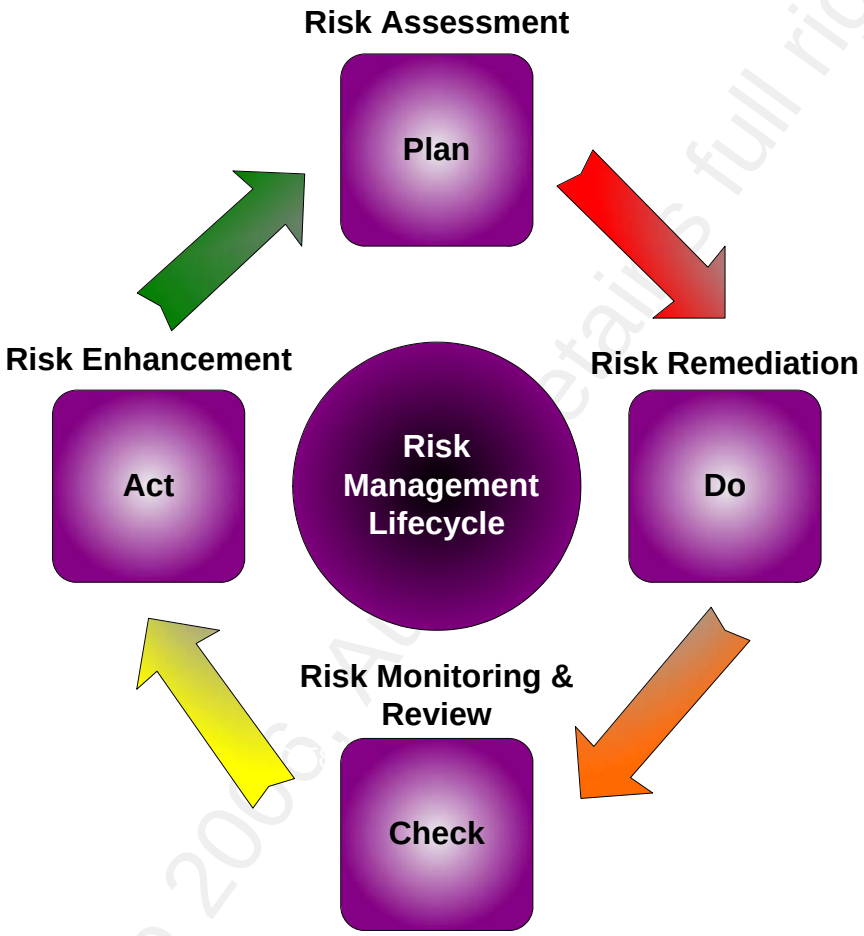
[3] British Standards Institute. (2005). *BS ISO/IEC 17799:2005, Code of practice for information security management.* London, U.K.: Author

- **Risk acceptance criteria** – An organization should define the circumstances in which it accepts risk. For example, if executive management has a high priority business initiative, the company may consider the associated risk as acceptable. However, this type of situation also requires looking at the level of risk as well as its potential consequences.

- **Risk acceptance levels** – The level of risk that is acceptable should also be defined. An organization can decide that it accepts all low level risks and some medium risks. However, all high risks and certain medium risks must be addressed by a risk treatment plan to lower their levels to the acceptable level. Additionally, the aggregate total of lower level risks can become significant and exceed acceptable levels.

- **Risk assessment and analysis** – This is the process of identifying vulnerabilities, their potential impact on assets, and the probability of exploitation by a threat. Risk has to be identified before it can be managed. The assessment should provide the information needed to do the risk analysis. The analysis should measure the risk against a predefined scale. Based on the analysis, a risk treatment plan can be developed.

Figure 2 – Risk Management Lifecycle



2.1 - Risk Assessment

There are a number of elements required to help understand a business' risk profile and management processes. These elements need to be identified in order to establish and maintain a risk management lifecycle. The following comprise the required activities to start the risk assessment process.

- Resources and assets are identified.

- Resources and assets are ranked by the importance of their business value. This importance should also take into consideration the business dependence and legal issues.

- Vulnerabilities and the threats that can significantly impact the resources and assets are identified.

- There is and an analysis of the probability and severity of threats exploiting vulnerabilities that can impact resources and assets. This should take into consideration any existing risk mitigating controls.

- There is a summarization of risk analysis using a risk measurement.

2.2 - Risk Remediation

This phase is where risks are addressed and is also called risk treatment. When addressing risks, a business can use preventative and detective controls along with risk transference, or acceptance. These constitute what actions a business is going to use (implement) to limit and manage its risks. These activities should consider:

- The business importance of resources and assets.

- The risk reduction benefit of various controls and strategies.

- The direct and indirect costs associated with each risk treatment.

2.3 - Risk Monitoring and Review

The primary aspect of this phase is monitoring and measuring risk controls for effectiveness. Security audits, vulnerability scans, security alerts, and security incident reviews usually provide validation of the effectiveness of security controls. Part of the monitoring should also be capable of identifying changes in the business environment. These changes can introduce new risks or reduce control effectiveness. Some of the aspects that should be monitored are:

- The results and trending of security audits and vulnerability scans.

- Security alerts from various network and system devices. This included routers, switches, firewalls, IDS/IPS, and malware detection systems (anti-virus, anti-spyware, spam).

- Security incidents to determine what happened, who did it, and how much damage occurred.

2.4 - Risk Management Enhancement

This phase of the risk management lifecycle is designed to determine if the risk management strategy is achieving its intended goals. It also serves as the feedback process for the risk management lifecycle. This is where changes are recommended based on all of the information and analysis. At this point, the following should be considered.

- The amount of variance from the targeted risk reduction goals versus the actual results.

- The amount of change to the environment and its impact on risk measurements.

- The amount of cost associated with addressing the risk in the organization.

- The identification of new processes and technology that can enhance risk management efforts.

Part 3 - Asset Identification and Business Criticality

3.1 - Asset Identification

Asset identification[4] is one of the first steps in establishing a risk management program. There are three pieces of information that are needed, at a minimum, for each asset. The asset should be inventoried; its owner identified, and its value to the organization determined.

Another characteristic to consider when evaluating an asset is any associated business and legal requirements. For example, if the company processes credit card transactions, there may be fines, lawsuits, and lost business if customer information is compromised. Visa (USA) fines can be as high as $500,000 per incident as described on Visa's website[5]. There may be additional legal problems if the business does not properly notify customers that their information has been exposed. According to the 2006 InformationWeek Global Security Survey[6], there are at least 33 states with laws requiring data compromise disclosure laws.

[4] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* 5.2 – Asset identification (pg. 10) and 5.3- Identification of legal and business requirements (pp. 10-11). London, U.K.: Author

[5] Visa USA. (2006, September). Cardholder Information Security Program. *Loss or theft of account information*. Retrieved on October 20, 2006 from http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

6 Greenenmeier, Larry, (2006, July 10) InformationWeek Global Security Survey 2006. *InformationWeek*. Retrieved October 20, 2006 from http://www.informationweek.com/news/showArticle.jhtml?articleID=190301155

There may also be specific business requirements beyond regulatory and legal requirements. Referencing the customer information mentioned above, an e-commerce site may also have availability requirements specifying access to customer information or a connection to the credit card processing networks. If these are not available or information is corrupted, the business can start sustaining losses because the e-commerce environment and assets cannot function properly.

3.2 - Business Criticality and Asset Valuations

Management teams know what is important to them in achieving their goals. They understand which critical functions and assets are required to support their efforts. However, they normally do not know the vulnerabilities for those assets.

The security team knows about the vulnerabilities on assets, but does not always know their value to the business. This creates a void where business people do not completely understand the actual risk in their operations. Conversely, the security team does not have clear guidance on what is most important to protect based on business value. This is why business risk management has emerged to fill this need to provide a better business-centric approach to managing security risk.

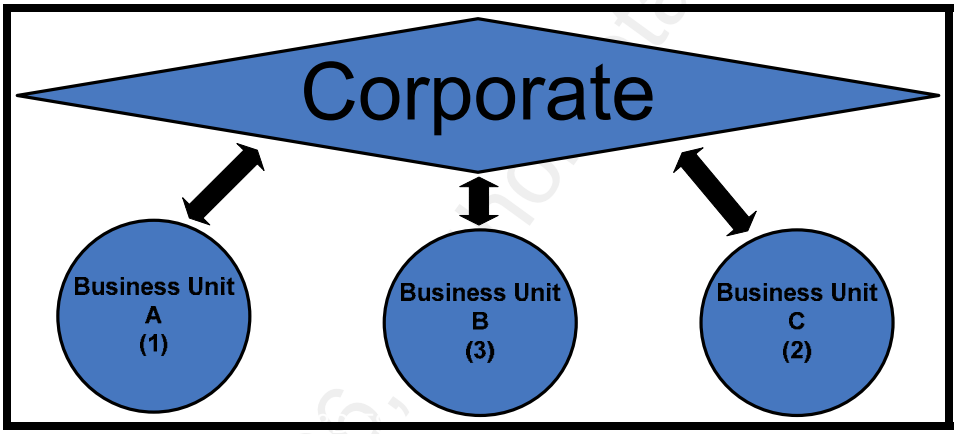
One way of determining an asset's valuation[7] is to identify the critical business functions it supports. This requires the creation of a multi-tiered business risk structure. It is designed to reflect the business' priorities by assigning an importance rating to business areas, functions, and assets.

