Case Study:

Securing an Enterprise Computer Network

With

Security Development Life Cycle

By

George H. Jordan

Spring 2009

Securing an Enterprise Computer Network
With
Security Development Life Cycle

Securing an enterprise computer network that is connected to the Internet is a challenging task in today's business world. The challenge that a network administrator faces is to minimize the network's risk of being infected with a virus, a worm, Trojan horse , Denial of Service attack or an intruder attack (hacker) to the network. The virus is a software program that attaches itself to another program and can cause damage when the host program is activated [9].

A worm is a type of virus that replicates itself constantly, without requiring another program to provided a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth [1].

The Trojan horse is a software program that hide its true nature, and reveal the designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages. Unfortunately, like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user [9]

Denial of Service attack (DoS) is an attack in which the abuser sends a large number of connection or information requests to overwhelm and cripple a target, such as web sever [1]

A hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work – both mechanically and electronically [9].
In recent years, hacker has taken on a new meaning – someone who maliciously breaks into systems for personal gain. Technically, these people are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable [9].

In securing the computer network for Omega, Inc., the Security Systems Development Life Cycle (SecSDLC) is used as the methodology to provide guidelines for a systematic approach to securing the network from the hacker, the virus, the worms, the Trojan horses, and the Denial of Service (DoS) attacks.

Security System Development Life Cycle

There are six phases of the Security Systems Development Life Cycle. The phases are the investigation phase, analysis phase, logical design phase, physical design phase, implementation phase, and the maintenance phase is an on going process to maintain the

up-to-date security procedures. The investigation phase will be used to determine the root concern for network security and who are the stake holder or stake holders that are driving force behind the project. Documentation will be produced to establish a view of the network by the stake holder or stake holders and their concerns of network access and intrusion.

In the analysis phase, the documentation that was produced in the investigation phase will be studied along with a preliminary analysis of existing security policies or programs. A check for current security threats and associated controls will be documented and compared to existing intrusion detection and prevention systems. This phase will also include an analysis of revalent legal issues and privacy laws that could effect the design of the security solution. The risk management task also begins in this stage. Risk management is the process of identifying, assessing , and evaluating the levels of risk facing an organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

In the logical design phase a blueprint diagram of the existing computer network will be developed to show the current security structure of the network the previous phases. Also, at this phase we will determine the incident response actions to be taken in the event of partial or catastrophic loss. After determining the incident response actions to be taken in the event of a partial or catastrophic loss, we are looking forward to having as a by product a disaster recovery plan.

In the physical design phase, the information security technology needed, if any, to support the blueprint outlined in the logical design phase is evaluated, alternative solutions are generated, and the final design is agreed upon with the stake holder or stake holders.

In the implementation phase, the security solutions are acquired (made or bought), tested, implemented and tested again.

The maintenance and change phase, thought the last, is perhaps the most important, given the current ever-changing threat environment. Today's information security systems need constant monitoring, testing, modification, updating and repairing.

Project Start

<u>The Investigation Phase</u>

In the investigation phase, a meeting with the management of Omega was determined that the president was in favor of having the company's computer network analyzed for security breaches from external and internal sources. The management of the company is especially concerned with social engineering on the company's computer network that could negatively impact the integrity and confidentially of the financial position of the company.

During the initial meeting, it was determined that managements view of the network is more software and personnel oriented than hardware oriented. Management's

view of the network is that the data flows from the point-of-sales (pos) operation over the Internet to a proprietary back office software program controlling the daily ledger.

Knowing how management perceives their network will assist in knowing how to present the recommendations that will needed to be implemented. In other words, if the management is technical, savvy, then the documentation presented to the management on the recommendations can use technical terminology to explain the recommendation (not to much where you have to rewrite to recommendations). If the management is not technically savvy, the recommendations can use clear and concise laymen terms to minimize confusion.

The figure 1 represents the conceptual view of Omega's management. Notice that management view excludes the hardware and the transport mechanism for the data. The view should be very rewarding to the network administrator for making the hardware and network software transparent to management.

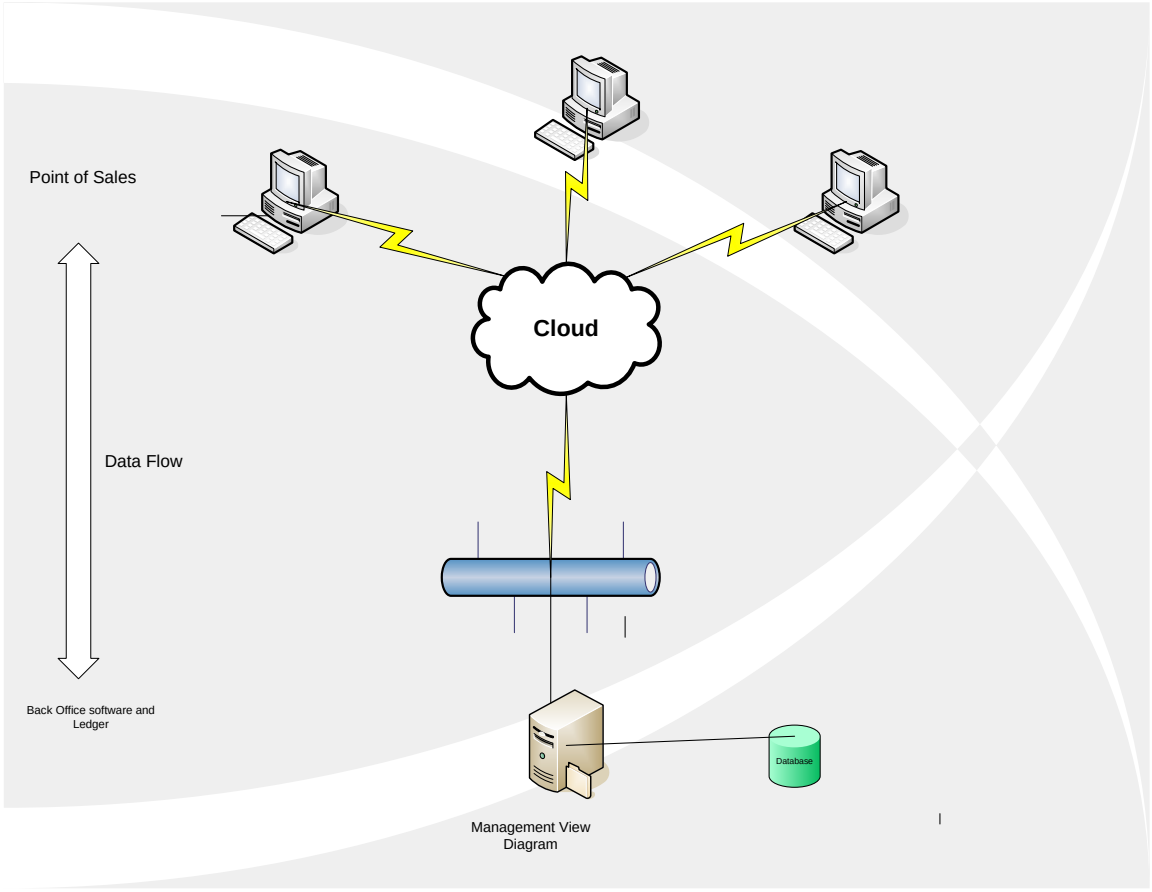

Figure 1 Management's Network View

Management's personnel view is the focus on the managers and their responsibility. Responsibility for the remote locations rely on the assigned territorial managers. The managers have the only access to the remote host systems communicating with the central server. POS employees did not have access to the host systems. A manager may have up to four remote locations that he or she is responsible for the daily operation.

Also, during the meeting with the owner of the company, is was disclosed that there are daily updates that must be accomplish. The daily upload to the remote host computers is via the Internet and the critical part of upload will be to products sold over the point-of-sales database consisting of over five-thousand products.

The most pressing concern, to Omega's management, is the requirement that a report to the franchise partner most be completed by 11 a.m. each day or face a two-hundred dollar fine per day until the report is filed.

The final request of the owner was to have the business analyzed for internal security breaches. That is, Omega's management would like to have an assessment of the access rights and authentication of the insiders to make sure that the correct insider are accessing only their assigned files and directories.

However, before permission was granted to perform the security analysis, Omega's management required documentation in the form of a Statement of Work and a Scope of Work. These forms would provide information so the management would know what was going to be done and the deliverables to expect from the network analysis. Below is the Scope of Work and Statement of work template used to meet the requirement of Omega's management request. The Scope of Work and Statement of Work also includes the expectations of the involvement Omega's management and/or assigned personnel.

