Abstract

Small Business Information Security

by

John Edwards Vail III

April, 2012

Director of Thesis: Dr. Erol Ozan

Major Department: Department of Technology Systems

Small businesses account for over fifty percent of the Gross National Product of the U.S. economy; and the security of their information systems is critical for them to operate, compete, and remain profitable. While many security studies have been conducted and reported on enterprise scale organizations, similar research on small businesses in the U.S. is limited. One small business was evaluated by an information security audit to determine if its information resources and network were adequately secure, and will be used as a test case to identify an approach a typical small business may take to secure their networks and data to avoid unnecessary liability exposure. By examining the specific risk factors in this case study, the author believes parallels can be drawn by other small businesses as a starting point for examining their own risk factors. Additionally this study provides a series of proposed mitigation processes to improve the small businesses' network security that can be adopted by other small businesses in like circumstances. The mitigation processes are specifically tailored to the small business industry itself, as opposed to a larger organization that has a greater exposure to risk vulnerability and that also has larger asset pools from which to secure their networks.

The method utilized for this research was qualitative in nature, using a form of Participatory Action Research (PAR). This approach was most appropriate in that it allows the researcher to act in partnership with the small business to attempt to affect social change that will help in securing the small business's information resources. An information security audit was performed on a small business to identify actual and potential threats, and an electronic questionnaire was distributed to the employees to gauge their individual perspectives of the clarity and comprehensibility of the business's security policy, the consequences of violations to the company's policy, how well the company's policy is disseminated and tracked for compliance, and if they have knowledge of steps to be taken in response to an incident or disaster. There were four objectives of this study. The first objective was to evaluate a small business's information security posture. The second objective was to determine if the small business had experienced any information technology security incidents. The third objective was to evaluate whether the incidents were caused by a lack of a policy, standard or procedure; an ineffective policy, standard or procedure; a lack of training and education; or a reluctance to enforce or monitor adherence to established policy, standards, or procedures. And the fourth objective was to recommend to the small business any changes or additions that would reduce the small business’s exposure to information security threats, risks and vulnerabilities through effective information security risk management.

Small Business Information Security

A Thesis

Presented To the Faculty of the Department of Technology Systems

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Technology Systems

by

John Edwards Vail III

March 30, 2012

Small Business Information Security

by

John Edwards Vail III

APPROVED BY:

DIRECTOR OF DISSERTATION/THESIS:

_____

Erol Ozan, PhD

COMMITTEE MEMBER:

_____

Tijjani Mohammed, PhD

COMMITTEE MEMBER:

_____

Te-Shun Chou, PhD

CHAIR OF THE DEPARTMENT OF TECHNOLOGY SYSTEMS:

_____

Tijjani Mohammed, PhD

DEAN OF THE GRADUATE SCHOOL:

_____

Paul J. Gemperline, PhD

TABLE OF CONTENTS

List of Figures

List of Tables

CHAPTER 1: INTRODUCTION

Companies and organizations struggle with information resource security and integrity. Information security policies range from non-existent to comprehensive. Even the organizations with comprehensive security policies experience security incidents. Additionally, businesses have legislative requirements that must be met; dependent upon the type of business the organization conducts. In today's interconnected communication landscape, it is not a matter of if an organization will be hacked but when. Information systems assets, such as networks, computers, servers, software systems, and confidential and proprietary data, must be safe-guarded from potentially destructive forces. Treating information security as an isolated technical concern is outdated. Securing information resources must be seen as a business problem, and addressed as such. "Delegating security to technologists also ignores fundamental questions that only business managers can answer. Not all of a company's varied information assets have equal value" (McKinsey & Company, Inc., 2002). Security must be viewed as an "essential mission need, equivalent to core business operational functions" (Westby & Allen, 2007). It must move "from an ad hoc, reactive approach to one that is systematic, planned, managed, and measured, or to any point in between that is suited to the balance of the organization's security needs and strategic drivers" (Caralli, 2004).

Most businesses acknowledge the need to protect their most valuable commodity – information. Just putting up a firewall or installing anti-virus is not enough. There needs to be a comprehensive framework or program in place from which a company, organization, institution or entity can begin securing information. A well designed program can be the framework from which any entity, regardless of their size or stature, may utilize to begin securing their information systems. It is important to have in place a business continuity plan in the event of

disruption. A comprehensive set of strategies, that include a range of related technical and non-technical measures, will guide the strategic deployment of a consistent and multilayered information security environment. This program must also be tied to and guided by the organization's strategic goals.

"There is no single silver bullet for Information Security – this means that Information Security can only be successfully and effectively implemented in a company if all the constituting dimensions are implemented in a holistic and comprehensive way" (von Solms, 2009). Protection of the company's information resources will be most effective when it is, "…systemic – woven into the very culture and fabric of organizational behaviors and actions" (Westby & Allen, 2007).

> To achieve and sustain an adequate level of security that directly supports the mission of the organization, senior management must shift their point of view (or frame of reference) and that of their organization from an information-technology-based, security-centric, technology-solution perspective to an enterprise-based, risk management, organizational continuity and resilience perspective. This requires moving well beyond ad hoc, reactive approaches to security (lacking process and procedure, and dependent on individual heroics) to approaches that are process-centered, strategic, and adaptive (Caralli, 2004).

The world is becoming increasingly interconnected, and as such the security considerations associated with information systems are becoming more complex (Ryan, 2000). Machines compromised at one location can be used to compromise machines at other locations. This can be done to mask the identity of the perpetrator, and/or done to create armies of zombie

computers that attack critical computers and networks creating denial of service, among other detrimental activities. A lack of proper information security practices at one business can have a worldwide impact.

Methodology

This thesis study conducted a security audit of a small business in order to evaluate that business's information security posture and recommended changes or additions that would reduce the business's exposure to information security threats, risks and vulnerabilities through effective information security risk management. In conjunction with the security audit, this study investigated the information technology security incidents that had occurred, and examined them to determine if causation was due to a lack of a policy, standard or procedure; an ineffective policy, standard or procedure; a lack of training and education; or a reluctance to enforce or monitor adherence to established policy, standards, or procedures. The research question this study seeks to answer is, "Has one small business in the healthcare industry adequately secured their information resources?"

Research Objectives

A form of Participatory Action Research (PAR) was chosen as the type of research design for this study. This approach seemed most appropriate for the qualitative research this thesis study is attempting, in that it allows the researcher to act in partnership with the small business to attempt to affect social change that will help in securing the small business's information resources.

The objectives of the study were to: (1) evaluate a small business's information security posture; (2) determine if the small business had experienced any information technology security

incidents; (3) evaluate whether the incidents were caused by a lack of a policy, standard or procedure; an ineffective policy, standard or procedure; a lack of training and education; or a reluctance to enforce or monitor adherence to established policy, standards, or procedures; and, (4) recommend to the small business any changes or additions that would reduce the small business's exposure to information security threats, risks and vulnerabilities through effective information security risk management.

Human subjects participating in the research were the owner of the small business and his employees. The participation was limited to anonymously answering an electronic survey regarding the information security policy at the small business. Consent to participate was accomplished through a statement at the beginning of the survey (Appendix A). Data was gathered from the information technology systems utilized by the small business relevant to the security of the information technology system. The study excluded all patient medical data.

The research process involved approaching businesses and organizations and inquiring if they were willing to participate in this research study. One small business, involved in Healthcare, agreed to participate, and an Audit Charter (Appendix C) was used to define the scope and responsibilities of the participation and evaluation. A security audit was conducted and data was collected pertaining to information technology security incidents using antivirus log files, reports generated by Microsoft Baseline Security Analyzer (MBSA), and an electronic survey.

The electronic survey was disseminated to the small business owner and employees to determine: (1) their individual perspectives of the clarity and comprehensibility of the business's security policy, (2) the consequences of violations to the company's policy, (3) how well the

company's policy was disseminated and tracked for compliance, and (4) if they had specific knowledge of steps to be taken in response to an incident or disaster. The results of the survey, along with the data collected pertaining to network or computer incidents were used to hypothesize whether those incidents could have been prevented through a more effective written policy, better enforcement, or better education. The questions utilized in the electronic survey were:

- Is your company's security policy written in clear and concise language so that it is easily understandable?
- Do you feel that your company's security policies are comprehensive?
- Do you feel that your companies security policies provide due diligence? That is, does your business make sure that information security risks are known and managed?
- Is there formal training and education pertaining to your security policies?
- If there is no formal policy and guideline training, how does your organization make you aware of its security policy?
- Is there a mechanism in place to prove an employee has read and understands the information security policy?
- Is compliance with the information security policy monitored?
- Are there clear consequences if the information security policy is violated?

- Do you feel everyone is treated the same when it comes to enforcement of the information security policy?
- How likely are you to be disciplined if you violate the information security policy?
- Do you have an Incident Response plan?
- Is it clear to whom you contact when there is a security incident or perceived security incident?
- Is it clear what steps you take when there is a security incident or perceived security incident?
- Are you aware of a business continuity and/or disaster recovery plan? That is, if a catastrophic event occurred do you have a plan in place to continue business operations?

Significance of the Study

Small businesses account for over fifty percent of the Gross National Product of the U.S. economy; and the security of their information systems is critical for them to operate, compete, and remain profitable. While many security studies have been conducted and reported on enterprise scale organizations, similar research on small businesses in the U.S. is limited creating a gap in research. Conducting an information security study on one small business is significant in a few ways. One way it is significant is that the researcher can act in partnership with the small business to affect a social change that will help the small business secure their information systems and data. This study will also contribute to the baseline understanding of information security practices used by the business community, specifically how one small business secures

their information systems. If successful, this study can be used as a test case for an approach that a typical small business may take to secure their networks and data to avoid unnecessary liability exposure. By examining the specific risk factors in this case study the author believes parallels can be drawn by other small businesses as a starting point for examining their own risk factors. Additionally, this study provides a series of proposed mitigation processes to improve the small businesses' network security that can be adopted by other small businesses in like circumstances and that are specifically tailored to the small business industry itself, as opposed to being tailored to a larger organization that has a greater exposure to risk vulnerability and that also has larger asset pools from which to secure their networks.

The data identified by the information security audit and electronic survey generated by this study contributes to the theoretical understanding of how information security must be engaged by management science as well as from a scientific research standpoint. Understanding how and if small businesses use information security policies, technologies, and tools will provide insights as to where further research activities are needed.

Thesis Organization

This Thesis is organized into five chapters. The first chapter contains the Introduction, which identifies the problem and provides background and the motivation for the study conducted. The first chapter describes the methodology, research objectives, survey questions, and the significance of the study. The second chapter is a review of the literature relevant to this study. The third chapter includes the small business's network diagram, and details the risks identified by the information security audit conducted and the results of the electronic survey. The fourth chapter explains the research analysis and recommendations to mitigate risk to

information systems. The fifth chapter explores the conclusions reached based upon the study findings and recommends avenues for further research.

CHAPTER 2: REVIEW OF THE LITERATURE

Most security models available are designed for large organizations and do not adequately address the needs of a small business (Bokharee, 1993). Ryan reported that the current state of small business information security practice was less than desirable (Ryan, 2000). Kotulic & Clark admitted that despite their best efforts they failed to achieve an acceptable response rate (Kotulic & Clark, 2003). Attempting to elicit information security data from organizations is seen as intrusive and there is a general mistrust of people attempting to gain insights as to an organization's information security (Kotulic & Clark, 2003). Keller, et al, took the advice of Kotulica and Clark that mass mailings would not generate an acceptable response rate; so they found eighteen (18) small businesses in the Midwest whose network administrators, or other person accepting the role of securing their information systems, that agreed to be interviewed. There is value to their study in that the researchers are trying to increase information security awareness in small businesses, and they do wish for their study to be used to create a survey instrument to collect data from a wider variety and larger number of small companies – which would be of considerable value. The problem therein was that as the authors observe that their data reflects only 22.2% of the companies interviewed reported any security incidents, while a Computer Security Institute survey from the previous year stated that 47% of their respondents had experienced at least one incident that year. Keller, et al surmised, "[e]ither all of the small businesses interviewed were extremely lucky, or the intrusions went unnoticed (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)." Gupta & Hammond did use a questionnaire that was mailed in their research conducted in 2004, reporting a response rate of 13.8%. They also reported that less than 50% of the respondents have any type of information security or computer use policy in place, and only 19% reported experiencing a security breach

the previous year (Gupta & Hammond, 2005). To insure an accurate reflection of the number of small businesses that have experienced a security incident within the past year, physical information security audits, as opposed to interviews or mailed questionnaires, should be conducted. This study experienced a similar situation in that at the beginning the small business agreeing to the study stated that they were willing to participate but had not experienced any incidents within the past year – something the security audit found *not* to be the case.

Spears and Barki suggest that engaged end users could be an important resource for information security because they have the business knowledge needed to implement more effective security measures (Spears & Barki, 2010). Pritchard reports a rising awareness among small businesses of information security threats and that they are more likely to monitor and report on these threats (Prichard, 2010). Hayes mentions why small businesses are at risk, and even mentions some approaches to addressing the risks and mitigating the risks that are best practices. However, the article does not specify what it is the small business needs to protect, and it also does not mention the frameworks already in place which require businesses to follow in order to protect their data and/or networks. Essentially, Hayes only notes that small businesses are less likely to have standards and regulations enforced.

The National Institute of Standards and Technology has over 140 publications related to computer security available at their Computer Security Resource Center online (National Institute of Standards and Technology, 2011). One of those, by Kissel, is targeted to small businesses and is a free resource for small businesses that want to secure their networks (Kissel, 2009). Microsoft also has available on the web, "Security Guide for the Small Business," which is another great resource for small businesses that want to secure their computers and networks (Microsoft, 2005).

Information Security, despite all the research and related publications, still seems to be problematic for businesses, organizations, and governments. According to the CSI Computer Crime and Security Survey of 2009, 64% of the respondents reported malware infection, 42 % reported laptop or mobile hardware theft or loss, 23% reported bots or zombies within the organization, 34% reported being fraudulently represented as senders of phishing attacks, 29% reported Denial of Service (DoS), and the list goes on (Peters, 2009 CSI Computer Crime and Security Survey, 2009). Small businesses represent 49.6% of U.S. private sector jobs (Small Business Profile, 2011), and produce close to 50% of the U.S.'s Gross National Product (GNP) (Small Business Information Security: The Fundamentals, 2009)- which makes the continued success of these small businesses critical to the financial well-being of our nation. It is imperative that these small businesses secure their information technology.

CHAPTER 3: SMALL BUSINESS AUDIT & ASSESSMENT OF DATA FINDING

A Security Audit was conducted on a small healthcare business. The purpose was to examine, evaluate, and report on information technology (IT) applications, related systems, operations, processes, and practices. The goal was to insure they provided reasonable assurance that security controls would: safeguard information assets and protect privacy; preserve the integrity and reliability of data; function as intended to achieve the entity's objectives; and comply with established and/or relevant standards, policy, and regulations. The outcome sought was to proactively detect vulnerabilities in elements of the small businesses information systems and/or networks before those vulnerabilities were exploited; to analyze the detected vulnerabilities to assess their potential impact on the security posture of the system/network element in which the vulnerabilities were found; and to quantify the level of risk that impact posed on the overall system/network.

The audit efforts were focused on areas presenting the highest degree of risk, as well as on those areas where risk mitigation would provide the greatest potential benefit. A risk assessment was conducted, and the system was documented. The system documentation provided a description of the system and the data it handles, as computing assets used to fulfill the organization's business mission. This documentation established a framework for subsequent risk assessment phases. Boundaries for the set of components that constitute the information system were established. The information system was defined as a group of computing and supporting components that share a business function, under common ownership and management. Figure 1 shows the network diagram generated from this documentation. A System Purpose and Description was conducted to identify the assets covered by the Risk Assessment,

provide a brief description of the function and purpose of the system and the organizational business processes it supported, including functions and processing of data.