[7] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* 5.4 – Asset valuation (pp. 11-12). London, U.K.

3.2.1 – Top Layer of the Business Risk Structure

The first step is breaking out the organizational structure into business units or departments. Obviously, these should follow the existing structure. Each of the business units should be rated by their importance or value to the business.

Figure 3 – Top Layer of Business Risk Structure



In Figure 3, Business Unit A is given a number one rating since it is the most important. The importance usually equates to revenue, but in an organization, the value could be determined by the critical functions being performed or other legal and business requirements. There can be as many units or departments that exist, but it is best to stay at a higher level to keep the structure more manageable. An example of some business units are sales, services, and administration.

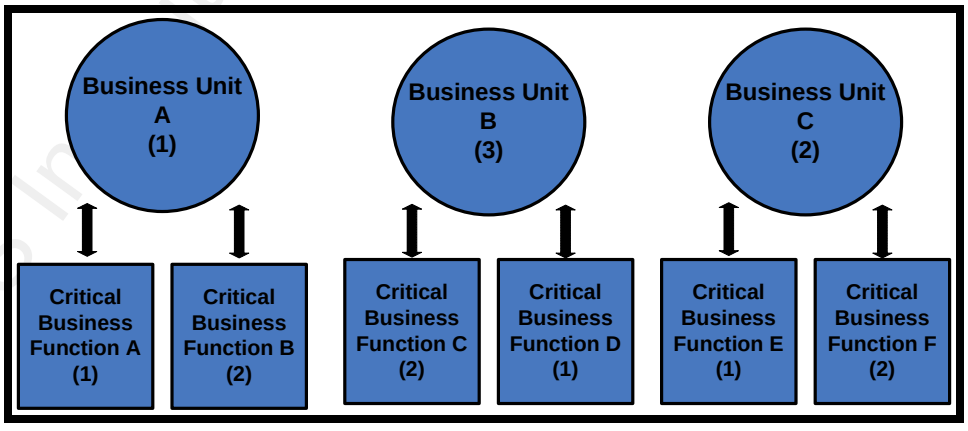
The rating is done by the senior management team based on their understanding of the business. This is the foundation of establishing the risk management structure. The relative importance value of each business unit or department flows down into critical functions and assets.

3.2.2 – Critical Function Layer

The next level is identifying the critical business functions. The focus for each of the business units, or departments, is defining what tasks are important to the unit achieving its goals. Customer service is normally a critical function of the sales business unit.

Once again, the emphasis is on identifying the major functions that provide value to the business. Depending on the organizational structure, there can be an additional sub-layer of critical business functions. This two-level structure within the Critical Function Layer provides the ability to better show the details of complex operations. Additionally, critical business functions within a business unit are also numerically rated against each other. This is helps with prioritization when determining risk remediation efforts later on.

Figure 4 – Critical Function Layer of Business Risk Structure



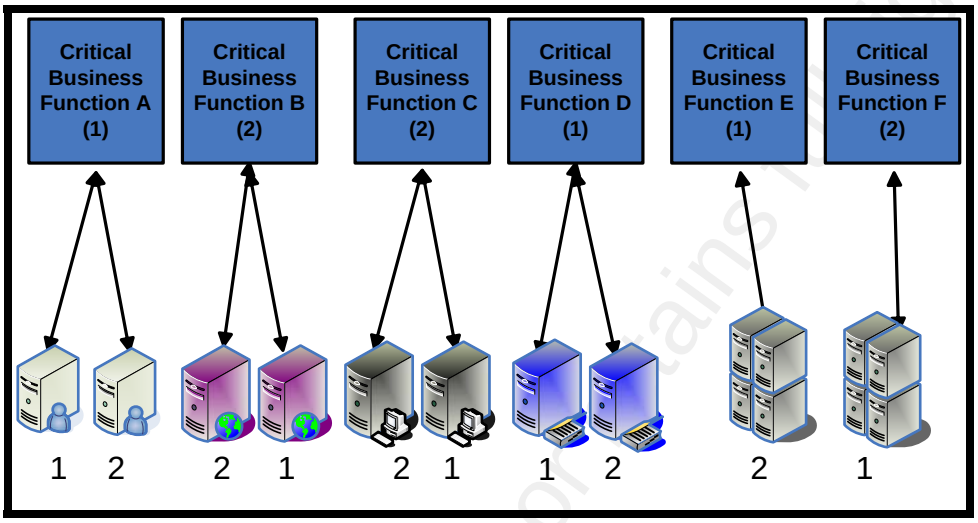
After the critical functions have been identified, the basic structure of the organization has been mapped. It is important to recognize that the structure is focused only on operational elements, not technologies, applications, or data. This progressive drill-down structure looks similar to a Business Impact Analysis (BIA) that is performed when doing business continuity planning (BCP).

In most situations, a BIA may be a good place to start. Conversely, this business risk management structure could also be used as an introductory part of a BIA as well. To clarify, a BIA is normally a more detailed analysis than the BRM. BRM is designed to provide a management-level view of risk and where it resides in the organization.

3.2.3 - Bridging the Gap to Assets

Up to this point, BRM has been focused on business and organizational operations. The next area that needs to be defined is what assets support the critical functions. Assets can be identified as applications, systems, facilities, inventory, processes, etc. Assets are the elements that permit critical functions to happen. This type of structure allows for flexibility in the definition of assets. For example, a business is using software for its accounting functions. This software resides on a number of servers that are connected to a SQL database. Both the accounting application and database software, along with the hardware it resides on, are considered assets that support the critical function of accounting.

Figure 5 – Aligning Assets to the Critical Function Layer



Assets, like business units and critical functions, are numerically rated as well. Because assets are associated with the critical business functions they support, they are rated against each other from the most important to the least important in their group.

3.3 - Vulnerability and Threat Assessment

Part 1 has already provided an overview of vulnerabilities and threats. The important thing to remember is that both of these elements must be present to impact an asset. If there is no vulnerability for a threat to exploit, there is no impact to an asset, and therefore, no risk.

Generally, it is easier to control risk through vulnerability mitigation than it is to try to stop threats. While it is possible to have a vulnerability that almost no threat could exploit, it seems unlikely. For most organizations, it is difficult to mitigate threats since these are primarily people-based.

External hackers and a certain number of internal employees/contractors are going to try to exploit vulnerabilities no matter what. This makes threats a constant. Threats should be used to determine the likelihood of vulnerability being exploited and the kind of impact that the asset would experience.

However, vulnerabilities are the element of this risk equation that usually can be controlled by a business. If there are very few vulnerabilities, there is not much a threat can exploit that would impact an asset.

3.3.1 - Identification

There are three elements to consider as part of the vulnerability and threat identification[8] process. The first two are simply the vulnerabilities and threats. The third area is any controls that are in-place. The controls should be inventoried and analyzed for their ability to mitigate vulnerabilities or to detect threats.

There are several methods to identify vulnerabilities in an environment. The most frequently used methods are vulnerability scanners, configuration analyzers, and security audits/surveys. Most automated tools can cover the technology side of the assessment. However, audits are needed for the people and process side. Audits normally consist of interviews and direct observation, especially for areas like physical security.

[8] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* 5.5 – Identification and assessment of threats and vulnerabilities (pp. 12-13). London, U.K.

Threats are classified by a variety of methods. From the four categories listed, one characteristic should be picked from each. While there are many more than are listed, these high-level categories capture most.

- Skilled or unskilled attacker
- External or internal source
- Intentional or unintentional effort
- Structured or unstructured approach

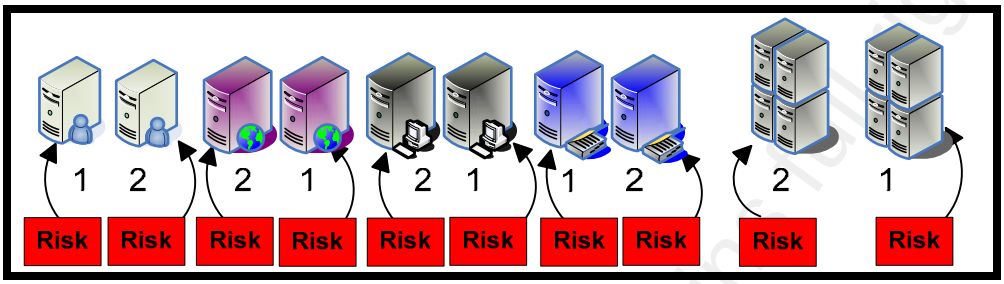
Even with these basic classifications, there are numerous combinations. It is probably easier to think of threats in terms of external hackers with malicious intent or internal users accidentally causing damage. There is reference to vulnerabilities and threats in BS 7799-3:2006, Part 3: Annex C[9]. Additionally, the National Institute of Standards and Technology's (NIST) Computer Security Research Center (CSRC)[10] and the SANS (SysAdmin, Audit, Network, Security) Institute[11] are good places to look for more detailed information on threats.

3.3.2 - Assessment

At this point, the three components of risk have been identified. The likelihood of occurrence and the degree of impact can now be determined. This also enables the calculation and evaluation of risk.