The use of the Statement of Work and Scope of Work will be an asset to obtain management's signed commitment for a project. Once, the project becomes sponsored by management, it will contribute to the success of the project.

Please note, in viewing the Statement of Work and the Scope of Work, that there is a phase II. Phase II came about during the investigation phase and another concern of Omega's management is the total business security. That is, Omega's management is deeply concerned with internal (insider) security threats. For example, insiders having access to the financial records, bank access, and payroll information.

Scope of Work and Statement of Work

Client Data			
Client:	OMEGA, LLC. 880 Lee Street Des Plaines, Il. 60016	Contact: Phone: Fax:	Clark Kent (555) 555.5555 (555) 555.5556

CMass Electronics, Inc. and OMEGA, LLC. agree as follows:

Conditions of Proposal

> *OMEGA, LLC. agrees that this proposal document, shall, unless otherwise expressly provided in writing by a duly authorized officer of CMass Electronics, Inc., not be disclosed by OMEGA, LLC. outside of OMEGA, LLC.'s operation (except and to the extent required to comply with applicable law, and then only upon written notice to CMass Electronics, Inc.) and be made available within OMEGA, LLC.s operation only to those employees of OMEGA, LLC. who may be working on this project.*

This proposal, when executed by both parties shall constitute the only legally binding commitment of the parties.

The pricing for this CMass Electronics, Inc. service is standard pricing based on a stable network environment. Additional time required to resolve an existing network or workstation problem or incompatibilities are out of the scope of this agreement and will be billed at an hourly rate of $150.00 ($225.00 after 5:00PM and Saturdays) per hour.

Scope of Work

Project Overview

It is CMass Electronics, Inc.'s understanding that ***OMEGA, LLC.***'s immediate and primary needs are the following:

The project will consist of two phases. Phases I will consist of a network security analysis to determine the strength and weakness of the current defenses to prevent unwanted intrusion from outside parties, protection against virus and Trojan acquisition, and Denial of Service attacks. The Security Development Life Cycle will be used to provide the necessary framework to provide supporting documentation in the network analysis.

Phase II of the project will be to secure the business operations for the day-to-day operations. This phase will focus on the access rights of the network file system, authentication of the proper users for file access, physical security, and to address disaster recovery procedures.

Assumptions

It is CMass Electronics, Inc. ‘s assumptions that OMEGA, LLC. will provide the following:

Telephone access to conduct all necessary business related to the project.

Reasonable and customary access to the network and network resources.

Provide all software that pertains to the current project.

All work will be performed between the hours of 8 a. m. and 5 p. m. Monday through Friday.

Provide an independent work area for CMass employees.

Provide hardware and software that is not reflected in this proposal.

Deliverables:

- Statement of Work
- Scope of Work
- Quantitative results from minimum & maximum documentation
- Logical network design & final network design
- Hardware/software recommendations
- Written report on network findings and recommendations

Statement of Work

Integration services will consist of the following:

Phase 1 – Network Security.

Security Development Life Cycle:

- Investigation Phase:
- Obtain managements approval to perform an analysis of the network and a basic understanding of the company’s operation and goals.
- Obtain any existing security policies or programs of documented threats and associated controls.
- Estimate the cost
- Analyze feasibility

Number of CMass Electronics, Inc. hours: 4.0
Number of ***OMEGA, LLC.*** hours: 4.0

Necessary Resources:
All ***OMEGA, LLC.*** and CMass Electronics, Inc. project team members are needed.

Number of CMass Electronics, Inc. hours: 4.0
Number of ***OMEGA, LLC.*** hours: 4.0

- Analysis Phase
- Analyze existing security policies and programs
- Analyze current threats and controls
- Examine legal issues
- Perform risk analysis
- Acts of human error or failure
- Compromise to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attacks
- Forces of nature
- Deviations in quality of service
- Technical hardware failures or errors
- Technical software failures or errors
- Technical obsolescence

Necessary Resources:
CMass Electronics, Inc. System Engineer
Number of CMass Electronics, Inc. hours: 16.0

Number of ***OMEGA, LLC.*** hours: 3.0
3.2 Demonstration and Client Approval

Necessary Resources:
CMass Electronics, Inc. Systems Engineers
Number of CMass Electronics, Inc. hours: 16.0
Number of ***OMEGA, LLC.*** hours: 0.0

- Logical Design Phase
- Develop a security blueprint
- Plan incident response actions
- Plan business response to disaster
- Determine feasibility of continuing and/or outsourcing the project

Necessary Resources:
CMass Electronics, Inc. Systems Engineers
Number of CMass Electronics, Inc. hours: 18.0
Number of ***OMEGA, LLC.*** hours: 1.0

- Physical Design Phase
- Select technologies to support solutions developed in the Logical Design Phase
- Develop definition of successful solution
- Design physical security measures to support technological solution/solutions
- Review and approve project

Necessary Resources:
CMass Electronics, Inc. Systems Engineers
Number of CMass Electronics, Inc. hours: 6.0
Number of ***OMEGA, LLC.*** hours 2.0

- Implementation Phase:
- Buy or develop security solutions
- Present tested package to management for approval

Necessary Resources:
CMass Electronics, Inc. Systems Engineers
Number of CMass Electronics, Inc. hours: 6.0
Number of ***OMEGA, LLC.*** hours 1.0

- Maintenance Phase

  Constantly monitor, test, modify, update, and repair to meet changing threats.

Necessary Resources:
CMass Electronics, Inc. Systems Engineers/ Network Engineers
Number of CMass Electronics, Inc. hours: Undefined
Number of ***OMEGA, LLC.*** hours Undefined

Phase II – Business Security Action items to be considered:

- **Physical Security**
- **Network Access Security**
- **Network Authentication**
- **Equipment use policy**
- **Network monitoring**

- Disaster Recovery
- Assist in developing a disaster recovery plan addressing:
- Acts of human error or failure
- Compromise to intellectual property

Necessary Resources:
CMass Electronics, Inc. Systems Engineers/ Network Engineers

Number of CMass Electronics, Inc. hours:
To be determined
Number of ***OMEGA, LLC.*** hours To be determined

Pricing Summary

In the event that ***OMEGA, LLC.*** changes the requirements of any phase of this project, CMass Electronics, Inc. reserves the right to alter hours or fees for services. Services outlined in the preceding statement of work will commence upon ***OMEGA, LLC.*** acceptance.

Description of Service	Hours	Hourly Rate	Total
Investigation Phase	4	$0.00	$0.00
Analysis Phase	16	$0.00	$0.00
Logical Design Phase	18	$0.00	$0.00
Physical Design	6	$0.00	$0.00
Implementation Phase	6	$0.00	$0.00
Maintenance Phase	undefined	undefined	
Phase II Business Security - to be determined			
Project Totals	**50**		**$0.00**

Payment is due within thirty (30) days of invoice date unless otherwise agreed in writing.

Terms and Conditions

1. Terms. Unless otherwise specified in writing, the parties agree that the terms of this Agreement will apply to all future dealings between them whether or not such dealings are encompassed by the work described in the Proposal.

2. Independent Contractor. The relationship of CMASS ELECTRONICS, INC. to OMEGA, LLC. is one of an independent contractor and nothing in this Agreement shall be construed to imply that CMASS ELECTRONICS, INC. or its employees are agents or employees of OMEGA, LLC., for any purpose, including, but not limited to, withholding of social security or state and/or federal income tax or entitlement to employee benefits of OMEGA, LLC.. CMASS ELECTRONICS, INC. will be solely responsible for payment of any and all taxes and insurance, including workers compensation, for its employees who perform any Services pursuant to this Agreement.

3. Ownership Rights in Data. CMASS ELECTRONICS, INC. does not convey nor does OMEGA, LLC. obtain any right or interest in any of the programs, systems, data or materials utilized or provided by CMASS ELECTRONICS, INC. in connection with the performance of this Agreement unless otherwise specifically set forth in writing.

4. Client agrees during the term of this Agreement and for a period of one (1) year after its termination, not to solicit, directly or indirectly (through individuals, subsidiaries, holding companies, partnerships, subcontractors or any other financially related firms), nor to tender an offer for employment nor place on their payrolls any employee who is or was, within ninety days prior to the time of such solicitation, offer or employment, on CMass Electronics, Inc.'s payroll. In the event Client hires or contracts with a CMass Electronics, Inc. employee in violation of the terms of this paragraph, the Client agrees to pay CMass Electronics, Inc. as liquidated damages, and not as a penalty, an amount equal to one half of the employee's annual compensation,

including but not limited to wages, bonuses and fringe benefits. This provision for liquidated damages shall not limit remedies against the Client for any other breach of this Agreement.