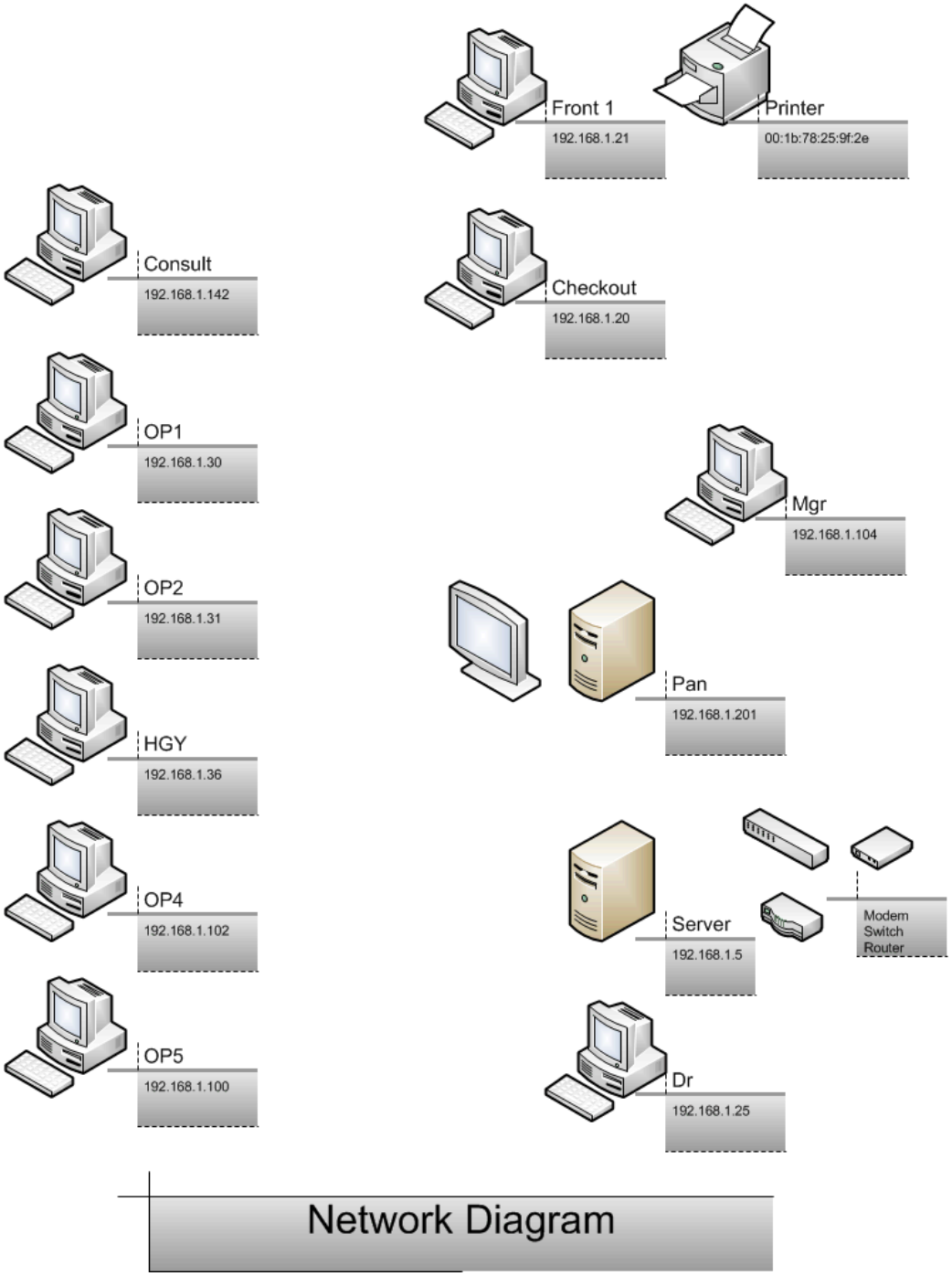

Figure 1. Network Diagram

The system's security level was documented and reported to the business owner. Documentation was of the information handled by the system and its sensitivity, and the overall system security level. This element includes a general description of the information, the information's sensitivity, and system criticality. It includes requirements for confidentiality, integrity, availability, auditability and accountability as dictated by the information security policy. In this case there is no comprehensive information security policy, so a proposed policy was included in the report, whose example was included earlier. Table 1 defines the potential impact levels. Table 2 shows the security levels of the different categories.

Table 1

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and

Potential Impact	Definitions
	duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 1. Potential Impact Level Definitions

The report accessed and reported on the controls that were currently being utilized. Management and technical controls were being used. There was a semblance of managerial control in that Section 3.3 of the Employee Handbook that did address use of company property, including computers and the internet. Technical Controls were also in place: passwords were required to access the software used to input and access patient data; and individual computers had antivirus software installed.

Table 2

Information Security Levels and Overall System Security Level	
Information Category	Debit/credit capture. Handled by third party, but dependent upon internet access.
Information Security Level	Medium.
Impact	Can have moderate impact if availability (internet) is not accessible. Will have a high impact if integrity is compromised.
Information Category	Banking deposits
Information Security Level	Low – Computer used to digitally deposit is infected with Win32 Cryptor

Information Security Levels and Overall System Security Level	
Impact	Can be high impact if external parties gain access to banking information.
Information Category	Patient Data
Information Security Level	Medium
Impact	Moderate impact if compromised
Information Category	Hardware: PC's, server, modem, router, switch
Information Security Level	Medium
Impact	Moderate impact
Overall System Security Level	Medium

Table 2. Security Levels of the Categories

Risk Identification

Each computer in the small business audited had Microsoft Baseline Security Analyzer installed, and then the analyzer was run to identify potential vulnerabilities. All twelve (12) computers returned that they were at severe risk due to one or more critical check failures. Nine (9) computers were identified as missing two security updates and seven (7) were identified as

not having all hard drives using the NT file system. The small business's server, arguably the most important computer in the office, had one hundred-twelve (112) Windows security updates, five (5) Exchange security updates, and one (1) SQL Server security update missing. Other vulnerabilities identified by Microsoft's Baseline Security Analyzer included Microsoft Office Suite Service Pack 3 (SP3) missing on one computer, the latest service pack not being loaded on one computer, the automatic update feature not being installed on one computer, and permissions on the SQL Server and/or MSDE installation folders not being set properly on two computers.

The information security audit discovered usernames and passwords taped to monitors and that antivirus signatures were not up to date on all computers. The computer used to make online banking deposits was found to be infected with Win32 Cryptor and two (2) Trojan horses, Agent3.ALJE and downloader.generic12.PIC. One registry key, two registry values, three registry data items, three folders, and one hundred twenty-four files were found to be infected.

Survey Results

A survey containing twelve (12) questions was made available to the employees and owner of the small business audited for information security threats and vulnerabilities. All respondents (100%) believed that (1) the information security policy was written in clear and concise language so that it was easily understandable, (2) there was no formal education pertaining to the information security policies, (3) and were aware of a business continuity and/or disaster recovery plan. Three quarters of the respondents (75%) believed (1) that there was a mechanism in place to prove an employee has read and understands the information security policy, (2) there were clear consequences if the information security policy is violated, (3) the information security policies were comprehensive, (4) the information security policies did not provide due diligence, (5) were unsure if compliance with the information security policy

is monitored, (6) were unsure of an incident response plan, and (7) were not clear what steps to take when there is an information security incident or perceived information security incident. Half of the respondents (50%) believed (1) everyone would be treated the same when it comes to enforcement of the information security policy, (2) thought it was somewhat likely they would be disciplined if they violate the information security policy, and (3) it was clear to whom they contact when there was an information security incident or perceived information security incident. One quarter of the respondents (25%) believed (1) compliance with the information security policy is not monitored, (2) there is not an incident response plan, and (3) it was unlikely or somewhat unlikely that they would be disciplined if they violate the information security policy.

CHAPTER 4 RESEARCH ANALYSIS & RECOMMENDATIONS

Companies and organizations struggle with information resource security and integrity. Information security policies range from non-existent to comprehensive. Even the organizations with comprehensive security policies experience incidents. Businesses also have legislative requirements that must be met; dependent upon the type of business the organization conducts. Pursuant to the proposed bill titled Personal Data Privacy and Security Act of 2005, "it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information." That bill has yet to be made into law. To protect one of small business's most valuable commodities – information – the small business needs to have a comprehensive and well thought out framework in place to begin to secure its information and the systems.

The first step in creating a framework to begin securing small businesses information and its systems is to determine the culture of the organization. "Security is a change agent, and people are generally resistant to change (Krause et al. 2010)." Understanding the company's (or organization, institution or entity's) underlying culture, then tailoring that policy to the culture, will insure a higher probability that the individuals within that organization (or company, institution or entity) will not only comply with the policy but will actively engage in the enforcement of the policy. "Knowing the policies is only half of the equation—staff need to know how they should comply, from a procedural perspective" (Rusecure 2002, as cited in von Solm & von Solm 2004). Upper management of the small business must initiate a culture that is characterized, "by an informed awareness of security risks; a willingness to report incidents or weaknesses; frankness in assessments of security compliance; and a degree of empowerment to

enable staff to take remedial action" (Lacey, 2010), and take steps to ensure the cooperation of the entire organization.

The Information Security Policy is that framework, and must not only align with the culture, it must also align with the business goals and objectives of the company or institution. The architects of the policy need to, "…be able to fully articulate the business value of the security program. Indeed, business alignment is the only way to gain the cooperation and buy-in from your business constituents that's critical to the success of the security program. Unless you truly understand the business, you can't accurately and forcefully strategize, deploy and communicate the value of the security function" (Krause et al. 2008). In addition, "… the alignment requires an understanding of the relative value of information, how information is used within and across business processes, and at what nodes within a process sensitive information is most vulnerable" (Spears & Barki 2010).

The task of creating an information security plan can seem overwhelming, which is why many businesses fail to adopt a comprehensive security plan. They also only see security as a cost and a business inhibitor instead of as a business enabler. The cost of an information security breech is both tangible and intangible. Lost productivity and the time it takes staff to restore operations is measurable. The intangible effects of a security incident are generally much greater. "Intangible effects include the impact on an organization's trust relationships, harm to its reputation, and loss of economic and societal confidence resulting from a publicly reported breach (Allen & Westby 2007)." Additionally, "[h]aving a good reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share (Allen & Westby 2007)."

A comprehensive security policy will help profitability when it is aligned with the business's, organization's, institution's or entity's strategic goals. Once established, these policies and procedures will foster an environment that maintains system security and availability, data integrity and individual privacy. The most progressive organizations strive to achieve multiple business benefits from security investments: streamlining business processes, reducing operational costs and enhancing their brand. Brand confidence is built on trust. Customers will chose the organization that they feel does the best job in protecting information. Protecting data from distortion or tampering is essential for both legal and competitive reasons. Having the information or data highly available is a requirement now for any business to stay competitive. A company (or organization, institution or entity) must have its networks or web presence always available. If not they will lose customers or negatively impact productivity. "It is therefore very important for companies to notice that their strength in attaining and sustaining competitiveness in the highly volatile, demanding and uncertain markets lies in their ability to securely protect their information assets and IT infrastructure" (Dlamini et al. 2009).

Information is an asset and requires security commensurate with its value, criticality and sensitivity. Measures must be taken to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, and to ensure its authenticity, integrity and availability. Fortunately there is a very large community that takes this matter seriously and provides information on the threat landscape and how to mitigate those threats. Most, if not all, of that information is available for free.

Risk Assessment

Once the culture and business goals are understood, an assessment needs to be undertaken to determine what the policy (and its procedures and guidelines) will be protecting, and the threats they will be facing. “Identifying and implementing suitable controls requires careful planning and participation of all employees in the organization is also vital for the success of information security management” (Kee 2001). Risk assessment is an on-going process of discovering, correcting and preventing security problems. This is also known as risk management: identifying the full scope and extent of the real risks that the enterprise is up against and creating processes for managing those risks. Companies (or institutions, organizations or entities) utilize both new and legacy systems that are interconnected, and those systems are used to accomplish critical missions and to conduct important business. “Explicit, well-informed management decisions are necessary in order to balance the benefits gained from the use of these information systems with the risk of the same systems being the vehicle through which adversaries cause mission or business failure” (Ross et al. 2008).

“Without a practical and easy to use method, individuals will tend to postpone or not complete the assessment, take a reactive posture, or incorrectly apply the risk process” (Ewell 2009). When done correctly, risk assessment will lead to appropriate levels of security by bringing together the best collective judgments of the individuals responsible for the strategic planning and the day-to-day operations of organizations. The end result will be the determination of the acceptable level of risk and the resultant security requirements. There is no need to spend hundreds of dollars on ten dollars worth of assets. It will also result in an inventory of assets allowing an organization to know exactly what it has and where. If an organization did not have a network diagram before, it will now.

A company or organization can begin this process by analyzing, then bringing information security risks under management control; which includes the information security elements of system and network management. A risk management plan needs to be drawn up that results in the development and maintenance of: a long term enterprise security strategy, an overarching enterprise security plan (which may be supported by underlying business unit security plans and security plans for individual systems), security policies, procedures, and other artifacts including guidelines, and the system architecture and supporting documentation (Westby & Allen, 2007). Undertaking a risk assessment, that when done correctly, will lead to appropriate levels of security by bringing together the best collective judgments of the individuals responsible for the strategic planning and the day-to-day operations of organizations. The end result will be the determination of the acceptable level of risk, and the resultant security requirements. It will also result in an inventory of assets, allowing an organization to know exactly what it has and where. Once those are detailed and documented the next step is to define the roles, structures and reporting lines for the information security management function and its relationships with others such as risk management, IT audit and general business management. An Information Security Program becoming an integral part of the operation structure will help insure that the company's bottom line remains healthy as well as insuring that all functional and business unit leaders within the organization understand security's importance to the business.

To keep the task from becoming overwhelming, and as a way to categorize so that there is a methodology to the task, it can be broken down into four areas: Compliance, Financial, Operational and Strategic. Compliance would include items relating to laws, regulations, contracts, standards or policies; financial would include physical assets or fiscal resources; operational would include ongoing management processes; and strategic would include anything

that has the ability to negatively affect the organization's ability to achieve its goals and objectives.

Threat sources need to be considered as well. They can be broken down into four categories as well: human intentional, human unintentional, structural, and environmental. Fraud and theft, malicious code, industrial espionage, or actions of a disgruntled employee are examples of items that would fall into the human intentional category. Untrained users, configuration, and programming errors are examples of items that would fall into the human unintentional category. The physical environment, power issues, or network outages would be examples of items classified as structural. Finally, the environmental category could include items like fire, water, or lightening.

This risk assessment report will include a list of threats and vulnerabilities, the system's current security controls along with its risk levels, as well as summarizing the system architecture and components and its overall level of security. It will show where this small business needs to concentrate its remedial work, and recommend safeguards including the expected level of risk that would remain when these safeguards are put in place. The completed risk assessment will also be used as input for the business continuity plan.

A risk assessment report applies to a selected information system. This study's working definition of an information system is a group of computing and network components that share a business function, under common ownership and management. The report reflects the security policies and objectives of the organization; and, should be presented in a face-to-face meeting with the system business and technical owners, the risk assessment manager, and other project team members.