[9] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* Annex C – Examples of assets, threats, vulnerabilities and risk assessment methods (pp. 33-46). London, U.K.: Author
[10] (NIST) Computer Security Research Center (CSRC). http://csrc.nist.gov/
[11] SANS (SysAdmin, Audit, Network, Security) Institute. http://www.sans.org

Figure 6 – Asset Vulnerabilities



In the BRM structure, assets are the *containers* of risk. The risk represented in Figure 6 is the composite of vulnerabilities that a threat can exploit to cause a negative impact to an asset. If an unskilled, external attacker can exploit a serious vulnerability on an e-commerce web server that is the primary source of the businesses revenue, the risk is rated high.

3.3.3 – Risk Scoring

There are many methods for scoring risk. The main consideration is using a method that is accepted by the organization. This means that when a risk is rated high or has certain score, the organization has accepted it as a valid measurement.

There are usually numeric scores behind the ratings of high, medium, and low. One of the most straightforward approaches is assigning a one to five scale for each of the three elements of risk. Five represents the high end of the scale and one is the low end. Figure 7 provides an overview of how this functions.

Figure 7 – Risk Scoring Table

ASSET NAME:		E-COMMERCE SERVER			
#	**Vulnerability Description**	**Vulnerability Rating**	**Threat Rating**	**Asset Impact**	**Total Risk Score**
1	O/S default guest login enabled	4	4	3	48
2	Cross-site scripting weakness	5	4	3	60
3	Open SSH vulnerability	3	4	3	36
4	Weak administrator passwords	5	4	5	100
Grand Total Risk Score					**244**

Using this approach, the greater the number of vulnerabilities and the higher their severity, the more risk there is for the asset. However, the scores still should be analyzed since a large number of low vulnerabilities could out score a few high or medium vulnerabilities. The organization may want to consider their risk acceptance or tolerance levels, which are mentioned in Part 2. Using this, the organization still focuses on the assets high and medium vulnerabilities even though they have a lower total score.

Each asset's risk score[12] can be compared to those in its business grouping. Remember, BRM rates an asset's importance to business function it supports. The importance rating is also used as a way to calculate the overall risk score for an asset. This is done by using the asset importance rating as a multiplier. Figure 8 provides an example how this multiplier affects an asset's score if the original numbers are all the same.

Figure 8 – Revised Risk Scores

ASSET IMPORTANCE RATING	ASSET NAME	ASSET SCORE	MULTIPLIER	REVISED RISK SCORE
1	E-commerce Server	244	1	244
2	E-commerce DB	244	0.8	195
3	Website	244	0.6	146

The multiplier can be any number as long as it represents the asset's importance rating. To better show the impact of importance, there is enough difference at each multiplier level so it provides a noticeable separation in the revised risk score. These scores have two primary purposes. The first is to be used as a comparison among other assets and an overall risk level. The second purpose is to use it as a baseline to track how it goes up or down over time as part of the risk monitoring phase.

[12] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* Section 5.7 – Risk calculation and evaluation (pp. 14-15). London, U.K.: Author

The same way that the multiplier is used at the asset level in Figure 8 can be applied all the way up the BRM structure. Once again, the business importance rating determines the relative value of multiplier. This shows the risk levels at the upper layers.

Part 4 – Risk Remediation

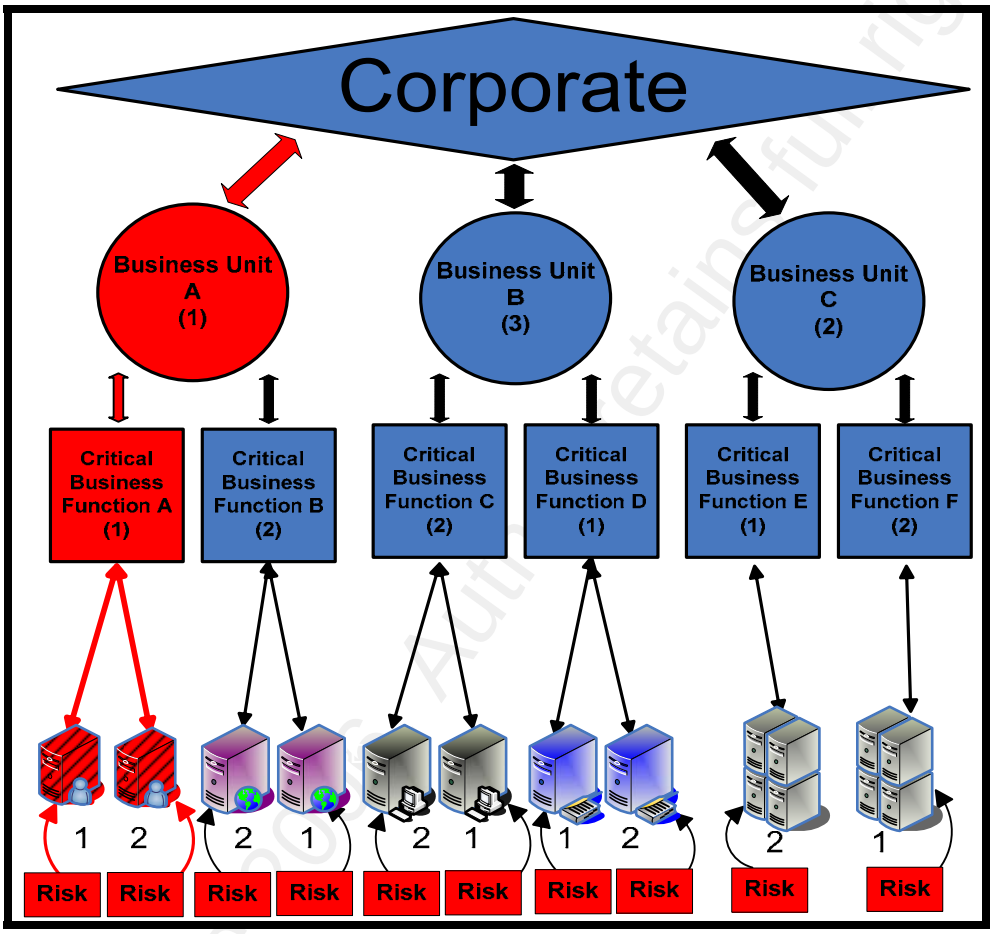
4.1 - Prioritization

With BRM, an organization could see where risk originates and how it potentially impacts business operations. This roll-up and drill-down nature of this approach is useful for different levels of management throughout the organization. For example, business owners may want to see what level of risk their critical functions are at in order to be able to set a prioritization[13] schedule for fixing vulnerabilities. Then, the IT manager further identifies where the risk specifically resides so system administrators apply patches or change configuration settings on individual devices to reduce vulnerabilities.

The ability to determine how identified risk impacts business operations is demonstrated in Figure 9. For example, Business Unit A is sales and Critical Business Function A is e-commerce transactions. The two systems associated with this business function have vulnerabilities that allow the systems to be brought down and have their customer sensitive information compromised. This type of exposure potentially impacts some of the company's most valuable assets. In Appendix B, the Risk Level by Lines of Business Comparison and Risk Level by Asset reports provide this kind of information.

[13] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* Sections 6.1 – 6.7 Risk treatment and management decision-making (pp. 16-19). London, U.K.: Author

Figure 9 – Risk Exposure and Business Impact



The BRM structure clearly shows this and helps both management and the security teams align and prioritize their efforts accordingly. Both teams should consider the following.

- The severity of the risk's potential impact to the business.
- The frequency of impacts, which is difficult to determine due to lack of historical statistics.
- The decision of whether to mitigate, transfer, avoid, or accept the risk.

- The potential cost of the chosen risk strategy. See Appendix A - Losses, Costs, and Return-on-Investment Metrics.

- The level of remaining risk after remediation efforts have been applied. This is frequently referred to as residual risk. The level of residual risk is reflective of the risk acceptance criteria and levels the organization has set. However, reducing risk to an acceptable level may simply not be possible due to costs or other circumstances. Senior management should accept the formally documented residual risk.

4.2 - Cost Justification

BRM creates the business-centric view of risk and what is important to protect. However, risk management is also about making smart choices based on potential risk mitigation costs versus potential losses (risk exposure). Put another way, why would a business spend $1 million on mitigation for a $100,000 exposure?

Unfortunately, most information security crime and loss metrics are not as established as traditional robbery and theft statistics. The Annual FBI/CSI Computer Crime and Security Survey[14] has been one measurement involving losses in the information security realm, but some individuals state that its loss figures are too understated, while some say they are overstated. Rather than debate the validity of these measures, it is useful to look at the metrics most organizations can quantify.

[14] Computer Security Institute. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Author

Three of the common measurements of potential losses are employee productivity impacts, revenue losses, and direct cost loss events. Virus and worm incidents are frequently cited when discussing impact on productivity[15]. For example, a virus hits 10,000 employees in a 40,000 person organization. Each infected system costs each impacted employee one hour of productivity. If each employee has a fully-burdened hourly wage of $30, then this is a $300,000 impact. Now that a potential loss figure has been established, it is easier to make a remediation decision.

Revenue losses should also be determined in a similar manner. If a business has e-commerce website that is producing $1 million of revenue each day, then a denial-of-service attack that lasts half a day creates a $500,000 loss. It is debatable whether this type of attack would merely force customers to delay their purchases or if they would simply go to another competitor. However, any perception of being the victim of a hacking attack, even if customer sensitive information is not stolen, usually scares some good customers away[16].

While productivity and revenues losses could be considered direct, organizations should also consider the number of additional labor hours required responding and recovering from an incident. Another direct cost could be additional hardware and software that is implemented as follow-on to an incident.