(a) Client will require all agencies and/or subcontractors working on Client's premises with CMass Electronics, Inc. employees to execute a document indicating their Agreement to the terms of this paragraph. In the event of a violation of this provision by a subcontractor or other third party on Client's premises, Client agrees not to use the services of such individual(s) hired by such subcontractor or third party.

(b) Client will require all agencies and/or subcontractors working on Client's premises with CMass Electronics, Inc. employees to execute a document indicating their Agreement to the terms of this paragraph.

(c) In the event of a violation of this provision by a subcontractor or other third party on Client's premises, Client agrees not to use the services of such individual(s) hired by such subcontractor or third party.

5. Warranties. CMASS ELECTRONICS, INC. warrants that, in performing the Services:

(a) the Services will reasonably conform to the descriptions set forth in the Proposal within thirty (30) days of completion of the Services. OMEGA, LLC. shall execute a Certification of Acceptance providing, among other things, that the Services furnished by CMASS ELECTRONICS, INC. hereunder are in accordance with the Proposal and acceptable to OMEGA, LLC.;

(b) CMASS ELECTRONICS, INC. will transfer or assign to OMEGA, LLC. any available and assignable product warranties of manufacturers and/or suppliers for any equipment or product purchased by OMEGA, LLC. and furnished by CMASS ELECTRONICS, INC. pursuant to this Agreement. CMASS ELECTRONICS, INC. makes no warranties concerning equipment or product supplied to OMEGA, LLC. under this Agreement, and all product and equipment furnished by CMASS ELECTRONICS, INC. is on an "as is" basis.

THE FOREGOING WARRANTIES IN THIS PARAGRAPH 5 ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR USE FOR A PARTICULAR PURPOSE OR YEAR 2000 COMPATIBILITY. CMASS ELECTRONICS, INC.'S LIABILITY UNDER THIS WARRANTY SHALL NOT INCLUDE ANY LIABILITY FOR SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING FROM THE SERVICES, INCLUDING, BUT NOT LIMITED TO, ANY PRODUCT, GOODS OR SERVICES SUPPLIED OR INSTALLATION THEREOF. IN NO EVENT SHALL CMASS ELECTRONICS, INC. BE LIABLE FOR ANY LOST PROFITS OR SALES OF OMEGA, LLC., AND AND AND CMASS ELECTRONICS, INC.'S LIABILITY UNDER ANY THEORY OF LAW SHALL NOT EXCEED THE AMOUNTS RECEIVED BY CMASS ELECTRONICS, INC. FROM OMEGA, LLC. PURSUANT TO THIS AGREEMENT.

6. Liability. CMass Electronics, Inc.'s entire liability and OMEGA, LLC.'s exclusive remedy for damages from any cause or source whatsoever, including, but not limited to, nonperformance or misrepresentation, and regardless of the form of action, shall be limited to a refund of the price paid by OMEGA, LLC. for the specific products or services that caused the damages or claims that are the subject matter of, or indirectly related to, the cause of action. In no event will CMass Electronics, Inc. be liable for damages caused by OMEGA, LLC.'s negligence, or for any lost profits, lost savings or other incidental or consequential damages, even if CMass Electronics, Inc. has been advised of the possibility of such damages, or for any claim against OMEGA, LLC. by any other party.

7. Termination.

(a) Either party may terminate this Agreement with 30 days prior written notice to the other.

(b) Default. In the event all sums due pursuant to this Agreement are not paid as set forth herein, CMASS ELECTRONICS, INC. shall have option to terminate this Agreement immediately upon written notice to OMEGA, LLC..

(c) Acts of Insolvency. CMASS ELECTRONICS, INC. shall have the option to terminate this Agreement by written notice to OMEGA, LLC. and to regard the OMEGA, LLC. as being in material default of this Agreement, if OMEGA, LLC. becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition for bankruptcy, suffers or permits the appointment of a receiver for its business or assets, or becomes subject to any proceeding under any bankruptcy or insolvency law, whether domestic or foreign, or has wound up its business or liquidated, voluntarily or otherwise. In the event that any of the above events occurs, OMEGA, LLC. shall immediately notify CMASS ELECTRONICS, INC. in writing of such occurrence.

(d) Force Major; Suspension and Termination. In the event that either party is unable to perform any of its obligations under this Agreement, or to enjoy any of its benefits because of (or failure to perform the Services is caused by) natural disaster, actions or decrees of governmental bodies or communication line failure, or any inability to perform which is not the failure of the affected party (hereinafter referred to as a "Force Major Event"), the party who has been so affected shall immediately give notice to the other party and shall do everything possible to resume performance. Upon receipt of such notice, all obligations under this Agreement shall be immediately suspended. If the period of non-performance exceeds thirty (30) days from the receipt of notice of the Force Major Event, the party whose ability to perform has not been so affected may terminate this Agreement, by giving written notice to the other party.

(e) Rights and Obligations of the Parties on Termination. Upon termination of this Agreement based on a material breach or default by OMEGA, LLC., CMASS ELECTRONICS, INC. shall be entitled to retain payments received to date of default or breach, as well as retain (including a demand to OMEGA, LLC. for return of) all data, manuals, materials, equipment and other items provided to OMEGA, LLC. as part of the Services under this Agreement, which have not been fully paid for by OMEGA, LLC. at

the time of termination and, in addition, shall have all other legal rights and remedies available as a result of such breach.

8. Confidential and Proprietary Information; Publicity:

(a) Confidential and Proprietary Information. OMEGA, LLC. acknowledges and agrees that any and all information concerning CMass Electronics, Inc.'s business disclosed in the course of performance of the Services under this Agreement is "Confidential and Proprietary Information", and OMEGA, LLC. agrees that it will not permit the duplication, use or disclosure of any such Confidential and Proprietary Information to any person (other than its own employee, agent or representative who must have such information for the performance of services hereunder), unless such duplication, use or disclosure is specifically authorized in advance in writing CMass Electronics, Inc. "Confidential and Proprietary Information" is not meant to include any information which, at the time of disclosure, is generally known by the public or any competitors of OMEGA, LLC. or CMASS ELECTRONICS, INC., but OMEGA, LLC. shall have the burden of establishing that any information sought to be disclosed to third persons or entitles is not subject to this provision of non-disclosure.

(b) Publicity; Trademarks. Neither party shall use the name(s), trademark(s) or trade name(s) (whether registered or not), of the other party in publicity releases or advertising or in any other manner, including OMEGA, LLC. lists, without securing the prior written approval of the other party.

9. Indemnification. OMEGA, LLC. does hereby indemnify and shall hold harmless (including reasonable attorney's fees), CMASS ELECTRONICS, INC., its corporate affiliates and any employee or agent thereof (each of the foregoing being hereinafter referred to individually as "Indemnified Party"), against all liability to third parties (other than liability solely the fault of the Indemnified Party) arising from or in connection with the violation of any third party's trade secrets, proprietary information, trademarks, copyright, or patent rights in connection with the performance of Services under this Agreement, The obligation to indemnify any Indemnified Party will survive the expiration or termination of this Agreement by either party for any reason. The Indemnifying Party may, at its option, conduct the defense in any such third party action arising as described herein and the Indemnified Party promises fully to cooperate with such defense.

10. Taxes. OMEGA, LLC. shall be responsible for the payment of all taxes imposed in connection with or as a result of this Agreement.

11. Assignment. Neither party shall assign or subcontract all or any part of this Agreement without the other party's prior written consent, however CMass Electronics, Inc. may use qualified temporary help or subcontractors to assist in performance of its obligations under this Agreement.

12. Applicable Law. This Agreement shall be governed by the laws of the State of Illinois.

13. Miscellaneous.

(a) Remedies. All remedies available to CMASS ELECTRONICS, INC. for breach of this Agreement are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

(b) Notices. Notice shall be given to the parties at their respective address as stated herein, by First Class United States Mail, postage prepaid.

(c) Waiver. No term or provision hereof shall be deemed waived and no breach excused unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented.

(d) Site of Services. If CMASS ELECTRONICS, INC.'s services are performed at OMEGA, LLC.'s offices, OMEGA, LLC. shall provide office space and facilities to CMASS ELECTRONICS, INC.'s staff commensurate with that provided to its own employees to the extent necessary to perform the Services.

(e) Modifications. If the OMEGA, LLC. requests in writing any modification of the Services, CMASS ELECTRONICS, INC. may perform such services at its sole discretion. If CMASS ELECTRONICS, INC. so performs, OMEGA, LLC. agrees that CMASS ELECTRONICS, INC. may expend the time CMASS ELECTRONICS, INC. deems reasonable and necessary to perform the modified Services and the charges for such modified Services shall be on a time and materials basis at CMASS ELECTRONICS, INC.'s hourly rates and charges then in effect, unless otherwise agreed to in writing by the parties.