Policies, Procedures, and Guidelines

Once the risk assessment is complete, and there is agreement as to the assets being protected and their value, a program may be begun to protect those assets. The company now knows what assets it has, their value, and the appropriate level of security. Policies, procedures and guidelines may be drawn up and begun being implemented. In addition to the information security policy, the organization, at a minimum, needs an acceptable use policy, an acceptable encryption policy, an e-mail use policy, an extranet policy, anti-virus guidelines, a firewall configuration policy, and a business continuity plan. Possibly the most important component of the implementation is training in security awareness. “Security awareness, awareness training, and education are all necessary to the successful implementation of any information security program” (CISO 2005).

“Information security can be viewed as being different, at different levels of management” (White 2009). Strategic management involves creating security policies, dealing with people issues, and evaluating threats and risks. Tactical management involves how the security systems are developed and implemented to meet policy requirements. Tactical management will also be concerned with incident management and security education and awareness. Operational management involves maintaining and monitoring the enforcement of information security policies, technical security and access control, asset identification and classification, and physical and environmental security. All levels of management, as well as all departments or units, need to be represented in the program. They need to be involved in the formation, as well as the implementation, of the information security planning process.

Technology and applications are unique to each organization and the safeguards used must be geared specifically to each organization, its nature, the information it needs to protect,

and its degree of vulnerability. The security program must be comprehensive as well as multi-layered (Rudman, 2010). It must include technical controls as well as addressing the human element.

Traditional technological controls of patch management, firewalls and antivirus are a great starting point for developing a security program. Make sure critical data is protected by implementing a regular back up – as well as making sure the back ups actually work by testing them. Encrypt sensitive data and set permissions. In setting permissions, the best practice is that of least privilege, which means setting access rights to the minimum levels required by users that allow them to fulfill their job requirements. Having an information security program, while comprehensive, does not need to be daunting. Plan and assess, document, and then implement. Have legal and human resources check the program, then test and monitor. Respond to incidents and continuously improve the program. Information technology and the threat landscape are continuing to evolve, and businesses (or organizations, institutions or entities) need to evolve as well.

An Information Security Program is a dynamic organism that continually evolves. It changes, grows and improves due to new threats and vulnerabilities discovered or by fixes to issues discovered during implementation, testing or monitoring. The Information Security Program, and all its policies, procedures and guidelines, need to be reviewed on a regular basis. The program, policies, procedures and guidelines should be reviewed every two years at a minimum, and more frequently as resources allow. Information technology is evolving at a fantastic rate, and the program that aims to secure information needs to evolve as well.

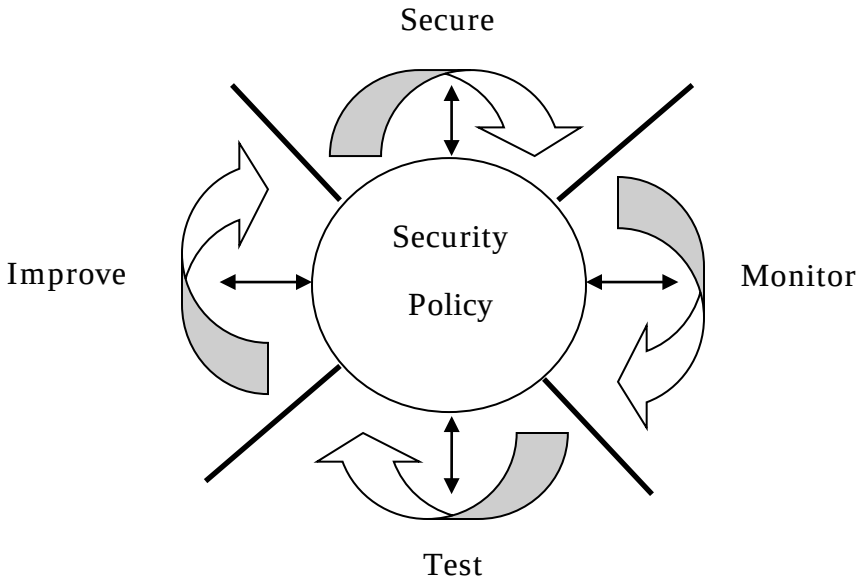

Figure 2. Security Wheel

The Security Wheel (Figure 2) is a diagram that illustrates the concept well. It shows a continuing process that interacts with and revolves around the security policy. This process involves: implementing, monitoring and responding, testing, and improving. Once established, the security policy needs to be documented and then implemented. Thus your program has started and you have begun the evolving process, the goal of which is to mitigate the risk to your data, information, and the systems that access, transmit and house it. Once started, it must be monitored for violations; and when there are violations there must be a proper response. Another critical part of this process is testing. This must be done to insure that what has been implemented actually works. One example is restoring a system from a backup. Another example is to scan for vulnerabilities, or to try social engineering techniques to determine if the education policies are effective. The time to catch errors is before an event occurs. Then the organization uses the information from these tests to improve the Information Security Program, and the cycle continues anew.

Central to the Information Security Program is the Information Security Policy. This policy's purpose is to create an environment within an organization (or company, institution or entity) that maintains system security and availability, data integrity and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to or loss of data. It is a document that needs to be clear and concise, and have input from all departments and units. This input will assist in implementation and compliance. If there are units that need more stringent controls, they need to have their own tailored policy that takes precedence for them.

Creation of policies, procedures, and guidelines need not be overwhelming since there are many examples and templates freely available. In a tenth of a second, Google returned about 90,500 results for the search of Enterprise Information Security Policy. Look at a few, then modify and tailor to your organization – unless the security policy you chose has copyright limitations. The Information Security Policy should be a comprehensive document. This policy should contain a statement of purpose, a general policy statement, and its scope. An Enterprise Information Security Policy will also contain sections dealing with compliance, updates, threats, a security philosophy that will detail basic principles, roles and responsibilities, and the detailed policy itself. Issue and system specific policies and guidelines need to be drafted as well. These should include Acceptable Use and Acceptable Encryption Policies, e-mail use, extranet, anti-virus guidelines, social media use, firewall configuration policy, and mobile device use policies. These policies need to be updated frequently, and contain issue statements that clearly define their applicability, roles and responsibilities, compliance, and point(s) of contact. The biggest aspect of these policies is user awareness and training. Everyone in the organization needs to know these policies, how to access them, and the consequences of non-compliance.

The small business audited, as evidenced by the results of the survey taken by its employees, had an information security policy in place that was written in clear and concise language and was easily understandable; and that the small business had a business continuity and/or disaster recovery plan. As far as compliance with the information security policy, the survey indicated that the majority knew there was a mechanism in place to prove an employee has read and understands the information security policy and there were clear consequences if the information security policy is violated, yet the survey also indicated that they were unsure if compliance was monitored, and only half thought it was somewhat likely they would be disciplined if they violate the information security policy. A comprehensive information security policy was created for the small business audited, and is included in Appendix D minus any identifying information.

Incident Response

When an information security incident occurs, despite the precautions taken by a small business, how the small business reacts is critical. Small businesses need a reactive capacity to rapidly detect an incident to minimize loss and/or destruction and restore operations. After actions could then be performed to mitigate the vulnerability exploited. The key to effective incident response is thorough planning and preparation. “Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data” (Scarfone, Grance, & Masone, 2008). Equally important is coordinating the involvement and expertise of human resources, legal, and law enforcement dependent upon the specific incident.

The incident response capability begins with the creation of an incident response policy and plan. Policies and procedures for performing incident handling and reporting based upon that plan need to be developed. Those policies and procedures need to delineate exactly what the incident response is to do, and exactly what should be accomplished. They also need to set guidelines for communicating with outside parties regarding incidents.

Incident response policies and procedures is another area within the overall security framework that needs to move away from the traditional approach. Figure 3 shows the classic six-step incident response model that when properly setup, implemented, enacted and supported, does a good job of mitigating and containing threats.

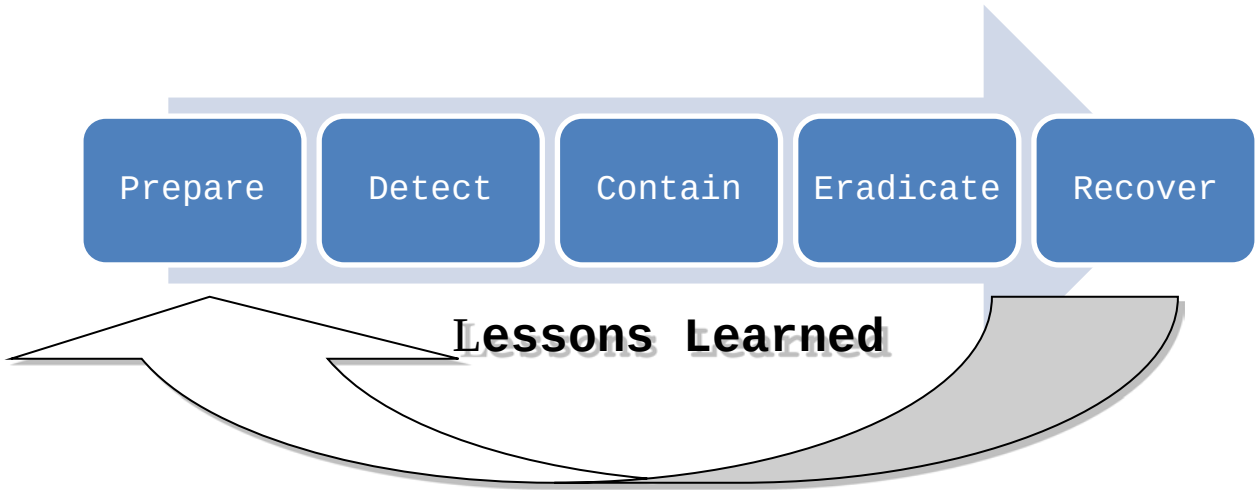

Figure 3. Six Step Incident Response Model

Done properly, the traditional six-step incident response approach can provide some strong benefits. However, these benefits are reduced or become nonexistent if any process within this cycle is not performed properly or completed. “To be more effective, the response to these evolving threats and risks posed by computer security incidents requires an incident handling capability that better prepares for and manages incident events” (Investment in Detection, 2007).

By integrating the handling of incidents into the daily business functions of the organization, and establishing strong linkages among those functions, better prevention and more effective handling of incidents can be achieved. Moving from a responsive approach to a managed approach minimizes disruption to an organization.

Things can get hectic quickly when there are problems created by an information security incident; and it might be during this time that outside parties like law enforcement, or other victims would need to be notified. To insure that only appropriate information is shared, well defined guidelines must be prepared in advance. If sensitive information is released it could lead to a greater disruption and financial loss than the actual incident itself. Also be aware that if the information system has been compromised, data like contact information for the person delegated to respond to the incident might not be available or accessible.

Once the policies and procedures are documented the next step is to then identify who will be contacted when there is either a real or perceived incident, and who will respond to investigate the notification. Establish an Incident Response Team whose members are qualified and authorized to respond to any incident, evaluate, and then execute the response plan. The team, in an optimum situation, should include a representative from business management, an Information Security Officer, technical support staff, and legal counsel. In smaller organizations, many of these roles may be performed by a single individual.

The business management representative will be the person who is accountable for the organization's operations, and will oversee and manage the entire response process, decide which courses of action will be taken, and determine if and when it is appropriate to share information outside the organization. The Information Security Officer (ISO) will be the initial

point of contact; access the situation and assist in correcting any problems; notify, brief management and the business management representative; and provide options and recommendations to management on how to respond. The ISO will coordinate activities and communication within the incident response team, as well as develop and maintain all documentation relating to the incident. Technical support staff will help and assist the Information Security Officer in assessing the situation, gathering data and information while helping in response and remediation. Legal counsel is there to provide advice as appropriate. A detailed document by The National Institute of Standards and Technology is Special Publication 800-61, titled Computer Security Incident Handling Guide, which is published to help both established and newly formed incident response teams. This guide is a great resource and can be found online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

If after careful consideration it is decided to contact law enforcement, there are various agencies available to investigate incidents. Examples include the Federal Bureau of Investigation (FBI), the U.S. Secret Service, district attorney's offices, or state and local law enforcement. The person (or persons) delegated with the incident response and/or reporting responsibilities should become acquainted with various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported, which agency is the correct one to contact, how the reporting should be performed, what evidence should be collected, and how evidence should be collected and preserved.

Employees of the small business need to know who to contact and what specifically to do and what not to do when they perceive that they have encountered an information (or network) security incident. The survey conducted with the small business indicated that the employees were unsure of the incident response plan and the employees were not clear on the steps to take

when there was an information security incident or perceived information security incident. There should be formal training pertaining to the information security policies, and there should be periodic refresher training to show employees what to look for and what to do when the notice suspicious behavior – either from their equipment or from people inside the office. According to the Garner Group, 70% of security breaches originate from within the organization (Gray, 2005).

Business Continuity

Disaster recovery begins long before a disaster actually occurs and, with careful planning, the effects of a disaster will be reduced and the loss mitigated. It is imperative to think outside the box to assure business continuity. Perform a risk analysis to determine what is at risk, and then look at those assets from all angles. By looking at those assets and imagining no longer having them, while planning accordingly, an organization is less likely to be surprised when the unforeseen happens. Avoid having a single point of failure by insuring high availability and high fault tolerances. Redundancy is a good way to insure this.

To assure an organization can continue operations, create detailed plans that clearly outline the actions the organization, and particular members of an organization, will take to help recover and restore its critical operations that may have been completely or partially interrupted. These plans need to be tested to make sure critical components have not been forgotten and to insure that the implementation of the plan works. The wrong time to realize something did not work is when you have lost your data or infrastructure. This disaster plan should dovetail into the organization's crisis management plan.

Recovering from a disaster can be a time consuming process with many unknown variables. In a catastrophic loss not everything can be brought back online simultaneously

(unless of course your organization maintains a hot, mirror site). The people charged with restoring operations need to know which critical items need to be addressed and brought back online first. In the day to day operations of any business some processes are critical and time sensitive. A business continuity plan ensures that critical business functions will be maintained. As with the other plans and policies mentioned, the subject of business continuity has many resources available to help an organization create a methodology, plan, and then implement this complex task. One comprehensive document is the Generally Accepted Practices for Business Continuity Practitioners drafted by the Disaster Recovery Journal and DRI International, located online at http://www.drj.com/GAP/gap.pdf. Business continuity planning is a proactive approach that will ensure a business will function normally no matter what the circumstances. The good news for the small business audited is that the survey indicated that the small business had a business continuity and/or disaster recovery plan.

Securing Mobile Devices

Mobile devices such as smartphones, tablets, laptops, personal digital assistants (PDAs) and Universal Serial Bus (USB) memory sticks have facilitated increased convenience for individuals as well as increased productivity in the workplace. Providing mobile access to corporate information increases productivity and is a vital part of today's business while at the same time it increases an organization's vulnerability. "From a security standpoint, stationary targets are generally much easier to protect than moving targets, but in our modern, networked business environment, movable data is quickly becoming the norm. Consequently, data that is, "…capable of moving or being moved is much harder to protect than data that remains stationary" (Fried, 2010). Mobility, as an area, is the hardest to secure.

Increasingly, mobile devices are being utilized in organizations. “Until recently, mobile users did not have the critical mass or present a sufficiently attractive challenge for hackers and virus writers. Now, though, virus writers are starting to turn their attention to mobile devices” (Ernest-Jones, 2006). Physical hardware does not need to leave an employee’s possession for data to be compromised, particularly when that equipment utilizes network connections in public places like Wi-Fi hot spots or hotels (Mortleman, 2009). These devices also now are being used to introduce malware to corporate networks. Centralized monitoring tools, when combined with an organization’s policy, can help reduce risks (Ernest-Jones, 2006). Encryption of sensitive data is a good policy, but it should be recognized that encryption is not foolproof. The trouble is business is becoming extremely agile and security restrictions should not prevent employees from accessing data. A very delicate balance must be achieved in this increasingly connected world. The CIO’s Guide to Mobile Security from Research in Motion provides an executive overview and checklist that contains a great deal of pertinent information, and can be found online at http://www.blackberry.com/solutions/resources/CIOs_Guide_to_ Mobile_Security_100606_online.pdf.