[15] Computer Security Institute. (2006). *2006 CSI/FBI Computer Crime and Security Survey (pp. 2 and 15)*. San Francisco, CA: Author

[16] Pappalardo, Denise & Messmer, Ellen. (2005, May 16). Extortion via DDOS on the rise. *Network World*. Retrieved October 20, 2006 from http://www.networkworld.com/news/2005/051605-ddos-extortion.html

For example, the security team makes the case for a new intrusion protection system (IPS) after experiencing several buffer overflow attacks. Most enterprise class IPSes are going to be anywhere from $50,000 to $150,000 per gateway. Once again, this is the cost of mitigation that has to be measured against.

4.3 – Risk Remediation Plan

The next step is the development of a risk remediation (treatment) plan[17]. It is the formal documentation of which risk reduction measures are going to be implemented. This plan should be driven by the business priorities and the assets importance to support them. In general, the most serious risks should be addressed first. However, some more moderate risk may be quickly remediated with minimal resources. The following are some factors that must considered as part of the risk remediation plan.

- Prioritized list of risks
- Ongoing meetings with affected stakeholders, including feedback to identify organizational issues and dependencies
- Estimated costs and resources for the risks
- Time period required to complete risk remediation tasks
- Expected residual risk and validation criteria
- Executive approval

[17] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* Section 6.8 – Risk treatment plan (pg. 20). London, U.K.: Author

Part 5 – Risk Monitoring and Review

Risk monitoring represents a set of ongoing activities to verify that controls are remaining effective. The changes in the organization and its environment requires that security is consistently reevaluated. New vulnerabilities, new business initiatives, and organizational restructuring are the most frequent sources of change that affect security risk.

Risk monitoring and review is about having a structured approach to identifying data that shows how the levels of risk are changing. Depending on the environment, there can be hundreds or thousands of data sources. Clearly, this requires a significant amount of effort to identify, monitor, and analyze. Rather than to try to address this level of complexity, this paper provides an overview of some major components.

5.1 - Monitoring

Technology plays a significant role in monitoring. For example, system scanning should take place on a regular basis to determine if compliance standards are met. Integrity monitors provide alerts when there are unauthorized changes to system parameters. Log files also provide a source of monitoring for security events.

Security metrics are a way to monitor security risk, or at least some of its critical components. No one metric, or set of metrics, satisfies all environments. However, they could be strategically used to show both risk levels and security systems performance. While complex algorithms and formulas could be used, it is preferable to have each metric use easily identified data.

A metrics program tells a story on how the security program is performing and providing value to business operations. It is a good idea to have different types of reports for different audiences. Executives want to see more of a dashboard that identifies which business units have the most risk and how much risk has been reduced along with the associated costs. This level of reporting contains graphs and charts with summary tables.

The next series of reports are for security management to provide more detailed information that is a drill-down from the executive level. This report shows risk in the aforementioned business unit broken-out by critical business functions such as those used in the BRM approach. The final level of reporting is more detailed to show the risk levels of application and systems that support the identified critical business functions. This reporting structure provides the appropriate level detail for the defined groups and it also follows a drill-down and roll-up approach. Appendix B has samples of various executive, managerial, and technical reports.

The security metrics invariably indicate that actions must be taken to address identified risks. When the comparisons are done against the baselines, benchmarks, and goals, vulnerabilities and non-compliant issues must be mitigated. The action items and plans determine what is done to fix the identified issues and the applied countermeasures. These activities are also crucial to the metrics that measure the security program effectiveness. Successful remediation efforts are tracked by the level of effort in terms of time and cost. This is all part of the information security management lifecycle.

5.1.1 – Raw Risk and Residual Risk

Residual risk is the measurement of the actual or net risk score when risk mitigation measures have been applied to the raw risk score. It is important to remember that most risk is never fully mitigated. Risk countermeasures must be carefully measured to prevent their mitigation rating from being overstated. The difference between the raw risk and residual risk numbers shows the effectiveness of the applied countermeasures. The following tables show how a basic residual risk determination is made.

Table 1 – Residual Risk Measurements (example)

Risk	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
Raw Risk	70%	72%	75%	75%
Countermeasures	-20%	-32%	-40%	-45%
Residual Risk	50%	40%	35%	30%

Table 2 – Residual Risk Measurements, with Costs (example)

Risk	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
Raw Risk	70%	72%	75%	75%
Countermeasures	-20%	-32%	-40%	-45%
Residual Risk	50%	40%	35%	30%
Remediation Cost	$1M	$1.6M	$2M	$2.5M

These two examples demonstrate some basic high-level measurements. Table 1 shows residual risk being tracked by quarter. The percentage of residual risk has progressively declined which generally indicates the effectiveness of the risk mitigation efforts. Table 2 is essentially the same, but the cost of risk reduction has also been captured. This is adding a ROI component to the residual risk figures. In this example, it appears that risk was reduced by 10% for every $500,000 spent. However, at a certain point, the cost of achieving further risk reduction rises considerably. The value this type of measurement provides is a direct correlation of the money spent on risk reduction to the actual results.

5.1.2 - Types of Metrics

Raw risk and residual risk numbers represent a combination of data from different sources. These fall into two major categories. The first is technology sources such as:

- Firewalls (network and host)
- IDS/IPS
- Router/switch/server event logs
- Anti-malware systems (anti-virus, anti-spyware)
- Content monitoring systems
- Vulnerability scanning
- Physical security intrusion detection systems
- Facility telecommunications and power systems alerts

The second area is more focused around people and processes. These metrics are typically gathered from interviews and direct observation. The activities used to gather these metrics come from:

- Policy compliance audits
- Security configuration audits
- Regulatory and standards compliance audits
- Security incidents and investigations

Risk monitoring[18] and its associated security metrics provide a way to measure risk management's performance. It also helps management review the risk management program. The metrics provide measurements and indicators about the risk management effort. For example in ISO 27001, the selected metrics should report on any significant changes to the ISMS.

These numbers make it easier for decisions to be made on funding risk mitigation efforts. If an executive understands there is a high-level of risk in the company's most significant revenue producing business unit, security metrics provide the quantification to validate this. Examples of this kind of information are in Appendix B's Risk Level by Lines of Business Comparison and the Risk Level by Asset reports.

[18] British Standards Institute. (2006). *BS 7799-3:2006, Part 3: Guideline for information security risk management,* Sections 7.1 – 7.3, Ongoing risk management activities (pp. 21-22). London, U.K.: Author

5.2 - Review

The review process is related to monitoring, but it focuses more on re-assessing risks. This is particularly important when changes occur to the organization's environment. The more frequently these occur, the easier it is to detect changes and make adjustments to keep risk at acceptable levels. However, this frequency is dependant on the level of effort required to do risk reviews.

Risk assessments and security audits are the most common activities associated with the review process. For example, if an organization had the ISO 27001 certification, the associated controls would need to be audited by an external auditor. These reviews cover the same areas as the original ones providing a comparative analysis. This shows how the overall and specific risk areas have changed. The changes are attributed to a number of scenarios such as the following:

- The risk increases or decreases due to the number of vulnerabilities being identified.
- There are more or less assets at the time of review.
- The organization has become higher profile target due to publicity.
- Risk mitigation strategies were/were not fully implemented or did/did not appropriately address the root cause of the risk.

It is important to remember to document corrective actions or the implementation of risk mitigation measures that have taken place since the last reviews. In Appendix B, there is a sample report called Asset Corrective Action Tracking Report that helps document remediation efforts. These should be catalogued and tracked to determine if they have been effective in reducing or eliminating risk exposure. The risk mitigation actions should identify the problems being addressed. For example, anti-virus software is risk mitigation for malware.

The review process is easier if the security controls are formally documented. The inventory of controls includes the owner responsible for maintaining each control and the groups affected by it. This list is updated when any significant changes take place and someone is assigned to maintain it. For those organizations with ISO 27001 certifications, the documented control list is necessary to support the ISMS.

5.3 - Reporting

There should be reporting and communications throughout the BRM approach. The reporting structure is designed to distribute to, and gather information from, the appropriate management and other key stakeholders in the organization. This also includes the defined intervals for the information. The output of the risk monitoring and reviews are essential to providing the status of risk management effort. Based on this information, critical decisions and responses are made. To support decision making, Appendix B has samples of various executive, managerial, and technical reports.

Part 6 – Risk Management Enhancement

The enhancement phase is the final one before starting the risk management lifecycle over again. This is when changes are made to the strategies based on how well the risk management targets were met. Some of these are small corrections or large scale overhauls due to significant environmental changes.

These enhancements are based on feedback and observations from each of the previous phases. The first full pass through the risk management lifecycle usually has some significant changes. However, these become progressively less and less as subsequent cycles are completed.

The fact that there are changes to the lifecycle and it related components is part of a continuous improvement process. This is the “Act” part of the “Plan, Do, Check, Act” approach. The following are some key areas to consider when changes are required to the risk management lifecycle.

- The amount of impact of the risk to business operations, especially by business owners.
- An increase or decrease in the amount of risk due to business operations, changing technologies, business partnerships, outsourcing, etc.
- The difference in the targeted risk reduction versus the actual.

- An increase or decrease in the organization's risk tolerance.
- Any gaps that were unable to be adequately addressed.
- The consistency and reliability of security data and metrics.
- The steps that can be taken to automate controls and reporting.