(f) Prior Negotiations. This Agreement constitutes the entire understanding of the parties and supersedes any and all prior or contemporaneous representations or agreements, written or oral, by the parties, and cannot be changed or modified unless in writing signed by the parties.

(g) Severability. If any part of this Agreement is found to be in violation of any law or is found to be otherwise unenforceable, this Agreement shall be construed and interpreted without reference to such part.

(h) Attorney's Fees. In the event that either party commences a proceeding to construe or determine the rights and obligations of the parties pursuant to this Agreement, or a breach thereof, the prevailing party shall be entitled to recover from the other party all reasonable attorney's fees and expenses incurred in obtaining a declaration or enforcement of rights and obligations or determining a breach by the other party under this Agreement.

Signature Page

OMEGA, LLC. Acceptance

Client Representative: _____ Date: _____

Title: _____

CMass Electronics, Inc. Representative: Date: _____
_____

Title: _____

Conclusion of the Investigation phase

At the close of the meeting, it was agreed upon that the deliverables would include a Statement of Work and Scope of Work, and a network diagram, quantitative results developed in the analysis phase, logical design and/or final design, and any recommendations.

The investigation phase did not produce any security documentation or an acceptable use policy.

Analysis Phase

Unfortunately, there were no documents to input for the analysis phase. One of the recommendations will be to establish an acceptable use policy for the company's network and Internet access.

Risk Management Task

As stated earlier, risk management is the process of identifying, assessing , and evaluating the levels of risk facing an organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

In the context of information security, a threat is an object, person, or entity that represents a constant danger to an asset. To make sound decisions about information security, management must be informed about the various threats facing the organization, its people, applications, data, and information systems. Below is a list of threat categories and examples of the danger that can harm the organization's assets that is recommended to be address during the SecSDLC[1].

Categories of Threat	Examples
1. Acts of human error or Failure	Accidents, employee mistakes.
2. Compromises to Intellectual property	Piracy, copyright infringement.
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection.
4. Deliberate acts of information extortion	Blackmail or information disclosure.
5. Deliberate acts of sabotage or vandalism	Destruction of systems information.
6. Deliberate acts of theft	Illegal confiscation of equipment or information.
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service.
8. Forces of Nature	Fire, flood, earthquake, lightning.
9. Deviations in quality of service	ISP, power, or WAN service issues from service provider.
10. Technical hardware failures or errors	Equipment failure.
11. Technical software failures or errors	Bugs, code problems, unknown loopholes.
12. Technical obsolescence	Antiquated or outdated technologies. [1]

Acts of Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, sometimes mistakes happen. Inexperience, improper training, and the making of incorrect assumptions are just a few circumstances that can cause these misadventures. [1]

One of the greatest threats to an organization's information security is the organization's own employees. Employees are the greatest threat-agents closet to the organizational data. Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentially, integrity, and availability of data. This is because erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, such as a desktop, Web site, or even in the trash can is a much as a threat to the protection of the information as is the individual who seeks to exploit the information, because one person's carelessness can create a vulnerability and an opportunity that another person may not be able to pass up[1].

The owner of Omega states that the act of human error or failure from his staff can negatively impact the reporting records of the organization. The slightest error of a point of sales cashier entering a few errors per transaction to the staff (managers, office personnel, and clerks) making reporting errors could reflect an inaccurate financial picture of the organization. These errors are considered to be accidental deletion or modification of data which could lead to questioning the integrity of the stored data.

Compromise to Intellectual Property

Many organizations create or support the development of intellectual property as part of their business operations. Intellectual property is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source." Intellectual property includes trade secret, copyrights, trademarks, and patents. Once intellectual property has been defined and properly indentified, braches to intellectual property constitute a threat to the security of this information. Employees may have access privileges to the various types

of intellectual property, and may be required to use the intellectual property to conduct day-to-day business [1].

Frequently an organization purchases or leases the intellectual property of the organization and must abide by the purchase or licensing agreement for its fair and responsible use. The most common intellectual property breach is the unlawful use or duplication of software-based intellectual property, more commonly known as software piracy. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, he or she is in violated the copyright[1].

The Omega management is cognizant of the compromise of intellectual property. Management is deeply concerned and aware of the licensing agreements and penalties of the improper use and distribution of the desktop operating system that the organization is using, the proprietary software that runs the point of sales operation, the franchise reporting software that report the daily financial information.

Deliberate Acts of Espionage or Trespass

Deliberate acts of espionage or trespass are a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques rare quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, *competitive intelligence*. When information gatherers employ techniques that cross the threshold of what is legal or considered ethical, they are conducting *industrial espionage* [1].

The deliberate acts of espionage or trespass for Omega, Inc. operation is the manipulation of the point-of-sales terminals to show an inaccurate number of transactions and/or the unauthorized manipulation of the prices that are sent to all stores. This a severe trespass violation for the organization.

Deliberate Acts of Information Extortion

The threat of information extortion involves the possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for the return or for an agreement not to disclose the information[1].

Omega's management considers the stealing of personnel and or payroll records by a trusted employee for compensation to be in this category. Also, if the trusted employee steals the daily pricing information that would have a crippling effect to the business and could warrant some kind of compensation to obtain the lost information.

Deliberate Acts of Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts range from petty vandalism by employees to organized sabotage against an organization [1].

Although not necessarily financially devastating, attacks on the image of an organization are serious. Organizations frequently rely on image to support the generation of revenue, and vandalism to a Web site can reduce consumer confidence, therefore reducing the organization's sales and net worth.[1]

Omega does not need an Web site to carry on day-to-day business, however, the deliberate acts of sabotage or vandalism is a major concern. The tampering of the point-of-sales terminals and retail store computers could lead to the loss in the thousands of dollars range. Also, the tampering with Omega's key software and payroll by trusted insiders can cost the organization hundreds of thousand of dollars in loss revenue

Deliberate Acts of Theft.

The threat of theft: The illegal taking of another's property, is a constant problem. Within an organization, property can be physical, electronic, or intellectual. The value of information suffers when it is copied and taken away without the owner's knowledge[1].

Physical theft can be controlled quite easily. Wide variety of measures can be used, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft is a more complex problem to manage and control. When someone steals a physical item, the loss is easily detected. With the theft of electronic information, the evidence of a crime is not readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until is far too late[1].

In the case of Omega, overriding sales is definitely a deliberate act of theft of the organizations revenue. The stealing of credit card numbers and the disconnecting of network equipment to eliminate the capture of credit card information is in violation of company policy and an offense punishable by current laws as a deliberate act of theft.

Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs software to attack a system. Most of this software is referred to as malicious code or malicious software, or sometimes malware. These software programs are designed to damage, destroy , or deny service to the target systems. Some of the more common instances of malicious code are viruses, worms, Trojan horses, and back doors[1].

In the case of Omega, it is surprisingly secure from the hacker and the major threat of picking up a virus, worm, or Trojan horse is minimized by the use of an anti-virus software on the company's desktop computers and firewall protection from Internet

access. The organizations external router is configure to protect the company's network from Denial of Service attacks.

The major concern that Omega's management has for deliberate software attacks comes from a possibility that a trusted employee that could destroy company files and or database data. This concern will be addressed by authorization, authentication, performing controlled backup of the organizations database files on a regular basis.

Forces of Nature

Forces of nature or act of God can pose on of the most dangerous and unexpected threats imaginable, because the threats cannot always be determined when and which one of the threats will occur. These threats can include lighting for thunderstorms, flash floods, earthquakes, fire, and tornados[1].

Lightning: A large-scale high-tension natural electric discharge in the atmosphere. Lightning can cause an organizations source of electric power to be interrupted such that information system will cease to function. Also, a direct lightning strike to the building can cause a power surge to the point that irreversible electrical damage to the internal components of the organizations computer systems are rendered inoperable[1].

Flash floods: The uncontrollable discharge of rain water flowing over land that is normally dry. The waters from the flash flood will render the organizations access to the building housing the information system inaccessible for an unknown extended period of time. Water damage from the flash floods coming into contact with the computer network information system equipment will cause hazardous contamination to human contact in the form of mold spores and mildew[1].

Earthquake: The movement of the earth's crust causing the normally still ground to move. The earth's movement in densely populated areas of people and building will cause physical damage to building housing information system equipment. The physical damage could range from fractural stress in the form of cracks to the building's structure to the total collapse of the building. Depending on the buildings condition, the information system could be rendered temporarily inoperable from the lack of electrical power, structural compromise for ingress and egress to the organization's building to having computer equipment buried and crushed under a pile of building rubble[1].