Change Management

“Implementing the information security components institutes change in the organization’s processes and will influence the way people conduct their work. An important consideration is that organizations do not change, but people do, and therefore people change organizations” (Verton, 2000). “Information security changes in the organization need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work” (Veiga & Eloff, 2007). Nothing stays the same and change is inevitable. Change control documentation provides information of changes that have been made to the

system and often provides back out steps in case of failure. It also provides valuable information when troubleshooting problems or upgrading systems, so the documentation should outline how changes were made and detail the steps.

Securing Routers and Switches

Information resources, such as networks, must be safe-guarded from potentially destructive forces. Treating securing information resources as a standalone, technical concern is outdated, and must be seen as a business problem and addressed as such. That is, information security needs to be addressed by both technologists and the business community of interests. "Delegating security to technologists also ignores fundamental questions that only business managers can answer. Not all of a company's varied information assets have equal value" (McKinsey & Company, Inc., 2002). Security must be viewed as an, "…essential mission need, equivalent to core business operational functions" (Westby & Allen, 2007). It must move "…from an ad hoc, reactive approach to one that is systematic, planned, managed, and measured, or to any point in between that is suited to the balance of the organization's security needs and strategic drivers" (Caralli, 2004). Technologists may have the understanding of how to best secure a network; however, they need the input of the business community of interests to know what needs to be protected, and what business processes are critical and which processes are less of a concern.

This section covers many of the security features related to routers and switches, including securing access, secure shell (SSH), layer 2 security and layer 3 security. Its content loosely follows the CCIE Routing and Switching written exam blueprint. The blueprint topics are:

- Access Lists
- Zone Based Firewall and Classic IOS Firewall
- Unicast Reverse Path Forwarding
- IP Source Guard
- Authentication, Authorization and Accounting (router configuration)
- Control Plane Policing (CoPP)
- IOS Intrusion Prevention System
- Secure Shell (SSH)
- 802.1x
- Device Access Control

Passwords are sent in clear text, unless configured otherwise. Encrypting using Service password is a start, but the encryption is not very robust. Publically available tools will decrypt. Hope.co.nz is just one site that uses a java script to decode cisco type 7 passwords (Hope). The password required by the enable command can be defined by either the *enable password* <password> command or the *enable secret* <password> command. If both are configured, the enable exec command only accepts the password defined in the enable secret command. Enable secret password is not affected by service password-encryption. Instead, it is always stored as an MD5-hashed value instead of being encrypted, resulting in a much harder to break password (Cisco, 2008). The *username* <name> *secret* <password> command uses the same MD5 hash as enable secret, for example: *username barney secret 5 1oMnb$Egf1zE5Qpip4UW7TTqQTR.*

Authentication, authorization, and accounting (AAA) is the cornerstone of any systematic discipline of information security. Authorization, or access control, manages who may interact with what resources, and governs what kinds of operations they may perform on those resources. Access controls usually rest on some notion of identity, which may be associated with a specific individual or account, or with a group to which that individual or account belongs (Chapple, Littlejohn Shinder, & Tittel, 2002). Authentication is the process of verifying who is requesting access. Accounting is the recording of the activities undertaken.

Routers and switches can be configured to check credentials against listings in a TACACS+ and RADIUS server, or to check the credentials locally. A simple way to create a local login authentication is to configure the router or switch using *username* <name> *secret* <password> command, and then configuring the various access methods with the login local command.

The strongest authentication method to protect the command line interface (CLI) is to use a TACACS+ or RADIUS server. RADIUS uses UDP while TACACS+ uses TCP. RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.

Cisco Secure Access Control Server can be installed on Unix, Linux, and several Windows platforms, and contains the set of usernames and passwords used for authentication. Routers and switches receive the username and password from the user, send it as encrypted traffic to the server, and receive a reply—either accepting or rejecting the user. Cisco AAA security services is an architectural framework for configuring a set of three independent security functions in a consistent manner. This can be enabled by using *aaa new-model* in global configuration mode. Combined with access lists, this is a very powerful and flexible way to secure access to routers and switches.

Telnet is a fundamentally insecure protocol (Kane, 2008). Telnet traffic is sent cleartext, so using secure shell (SSH) is a more secure way to access text-based legacy applications or remotely managing servers and network equipment. There are two versions of SSH, with version 1 being more vulnerable to Man in the Middle attacks.

The Cisco SAFE Blueprint document (available at ttp://www.cisco.com/go/safe) suggests a wide variety of best practices for switch security. In most cases, the recommendations depend on one of three general characterizations of the switch ports: unused ports, user ports, and trusted ports. Unused ports are switch ports that are not yet connected to any device. As an example, switch ports that are pre-cabled to a faceplate in an empty cubicle. User ports are ports cabled to end-user devices, or any cabling drop that sits in some physically unprotected area. Trusted ports or trunk ports are ports connected to fully trusted devices, like other switches known to be located in an area with good physical security. The common element between unused and user ports is that a malicious person can gain access once they get inside the building, without having to gain further access behind the locked door to a wiring closet or data center. Some best practices that apply to both unused and user ports are:

- Disable unneeded dynamic protocols like CDP and DTP.
- Disable trunking by configuring these ports as access ports.
- Enable BPDU Guard and Root Guard to prevent STP attacks and keep a stable STP topology.
- Use either Dynamic ARP Inspection (DAI) or private VLANs to prevent frame sniffing.
- Enable port security to at least limit the number of allowed MAC addresses, and possibly restrict the port to use only specific MAC addresses.
- Use 802.1X user authentication.
- Use DHCP snooping and IP Source Guard to prevent DHCP DoS and man-in-the-middle attacks.

In addition to the preceding recommendations specifically for unused ports and user ports, the Cisco SAFE Blueprint makes the following additional recommendations.

- For any port (including trusted ports), consider the general use of private VLANs to further protect the network from sniffing, including preventing routers or L3 switches from routing packets between devices in the private VLAN.
- Configure VTP authentication globally on each switch to prevent DoS attacks.
- Disable unused switch ports and place them in an unused VLAN.
- Avoid using VLAN 1.
- For trunks, do not use the native VLAN.

- Limiting the number of MACs that can be associated with the port.
- Limiting the actual MAC addresses associated with the port, based on three methods:

    1. Static configuration of the allowed MAC addresses
    2. Dynamic learning of MAC addresses, up to the defined maximum, where dynamic entries are lost upon reload.
    3. Dynamically learning but with the switch saving those entries in the configuration (called *sticky learning).*

A switch can use dynamic ARP inspection (DAI) to prevent certain types of attacks that leverage the use of IP ARP messages. Switches use DAI to defeat ARP attacks by examining the ARP messages and then filtering inappropriate messages. DAI considers each switch port to be either untrusted (the default) or trusted, performing DAI messages only on untrusted ports. DAI examines each ARP request or reply (on untrusted ports) to decide if it is inappropriate. If DAI determines the ARP request or reply to be inappropriate, the switch filters the ARP message.

DHCP snooping causes a switch to examine DHCP messages and filter those considered to be inappropriate. DHCP snooping also builds a table of IP address and port mappings, based on legitimate DHCP messages, called the *DHCP snooping binding table*. The DHCP snooping binding table can then be used by DAI and by the IP Source Guard feature.

When configured, it filters all messages sent exclusively by DHCP servers. The switch checks DHCP *release and decline* messages against the DHCP snooping binding

table. If the IP address in those messages is not listed with the port in the DHCP snooping binding table, the messages are filtered. Optionally, it compares a DHCP requested client hardware address value with the source MAC address inside the Ethernet frame. DCCP snooping, when configured, will prevent a fake DHCP server from completing a man-in-the-middle attack. It can also prevent an attacking host from releasing a legitimate host's DHCP lease, then attempting to request an address and be assigned the same IP address— which would take over any existing connections from the original host. DHCP snooping can prevent a DoS attack whereby a host attempts to allocate all the IP addresses that the DHCP server can assign in the subnet.

When enabled along with DHCP snooping, IP Source Guard checks the source IP address of received packets against the DHCP snooping binding database. Alternatively, it checks both the source IP and source MAC addresses against that same database. If the entries do not match, the frame is filtered. IP Source Guard is enabled using interface subcommands.

IEEE 802.1X defines some of the details of LAN user authentication, but it also uses the Extensible Authentication Protocol (EAP), an Internet standard (RFC 3748), as the underlying protocol used for authentication. EAP includes the protocol messages by which the user can be challenged to provide a password, as well as flows that create one-time passwords (OTPs) per RFC 2289. Switches can use IEEE 802.1X to perform user authentication, which requires the user to supply a username and password, verified by a RADIUS server, before the switch will enable the switch port for normal user traffic.

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from

being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control (also called traffic suppression) can be configured to set rising and falling thresholds for each type of port traffic (unicast, multicast and broadcast). Each rate limit can be configured on a per port basis, and can be controlled by a packet rate or a percentage of interface bandwidth.

When the configured threshold is passed, the switch will rate limit by discarding excess traffic. The switch could stop there, or additionally shut down the port and/or send an SNMP trap. Do not configure traffic storm control on ports that are members of an EtherChannel. Configuring traffic storm control on ports that are configured as members of an EtherChannel puts those ports into a suspended state.

The Cisco SAFE Blueprint document also has a wide variety of best practices for router security. Key recommendations from the Safe Blueprint include:

- Enable secure Telnet access to a router user interface, and consider using Secure Shell (SSH) instead of Telnet.
- Enable SNMP security, particularly adding SNMPv3 support.
- Turn off all unnecessary services on the router platform.
- Turn on logging to provide an audit trail.
- Enable routing protocol authentication.
- Enable the CEF forwarding path to avoid using flow-based paths like fast switching.

RFCs 2827 and 3704 outline other recommended best practices:

- If a company has registered a particular IP prefix, packets with a source address inside that prefix should not be sent into that autonomous system from the Internet.
- Packets should never have anything but a valid unicast source IP address, so packets with source IP addresses of loopback (127.0.0.1), 127.x.x.x, broadcast addresses, multicast addresses, and so on, should be filtered.
- Directed (subnet) broadcasts should not be allowed unless a specific need exists.
- Packets for which no return route exists to the source IP address of the packet should be discarded (reverse-path-forwarding [RPF] check).

A very large part of securing routers and switches is the access control list (ACL). ACL's can be used as packet filters, like a firewall; but they also are used as a way to influence traffic. The access list is a group of statements, and the Cisco IOS processes the Access Control Entries (ACEs) of an ACL sequentially – either permitting or denying a packet based on the first ACE matched by that packet in the ACL. Newly configured ACEs in numbered IP ACLs are always added at the end of the existing ACL, and ACEs in numbered IP ACLs cannot be deleted one at a time. Standard ACLs can only match the source IP address field, and numbered standard ACLs are identified with ACL numbers of either 1–99 or 1300–1999. Extended numbered IP ACLs range from 100–199 and 2000–2699.

For an individual ACE, all the configured values must match before the ACE is considered a match. The Port Number field is only matchable when the protocol type in an extended IP ACL ACE is UDP or TCP. ICMP does not use port numbers, but it does include different message types, and some of those even include a further message code. The IP ACL

commands allow these to be matched using a rather long list of keywords, or with the numeric message type and message code.

Other parameters can also be checked. For example, the IP precedence bits can be checked, as well as the entire ToS byte. The established parameter matches if the TCP header has the ACK flag set—indicative of any TCP segment except the first segment of a new connection setup. Also, the log and log-input keywords can be used to tell Cisco IOS to generate periodic log messages when the ACE is matched—one message on initial match, and one every 5 minutes afterwards. The log-input option includes more information than the log option, specifically information about the incoming interface of the packet that matched the ACE.

The Cisco IOS Firewall contains multiple security features, has stateful packet inspection, and relies on Control Based Access Control (CBAC). CBAC controls protocols to inspect, interfaces on which to perform inspection, and the direction of traffic to inspect, per interface. Authentication proxy controls access to hosts or networks based on user credentials stored in a AAA server. If encrypted traffic is exchanged between two routers, and the firewall is in between the two routers, CBAC might not work as anticipated. This is because the packets' payloads are encrypted, so CBAC cannot accurately inspect the payloads. Also, if both encryption and CBAC are configured at the same firewall, CBAC will not work for certain protocols. In this case, CBAC will work with single-channel TCP and UDP, except for Java and SMTP. But CBAC will not work with multichannel protocols, except for StreamWorks and CU-SeeMe. So if you configure encryption at the firewall, you should configure CBAC for only the following protocols: Generic TCP, Generic UDP, CU-SeeMe, StreamWorks.

Multi-VRF firewall offers firewall services on virtual routers with virtual routing and forwarding (VRF), accommodating overlapping address space to provide multiple isolated private route spaces with a full range of security services. Transparent firewall adds stateful inspection without time-consuming, disruptive IP addressing modifications. Application inspection controls application activity to provide granular policy enforcement of application usage, protecting legitimate application protocols from rogue applications and malicious activity.

The Cisco IOS Firewall does have several caveats. CBAC comes after access-list filters and does not protect against attacks from within a network. To inspect traffic other than TCP or UDP, configure a named inspection rule. CBAC does not inspect traffic destined for or originating from a router, and has restrictions handling encrypted traffic.

Cisco also has a zone-based firewall where router interfaces are placed into security zones. Traffic is blocked by default from travelling between zones, and blocked between zones that have a security zone and those that do not.

Cisco's IOS also has an Intrusion Prevention System (IPS) that also provides deep packet inspection. If a signature is matched, a router can drop the packet, reset the connection, send an alarm message, block traffic from the packet source, and block traffic on the connection.

Control plane policing (CoPP) allows a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. Control plane packets are network device generated or received packets that are used for the creation and operation of the network itself. From the perspective of the network device, control plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor.

Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together. The control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Planning is key to a successful CoPP implementation. A typical procedure is to configure the class maps, allowing all traffic while monitoring it, so that the nature of the traffic is understood. It is also important to carefully consider the number of classes, the types of traffic grouped into each class, and the bandwidth allowed per class. The only layer 2 protocol that can be assigned to a class in CoPP is ARP while all others fall under the default class.

In a typical IPSec hub and spoke environment, the hub router must have separate, statistically configured crypto maps, crypto access lists, GRE tunnels, and isakmp peer statements for each spoke router. Dynamic multipoint VPN allows for a simpler hub router configuration. Another benefit is that the hub router does not require configuration as new spoke routers are brought online. Dynamic multipoint VPN automatically initiates Ipsec encryption, includes dynamic addressing support for spoke routers, dynamically creates spoke to spoke tunnels, and allows for VPN routing and forwarding identifier (VRF) integration for MPLS environs.

Information resources, such as networks, must be safe-guarded from potentially destructive forces. Cisco's secure blueprint for enterprise networks is a framework of best practices to secure a network, and utilizes an in-depth approach to network security design (Convery & Trudel, 2000). Cisco's Routing and Switching Official Exam Certification Guide chapter on Security relies heavily on the SAFE Blueprint. To begin effectively securing a network, secure access and be aware of the ease of service password decryption. Be aware Telnet is not a secure method of access. Secure layer 2 with port security, dynamic arp

inspection, DHCP snooping, IP Source Guard, 802.1X Authentication Using EAP, and storm control. Secure layer 3 with access control lists, firewalls, intrusion prevention systems, control plane policing, and Dynamic Multipoint VPN.