Changes to the risk management approach should be done carefully. There must be documented justifications for enhancements. The main goal is to make corrective changes that increase the accuracy and efficiency of the risk management lifecycle.

Summary

The goal of BRM is providing a framework for a direct understanding between management and security operations on where risk is and how it can impact business operations. This creates an alignment of business goals and security program focus. BRM helps the organization determine its overall risk level. Business units, or departments, see what critical functions are at risk. This allows security managers to better prioritize their efforts to reduce risk for critical business functions.

BRM makes it is easier to produce meaningful metrics for risk management and provide some return-on-investment (ROI) measurements. Perhaps the most significant benefit is that business management has a much better understanding of the value that security provides to their operations without having to understand security *geek-speak*. This approach creates an alignment among security and business goals to help ensure the organization is properly managing risk by allocating the appropriate funding to achieve this.

The other benefit is that BRM and the risk management lifecycle can be used to support, and be aligned with, *BS 7799-3:2005, Part 3*. This also helps meet the requirements for ISO 27001 and its ISMS. However, the bottom line is that risk management lifecycle provides a consistent approach to identifying, measuring, mitigating, and monitoring risk. This enables organizations to better understand and control the impact that risk has on their operations.

Appendix A - Losses, Costs, and Return-on-Investment Metrics

The figures or metrics that management usually wants to see are those associated with losses, costs, and ROI. Since operations are focused on revenues and budgets, security should try to provide a set of metrics they can more easily understand. It helps the entire organization better understand the value security provides.

Losses are typically those events that affect revenue and productivity. If an e-commerce website goes down due to a DoS attack, then revenue is lost because people cannot reach the site and then buy from organization's competitors. In today's environment where there is not much brand loyalty, a site that is down can have some serious financial impact. Of those customers that still may be loyal, a down or hacked website erodes their confidence in protecting their accounts and/or transactions.

A recent Harris Interactive poll published by InformationWeek indicates that 40%[19] of consumers abandon their transactions entirely or go to a competitor if they have a problem completing their online transaction. Perhaps even more damaging is that 91% of online consumers, in the same poll, who experienced problems with their transactions are somewhat likely to question the company's ability to keep their private data secure if there were any problems completing an online transaction. While the issue that caused the transaction failure may not be security related, customers had an overwhelming perception that it was.

[19] Jones, K.C., (2006, September 25th) Study: Online Transaction Gaffes Push Users Into Rivals' Arms. *InformationWeek*. Retrieved October 20, 2006 from http://www.informationweek.com/story/showArticle.jhtml?articleID=193005349

Productivity Losses

Security incidents that impact revenue often impact employee productivity. When employees cannot work due to a security incident like a worm outbreak, the company is losing money because they are paying the wages on people that cannot be productive. There are several ways to look at productivity costs. The first formula is simply to take the number of affected employees and multiply this number by their average hourly wage and then by the number of hours they're impacted.

The other formula is revenue per employee per hour. This formula essentially takes the organization's total revenue for a year and divides it by the number of employees. To determine the hourly rate, this can be divided by the number of hours in a standard business year, which are 2,080. If the company generates $300,000 of revenue per employee per year, the hourly rate is about $144 per employee. When considering this kind of formula, the actual revenue losses will probably not be 100% of the potential/estimated loss. However, the more competitors a company has that can respond quickly if customer cannot buy from the company, the closer the actual and potential loss numbers are going to be to each other.

Table 3 – Incident Productivity Losses (example)

Type of Incident	No. of Affected Employees	Average Hourly Wage	Downtime (hours)	Total Loss of Productivity
Virus/Worm	5,000	$30	1	$150,000
Denial-of-Service	10,000	$30	4	$1,200,000
DNS Corruption	2,000	$30	2	$120,000

Table 4 – Incident Employee-based Revenue Losses (example)

Type of Incident	No. of Affected Employees	Hourly Revenue per Employee	Downtime (hours)	Total Loss of Revenue
Virus/Worm	1,000	$144	1	$144,000
Denial-of-Service	4,000	$144	4	$2,304,000
DNS Corruption	2,000	$144	2	$576,000

Revenue Impacting Losses

Revenue impacting losses are the ones that usually get the most attention from management. As mentioned previously, the amount of revenue lost depends on how long the customers cannot purchase from the company and how strong the competition. For example, if customers wanted to buy a ticket from one airline and their web site is down, they typically go to a competitor's site and make a purchase as long as the tickets are close to the same price. This situation usually applies to most transactions. The fact that more of companies' revenue is coming from the e-commerce environment also makes their electronic infrastructure even more critical. Once again, companies cannot depend on strong brand loyalty as much as they did in the past.

One of the easiest examples of a revenue loss calculation is to use a company's annual revenue divided by a standard business year of 2,080 hours. So if a company has $2.4 billion a year in revenue, their monthly revenue is $200 million and their hourly amount is about $116,000 per hour. The estimated losses do not include any of the response, recovery, and remediation costs, which can surpass the revenue losses.

Table 5 – Incident Revenue Losses (example)

Type of Incident	Revenue Per Hour	Downtime (hours)	Total Loss of Revenue
Virus/Worm	$116,000	2	$232,000
Denial-of-Service	$116,000	8	$928,000
DNS Corruption	$116,000	4	$464,000

The next area of potential revenue impact is the delay of new products and services hitting the market due to a security incident. If these new offerings have the potential of $1 million per day in additional revenue, it becomes a significant loss scenario rather quickly. These types of figures should be available from the product or service business plan's projected revenue.

One of the most significant, and yet difficult to calculate, is the theft of intellectual property. If a company's competitor launches a new product or service first due to previously stolen intellectual property, this could determine who leads a market and who is playing catch-up. It could also be devastating in terms of who was able to file for a patent first. Intellectual property theft is an area that is particularly difficult to stop.

Usually when intellectual property is stolen, it is not physically removed, but it is merely copied. These types of losses have a much longer timeframe of impact since the expected revenue normally extends over a number of years and is not limited to the duration of a single incident.

Another area to consider measuring is the value of companies' stock before and after they have announced a security incident. It may be difficult to ascertain since other factors can cause stocks to go up and down. Additionally, the duration of the effect a security incident may have on a stock may be minimal over time. However, it may be useful to show that even a small effect of a few percentage points on a company's stock value can add up to a significant monetary amount. If executive bonuses are tied to stock performance, it can definitely have an impact on management's thinking and actions.

Annual Loss Expectancy

Annual Loss Expectancy (ALE) is used to determine how much loss can be expected in a year. This is a basic formula that takes the monetary loss amount of an incident and multiples it by the frequency of its occurrences in a year. For example, the theft of intellectual property (IP) is estimated to create a $5 million loss. However, it is predicted to only happen once every five years. Therefore, the ALE for IP theft is $1 million ($5 million x .2 = $1 million ALE). This information could then be used in return-on-investment (ROI) calculations and analysis.

One of the primary problems with ALE in the information security world is that incidents are constantly evolving and changing. This means there is not much statistical information on the losses and their frequency of occurrence other than the Annual CSI/FBI Computer Crime and Security Survey[20] along with some other similar studies from Deloitte[21] and PWC[22]. By now, some of the cyber insurance carriers may have some actuarial tables on information security incidents that may be useful in ALE calculations.

Some companies have decided to forego the ALE calculations and simply use the previously mentioned productivity and revenue losses that are not specifically tied to a timeframe. However, the frequency of occurrence should be considered at some level in all scenarios. This is a factor that the security organization needs to decide as the security metrics program is being structured.

Costs

Costs come in many forms ranging from overtime wages and new security measures, to fines and service level agreement penalties. These are broadly categorized as direct and indirect costs. These are valuable metrics if they have been captured from previous incidents or are referenced from a reliable, external source.

[20] Computer Security Institute. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Author
[21] Deloitte Touche Tohmatsu. (2006). *2006 Global Security Survey*. New York City, NY: Author
[22] Holmes, Allan & PriceWaterhouseCoopers. (2006, September 15). The Global State of Information Security 2006. *CIO Magazine*. Retrieved October 20, 2006 from http://www.pwc.com/extweb/pwcpublications.nsf/docid/3929AC0E90BDB001852571ED0071630B

The first area is the additional wages, services, software, and equipment that had to be used in order to respond and recover from a security incident. Chances are that wages are a large cost along with hiring specialized consultants and buying additional security solutions. Not only do new security solutions have their initial costs, but there is ongoing maintenance as well.

The next area of direct costs is fines and penalties associated to the security incident. These costs could be governmental fines or monetary penalties for not maintaining a contractually specified service level. These must be considered when analyzing any potential or actual cost/loss scenarios. Sarbanes-Oxley is one of the new types of legislation that is making it more difficult for management to claim they did not know what was happening. Additionally, these are costs that do not include any lawsuits that are filed from shareholders and other affected parties.

There is also a real, but somewhat intangible cost of lost customer, partner, and employee confidence. These factors are somewhat akin to the “death by a thousand cuts” scenario. Sometimes customer and partner reactions are quick and significant in terms of revenue impact. However, customers and partners usually start looking for another company that provides the same products or services. Key employees now have to deal with a tarnished reputation and potentially slowing revenue that effects their compensation. While these types of costs may never be able to be fully measured, they should be acknowledged as part of security incidents’ impact.

Cost Savings

The majority of security metrics to this point have been associated with losses and costs. However, there are some metrics which are viewed in a more positive light. These have to do with cost savings and productivity enhancements.