Fire: Meant in this context would be the structural damage to the building that housed the information system of the organization. A fire can happen from a direct lightning strike to the building housing the organization's information system. The resulting fire could and most probably will encompass smoke and water damage from the sprinkler system and/or fire fighters [1].

Tornados: A rotating column of air usually accompanied by a funnel-shaped downward extension of a cumulonimbus cloud and having a vortex several hundred of yards in diameter whirling destructively at speeds of up to 300 miles per hour. The

devastating effect that a tornado can have to a building housing an information system would be catastrophic. The resulting devastation of a tornado coming in contact with the building housing the information system would make the reassembly of the information system network a next to an impossible task. The past history of the destruction of tornados has provided evidence that material from a building wreckage has been found several miles away from the building's original location [1].

This list does not include or attempt to include all of the possible acts of the force of nature. One cannot ignore the fact that in a majority of different parts of the world there are different forms of the force of nature that can and will happen, such as landslide or mudslide, tsunami, and hurricane. The best way to mitigate the force of nature or the act of God is through some form of casualty insurance and/or business interruption insurance.

Deviations in the quality of service

Deviations in the quality of service: The loss of electrical power, loss access to the Internet Service Provider (ISP), loss of service vendors, etc. can interrupt network usage and access. For example, the utility company providing electrical power can suffer from power shortage resulting in brown outs or no power supplied through power grids. The Telephone Company (Telco) can have a loss of phone service that will interrupt service to ISP for Internet access. Or, a virus or worm can attack the Domain Name Servers (DNS) that can interrupt Internet access for an indefinite amount of time [1].

Omega's management concern with the deviations in the quality of service is the Internet interruption to online banking and the interruption of uploading product pricing to the remote host. Also, their concern is the loss of electrical power to the building that could cause the loss of data and recovery of data. For example, if the building suddenly lost power and caused a hard drive head crash on an important sector or section of the disk drive, how would the data be recovered?

Technical hardware failures or errors

Technical hardware failures or errors: Computer operations be interrupted or compromised due to computer components operating failures. Interruptions can include the central processor unit (CPU) failing to perform program instructions or fail to function. There are crystal oscillators on the system board (motherboard) in the computer that could start varying their clock cycles to inhibit overall computer functionality of the computer, corrupt data transfer on the computer input bus and output bus to and from memory, hard disk drives, and the central processing unit. Faulty keyboards can effect the keyed input to store erroneous data in program fields [1].

Omega's management concern with the technical hardware failures or errors as equating to computer down time in period of a day or days. The concern ranges from the host computers to the file server.

Technological software failures or errors

Technological software failures or errors: Software programs that are not completely free from errors or failures. These software programs can be commercial software applications that have been marketed with know problems (known as bugs) or known errors that can happen under certain circumstances. Or, technological software failures or errors can be induced by hardware memory failures to the software running on the faulty machine. In this case the software failures are local only to the failing host computer [1]

.

Omega's management view of the technological software failures or errors as having the same impact as the technical hardware failure or errors.

Technical obsolescence

Technical obsolescence: The equipment and or software used currently is not being support be equipment manufacturers or software providers. Running the risk of keeping equipment to pass the point to when a hardware failure happens that the needed replacement part cannot be obtained. Also, software obsolescence would be keeping pass the point where support for the product cannot be obtained[1].

Minimum-Maximum Form

To gain an insight on how Omega's management viewed each of the threat categories, they were presented the minimum-maximum form asking for their input as to how they saw the categories and to quantify the risk threats. The management was asked to considered the least cost of the threat (minimum) and the most significant cost of the threat (maximum) and it was optional for them to calculate the average (avg.).

The concept of the form is to involve management in the security process and to enlighten management of the broadness and depth of the threats. With management's input of the possible dollar values that the threats could cost the organization, the quantitative process is provided with management's dollar value to the quantitative risk assessment. In other words, the dollar amounts provided were not guess work of a technical person or project manager, but from the management's perspective. The form will provide a vehicle for management to express their concerns in the listed threat categories that they would like to be included in the risk assessment. The form offers the flexibility for management to remove categories that they did not feel relevant to the size or the nature of their business. For example, an organization may not produce any intellectual property to be include in their risk assessment. Or, the organization may not have a web server that would face a deliberate acts of information extortion or Denial of Service, such as Omega. The minimum-maximum form is flexible enough to used for small to medium organizations.

Minimum-Maximum form.

1. Acts of human error or Failure Min:$_____ Max: $ _____ Avg.:$ _____
(Accidents, employee mistakes)

Min. failure description:
Max. failure description:

2. Compromises to intellectual property: Min$_____ Max.$_____ Avg.$_____
(Piracy, copyright infringement)

Min. failure description:
Max. failure description:

3. Deliberate acts of espionage or trespass: Min.$_____ Max. $_____ Avg.:$_____
(Unauthorized access and/or data collection)

Min. failure description:
Max. failure description:

4. Deliberate acts of information extortion. Min.$_____ Max:_____ Avg.$_____
(Blackmail or information disclosure)

Min. failure description:
Max. failure description:

5. Deliberate acts of sabotage or vandalism Min. $_____ Max. _____ Avg. $_____
(Destruction of systems information)

Min. failure description:
Max failure description:

6. Deliberate acts of theft Min. $_____ Max $_____ Avg. $_____
(Illegal confiscation of equipment or information)

Min. failure description:
Max. failure description:

7. Deliberate software attacks. Min. $_____ Max. $_____ Avg.$_____
(Viruses, worms, macros, denial-of-service)

Min. failure description:
Max failure description:

8. Forces of nature Min.$_____ Max.$_____ Avg.$_____
(Fire, flood, earthquake, lightning)

Min. failure description:
Max failure description:

9. Deviation in quality of service Min.$_____ Max.$_____ Avg.$_____
(ISP, power, or WAN service issues from service)

Min. failure description:
Max. failure description:

10. Technical hardware failures or errors Min$_____ Max.$_____ Avg.$_____
(Equipment failure)

Min. failure description:
Max. failure description:

11. Technical software failures or errors Min.$_____ Max $_____ Avg.$_____
(Bugs, code problems, unknown, loopholes)

Min. failure description:
Max failure description:

12. Technical obsolescence Min. $_____ Max. $_____ Avg. $_____
(Antiquated or outdated technologies)

Min. failure description:
Max. failure description:

End of Minimum-Maximum Form

As you can see, the minimum-maximum form is a simple and clean form. The form is designed to be user friendly to encourage executives to complete the form. Listing the threats in the heading with a simple example to represent the threat category provides a guideline about the particular threat that we are looking to mitigate. The minimum and maximum description fields allow the executive to express the organization's concern and the associated financial loss should the threat occur.

The completed form will serve as the following:

- The dollar values on the form will serve as input to the Risk Management Tool software program developed to assist in quantifying each risk category.
- The form will serve as an aid in developing the recommendations for mitigating the risk threats.
- As a deliverable as stated in the Statement of Work.

Risk Management Tool

The Risk Management Tool was developed to assist in providing a visual aid in presenting the quantifying data to management and to automate the ranking order that should be address in mitigating the risk threats. Figure 2 is the program flow for the Risk Management Tool.