Information technology, and the threat landscape, is evolving at a fantastic rate, and the program that aims to secure information needs to evolve as well. The key for building a secure network is to define what security means to your organization. Once the technologists and the business community of interest formulate a policy, everything that goes on with the network can be evaluated with respect to that policy to determine whether what is proposed will conflict with the security policies and practices.

Intrusion Detection

Securing data and the information systems on which they reside and travel is generally approached by either introducing safeguards to prevent unauthorized access (i.e., user authentication/authorization, encryption, firewalls, etc.) or by a mechanism that recognizes an attack, like an intrusion detection system. An intrusion detection system (IDS) is software that automates the process of monitoring events in an information system, looking for signs of misuse or attacks. IDSs are characterized by where they reside; and are host-based, are network-based, or are a hybrid of the two. Host-based intrusion detection systems (HIDS) operate on individual devices or hosts on a system. HIDSs monitor incoming and outgoing packets only on the device on which they reside. Network-based intrusion detection systems (NIDS) are installed directly on the network, inspecting all incoming and outgoing packets on that network. One concern with NIDS is that since all network traffic flows through them latency could be a concern. IDSs are also characterized by how they detect attacks. IDSs are said to be signature-based when their

method for detecting attacks checks network packets against signatures of known threats. This is similar to how most anti-virus software detects malware (Intrusion Detection System). IDSs are said to be anomaly-based when they monitor 'normal' network traffic to build a statistical model describing normal network behavior, then any network traffic deviating significantly from the statistical model is seen as an attack (Bolzoni & Etalle, 2008). Accurately identifying malicious traffic is one critical way to begin appropriately defending networks (Yu & Frincke, 2005).

The goal of a properly configured IDS is to recognize network traffic that has malicious intent without incorrectly identifying legitimate network traffic. Rules, if too generalized will generate an unacceptable number of false positive reports. The term false positive is used to mean an IDS alert sent when there is not malicious traffic – meaning the alert is incorrect. Incorrectly identifying normal traffic as malicious and logging it creates small, but potentially significant issues. One issue with normal traffic being incorrectly logged is that the log file becomes large, which not only takes up disk space, but also makes it harder to discern possible incident traffic. The security analyst, while perusing the log file, would then have to disregard the packets incorrectly logged. This large amount of logged traffic makes the possibility of missing something greater. Extraneous logged traffic would also consume bandwidth that could be better utilized elsewhere in the network. Rules that are too specific or rules that are incorrect will not accomplish the goal of restricting network traffic to legitimate, authorized users. Not having to determine whether or not an IDS alert is legitimate allows more time spent actually tracking and denying threat traffic. Having fewer false alerts creates a greater probability that the network will be able to deny malicious traffic, which also in turn allows legitimate traffic access to the data and systems they need to be productive.

New exploits are being created regularly, and to be effective, an IDS needs to be regularly updated to detect these new exploits. Snort is one IDS that can be updated with new rules both from snort.org, as well as by someone who can write their own effective rules. The small business has the advantage here over a larger enterprise in that little mistakes in IDS configuration would create only minor issues in the small business, but could potentially create very big problems in the larger organization due to the volume of traffic on its network.

Securing Social Media

The World Wide Web has evolved from a static, mostly read only web to one that is much more interactive. The terms Social Web or Web 2.0 refer to the fact that websites now encourage interaction (Websense, 2011), and many sites now have user generated content like blogs and wikis. “Whether a social networking site, video sharing application, blogging platform, or news forum, 65 percent of the top 100 most commonly visited sites today are based on this notion of collaboration and content generation” (Websense, 2010). With the rise of the mobile web, people can share whatever they want, wherever they are, whenever they want. Conversely, they can access content on the web anytime, anywhere. We have come to the point where the web is a personal portable one (Agarwal, 2009), and it is known as the Semantic Web or Web 3.0. This evolution enables people to find, combine and share content almost effortlessly. Information Communication Technology (ICT) is a combination of information technology and communications technology, and is another term being used when describing this evolution. Information Communication Technology, in a general sense, lumps together all the technologies which enable users to create, access, and manipulate information. These same characteristics that enable creativity, productivity and collaboration also make it easier for those who wish to successfully attack organizations and steal (Pescatore & Feinman, 2008).

"The social Web is a critical, new business tool with too much potential to pass by" (Websense, 2011). According to a survey conducted online by McKinsey Quarterly, "69 percent of respondents report that their companies have gained measurable business benefits, including more innovative products and services, more effective marketing, better access to knowledge, lower cost of doing business, and higher revenues" (McKinsey Global Survey Results, 2009). Additionally, people are becoming more adept with current technologies and are insistent on utilizing them at work (Bradley, 2007). They often differ on their views of work habits, access to data, and multi-tasking; and often rebel within established work environments and policies where access to the web is tightly controlled (Cavoukian & Tapscott, 2006). As customers and employees become more comfortable using social and other emerging technologies they will require more transparency (Li, 2010). To truly benefit from the potential offered by the new paradigm of the social web, organizations need to, "recognize you are not in control – your customers, employees, and partners are" (Li, 2010).

When done right, these new, emerging technologies enable organizations to let go of control. The key is to shift the control to those you have the confidence in to behave responsibly when using the technology. Some, like the AntiSec movement are going to force organizations to be more transparent and accountable. The social web allows for better and cheaper communication channels that give organizations intimate familiarity with what their customers and employees are expressing and doing on the social web. These are new relationships that the organization can build, and like any successful relationship they need structure. So in the defining of these new relationships, be clear. Be upfront and candid in setting expectations. Charlene Li, author of Open Leadership, states it quite eloquently, "People need to know what to expect and how to behave in a new open environment" (Li, 2010). When these expectations are

clearly stated trust will develop – on both sides. A way to manage these new relationships is Open Leadership, which Charlene Li defines as, “having the humility to give up the need to be in control while inspiring commitment from people to accomplish goals” (Li, 2010).

The potential benefits of these new relationships, forged through the social web, can reap great rewards for any organization that takes a studied approach and then engages in social media. Ways organizations can benefit abound. Employees, being interconnected, can encourage collaboration, a deep knowledge pool, and increase employee satisfaction and engagement. Organizations can improve their bottom line by decreasing costs associated with travel, communication and operations by utilizing these free or low cost emerging technologies. Organizations also benefit by engaging directly with their customers, suppliers and partners through the social web. This two way channel allows customers to better understand an organization’s products and services, and lets the organization quickly know the customer’s unfiltered thoughts on those same products and services. Organizations that effectively engage their customers, partners and suppliers are more likely to be nimble enough to adjust to changing markets. McKinsey reports, “these customer interactions have resulted in measurable increases in revenues” (McKinsey Global Survey Results, 2009). This constituency has been labeled the Fifth Estate; and in addition to watching the watchdogs (journalism) and the politicians, they are watching, and commenting publicly on, organizations. This constituency is changing the rules of social interaction and the way business in being conducted (van Zyl, 2009). Now it is no longer a few people in a back room deciding what is important – who are deciding values, goals, and performance outcomes. It is collectively the people that use the social web (O'Reilly, 2005). An interesting and telling statistic from Websense Security Labs is that 90 % of the top 100 sites are

categorized as Social Networking or Search, with more than 45 % of these sites supporting user-generated content (Websense Security Labs, 2008).

If your organization isn't formally involved with social media it probably should be. A 2007 Clearswift survey reveals:

- **83%** of US office workers have accessed social media of some description from work
- **63%** of US office workers accessed social media at least once a day and **82%** at least a few times a week
- Almost one third (**30%**) of office workers in the US have discussed work-related issues via social media.
- **19.1%** of IT and business decision-makers didn't have a policy governing appropriate use of the Internet including social media sites and **2.8%** didn't know whether they did or not
- Almost half (**48.3%**) of those polled didn't know whether they had lost confidential information via social media outlets

Nor are they embracing these emerging technologies in order to benefit their companies:

- **40.8%** of IT and business decision-makers considered social media to be relevant to today's corporate environment, yet only **11.1%** were already making use of it from a business perspective. (Clearswift, 2007)

Customers, when they feel they haven't received a service or product as advertised (or even as perceived), may take their business elsewhere which is detrimental to the organization

(Jones, 2005). More importantly, they can harm the organization by engaging the social web and telling the world about their negative experience. By not having a social presence an organization loses the opportunity to engage their customers. Having a structured and well defined social presence allows an organization to address customer's, supplier's and partner's concerns directly, collaborate with their customers to deliver the products and services they desire, and show a transparency that builds trust and shows competency. Information and communication technologies can be used as a cost-effective and convenient means to promote openness and transparency (Bertot, Jaeger, & Grimes, 2010).

Additionally, employees have been posting negative comments online on their personal social networking sites for some time now; concerning their job, organization, customers, clients, fellow employees, et cetera. These comments are simple to find using any one of a number of tools (search engines or websites like glassdoor.com) and might be available indefinitely (van Zyl, 2009). Customers also have the ability to post negative comments about organizations on their personal sites, third party sites, and/or the company's web site. By formally engaging the social web, an organization can mitigate these exposures. One way to mitigate this exposure is for an organization to have a place where people can post concerns, ideas, et cetera. This allows the organization to address concerns quickly and directly, instead of finding out through other channels, and after much damage has been done to the organization's reputation and stature. It is important to note that these areas must be monitored for quick response – not only to respond to negative criticism, but to also make sure the posts are respectful of others, and/or are accurate. Encouraging people to post to these areas within clearly stated and defined guidelines that the posters are expected to follow gives an organization the platform to develop the relationship and build community. These guidelines also provide a framework that makes it easier for employees

to post, knowing that there are doing so with the company's blessing if they stay within the framework of the posting guidelines. If an employee strays outside the guidelines then management has the tools it needs to effectively deal with an offending post, as well as showing due diligence should the need to do so arise in any future legal proceedings or inquires..

IBM, as an example, has guidelines that among other things, tell their employees that they are personally responsible for the content they publish, that they should identify themselves clearly and in the first person. Additionally, the guidelines should require employees to use disclaimers that say their views do not necessarily reflect those of the company; and that the employees will respect copyright, fair use, and financial disclosure laws, avoid fights, and try to add value (Jander, 2009). When developing policies and guidelines, it is best to have the legal department, human resources, upper management, as well as IT involved. Information is both an asset and a liability that requires responsible management practices (Cavoukian & Tapscott, 2006).

Implementing the social web infrastructure and/or tools by an organization is termed Enterprise 2.0 (Levy, 2009). Enterprise 2.0 can be characterized by flatter hierarchies, greater collaboration, devolved decision-making, more risk-taking, high flexibility, agility, adaptability, and innovation (Cavoukian & Tapscott, 2006). However, by engaging the social web the organization needs to weigh the risks along with the benefits. The bottom line is that it is the organization's job to protect its content although many businesses are not equipped with the correct security and control technologies to mitigate the risks that go along with the decision to engage the social Web (Websense, 2011). The social web exposes businesses to new threats which are developed specifically to target those technologies (Clearswift, 2007), provides new delivery platforms, and widens the attack surface (Livshits & Erlingsson, 2007). The open

directories that allow for interaction and collaboration in the social web also allows hackers access to huge troves of information that can be used against the organization – a social engineering attack being just one vector. Social networking sites are also rich in data that would help a potential hacker gain the organization's footprint. Those sites tend to list names, job titles, phone numbers, e-mail addresses, and other important information that again can be used against the organization. Social networking sites can contain embedded viruses, worms or hyperlinks to sites that contain malware (van Zyl, 2009).

Organizations are reluctant to engage in the social web because productivity could possibly be negatively affected when employees spend company time in activities that the company sees as not relevant to the organization. They are also reluctant because an employee, either maliciously or unwittingly, may allow confidential or sensitive information to be seen by someone other than those authorized; which could then lead to financial loss, embarrassment, or legal liability.

After carefully considering the benefits and risks inherent in adopting social media, an organization can start mapping out a strategic plan and its implementation. Possibly the most important part of the strategic plan is figuring out exactly what the organization is trying to gain. The organization should realize, as a whole, that they must be consistently open to new learning, and that these new relationships will be more like dialog among equals. They should also be committed to shifting communications from transactional, short term, and impersonal to ones that are more long term focused, personal, and intimate (Li, 2010). Other gains that can be included in an organization's social media strategy include customers helping other customers for technical support, and utilizing crowdsourcing for new ideas.

Once the organization has mapped out their strategic plan, they then know what it is they need to protect and can start planning accordingly. The security plan for engagement of the social web needs to integrate seamlessly with the security program already in place. If your organization does not have an information security program, now would be a good time to start.

Address the human element by creating (or updating) an internet usage policy. Specifically address whether employees are allowed to browse the web for personal use as well as business purposes, and if they are allowed to use the company computers and networks, let them know when they are allowed to do so. Inform employees that the organization monitors computer use and that the employees should have no expectation of privacy while utilizing company computers and networks. Address web activity that is not allowed; specifically pointing out unacceptable behavior in detail such as offensive content, threatening or violent behavior, or any other illegal activity. Explain to employees the reasons for these restrictions and why they are important.

Make sure employees understand how to safely navigate the web. Recommend they only visit trusted sites, never browse the web from a server, and not allow websites to install programs unless they implicitly trust the website and know what the program does. From an organizational standpoint utilize firewalls and properly configured routers, and consider content filtering or a unified threat management solution.

Create a security policy that is only as strict or as complicated as the organization is willing to enforce. The security policy is a living document that grows to accommodate new threats, technologies, and ways of thinking. The SANS Institute defines several elements that you should include in a good security policy:

- Objectives. This section clearly states the reason the security policy exists.
- Scope. This section identifies the people and systems affected by the policy.
- Protected Assets. This section identifies the assets that the policy protects. Mail servers, databases, and websites are common business assets that need to be protected. Think of this section as an expanded discussion of the objectives.
- Responsibilities. This section of the policy identifies the groups or individuals responsible for implementing the conditions of the policy.
- Enforcement. This section of the policy discusses the consequences for violating the policy. Some authorities recommend referring to the appropriate location in the employee handbook as opposed to carrying enforcement directly in the security policy to avoid legal issues.
- Remote Access Policy. Outlines acceptable methods for remotely connecting to the internal network, such as whether employees are allowed to connect to the network from their home computers.
- Information Protection Policy. Provides guidelines to users on the processing, storage, and transmission of sensitive information.
- Virus Protection Policy. Provides baseline requirements for the use of antivirus software as well as guidelines for reporting and containing virus infections.
- Password Policy. Provides guidelines for how user-level and system-level passwords are managed and changed.

- Firewall Security Policy. Describes, in general, how firewalls are configured and maintained, and by whom. (Microsoft, 2005)

In a comprehensive information security policy, there should also be strong social media guidelines. If, despite all the compelling reasons to do so, the organization decides not to engage in social media, guidelines are needed to state that position. The organization should further identify that if employees do engage social media on their own, and post anything that might be relevant to the organization, its industry, its products or services, or even the organization's competitors, employees must be clear in their comments that their statements do not necessarily reflect those of the organization. This would also be a good time to educate employees on net and post etiquette.

If, on the other hand, the organization does decide to engage in social media, the guidelines should be encouraging, and explain why the organization needs these guidelines. The social media guidelines need to explain when and who the policy applies to, particularly when it applies to an individual's personal use of social media. The social media guidelines need to be easy to read and reference.