One of more frequently cited areas for cost savings is password management and resets. This issue incurs two costs. The first cost is the Help Desk and the amount of time they spend resetting passwords. The other cost is the loss of productivity by the person waiting for the reset to occur. Some help desks spend as much as 20-25% of their time resetting end user passwords[23].

The next area of costs to examine is the amount of time end users spend logging into all of their different systems with separate user IDs and passwords. While individual users may only spend an extra few minutes per day, if that amount is multiplied by all of the users in the organization, the costs can start to add up quickly. There is also the cost of separately managing all of the users and their password changes. After determining these costs, there may be a very compelling cost saving potential for using a single sign-on solution.

[23] TechRepublic. (2005, October). *TechRepublic Real World Guide: Identity Management* (pg.6). Louisville, KY: Author

Another way to achieve some potential cost savings is through reduced insurance premiums. Cyber insurance is still a relatively new offering and a significant portion of the premiums can be determined by the organization's security posture. If the insurance premium can be lowered by a good security program, this should be considered a cost savings. While the insurance savings are direct savings, the reduction in liability and showing due diligence is valuable if there is ever litigation involving the organization's security.

The recovery of assets and income is also an area for security to provide value. This is especially true of companies that offer their intellectual property as software or specialized content like entertainment media. Music, movie, and software piracy has impacted the revenues of many of the media companies. In 2005, the United States lost $6.9 billion as a result of software piracy[24].

Even for service providers, the recovery of unauthorized services can be a valuable security metric. While this is not generating true revenue, these recovery efforts should be viewed as a type of revenue that, at the very least, should off-set the cost of the security effort.

[24] Business Software Alliance. (2006, August). *Software Piracy in the United States – Fact Sheet*.

Return-on-Investment

Return-on-investment (ROI) takes the component of cost security efforts and compares them to a benefit, potential monetary return, or loss avoidance. ROI is not about being overly precise, but more of a ballpark measurement. Yes, ROI calculations can be very complicated and detailed if all potential factors are considered. It is suggested that simpler is better to start with and more details can be added as the process matures.

For example, the password reset effort reduction identified in a previous section was 25% by a using single sign-on (SSO) solution. If the help desk costs are $1 million per year, then a potential of $250,000 of costs could be saved by using the SSO. If the SSO only costs $125,000 to implement, then it pays for itself within 6 months. After that, its annual costs are $83,000 in the next two years so it is achieving a 3-to-1 ROI ratio for years two and three.

In Table 4, the denial-of-service (DoS) attack that lasts four hours and affects 10,000 employees potentially costs $2.3 million. The proposed solution of specialized IPS and load balancers costs $5 million for all network gateways. This solution now becomes a real tough sell.

It also forces the security department to look for alternatives such as protecting only the primary network gateway for $1 million. Upon further analysis, it was determined that this is where 80% of the risk resides for a DoS attack.

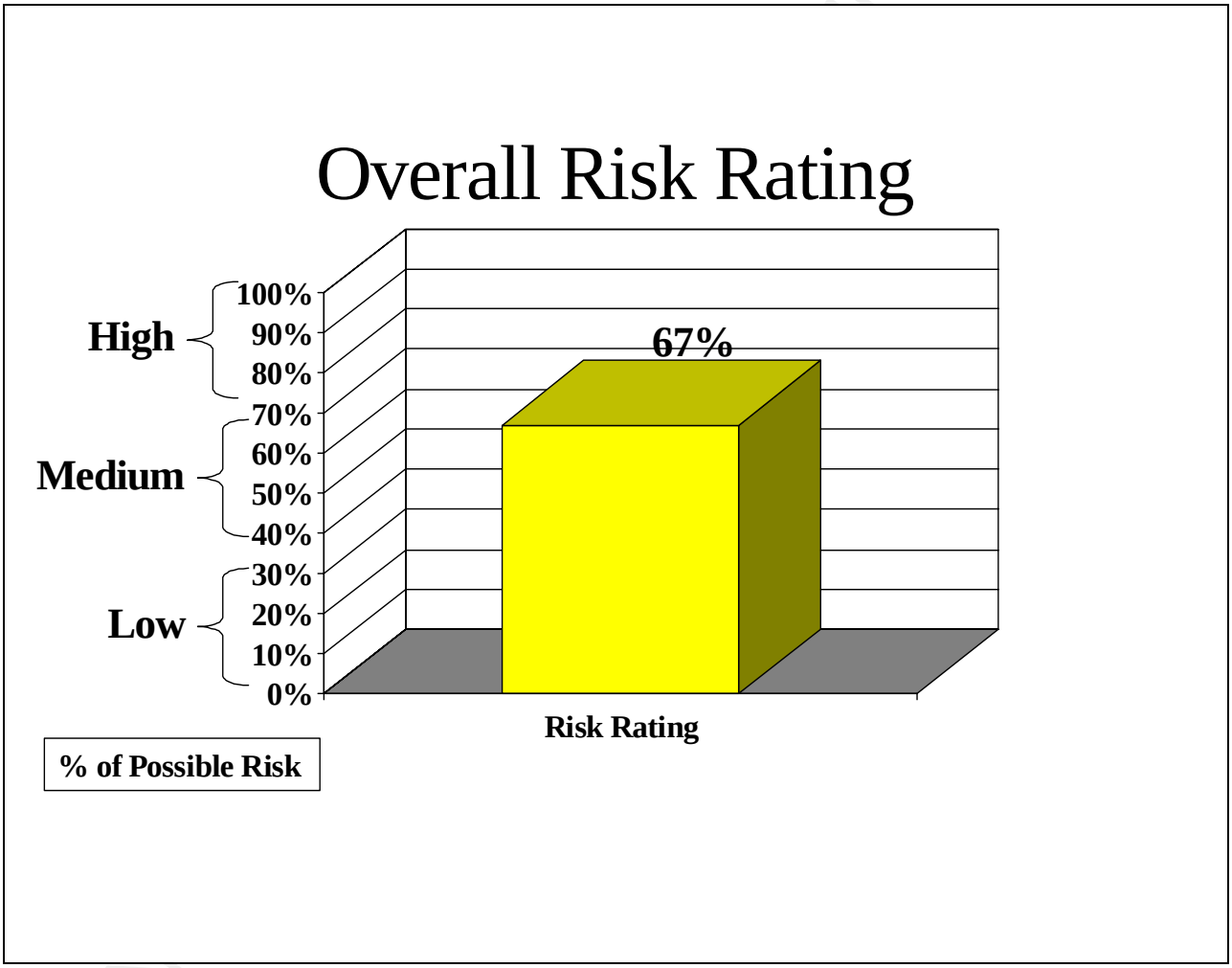
It is prudent to do the additional research that helps quantify as much of this information before presenting to the balance sheet savvy executives, especially the CFO. Chances are that they will be more than happy to help when they understand the objectives. This helps shift the perception of the security effort from a specialized technology focus into helping add value to the bottom line.

Executive Level Reports

OVERALL RISK LEVEL

Project Name: Q4 Review **Date:** December 31, 2005

This report shows a graph of the overall risk for all the objects, number of vulnerabilities, and the total value of the Lines of Business. The number vulnerabilities are calculated by totaling the number of questions that had a negative result and the number of vulnerabilities the primary network scanner found. This report is highest level view of security posture. Overall Risk number is determined by results of all of the subcategories selected and answered.

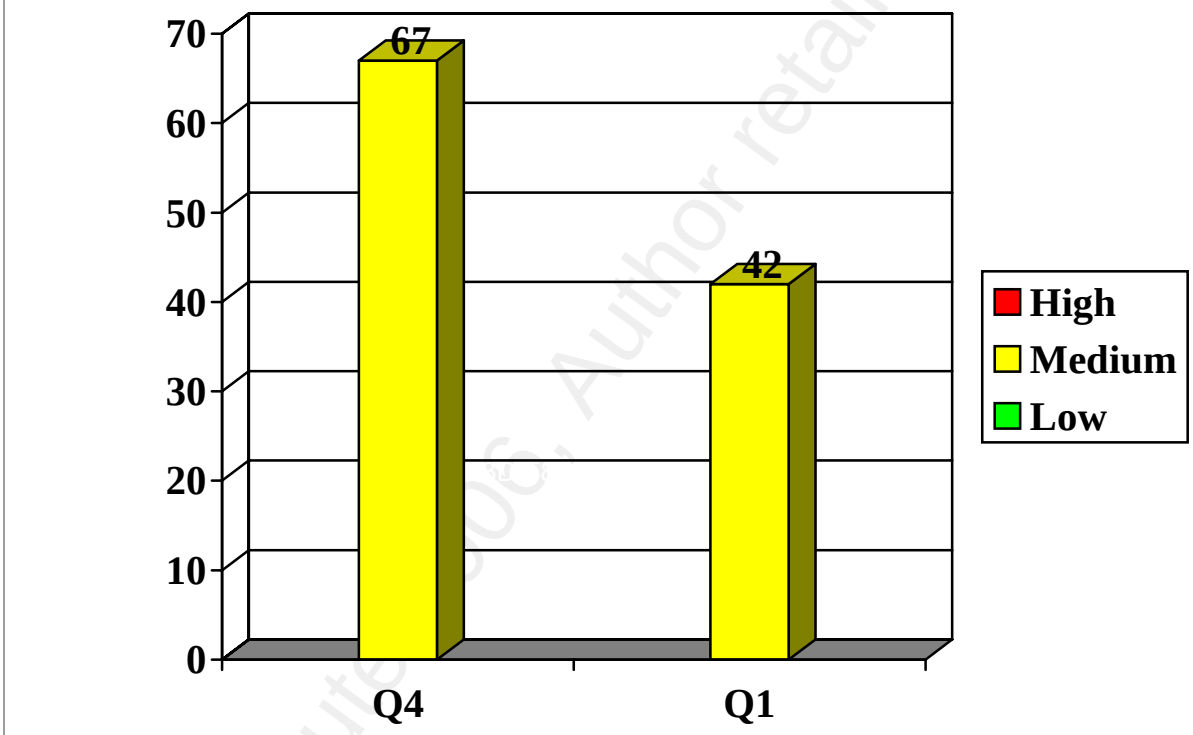


OVERALL RISK SUMMARY	
Overall Security Risk Rating:	Medium - 67%
Number of Total Vulnerabilities:	7,161
Value of All Lines of Business:	$100,000,000.