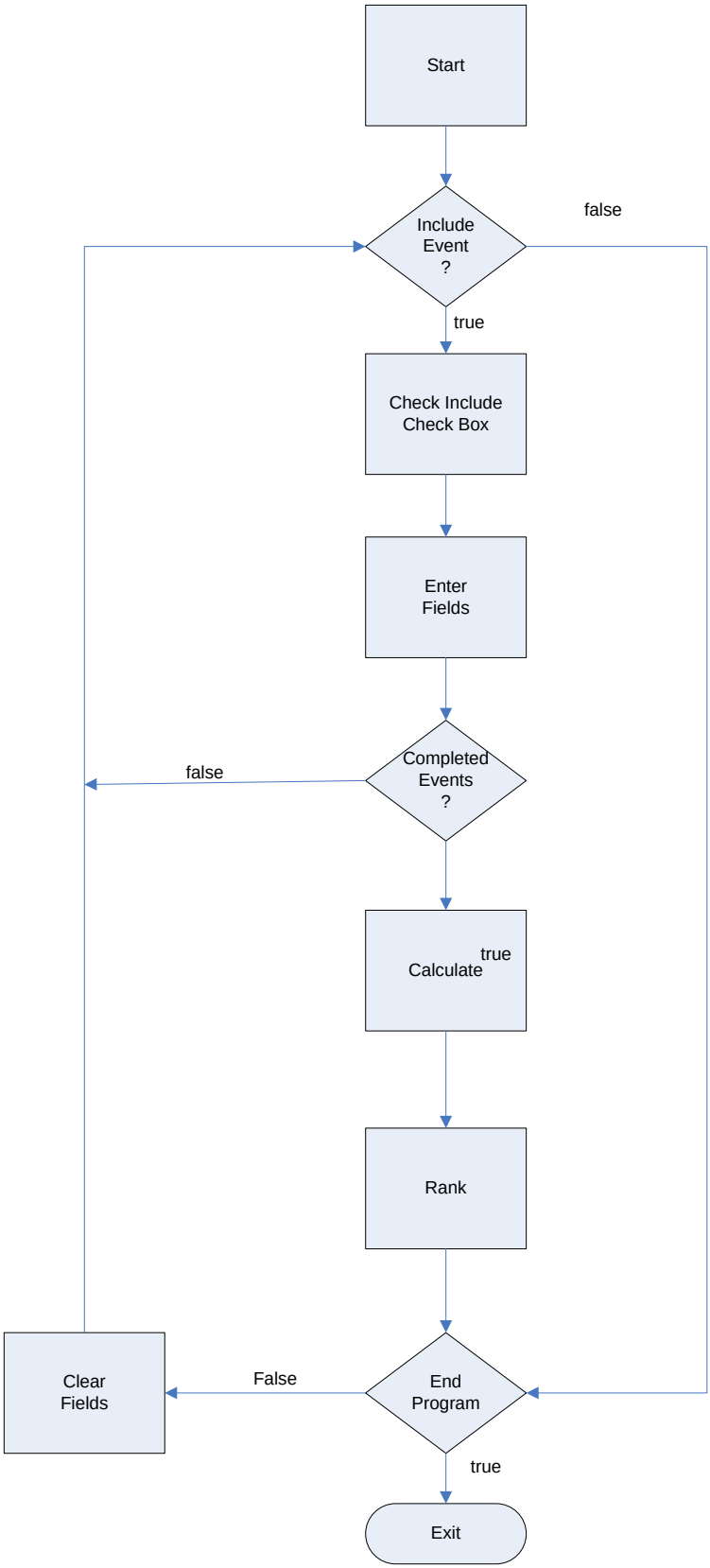

Figure 2. Risk Management Program Flow

The concept of the Risk Management Tool, as mentioned, is to capture the view of management's concept of the severity of the threat of the risk, that is, how severe do they think the possibility of the risk can be. The Risk Management Tool will use the dollar amounts entered on the Minimum-Maximum form and then calculate the average of the dollar amount for each risk category. Then the risk categories can be ranked to determine how soon action should be taken to mitigate the risk.

The Risk Management Tool headings consist of Event, Include, Severity of Outcome, Duration of Impact, Probability of and Incident, Minimum Cost of Loss, Maximum Cost of Loss, Average Cost of Loss, Expected Loss, and Rank of Loss.

The Event column list the 12 categories of the risk threats list in the Minimum-Maximum form and the risk that we want to mitigate.

The Include column is a check box that will include that risk threat that the organization's management would like to have analyzed.

The Severity of Outcome has three values of high, medium, or low. The High rating should represent to management that if the threat happens that is a catastrophic event. Meaning it is business ending event and the threat should not be taken lightly.

The Medium rating given by management should be less than catastrophic, but warrants a quick response to avoid moving to the catastrophic state.

The Low rating by management should represent that the risk can be tolerated for a period of time, if the risk is not mitigated.

The Duration of Impact is the management's estimation of how long it would take to discover and recover from a threat in the included category. The Duration of Impact has values ranging from 1 day to 180 days. Depending on the threat, it could take up to 180 days to even discover that a threat has happen. For example, a Trojan horse could reside on the file server and slowly infect the workstations as they access the infected directory. A packet sniffer could be planted on an unsuspecting workstation and quietly capture packets that are moving across the network to be later uploaded to a hacker's computer.

A malicious virus that is designed to destroy data on hard drives will be discovered immediately.

Therefore, in deciding the Duration of Impact, management must take into account the minimum period and the maximum period that the threat will last to come up with a balance or average time that the duration of the threat may last.

The Probability of an Incident is a percentage of when the risk threat will happen at any given time. The percentage range from 5 percent to 50 percent in increments of 5 percent. This percentage will and can vary. The variance will be determined by the

organization's industry category. For example, consider the banking industry. Recently hackers have increase their attacks on the banks by using injection attacks on sql databases. "SecureWorks, a leading Managed IT Security Services Provider, announced that it has seen a dramatic increase in the number of hacker attacks attempted against its banking, credit union and utility clients in the past three months using SQL Injection (a type of Web application attack). "From January through March, we blocked anywhere from 100 to 200 SQL Injection attacks per day," said SecureWorks CTO Jon Ramsey. "As of April, we have seen that number jump from 1,000 to 4,000 to 8,000 per day," said Ramsey." [2]

The Minimum Cost of Loss is inputted here from the Minimum-Maximum form. The dollar amount entered here represents the least impact that an insider or hacker can cause in the threat category.

The Maximum Cost of Loss is inputted from the Minimum-Maximum form. The dollar amount entered here represents the maximum known impact that a successful attack can cause in the threat category.

The Average Cost of the Loss is calculated by the Risk Management Tool software program by adding the minimum cost with the maximum cost and then divided by two. The average loss can be viewed as a baseline value of the successful attack for the risk threat.

The Expected Loss field is the result of multiplying the Probability of the an Incident times the Average Loss field. This field represents the anticipated loss of dollars if nothing is done to mitigate the risk. In other words, the Expected Loss field will represent an acceptable loss for doing nothing to mitigate the risk.

The Rank of Loss is determined by the dollar amount that is established in the Risk Management Tool software program. Currently, the program considers any value less than $1,999.99 to be ranked as Low, any value greater than $2,000.00 and less the $74,999.99 to be considered Medium, and any value greater than $74,999.99 to be ranked as High..

The ranking should be intuitive. That is, the rank should reflect the dollar impact to the organization if the threat attack is successful. Now a balance has to be addressed between management's view of the attack in the column of Severity of Outcome and the dollar amount impact as indicated by the Rank field. For example, if the Rank is "High" for the threat and management's view in the Severity of Outcome is "Low," then management may want to change their view and apply the necessary resources to mitigate the risk. Figure 3 presents an example of the Risk Management Tool software application program.

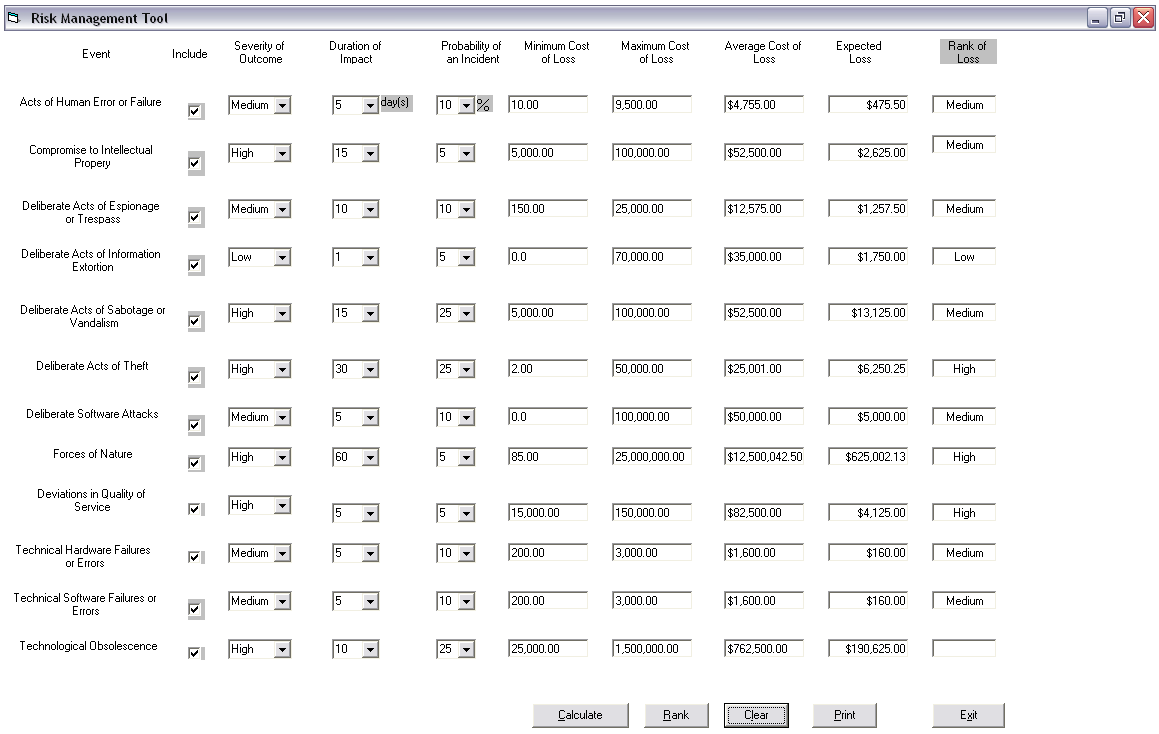

Figure 3. Risk Management Tool

The Logical Design Phase

From input from the analysis phase it is recommended that Omega develop an acceptable use policy (AUP) regarding the use of the company's computers. An acceptable use policy is a set of rules applied by the owner or manager of a network, website or large computer system to restrict the ways in which the network site or system may be used. [3].