Points to be covered in the social media guidelines include identifying oneself, taking personal responsibility for comments, confidentiality, and use of common sense and good judgment. When posting, people need to identify themselves, and dependent upon the context, by what company or department they are employed, where appropriate. Unless they are posting for the organization in an official capacity, letting everyone know who they work for may prevent any potential conflicts of interest. When posting from a personal standpoint, it is probably prudent to include a disclaimer to the effect that the comments are their own and are not

necessarily those of the organization. People should be urged not to post anonymously, show respect for others, and not let it interfere with their normal duties. The social media guidelines should list what is allowed to be shared, as well as what should not be shared. For example, an organization's proprietary or confidential information, gossip, or other's personal and private details are not to be posted. Possibly the most important guideline businesses can issue is the most obvious – use judgment and common sense. Let employees know it is okay to ask for guidance when unsure and tell them who they can go to when seeking advice. When a comment results in an undesired outcome there also needs to be clear explication of what the consequences are when the guidelines are not followed.

If your organization decides to enter into social media, it should also institute a best practices guidelines for those engaged in posting in an official capacity as an organizational spokesperson. Points to be covered in these guidelines include quality and trust building (Li, 2010). It is important to pay attention to the details to insure quality. Comments and posts should never have basic mistakes in grammar and spelling. The content should add value and not be inconsequential in nature that would waste people's time. The point of this open engagement is to build trust, so make sure responses are timely and relevant. Speak to areas of expertise and make sure any facts included are accurate. Cite and link to sources, which are another great way to build community. Practice good content management, which should also include clearing out and archiving content once it's outdated (Jander, 2009).

Customers need a set of guidelines to follow as well. Customers will inevitably post negative comments, but those will give credibility to the organization's site. And it gives your organization the opportunity to engage with customers to try and resolve the issue. The real problem is when someone posts something unacceptable – if the post is defamatory, obscene,

copyright violation, off topic, for example. These customer guidelines should spell out exactly what the organization will do when they encounter these posts or comments.

It may seem counterintuitive to advocate openness with all the risk inherent in the social web and emerging technologies, but we've already started moving past web 2.0 to web 3.0, so it is even more important for organizations to have a formal strategy to deal with these new opportunities and technologies. The Internet is rapidly converging with mobile technology, changing the nature of online participation and information exchange (Song, 2010), while at the same time it is in the process of moving from a presentation medium to a global computational platform (Cavoukian & Tapscott, 2006).

Allowing employees to engage in the social web will increase job satisfaction and in so doing can increase productivity (van Zyl, 2009). For example, the American Red Cross first engaged the social web out of a desire to control. After a time the American Red Cross understood the benefits of openness and engaging those that had already engaged them (Li, 2010). Entering into the social web should not be done without structure and strategy. The organization needs to go in with definable and measurable expectations. Being open should not equate to everyone from customers to competitors having access to all information, and everyone being involved in all decisions. Such an unrealistic extreme of complete openness is untenable if a business is to sustain its competitive advantage and ability to execute its plan (Li, 2010). When entered in a structured and secure manner, the social web can bring great rewards to the organizations that are forward thinking enough to engage it.

Information Technology Due Diligence

The widespread adoption of the Internet has challenged legal authorities specifically due to its pervasiveness worldwide. A computer here in the United States can be connected to a computer half way around the world thanks to the Internet and the World Wide Web. A rapidly evolving area of the law is the question of jurisdiction over a person or subject matter. Additionally, laws and regulations regarding business use of technology are still being developed. Technology, in the areas of computing and networking, has become so pervasive and critical that it has created a paradigm shift in law (Legal aspects of computing, 2012).

The Internet has grown beyond its primarily research roots to include both a broad user community and increased commercial activity. The growth of commercial usage has brought with it increased concern regarding the standards process used to insure the Internet's viable operation. The community of people that created, and oversee the expansion and use of the Internet, have paid close attention to insure the process and access are open and fair.

To begin the discussion on regulation and law related to information security and technology in the modern world, one must look at the roots of the legal system and those roots are firmly embedded in general socially determined ethical codes. The Internet Advisory Board (IAB) Request For Comment (RFC) 1087 "Internet Ethics" dated January 1989 proposes that, "Access to and use of the Internet is a privilege and should be treated as such by all users of this system (Network Working Group Internet Activities Board, 1989)." The IAB Network Working Group endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure, which defines any activity as unethical and unacceptable which purposely:

(4) seeks to gain unauthorized access to the resources of the

Internet,

(b) disrupts the intended use of the Internet,

I wastes resources (people, capacity, computer) through such

actions,

(d) destroys the integrity of computer-based information,

and/or

I compromises the privacy of users (Network Working Group Internet Activities Board, 1989).

RFC 1087 goes on to express, "[n]egligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable (Network Working Group Internet Activities Board, 1989)."

Throughout its growth, the Internet has influenced more than just the technical fields of computers and networking. It has also been a major influencer of society itself as the Internet is increasingly used as a means to disseminate and acquire information, as well as a means to conduct business. "The Internet is as much a collection of communities as a collection of technologies, and its success is largely attributable to both satisfying basic community needs as well as utilizing the community in an effective way to push the infrastructure forward (Leiner, et al., 2011)." The relatively rapid rise of the technology that is the Internet and the World Wide Web has created opportunity for small businesses to compete with larger organizations on a more equal footing.

As the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress the potential for its misuse also rises. Small businesses need to be aware of the current laws and regulations as they pertain to information security and they need to be aware of what they can do to evidence due diligence in the protection of their data and their networks – either as a response to governing laws and regulations or as a proactive way to be responsible corporate citizens. Small businesses need to be aware of their options, what must be considered, and what steps they should take to address a computer or network incident *prior* to its discovery.

To remain viable in the marketplace small businesses need to possess, at the very least, a rudimentary knowledge of the legal framework that their organization operates within. Due to the rise of the social web, small businesses must be extremely cognizant of how they are perceived. Being perceived as ethical is one way for a small business to positively influence its public image. Any organization that recognizes their moral responsibilities increases their legitimacy, and is in a better position to acquire the resources necessary to remain competitive. Being perceived as trustworthy can be critical to a small business's survival (Culnan & Williams, 2009).

Ethics, as a field, "involves systematizing, defending, and recommending concepts of right and wrong behavior (Fieser, 2009)." Normative ethics are the moral standards that define proper conduct. The Golden Rule is a classic example: do not do to others that which we do not want done to us; and is an example of a single principle against which we can judge actions (Fieser, 2009).

Laws are written to set behavioral standards as well as to normalize a system of compliance. Those laws are mostly drawn from the ethics of the prevailing culture, defining social acceptable behavior conforming to the principles held by that society. Succinctly, laws require us to do (or not do) something, while ethics remind us of what we are supposed to do. The sticky question here is which laws apply? Compounding the challenge of determining exactly which laws are applicable is the question of what court, in what country or which state, has jurisdiction over a given conflict or legal issue.

Most jurisdictions enforce their laws and subsequent actions of their courts against businesses by the threat of seizing the organization's assets. A company without any assets or desire to conduct future business in a jurisdiction is effectively judgment-proof (Tipton & Krause, 2005). This reality holds true when a small businesses information system is attacked: if the attacker does not have any assets within a jurisdiction that has the means or desire to prosecute, the small business will not have much recourse for recovery of any losses incurred. However, most legal trouble can be avoided by protecting against negligent claims by having strong evidence that the company meets traditional due diligence standards. Most U.S. Federal laws in this area, for example, provides safe harbors if there is evidence of due diligence.

Small businesses, mostly by necessity, spend much of their energies and resources focusing on remaining profitable. Most small businesses do not have the knowledge, let alone the time required, to harden their data and information systems against any misuse or all attacks. What they can do, however, is prove they are doing all that is reasonable to protect their data and information systems.

Small businesses not only need to protect the privacy of any consumer data they may have, but they must also consider the privacy concerns of their employees, vendors, and anyone else that legitimately connects to the small businesses network. The small business must also make sure that there are safeguards in place so that when someone does access the network and/or data without specific authorization, or tampers with the small businesses network or its data, they can be identified and appropriately managed in the sense that internal employees might be reprimanded, terminated, or even prosecuted. External entities might be managed simply by denying access.

In some instances of data or network breaches, law enforcement involvement is mandatory. The National Conference of State Legislatures reports that, "[f]orty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information (State Security Breach Notification Laws, 2012)." Businesses are to report data breaches to those that are, or might be, affected. Most of the legislation requires notice to consumers of breach in the security of unencrypted personal information unless there is no reasonable likelihood of harm to the consumer (Consumers Union, 2007). The ramifications of notification regarding an information security incident must be carefully weighed. For most small businesses, the cost associated with investigation of the computer crime could be prohibitive. The effect of an external investigation and any negative press that might arise must be thoroughly examined. Employee productivity could also be hampered by the inquiry process. Proprietary data could be subject to disclosure. Publicity surrounding the incident might negatively influence customer confidence in the small business. Disclosure of the incident could additionally trigger copycat attacks. Equipment deemed evidence would leave the organizations control to be used in prosecution. That

equipment might be critical to the successful operation of the small business, or contain data that is critical to the successful operation of the small business. If and when the equipment taken away as evidence does make it back to the small business, the data it contained, or even its operational ability, could be compromised. All of these issues must be carefully weighed before deciding on exactly whom to notify and when.

Businesses have legislative requirements that must be met; dependent upon the type of business the organization conducts. Pursuant to the proposed bill titled Personal Data Privacy and Security Act of 2005, "it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information." This bill never became law because at the end of the session all proposed bills and resolutions that haven't passed are cleared from the books. This bill has been reintroduced in succeeding sessions – the latest as the Personal Data Privacy and Security Act of 2011; whose stated purpose is, "[t]o prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information" (Leahy, Schumer, Cardin, Frankin, & Blumenthal, 2011).

Businesses involved in Healthcare are mandated to meet or exceed the Health Insurance Portability and Accountability Act (HIPAA) legislative requirements. HIPAA is a very broad and far reaching legislation, and contained within this legislation are the standards for information transactions and data elements. SEC. 1173. (a) specifies the standards to enable electronic exchange:

‘‘(d) SECURITY STANDARDS FOR HEALTH INFORMATION.—

‘‘(1) SECURITY STANDARDS.—The Secretary shall adopt security standards that—

‘‘(A) take into account—

‘‘(i) the technical capabilities of record systems used to maintain health information;

‘‘(ii) the costs of security measures;

‘‘(iii) the need for training persons who have access to health information;

‘‘(iv) the value of audit trails in computerized record systems; and

‘‘(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

‘‘(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

‘‘(2) SAFEGUARDS.—Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

‘‘(A) to ensure the integrity and confidentiality of the information;

‘‘(B) to protect against any reasonably anticipated—

‘‘(i) threats or hazards to the security or integrity of the information; and

‘‘(ii) unauthorized uses or disclosures of the information; and

‘‘I otherwise to ensure compliance with this part by the officers and employees of such person. (104th Congress, 1996)

Section 1176, “GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS” provides for the penalties for violations by disclosure of individually identifiable health information.

Table 3

Goals	**Requirements**
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Protect Cardholder Data	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 3. Goals and Requirements of the Payment Card Industry Data Security Standard

Any small business accepting credit cards as payment are subject to the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS applies to all entities that store, process, and/or transmit cardholder data, and covers technical and operational system components included in or connected to cardholder data. PCI DSS consists of common sense steps that mirror security best practices, shown in Table3.

Financial institutions are subject to the Gramm-Leach-Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999. It also applies to companies, regardless of whether they are financial institutions, who receive customer's personal financial information. To be in compliance with GLB, the organization must have a policy in place to protect the information from foreseeable threats in security and data integrity. The GLB has a Safeguards Rule that requires a written information security plan that describes how the organization is prepared to protect nonpublic personal information.

Publically traded companies need to be aware of the Sarbanes-Oxley Act of 2002 (SOX). Financial data, because it now resides within and travels through information systems, must be shown to be secure and accurate, and that the system is reliable and in compliance with SOX Section 404: Assessment of internal controls (Whitman & Mattford, Management of Informaton Security, 2010). However, there is a significant fixed cost involved in completing the assessment

so that smaller companies are disproportionately impacted. Effective as of September 21, 2010, the Securities and Exchange Commission (SEC) ruled that organizations that are not accelerated or large accelerated filers are exempt (Murphy, 2010).

The Digital Millennium Copyright Act (DMCA) was enacted to reduce the impact of copyright, trademark, and privacy violations. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. While most small businesses themselves do not violate the DMCA, if an employee uses the small businesses information technology system to download copyrighted content the small business could be held liable unless due diligence is proved.

18 USC § 2701 – Unlawful access to stored communications was enacted in 1986 to provide penalties for anyone that intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility, and obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in that system (USC > Title 18 > Part I > Chapter 121 > § 2701, 2012). 18 USC § 1030 – Fraud and related activity in connection with computers was also enacted in 1986 to provide penalties for those that intentionally access a computer without authorization or who exceed authorized access, and obtain information from any protected computer – among other provisions. These two laws, along with the five other laws previously mentioned are just a sample of major U.S. legislation that the U.S. Federal government has enacted regarding information technology as it pertains to businesses. Individual states also have enacted laws and regulations pertaining to information security, and it is up to the small business to ensure that their organization's security policies and procedures comply with their state's laws and regulations.

Information security is the term generally used to describe the ongoing process of exercising due care and due diligence to protect information and the systems upon which they rely from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. In protecting the network and the organization's data, it is extremely important to show that legitimate attempts were made to secure the data and network access because, as we have seen over and over again, no information system in impenetrable.

A small business has done its due diligence when it has undertaken a comprehensive effort to protect information they have created or had entrusted to their care. Additionally, putting in place security to protect the technology systems upon which that information relies also helps support due diligence defenses. Due care is another legal concept that concerns the specific controls an organization utilizes in the attempt at the broader due diligence standard, and can be met when a small business implements safeguards used effectively by other organizations that have similar business objectives to their own. A small business could use stricter standards imposed by other industries to show due care was exercised as well. For example, a small business, even one not involved in healthcare, using the safeguards proposed by HIPAA would have a strong argument that they have provided due diligence in protecting privacy.

The Federal Information Processing Standards (FIPS) Publication 200 specifies minimum security requirements for information and information systems supporting the United States federal government, and specifies a risk-based process for implementing the security controls necessary to satisfy due diligence. The purpose of this publication was to, "… promote the development, implementation, and operation of more secure information systems within the federal government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying

security controls for information systems that meet minimum security requirements" (FIPS PUB 200, 2006). Small businesses, in the process of securing their information and networks, need to show that they have made reasonable attempts in this regard. If they follow a framework established as viable by organizations with similar business objectives, or utilize frameworks developed to a stricter standard (like HIPAA or SOX); regularly assess security controls established for the information and information systems to determine if the controls are effective; correct any deficiencies and mitigate any vulnerabilities identified; and continuously monitor and test the safeguards emplaced to protect the small businesses' data and networks to confirm their effectiveness, a small business can reasonably state that they are providing due care and thereby evidencing due diligence in the broader legal sense. It is interesting to note that the survey of the small business audited indicated that the employees thought the information security policies were comprehensive, yet three quarters of the employees responding did not believe the information security policies provided due diligence.

Keeping small business information, networks, and the systems upon which they rely secure is an ongoing process. By exercising due care and due diligence to protect their information technology from unauthorized access, use, disclosure, destruction, modification, disruption or distribution, a small business can insulate itself from most litigation that may arise if their information systems or confidential data have been compromised.