OVERALL RISK HISTORICAL COMPARISON

Project Name: Q4 to Q1 Comparison **Date:** March31, 2006

The report shows the risk levels from the from two different time periods. This information shows the change between the two. With this information, the risk mitigation efforts can be measured.



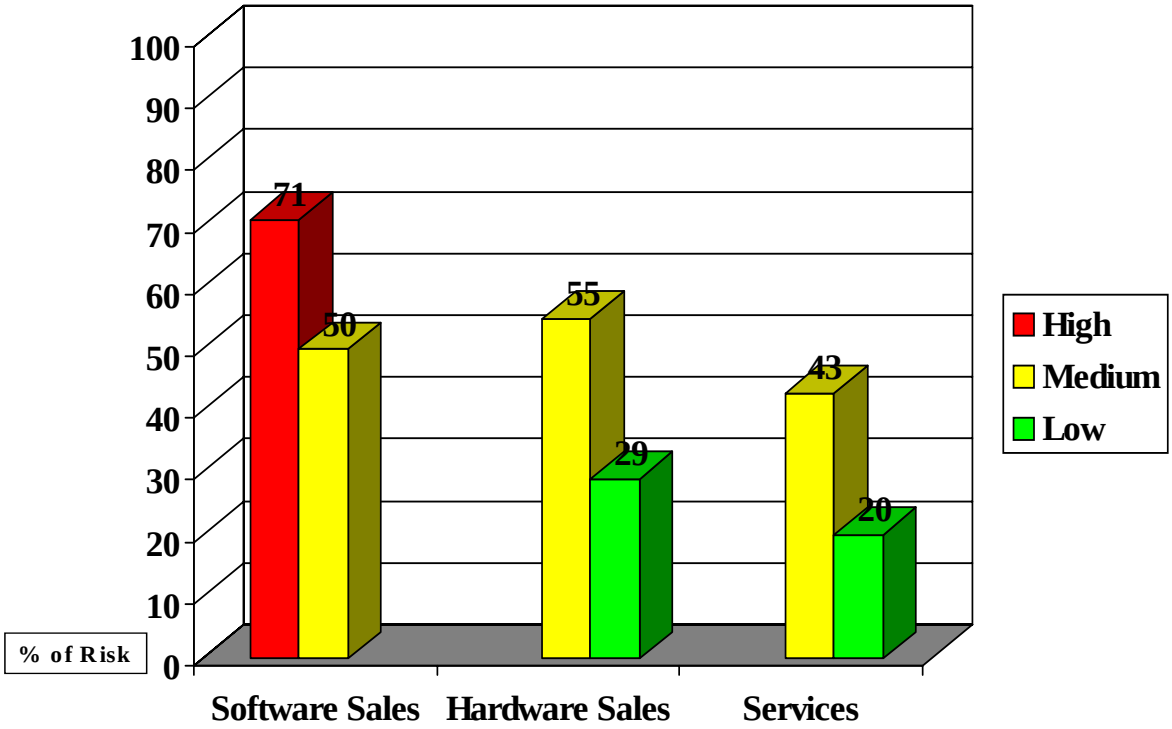
Summary of Overall Risk

Project Title	Q4	Q1	Change +or -
Date of the Project	December 31, 2005	March 31, 2006	
Overall Risk Level	67%	42%	-25%
Network Security Risk	43%	34%	-9%
Operational Security Risk	74%	64%	-10%
Physical Security Risk	50%	44%	-6%
Number of Total Vulnerabilities	590	472	-118
Value of All Lines of Business	$50,000,000	$55,000,000	+10%

RISK LEVEL BY LINES OF BUSINESS COMPARISON

Project Name: Q4 to Q1 Comparison **Date:** March31, 2006

The report shows the risk levels from the from two different time periods by lines of business. This information shows the change between the two. With this information, the risk mitigation efforts can be measured.

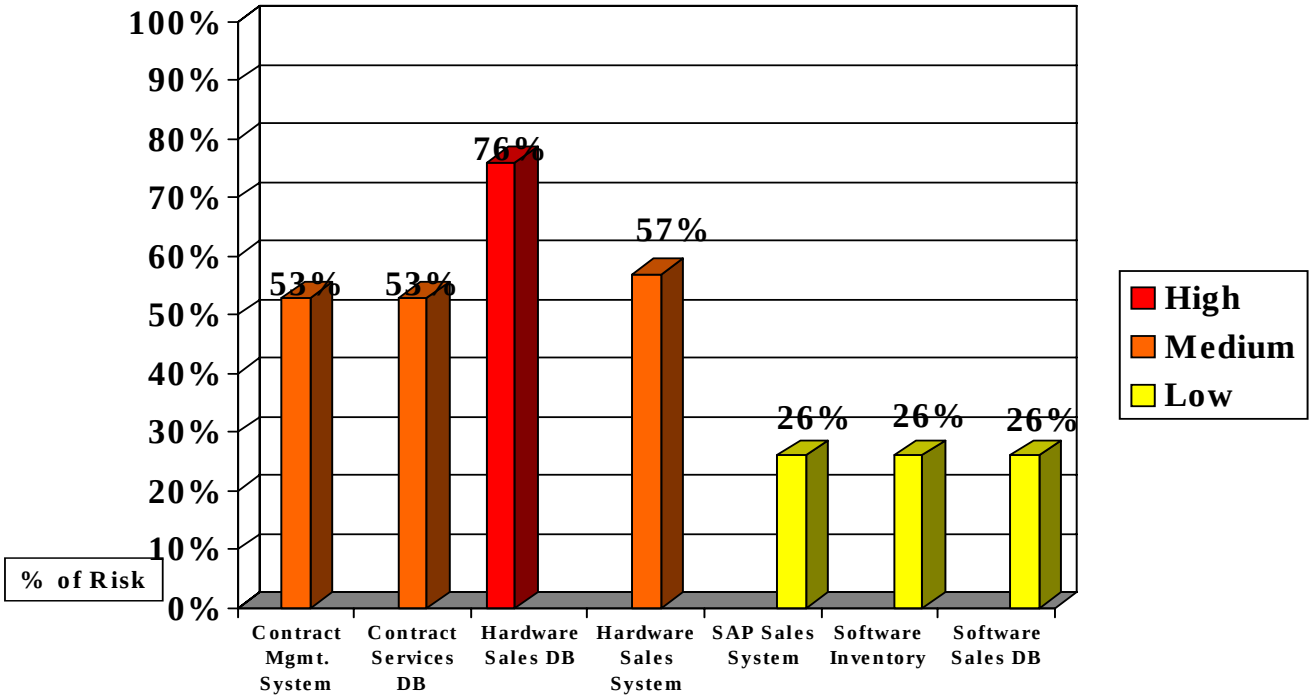


OVERALL RISK BY LINES OF BUSINESS SUMMARY			
Project Name	**Q4**	**Q1**	**Change + or -**
Software Sales Risk	71%	50%	- 21%
Hardware Sales Risk	55%	29%	- 26%
Services Risk:	43%	20%	- 23%

RISK LEVEL BY ASSET REPORT

Project Name: Q1 Review **Date:** March 31, 2006

The report shows the risk levels from the subcategory questions' results for each Asset. This information shows which Assets are at the highest risk. With this information, the risk mitigation recommendations can begin to be made that have the most significant impact to business operations.



CURRENT SUMMARY	
Contract Management System	53%
Contract Services DB	53%
Hardware Sales DB	76%
Hardware Sales System	53%
SAP Sales System	26%
Software Inventory	26%
Software Sales DB	26%

Management Level Reports

RISK BY SUBCATEGORY FOR ALL ASSETS

Project Name: Q1 Review **Date:** March 31, 2006

This report shows a table of the Overall Risk by major category and by the subcategories for all assets. The report shows risk levels at the individual subcategory level and which of these areas are contributing the greatest risk.

OVERALL RISK BY CATEGORY SUMMARY	
Physical Security Risk	44%
Operational Security Risk	64%
Network Security Risk:	36%

OVERALL RISK FOR EACH SUB-CATEGORY	
Physical	
Closed-Circuit Television (CCTV)	41%
Lighting Assessment	47%
Locking Systems and Procedures	44%
Operational	
Security Organization Concerns	64%
Network	
Basic Intrusion Detection	50%
Network Systems (Local Area Networks)	39%
Remote System Access Security	33%
Telecommuting	24%

RISK BY SUBCATEGORY COMPARISON

Project Name: Q4 to Q1 Comparison **Date:** March 31, 2006

The report shows the risk levels from the from two different time periods. This information shows the change between the two. With this information, the risk mitigation efforts can be measured.