AUP documents are written for corporations, business, universities, schools and internet service providers, website owners often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

The AUP should clearly detail what is acceptable use, when should the computers are utilized and especially, what is acceptable Internet and e-mail use.

To mitigate the software risk and hacker attacks to the organization, Omega should at a minimum, install hardware firewall appliances at each of the remote locations to provide intrusion detection system and intrusion protection system to counter Denial

of Service attacks (DoS), Distributed Denial of Service Attacks (DDoS), virus, spyware, Trojan horse, and the Hacker using malformed packets.

It has been found that at least one of the managers has disabled the software firewall on the host system to access web sites for personal use. The disabling of the software firewall provides a compromise to the host system and the network. With the implementation of the hardware configurable firewall, the company's personnel would not be able to reconfigure the firewall setting to prevent unwanted Internet access that could compromise the host workstation and the company's network.

Also, a hardware firewall should be placed that the file server. Looking at the server log, it was spotted that an invalid Internet Protocol (IP) address was attempting access the file server.

The placement of these firewalls will provide the need security protection buffer between the host systems an the attackers.

The logical in figure 4 is a representation of the recommended placement of the configurable hardware firewalls that are currently not implemented in the Omega organization.

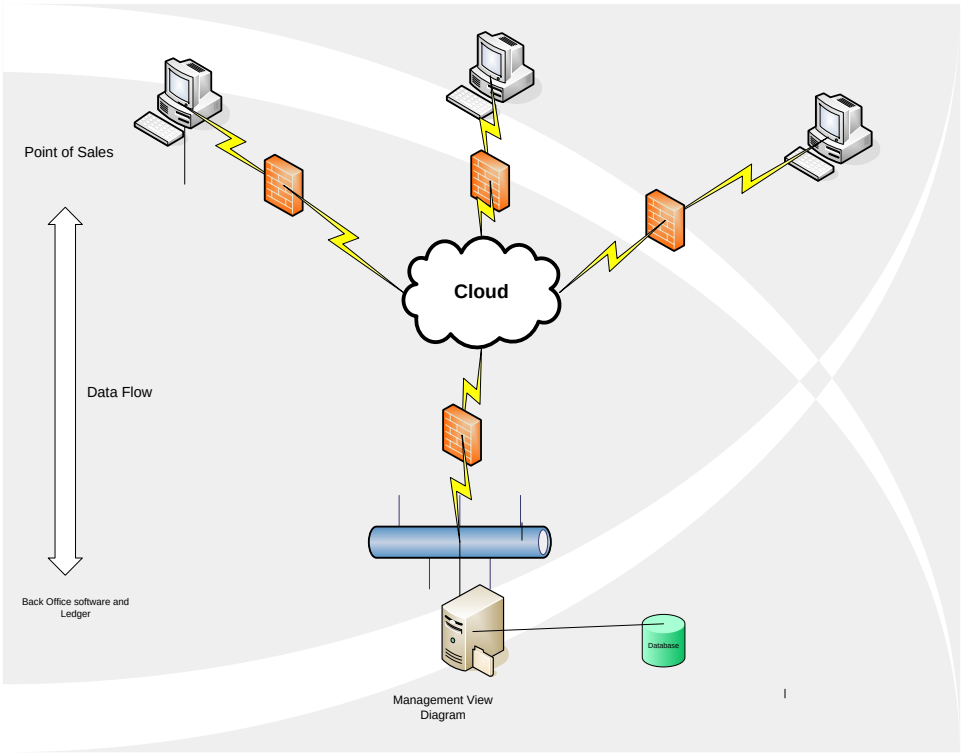

Figure 4. Logical Diagram

Continuity Planning

How will business continue in the event of a loss? It is the goal of Omega to keep the potential of a loss to the minimum or mitigated side of the Minimum-Maximum form. With the successful completion of the goal, the business operation would not be cease more than fours. The loss would be addressed through the daily backup Currently, Omega's software is backed up on a daily basis using a CD-ROM tower to be able to store software loss to the day before the loss.

Incident Response

What steps are taken when an attack occurs ? The steps that are taken when an attack occurs are the following:

- An alarm is sent to the network administrator that notifies the administrator that an intrusion actively taken place.
- The network administrator will then respond to the alarm and start checking workstation logs, file server logs, router logs, and firewall logs to determine the nature of the intrusion.
- Configure firewall to disallow access to the Internet Protocol address that is causing the intrusion attack.
- If necessary , disconnect the segment of the network that is being attacked.

Disaster Recovery

What must be done to recover information and vital systems immediately after the disastrous event? To recover information and vital systems immediately after the disastrous event would be to rebuild the file server with the current or upgraded version of the network operating system and restore system and data files using the CD-ROM backup system.

Part of Omega's disaster recovery plan is based on having the ability to have any hardware replacement of a workstation or file server completed within twenty-four hours.

If the disastrous event is from the Force of Nature, then a remote location would have to be obtained to house the organizations personnel and office equipment. The re-establishment of Internet connectivity to the current Internet Service Provider would have to occur. Since, Omega's business is conducted over the Internet to remote locations and not all operations housed under one roof, a disastrous event would temporarily cripple the business operation, but would not stop Omega from continuing business operations.

Physical Design Phase

The information security technology needed to support the blueprint outlined in the logical design is a hardware firewall that includes an intrusion detection system and

intrusion prevention system. The hardware firewall was chosen because of the ease that a user had in disabling the firewall configuration setting in the software firewall on the workstation. With the hardware firewall, the network administrator will be able to configure the firewall to block unwanted access to specific web site along with other intrusion detection and intrusion prevention systems

With the Omega's network presently installed, the addition of hardware firewalls would increase the current protection of the remote locations and the corporate network file server and the database that resides on the current server.

Creating a separate database would increase protection to the company's data files incase the network server is compromised.

The physical diagram shown in figure 5 represents the placement of the hardware firewall on Omega's network that was agreed upon.