Recommendations Made to Mitigate Liabilities Discovered

After the information security audit was conducted and the electronic survey completed, recommendations were made to the small business to mitigate the liabilities discovered. It was highly recommended: (1) to reinstall the operating system for the computer used to make the

banking deposits to get rid of the persistent worm, (2) that the operating systems and any office suites have the most current updates and patches installed, and (3) inform the employees of the steps to take when they encounter something wrong with a computer. A security education and awareness training program can be set up with very little cost or time investment.

It was also mentioned to the small business audited that having a screensaver password and forcing individual logins to the computers may inhibit ease of use for the employees, but should be considered. Ease of access for the employees also means ease of access for others. A virtual private network was recommended for use instead of logmein.com. Logmein does come with a number of security controls (SSL logins, data encryption capabilities and multiple layers of firewalls and gateways). However, it is still basically a Web application running as a Web service, featuring all of the Web service's security vulnerabilities. As a Web-based service, it has the potential to expose the internal corporate network to the Web. It was recommended to turn off any unneeded services running on the server, and to simulate a data loss and testing of data back up to make sure there are no issues when/if there is an actual need. I addition to the recommendations, a comprehensive security policy written specifically for the small business audited, along with specific policies, procedures, and guidelines was included with the report containing the recommendations (Appendix D).

CHAPTER 5: CONCLUSIONS AND FURTHER RESEARCH

Information security must be considered an integral part of doing business, not something done as an afterthought. To properly manage information security, every facet of the company needs to be involved, not just the owner, or the person or department relegated to securing the network and the information traversing and contained within. Soliciting information and feedback from all departments will not only create buy in, but this will also make it less likely that items and areas are overlooked. All departments are affected and need to feel they have input and some degree of control because, in the end, these are the people that will be implementing and helping to insure compliance with these policies. The information security program must also be tied to, and guided by, the organization's strategic goals. By making the Information Security Program an integral part of the operation structure, businesses will insure that the bottom line remains healthy as well as insuring that all employees in the organization understand security's importance to the business.

Because small businesses account for over fifty percent of the Gross National Product of the U.S. economy, the availability of uncompromised information systems is critical for them to operate, compete, and remain profitable. This study was designed to evaluate a small business's information security to determine if its information resources and network were adequately secure and discover what vulnerabilities exist. The answer to the research question posed by this study, "Has one small business in the healthcare industry adequately secured their information resources", was no. The small business audited had experienced information security incidents, which was to be expected despite the small business perception that there had been no security incidents. Issues unexpected to be found included: software had gone unpatched, not all hard drives were using the most secure file system, user names and passwords were out in plain view,

and the computer used to make the online banking deposits had been compromised by viruses. While the small business did have an information security policy in place that was understood and acknowledged by the employees, there was significant room for improvement. The findings indicated employees were unclear if compliance to the information security policy was monitored, unsure if they were found to be in noncompliance with policy that they would be disciplined, and unsure what to do if they encountered a security incident. All of which would be corrected by a regularly occurring security education and awareness program.

It was also designed so that the researcher might act in partnership with the small business to attempt to affect social change that will help in securing the small business's information resources. When the small business was initially contacted with regards to study participation, the small business had reservations because they believed that they had not experienced any information security incidents. The small business was concerned that there would not be enough data for a meaningful study. Even if that had turned out to be the case, a small business not experiencing any information security incidents is well worth documenting.

Future research has already begun by small business audited agreeing to a second audit in approximately one year. The goals of the second audit are to ascertain whether the recommendations were actually implemented; and if so, whether those recommendations reduce the amount of security incidents experienced by the small business during the year interval. If the recommendations were implemented *and* the small business did experience a significant reduction in information security incidents, this study could be used as a test case for an approach that a typical small business may take to secure their networks and data to avoid unnecessary liability exposure. The methods specified here in this study, and implemented by the small business audited with success, could be ported to a larger group of small businesses and

researched to confirm the validity of the results. Other areas of future research identified include a study that determines what percentage of small business owners are aware of, and utilize, the abundance of free resources available to help them secure their information systems.

References

104th Congress. (1996, August 21). *PUBLIC LAW 104–191—AUG. 21, 1996.* Retrieved November 6, 2012, from GPO.gov: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

FIPS PUB 200. (2006, March). Retrieved March 19, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Small Business Information Security: The Fundamentals. (2009, 10). Retrieved 11 6, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Small Business Information Security: The Fundamentals. (2009, October). Retrieved November 6, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Small Business Profile. (2011, February). Retrieved November 6, 2012, from Small Business Administration: http://www.sba.gov/sites/default/files/files/us10.pdf

Legal aspects of computing. (2012, March 02). Retrieved March 17, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Information_technology_law#cite_note-5

State Security Breach Notification Laws. (2012, Fenruary 12). Retrieved March 22, 2012, from National Conference of State Legislatures: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

USC > Title 18 > Part I > Chapter 121 > § 2701. (2012, February 21). Retrieved March 19, 2012, from Cornell University Law School: http://www.law.cornell.edu/uscode/text/18/2701

Agarwal, A. (2009, May 30). *Web 3.0 Concepts Explained in Plain English (Presentations).* Retrieved July 15, 2011, from digital inspriration: http://www.labnol.org/internet/web-3-concepts-explained/8908/

APM Group Limited. (2011, July 28). *ITIL Foundation*. Retrieved January 01, 2012, from ITIL: http://www.itil-officialsite.com/Qualifications/ITILQualificationLevels/ITILFoundation.aspx

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media asopenness and anti-corruption tools for societies. *Government Information Quarterly*, 264–271.

Bokharee, M. N. (1993). *SMALL BUSINESS INFORMATION SYSTEMS: A THEORETICAL MODEL AND AN INTERACTIVE EXPERT DECISION SUPPORT SYSTEM FOR MANAGEMENT.* Retrieved November 6, 2012, from http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?vinst=PROD&attempt=1&fmt=6&startpage

=-1&ver=1&vname=PQD&RQT=309&did=747461231&exp=11-04-2016&scaling=FULL&vtype=PQD&rqt=309&TS=1320619777&clientId=15121

Bolzoni, D., & Etalle, S. (2008). Approaches in Anomaly-based Network Intrusion Detection Systems. *Advances in Information Security Volume 38*, 1-16.

Bradley, A. (2007). *Key issues in the enterprise application of Web 2.0, practices, technologies, products and sevices.* Gartner.

Caralli, R. (2004, December). *Managing for Enterprise Security.* Retrieved April 15, 2011, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/reports/04tn046.pdf

Cavoukian, A., & Tapscott, D. (2006). *Privacy and the Enterprise 2.0.* New Paradigm Learning Corporation.

Chapple, M., Littlejohn Shinder, D., & Tittel, E. (2002). *TICSA Certification: Information Security Basics.* Pearson IT Certification.

Cisco. (2008, July 08). *Cisco IOS Password Encryption Facts*. Retrieved December 5, 2011, from Cisco: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

Clearswift. (2007). *Content Security 2.0 The Impact of Web 2.0 on Corporate Security.* Clearswift Limited.

Clinch, J. (2009, May). ITIL V3 and Information Security. *Best Management Practice*. TSO.

Consumers Union. (2007, August 21). *Notice of Security Breach State Laws.* Retrieved February 09, 2012, from Consumers Union: http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf

Convery, S., & Trudel, B. (2000). *Cisco SAFE: A Security Blueprint for Enterprise Networks.* Retrieved December 5, 2011, from Cisco: http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1953/product_implementation_design_guide09186a00800a3016.pdf

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 673-687.

Ernest-Jones, T. (2006). Pinning down a security policy for mobile data . *Network Security Volume 2006, Issue 6*, 8-12.

Fieser, J. (2009, May 10). *Ethics.* Retrieved February 14, 2012, from Internet Encyclopedia of Philosophy: http://www.iep.utm.edu/ethics/

Fried, S. (2010). *Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World .* New York: Auerbach Publications.

Gray, T. (2005, May 6). *How Much is Too Much Data Loss?* Retrieved March 29, 2012, from INternet News: http://www.internetnews.com/security/article.php/3503331

Grossetete, P., Popoviciu, C., & Wettling, F. (2008). *Global IPv6 Strategies.* Indianapolis: Cisco Press.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses:An empirical examination. *Information and Security Management*, 297-311.

Hayes, B. (2011). Who's Protecting America's Small Business? *Security Technology Executive*, 34-36.

Hope, D. (n.d.). *Cisco Password Decrypter*. Retrieved December 5, 2011, from Hope.co.nz: http://www.hope.co.nz/projects/tools/ciscopw.php

Intrusion Detection System. (n.d.). Retrieved October 27, 2012, from Intrusion Detection System: http://www.intrusiondetectionsystem.org

Investment in Detection, R. a. (2007). *National Information Assurance (IA) Approach to Incident Management(IM).* Fort George G. Meade, MD: Committee on National Security Systems Secretariat/I922 National Security Agency.

ISACA. (2008). *ITAF: A Professional Practices Framework for IT Assurance.* Rolling Meadows: ISACA.

Jander, M. (2009, Feburary 16). The Web 2.0 Balancing Act. *InformationWeek*, pp. 42-48.

Jones, J. (2005). *An Introduction to FactorAnalysis of Information Risk (FAIR).* Risk Management Insight.

Kane, S. (2008, November 18). *Blog*. Retrieved December 5, 2012, from Interwork Technologies: http://www.interwork.com/blog/2008/11/18/qa-how-to-eliminate-the-security-risks-associated-with-telnet-ftp/

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management*, 7-9.

Kissel, R. (2009). *Small Business Information Securiity: The Fundamentals.* Gaithersburg: National Institute of Standards and Technology.

Kotulic, A. G., & Clark, J. G. (2003). Why there aren't more information security research studies. *Information & Management*, 598-608.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security Vol. 10 No 1*, 4-13.

Leahy, Schumer, Cardin, Frankin, & Blumenthal. (2011, September 22). *S.1151 - Personal Data Privacy and Security Act of 2011.* Retrieved February 09, 2012, from Open Congress: http://www.opencongress.org/bill/112-s1151/text

Leiner, B. M., Cerf, V. G., Clark, D. D., Kleinrock, L., Lynch, D. C., Postel, J., et al. (2011). *Brief History of the Internet.* Retrieved March 22, 2012, from Internet Society: http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet

Levy, M. (2009). WEB 2.0 implications on knowledge management. *JOURNAL OF KNOWLEDGE MANAGEMENT*, 120-134.

Li, C. (2010). *Open Leadership.* San Francisco: Jossey-Bass.

Livshits, B., & Erlingsson, U. (2007). Using web application construction frameworks to protect against code injection attacks. *Proceedings of the 2007 workshop on Programming languages and analysis for security*, 95-104.

McKinsey & Company, Inc. (2002). Managing Information Security. *McKinsey Quarterly*, 12-15.

McKinsey Global Survey Results. (2009). *How companies are benefiting from Web 2.0.* McKinsey & Company.

Microsoft. (2005). *Security Guide for Small Business-Microsoft.* Retrieved July 16, 2011, from www.microsoft.com/smallbusiness: http://download.microsoft.com/download/3/a/2/3a208c3c-f355-43ce-bab4-890db267899b/Security_Guide_for_Small_Business.pdf

Mortleman, J. (2009, November 2). Protect data while travelling. *Computer Weekly*, pp. 20-21.

Murphy, E. M. (2010, September 15). *INTERNAL CONTROL OVER FINANCIAL REPORTING IN EXCHANGE ACT PERIODIC REPORTS OF NON-ACCELERATED FILERS.* Retrieved March 19, 2012, from U.S. Securities and Exchange Commission: http://www.sec.gov/rules/final/2010/33-9142.pdf

National Institute of Standards and Technology. (2011, September 30). *Computer Security Resource Center.* Retrieved November 6, 2012, from NIST Information Technology Laboratory: http://csrc.nist.gov/publications/PubsSPs.html

Network Working Group Internet Activities Board. (1989, January). *Request for Comments: 1087.* Retrieved February 14, 2012, from Internet Engineerring Task Force: http://tools.ietf.org/pdf/rfc1087.pdf

O'Reilly, T. (2005, September 30). *Design Patterns and Business Models for the Next Generation of Software*. Retrieved July 16, 2011, from O'REILLY: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1

Pescatore, J., & Feinman, J. (2008). *Security Features Should Be Built Into Web 2.0 Applications.* The Gartner Group.

Peters, S. (2009). *2009 CSI Computer Crime and Security Survey.* Computer Security Institute.

Peters, S. (2009). *2009 CSI Computer Crime and Security Survey.* Computer Security Institute.

Prichard, S. (2010). Navigating the black hole of small business security. *info security*, 18-21.

Rudman, R. J. (2010). Framework to identify and manage risks in Web 2.0 applications. *African Journal of Business Management Vol. 4(13)*, 3251-3264.

Ryan, J. (2000, December 29). *Information Security Practices and Experiences in Small Business*. (Doctoral Dissertation). Retrieved from Dissertations and Theses database. (UMI No. 9998885).

Scarfone, K., Grance, T., & Masone, K. (2008). *Computer Security Incident Handling Guide.* Gaithersburg: Computer Security Division Information Technology Laboratory National Institue of Standards and Technology.

Song, F. W. (2010). THEORIZING WEB 2.0. *Information, Communication & Society, 13: 2*, 249 —275.

Spears, J. L., & Barki, H. (2010). User Participation in Information System Security Risk Management. *MIS Quarterly*, 503-522.

Tipton, H., & Krause, M. (2005). *Information Security Handbook.* Tayor & Francis Routledge.

van Zyl, A. S. (2009). The impact of Social Networking 2.0 on organizations. *The Electronic Library*, 906-918.

Veiga, A. D., & Eloff, J. H. (2007). An Information Security Governance Framework. *Information Systems Management*, 361-372.

von Solms, S. v. (2009). *Information Security Governance.* Springer.

Websense. (2010). *2010 Threat Report.*

Websense. (2011). *Securing the Social Enterprise.*

Websense Security Labs. (2008). *State of Internet Security Q1-Q2, 2008.* Websense.

Westby, J. R., & Allen, J. H. (2007). *Governing for Enterprise Security (GES) Implememtation Guide.* Pittsburgh, PA 15213: Carnegie Mellon University.

Whitman, M., & Mattford, H. (2010). *Management of Information Security.* Boston: Course Technology.

Whitman, M., & Mattford, H. (2010). *Management of Informaton Security.* Boston: Course Technology, Cengage Learning.

Yu, D., & Frincke, D. (2005). *43rd ACM Southeast Conference* (pp. 2-142 through 2-147). Kennesaw: ACM.

Appendix A

IRB Approval

EAST CAROLINA UNIVERSITY
University & Medical Center Institutional Review Board Office
1L-09 Brody Medical Sciences Building· Mail Stop 682
600 Moye Boulevard · Greenville, NC 27834
Office 252-744-2914 · Fax 252-744-2284 · www.ecu.edu/irb

Notification of Initial Approval: Expedited

From: Social/Behavioral IRB
To: John Vail
CC:
Erol Ozan
Date: 11/18/2011
Re: UMCIRB 11-001202
Small Business Information Security:

I am pleased to inform you that your Expedited Application was approved. Approval of the study and any consent form(s) is for the period of 11/17/2011 to 11/16/2012. The research study is eligible for review under expedited category #7. The Chairperson (or designee) deemed this study no more than minimal risk.

Changes to this approved research may not be initiated without UMCIRB review except when necessary to eliminate an apparent immediate hazard to the participant. All unanticipated problems involving risks to participants and others must be promptly reported to the UMCIRB. The investigator must submit a continuing review/closure application to the UMCIRB prior to the date of study expiration. The Investigator must adhere to all reporting requirements for this study.