OVERALL RISK BY CATEGORY SUMMARY			
Project Title	**Q4**	**Q1**	**Change + or -**
Network Security Risk	43%	34%	-9%
Operational Security Risk	74%	64%	-10%
Physical Security Risk:	50%	44%	-6%
RISK FOR EACH SUB-CATEGORY			
NETWORK			
Project Title	**Q4**	**Q1**	**Change + or -**
Back-up and Information Storage Protection	39%	37%	-2%
Computer Area Fire Suppression	20%	20%	0
Computer Intrusions and Thefts	48%	46%	-2%
Computer Area Emergency Contingency Plan	78%	76%	-2%
Information Input Controls	67%	63%	-3%
Information System Access	33%	33%	0
OPERATIONAL			
Security Organization Concerns	62%	59%	-3%
Information Protection	71%	67%	-4%
Disaster Recovery Planning	53%	50%	-3%
PHYSICAL			
Access Control	49%	49%	0
CCTV	60%	58%	-2%
Gate Security and Construction	28%	28%	0
Grounds Security and Protective Clear Zones	38%	38%	0
Intrusion Alarms	17%	17%	0
Lighting Assessment	73%	70%	-4%

ASSET SUMMARY

Project Name: Q1 Review **Date:** March 31, 2006

This report is the information on how each asset was characterized in the Lines of Business section. It includes the object that belongs to an asset and which Line of Business it is tied to. It also provides ratings for an asset's importance, time sensitivity, and the impact of the asset being corrupted or damaged.

Asset Summary

Asset Name	Object Name	Asset Type	Importance Rating	Time Sensitivity	Corruption Impact	Business Line Supported	Asset Value
SAP Sales System	Masonic Bldg.	Process	5	5	5	Software Sales	$5,000,000
Software Sales DB	Masonic Bldg.	Information	4	4	5	Software Sales	$1,000,000
Software Inventory	Masonic Bldg.	Physical	3	2	2	Software Sales	$10,000,000
Hardware Sales DB	Masonic Bldg.	Information	4	4	5	Hardware Sales	$2,000,000
Hardware Sales System	Bellevue Center	Process	3	2	2	Hardware Sales	$3,000,000
Contract Mgmt. System	Bellevue Center	Process	4	4	5	Services	$500,000
Contract Services DB	Bellevue Center	Information	4	4	2	Services	$500,000
Total							$22,000,000

PROJECT SAFEGUARD SUMMARY REPORT

Project Name: Q1 Review **Date:** March 31, 2006

This report shows the costs associated with all of the assessor's recommendations. It then compares the total cost of all recommendations against the potential losses of low, medium, and high loss events. The report also provides a ROI Ratio for these two sets of figures. It is crucial to show a justification for the investment in the identified recommendations.

Priority Rating	Vendor and Specified Product	Network Security	Operational Security	Physical Security
5	Server Authentication	$80,400		
5	Desktop IDS for End-Users	$40,200		
4	Intranet Firewall (NS-50)	$29,200		
3	Update Security Policies		$ 10,000	
2	Security Awareness Program		$ 20,000	
1	Access Control Upgrade			$5,400
1	CCTV Camera Additions			$15,800
Sub Totals		$149,800.00	$30,000.00	$21,400.00
GRAND TOTAL	**$201,000.00**			

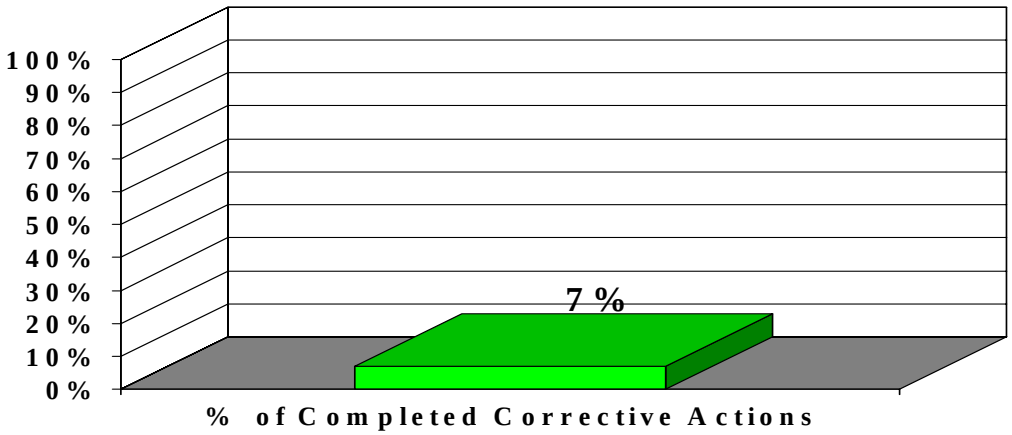
SUMMARY OF RETURN ON INVESTMENT			
Potential Security Loss Incidents	**Significant Loss Event** Ex. - Destructive virus or lost sales database.	**Moderate Loss Event** Ex. – Disgruntled employee act, or prolonged DoS attack.	**Low Loss Event** Ex. – Small nuisance virus infection.
Total Potential Losses	**$9,969,230.00**	**$4,984,615.00**	**$2,492,307.00**
ROI Ratio	**49.5 to 1**	**24.8 to 1**	**12.4 to 1**

Technical Level Reports

CORRECTIVE ACTION COMPLETION SUMMARY

Project Name: Q1 Review **Date:** March 31, 2006

This report provides a high-level graphical summary of the total corrective actions identified as well as listing this information in a table. These are then divided into the two tabular areas of assets and scanner results so each area can be tracked separately. The primary purpose of this report is to show the number, progress, and costs of corrective actions.



OVERALL CORRECTIVE ACTION COMPLETION SUMMARY	
Percent Corrective Actions Complete:	7%
Number of Total Corrective Actions:	761
Number of Corrective Actions Complete:	57
Number of Corrective Actions Remaining:	704
Total Cost of All Corrective Actions:	$57,000
Percent Asset Corrective Actions Complete:	8%
Number of Total Asset Corrective Actions:	434
Number of Asset Corrective Actions Complete:	37
Number of Asset Corrective Actions Remaining:	397
Total Cost of All Asset Corrective Actions:	$37,000
Percent Scanner Corrective Actions Complete:	6%
Number of Total Scanner Corrective Actions:	327
Number of Scanner Corrective Actions Complete:	20
Number of Scanner Corrective Actions Remaining:	307
Total Cost of All Scanner Corrective Actions:	$20,000

ASSET CORRECTIVE ACTION TRACKING REPORT (STATUS COMPLETE)

Project Name: Q1 Review **Date:** March 31, 2006

The report lists all of the corrective actions that been completed for assets. These are organized under the corresponding assets. The report lists the details of when the corrective action was started, completed, who completed it, the cost, and the proof it was actually completed.

Masonic Building

Subcategory: Security Organization Concerns
Corrective Action: A formalized training program should be implemented to help employees achieve the appropriate skill level to be the most effective in their job functions. The training program can also be the basis for promoting employees to more senior positions.
Percent Complete: 100% Start Date: 6/5/2006 **End Date:** 6/28/2006 **Completed By:** M Smith **Cost: $10,000**
Proof of Completion: See Invoice #5571 dated 7-2-2006
Remarks: This is required for all employees.

Subcategory: Security Organization Concerns
Corrective Action: The formalized training program should be organized to take a security department employee through the required basics all the way to advanced knowledge areas. These should be divided into different curriculums that provide study materials, practical exercises, and tests that demonstrate the employee's understanding of the subject areas. All security department employees should be required to complete all areas as part of their job.
Percent Complete: 100% Start Date: 6/5/2006 **End Date:** 6/28/2006 **Completed By:** M Smith **Cost: $10,000**
Proof of Completion: See Invoice #5580 dated 7-7-2006
Remarks: This is required for all security department employees.

Subcategory: Security Organization Concerns
Corrective Action: All employees and visitors should be required to wear identification badges at all times. It is important that employees have their own badge design that is visually different from visitor badges. It should be very easy to quickly identify if an individual is wearing an employee badge or a visitor badge. A visitor badge should not allow an individual into sensitive areas without an employee escort at all times.
Percent Complete: 100% Start Date: 6/5/2006 **End Date:** 6/28/2006 **Completed By:** M Smith **Cost: $1,000**
Proof of Completion: See Security Policy dated 7-2-2006, pg. 40
Remarks: This is required for all employees.

Subcategory: Information Protection
Corrective Action: There should be established procedures for the physical transfer of all proprietary information to other company locations or to other business partners. These procedures should require information documents be sealed in a tamper proof envelope and placed in a locked briefcase for a designated member of the security team to carry. A pre-screened and approved courier could also be used instead of a company employee. Specialized mail carriers, such as FedEx and UPS, may also be a reasonable alternative if they can provide chain of custody guarantees and the package will arrive safely.
Percent Complete: 100% Start Date: 6/5/2006 **End Date:** 6/28/2006 **Completed By:** M Smith **Cost: $1,000**
Proof of Completion: See Security Policy dated 7-2-2006, pg. 55
Remarks: This is required for all employees and partners.