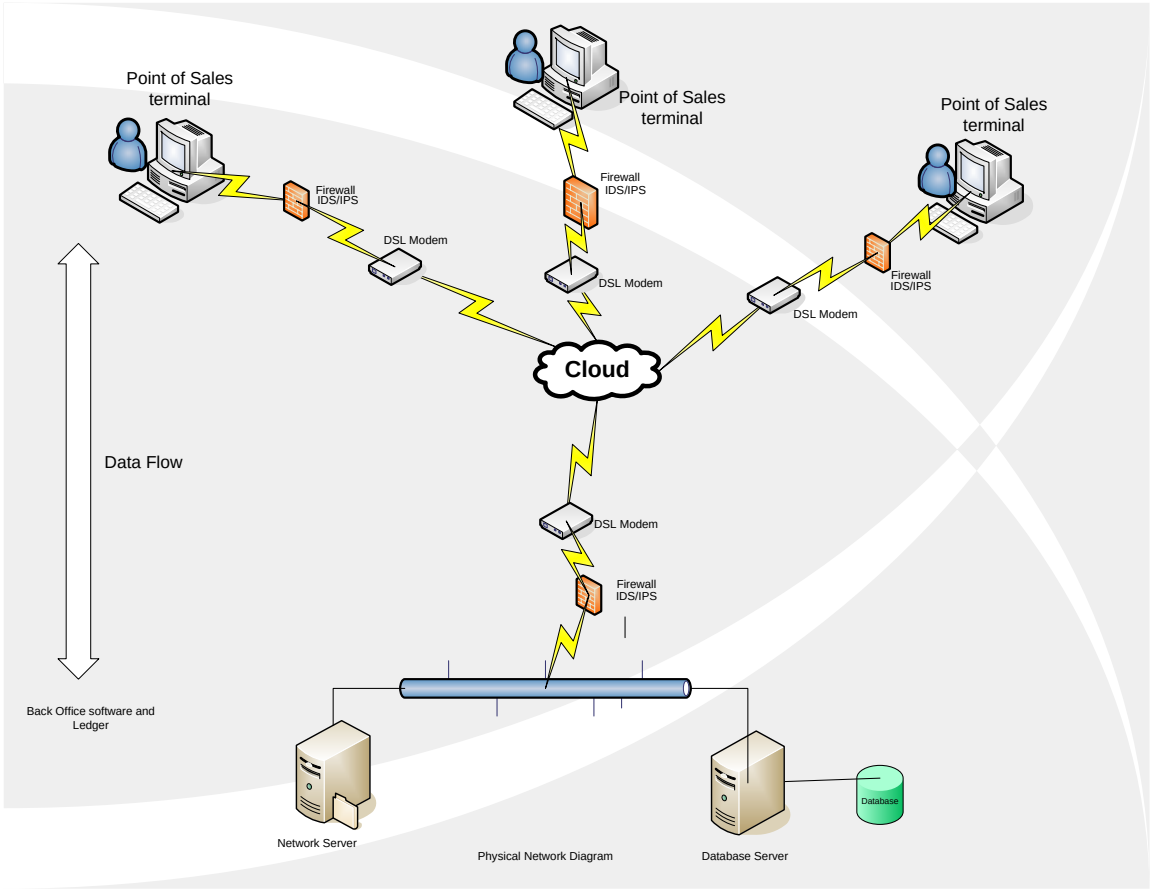

Figure 5. The Physical Diagram

Implementation Phase

At the time of this writing, the implementation phase has not been completed.

Omega is currently evaluating two inexpensive hardware fire walls for the remote location and one of three possible WatchGuard Firebox X10e X Edge e-series fire walls.

Omega is considering the NETGEAR FVS114 and the D-Link DIR 130 Firewalls for the remote locations.

The comparison table in figure 6 [4] provides a view of what is facing Omega's management decision making of which would be the best firewall for the organization. Omega's management will be strongly relying on CMass Electronics for input.

Brand	NETGEAR	D-Link

Model	FVS114	DIR-130
Cost	Sale price $59.99	$99.99
Specifications		
Type	Wired	Wired
Standard	Network: IP routing, TCP/IP, UDP, ICMP, PPPoE IP Addressing: DHCP (client and server) Routing: RIP v1, RIPv2 (Static Routing , Dynamic Routing	IEEE 802.3/3u
Throughput	Up to 11.5 Mbps WAN-t0-LAN, up to 2.1 Mbps for 3DES	
Maximum Users	LAN: Up to 253 users	
Ports	LAN ports: Four 10/100 Mbps auto-sensing, Auto Uplink, RJ45 ports. WAN Port: 10/100BASE-T Ethernet RJ-45 port to connect to any broadband modem, such as DSL or Cable	8 10/100 LAN; 1 10/100 WAN; 1 usb
Wired Speed	10/100 Mbps	10/100Mbps
Security	SPI Firewall: Stateful Packet Inspection (SPI) to prevent notorious Denial of Service (DoS) attacks, Intrusion Detection System(IDS) including logging, reporting and e-mail alerts, address, service and protocol, Web URL keyword filtering, prevent replay attack (reassembly attack), port/service blocking. Advanced features include block Java/URL/ActiveX based on extension, FTP/SMTP/RPC program filtering.	Encryption Transform: DES, 3DES, AES; XAUTH (Extended Authentication for IPSec Authentication; Firewall Security: Stateful Packet Inspection(SPI), Network Address Translation (NAT), Policy-Based User Authentication, Internal User Database (20 records) RADIUS Client
Encryption Standard	IPSec (ESP, AH), MD5, SHA-1, DES, #des, IKE, PKI, AES	
VPN	Eight dedicated VPN tunnels, Manual key and Internet Key Exchange Security Association (IKE SA) assignment with pre-shared key and RSA/DSA signatures, perfect forward secrecy (Diffe-Hellman groups 1 and 2 and Oakley support), operating modes (Main, Aggressive, Quick), fully qualified domain name (FQDN) support for dynamic IP address VPN connections.	VPN Security: VPN Tunnels: 8 (IPSec, PPTP, L2TP). IPSec LAN-to-LAN / Roaming User; PPTP/L2TP Pass-through; IPSec NAT-Traversal; DHCP over IPSec;
Dimensions	5.5" x 3.9" x 1.1"	7.5" x 4.7" x 1.2"
Weight	0.81 lbs	0.7 lbs
System Requirements	Cable, DSL, Satellite, or Wireless Broadband modem and Internet Service. Ethernet connectivity from Broadband modem. Network card for each connected PC. Network Software(e.g. Windows) Internet Explorer 5.0 or higher or Netscape 7.2 or higher	Not specified
Processor	200 Mhz 32-bit RISC	Not specified
Memory	2MB Flash, 16MB SDRAM	Not specified

Figure 6

Omega is considering the WatchGuard Firebox X10e X Edge e-Series appliance firewall for file server external protection and data encryption.

Summary

Using the Security System Development Life Cycle methodology to secure an existing Internet connected computer network proved to be very a good choice in determining weaknesses and vulnerabilities in the network that needed to mitigated. In the investigation phase the CMASS, Inc. discovered how Omega's management viewed the network and was concerned with the vulnerability of the sales transactions from the point-of-sales terminals to the central database and the updates sent to the point-of-sales terminals. We also found out that Omega did not have enforce an acceptable use policy to protect the company against any potential law suits.

In the Analysis Phase, the CMASS, Inc. team saw that an insider could reconfigure the host software fire wall to traverse the Internet for personal usage. The risk management task was to address the 12 categories using the newly created Minimum-Maximum form and saw that Omega has made preparations for most of the threats that the organization would face and using the Risk Management Tool to assist in quantifying the cost of not mitigating the threat.

In the Logical Design Phase, we showed in the design that the addition of hardware firewalls at the remote locations and at the corporate file server would help prevent threats from Denial of Service, intrusion detection, and intrusion prevention. Omega will relay on the anti-virus software to detect and clean any malware, such as a virus, Trojan horse, spy-ware, phishing, and ad-ware.

In the Physical Design Phase, the CMASS, Inc. team showed where the firewall should be placed and determined the requirements for compatible connections to the current network. We determined that the firewall should have DSL connectivity and Ethernet 10/100 Mbps speed with at least 1 RJ45 port. The most important feature of the firewall would be that the insiders cannot reconfigure the firewall once the network administrator sets the configuration. It would be most imperative that the network administrator keep the firewall software configuration program in a secure location.

In the Implementation phase, the brand of firewall was not determined at the time of this writing. However, Omega is considering one of two brands for their purchase.

For the maintenance of the security of the network, Omega has selected to extend it's relationship with CMASS Electronics, Inc. for the continued hardware, software, and network security.

Reference:

1. Whitman, Michael E and Mattord, Herbert J.; *Principles of Information Security*; Second edition; Thomson Learning, Inc.; 2005

2. "Increase in SQL Injection Hacker Attacks against Banks and Credit Unions"; Computer Security. Retrieved May 5, 2009 http://www.techtalkz.com/computer-security/2221-increase-sql-injection-hacker-attacks-against-banks-credit-unions.html

3. "ISI's Acceptable Use Policy." http://wos.isitrial.com/policy/Policy.htm. Retrieved April 25,2009

4. Purcell, James. "Building Security into the System Development Life Cycle" http://www.giac.org/resources/whitepaper/application/442.pdf

5 "Firewalls" Retrieved May 1, 2009 http://www.newegg.com/Store/SubCategory.aspx?SubCategory=529&name=Firewalls

6. Scarfone, Karen, Souppaya, Murugiah, Cody, Amanda, Orebaugh, Angela. "Technical Guide to Information Security Testing and Assessment. Special Publication 800-115 National Institute of Standards and Technology. Retrieved April 12,2009. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

7. Grance,Tim, Hash, Joan, Stevens, Marc. "Security Considerations in the Information System Development Life Cycle". Special Publications 800-64 National Institute of Standards and Technology. Retrieved April 12,2009. http://www.iwar.org.uk/comsec/resources/security-life-cycle/sp800-64.pdf

8. Information Resources Management. "The Department of Justice Systems Development Life Cycle Guidance Document. January 2003. Retrieved April 11, 2009. http://www.usdoj.gov/jmd/irm/lifecycle/table.htm

9. Young, David, "Computer Security Basics". Cytoclonal Pharamaceutics, Inc. Retrieved May 1, 2009 http://www.ccl.net/cca/documents/dyoung/topics-orig/security1.html

10. Virginia's Community College Community Colleges Information Technology, Technology Standard, "IT Systems Security – IT System Development Life Cycle Security ", Version 1.0 Retrieval April 30,2009. http://system.vccs.edu/its/InformationSecurityProgram/ITSystemDevelopmentLifeCycleSecurity.htm