The approval includes the following items:

Name	Description
audit charter.docx | History	Dataset Use Approval/Permission
Small Business Information Security Eval Risk Mgmt in a Healthcare Setting prospectus.docx | History	Study Protocol or Grant Application
Survey questions.docx | History	Surveys and Questionnaires
Survey-Consent-Letter.doc | History	Consent Forms

The Chairperson (or designee) does not have a potential for conflict of interest on this study.

Appendix B

Survey Consent

Dear Participant,

I am a student at East Carolina University in the department of technology. I am asking you to take part in my research study entitled, Small Business Information Security: Evaluating Risk Management in a Healthcare Setting.

The purpose of this research is to conduct a security audit of a small business, looking to evaluate that businesses information security posture and recommending, if any, changes or additions that would reduce the business's exposure to information security threats, risks and vulnerabilities through effective information security risk management. By doing this research, I hope to learn if a typical small business's information resources are adequately secure. Your participation is voluntary.

You are being invited to take part in this research because you are an employee. The amount of time it will take you to complete this study is less than five minutes.

You are being asked to answer an electronic survey that inquires about the company's security policy, and how it may affect you.

Because this research is overseen by the ECU Institutional Review Board, some of its members or staff may need to review my research data. However, the information you provide will not be linked to you in any way. Therefore, your responses cannot be traced back to you by anyone, including me.

If you have questions about your rights as someone taking part in research, you may call the UMCIRB Office at phone number 252-744-2914 (days, 8:00 am-5:00 pm). If you would like to report a complaint or concern about this research study, you may call the Director of UMCIRB Office, at 252-744-1971.

You do not have to take part in this research, and you can stop at any time. If you decide you are willing to take part in this study, please continue with the survey.

Thank you for taking the time to participate in my research.

Sincerely,

John Vail Principal Investigator

Appendix C

Audit Charter

AUDIT CHARTER

This Audit Charter directs John Vail to perform an Information Security Audit for the X practice. The purpose is to examine any policies related to computer and network security for the practice, and to examine data provided relating to network and computer security incidents. The aim is to review the security policies and procedures, or lack thereof, and the incidents experienced, then determines if the reasons incidents happen are due to ineffective policy, lack of training and education, or lax enforcement and/or monitoring.

The audit process will begin with initial research and review of the applicable laws and regulations relevant to this industry, and a survey to determine the organization's business goals for Information Technology, Information Technology goals, and how they are currently being realized through Information Technology processes and Information Technology. Security policies and procedures will be examined to create a baseline of the organization's current security posture, and to make sure all areas of concern are addressed. Information will be gathered to map out the organization's internal network, how it connects to external networks, and to determine the system's boundaries. A detailed risk assessment will be conducted to identify threats to the practice's security, and identify any vulnerability. The risk assessment will then be aligned with the organization's strategic goals and objectives to insure that the practice's mitigation costs are appropriate to the asset value that they are protecting. The last step of this audit process will be the reporting of the documentation of the audit, and recommendations made, including a corrective action plan, to Dr. X for his review and use.

John Vail will have the authority and right of access to information, personnel, locations and systems relevant to the performance of this audit, with the exception of access to patient information.

Dr. X	Date	John E. Vail III	Date

Appendix D

Information Security Policy

Information Security Policy
For [Company Name]

Purpose

The purpose of this Enterprise Information Security Policy is to create an environment within [Company Name] that maintains system security and availability, data integrity and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to or loss of data. If there is a difference between this policy and other required policies, those with the more stringent control take precedence.

This document describes an enterprise level policy. Enterprise standards, processes and procedures will be developed to assist in the implementation. If it is determined that more stringent measures are needed, each organizational unit is responsible for developing the policies, standards processes and procedures to meet that higher level of security.

General Policy Statement

Information is a [Company Name] asset requiring security commensurate with its value, criticality and sensitivity. Measures must be taken to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, and to ensure its authenticity, integrity and availability. When information is transferred either internally or externally to [Company Name] information systems and networks, it must be protected from origin to destination. Information technology processes, procedures, and practices may contain information (confidential or private) about [Company Name] business, communications, and computing operations or employees. Policies, standards, processes and procedures for distribution of any related documentation should consider both the sensitivity of the information and related statutory exemptions before public disclosure. Availability of information systems and data resources must be maintained to ensure continued service and continuity of operations. [Company Name] must consider security threats and guard against any action or inaction which interrupts the availability of information systems and data resources.

Scope

For the purposes of this policy, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by any organizational unit. Security also involves the ability to protect information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction. In general, information technology assets covered by this policy include those that process, store, transmit or monitor digital information. It includes the security of information technology facilities and off-site data storage; computing, telecommunications and applications related

services purchased from other commercial entities; and Internet-related applications and connectivity.

Compliance

All [Company Name] employees, interns, volunteers and contractors that use, develop, implement or maintain information technology systems covered by the enterprise information security policy are responsible for understanding and complying with all [Company Name] enterprise information security policies, standards, processes and procedures. This includes using, building, configuring and maintaining systems in accordance with these policies, standards, processes and procedures. Depending on the severity, those who intentionally violate these policies, standards, processes and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal and/or criminal prosecution.

Outsourced processing and storage facilities, such as vendors, partnerships and alliances, must be monitored and reviewed to ensure compliance with enterprise and organizational unit policies. Any exceptions to this policy must be specifically approved by Corporate. Requests must clearly explain the rationale and implications of the exception. Corporate will either approve or deny the request within 15 days of submittal.

Updates

This document will be reviewed at least every two years and updated as needed.

Threats

[Company Name] information resources are vulnerable to many threats that must be considered when making risk management decisions. The potential impact of all threats should be considered when conducting a risk assessment. Threats can be categorized both by source and function. The following threats are representative and not all encompassing.

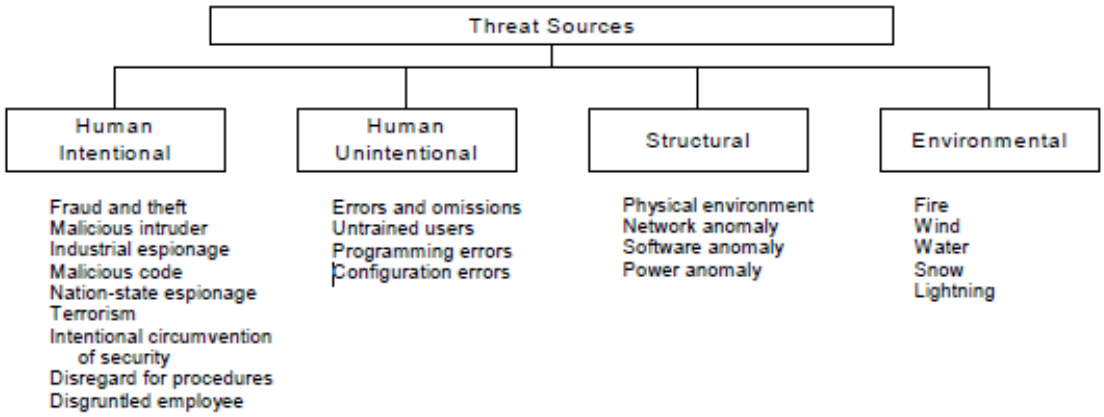

Figure 4. Threat Category

SECURITY PHILOSOPHY

Basic Principles

The basic security principles are to protect the confidentiality, integrity and availability of the information and information resources entrusted to [Company Name].

- **Confidentiality** means that information deemed sensitive or confidential is protected and unavailable to those who do not have the necessary approvals to view it.
- **Integrity** means that information is correct and has not been altered or corrupted in some way. It also means that programs, applications, procedures and systems function as intended.
- **Availability** means that access to information and information systems is not denied to authorized users.

  Security is an enabler critical to the success of technology initiatives and should not be viewed as a deterrent or irritant.

Information Assurance

Information security encompasses many disciplines, including computer security, network security, communications security and physical security. For [Company Name] systems, security will follow the concept of information assurance. The overall goal of information assurance is to protect and defend information and information systems. Disruptions in today's environment are not preventable 100 percent of the time; therefore, [Company Name] must be prepared to respond appropriately and recover to ensure the confidentiality, integrity and availability of its information and information systems. Information assurance entails information protection, event detection, appropriate response and restoration of information and services.

Defense in Depth

In [Company Name], servers, PC's, networks, network components and other information technology devices will be implemented using the principle of "defense in depth." Network and system security can be significantly improved when defense and detection measures are implemented in layers, so there are multiple opportunities to stop problems. This approach, in combination with an information assurance strategy, provides the best opportunity to reduce risks to appropriate levels.

Risk Management

It is impossible to eliminate all risk, but security measures are used to mitigate risk to acceptable levels, and all security decisions should be made with risk management in mind.

Access Control

Access control involves restricting physical access to resources and logical access to computers and networks. Access control decisions should be made based on the concept of least privilege, which means that individuals are given only those necessary accesses and rights, usually based on job duties and responsibilities.

Enterprise Information Assurance

[Company Name] computer systems and networks are increasingly interconnected, so a risk accepted by one organizational unit is often a risk imposed on others. Therefore, an enterprise approach to security with common security policies, standards, processes and procedures is needed. Security measures are most effective when considered end-to-end; that is, from the point of origin to the point of delivery.

ROLES AND RESPONSIBILITIES

Information assurance requires the active support and ongoing participation of all involved parties. It requires support from the executive level and universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with the development, implementation, operations, use and maintenance of [Company Name] information systems. Each person shall satisfy the requirements as they relate to the portion of each information system under their control. Implementation, acceptance and maintenance of adequate system and network security is a shared responsibility of all [Company Name] employees, supporting and using organizations, technology providers and users. Senior managers, technical staff and security personnel are responsible for evaluating the level of risk associated with any particular information system and implementing adequate security controls to reduce the risk to an acceptable level.

The following are specific roles and responsibilities both at the management and staff level.

Corporate

Under the leadership of the Chief Executive Officer, the Corporate Office develops and implements an enterprise risk management program, publishes enterprise level security policies, standards, processes and procedures, and provides programs and processes to facilitate the implementation of this policy. The Corporate Office will serve as a central coordinating group to establish cyber security response procedures, ensure that best practices are shared, coordinate training and act as a catalyst to improve overall cyber security.

The Corporate Office also coordinates the development of security service offerings and functions to ensure needed security services are available across [Company Name] organizational units. The Corporate Office is responsible for maintaining a relationship with organizational units; coordinating relevant information flow between organizational units and the Corporate Office, and disseminating appropriate information throughout the Enterprise.

Organizational Unit Supervisor

Organizational unit supervisor (or equivalent), in coordination with the corporate office, are ultimately responsible for the implementation of the enterprise information security policy in their organizational unit and the development and implementation of organizational unit security policies, standards, processes, and procedures. Managers and supervisors are responsible for ensuring their staff members know and understand appropriate security policies, standards, processes and procedures.

User

Each user shall, within his or her capabilities, protect information and system/network resources against occurrences of sabotage, tampering, denial of service, fraud, misuse or release of information to unauthorized persons. This includes protecting passwords and other account information; following appropriate policies, standards, processes and procedures; and notifying appropriate authorities when incidents occur.

System Administrator

The term “system administrator” is used here in the general sense, and includes system, network, firewall and other technology administrators that provide technical support to specific systems or networks. System administrators monitor performance, provide problem determination and production support and perform system back-ups. Security-related responsibilities include but are not limited to ensuring that:

• Applicable patches, service packs and updates are installed;
• Only authorized software is installed via authorized means;
• Systems are developed and implemented in a secure manner, following established enterprise security policies, standards, processes and procedures;
• Approved security procedures are followed and established where necessary;
• Systems are recovered in a secure manner;
• Ad hoc system reviews are performed to identify unusual activity;
• Security administrators are notified of changes to software that might impact system security features before installation of those changes; and,
• Procedures for software license validation and virus testing have been followed.

Security Administrator

Security administrators provide security-related administration tasks for critical systems. Where practical, separate system and security administration functions should exist; but in every case, both system and security administrative functions must be performed. When the system and security administration functions are performed by the same individual, care should be taken to ensure a secure approach is utilized. Security administration responsibilities include, but are not limited to:

- Development and implementation of system-specific security policies, standards, processes and procedures;
- Authentication (add, change, delete) services;
- Authorization (add, change, delete) services to provide access to applications;
- Generation and distribution of reports for monitoring access and potential security breaches; and,
- Developing incident handling procedures.

Database Administrator

Database administrators ensure the confidentiality, integrity, and availability of databases under their control. Security responsibilities include, but are not limited to:

- Designing, developing, organizing, managing and controlling databases in accordance with applicable security policies; and,
- Recovering databases in a secure manner when damaged or compromised.

Application Developer

Application developers develop secure applications consistent with established policies, standards, processes and procedures. Applications shall protect individual privacy, the confidentiality of electronic commerce information and the integrity of both the information it processes and the application itself. Applications must log significant security events, protect the log files appropriately and prevent co-mingling of data within the application.

INFORMATION SECURITY POLICY GUIDELINES

It is the information security policy of [Company Name] that:

1. Each organizational unit operates in a manner consistent with the maintenance of a shared, trusted environment within [Company Name] for the protection of individual privacy and the assurance of data and business transactions. Each organizational unit shall not jeopardize the confidentiality, integrity or availability of the information systems; or the information stored, processed and transmitted by any [Company Name] information systems.

2. Each organizational unit follows established enterprise security policies, standards, processes and procedures, except where the organizational unit policy provides a higher level of security.

3. Each organizational unit is responsible for developing policies, standards, processes and procedures to meet this policy. If it is determined that more stringent measures are needed, the organizational unit is responsible for developing the policies, standards processes and procedures to meet that higher level of security.

4. Each organizational unit will develop, implement, and exercise an organizational unit business continuity plan. The plan will be based on asset criticality and be consistent with the enterprise business continuity plan.

5. Each organizational unit will implement a security awareness, training and education program for all staff including both technical and non-technical staff. The term “program” is intentionally used here. Each department is expected to offer an on-going, systematic training program using a system-wide approach. Every new employee will be provided basic information technology security training before being authorized to access [Company Name] computer resources. All employees, including interns, contractors, temporary and part-time employees, must agree in writing to follow enterprise and department security policies before being authorized to access [Company Name] computer resources.

6. Each organizational unit is subject to an annual security audit to assure compliance with this and other enterprise level policies, standards, processes and procedures. An audit or review performed under another authority, such as an approved outside contractor, may be substituted if similar in scope and approved by Corporate.

7. Each organizational unit will have a vulnerability assessment performed on its information systems at least annually to gauge the effectiveness of security measures. Assessment results may be used to identify, prioritize, plan for and implement additional security measures and to update the organizational unit risk assessment.

8. Each organizational unit will have an information systems risk assessment performed at least every two years. This assessment will be used to identify, prioritize, plan for and implement additional security measures. The assessment methodology will be developed and distributed by the Corporate Office.

9. Security requirements will be formally defined and addressed throughout the life cycle of all information technology projects, including business requirements definition, design, development, testing, implementation and operation.

10. Each organizational unit manager or supervisor will assure to the best of his or her ability that information systems under their control meet enterprise and organizational unit security policies, standards, processes and procedures prior to being placed in production or after significant changes to the system. The Corporate Office will randomly assess the self-certification process and individual systems to ensure adherence to policy.

11. All organizational units will comply with appropriate [Company Name] information security requirements. However, if any requirements are inconsistent with established organizational unit policy or standard, in whole or in part, then Corporate may grant a waiver from the inconsistent portions of policy or standard. Requests for a waiver must be submitted in writing and demonstrate that granting the waiver will not result in undue risk for the company as a whole or to the organizational unit.

12. Individual privacy will be protected at all times according to established laws, policies and rules.

13. Monitoring of information system usage for malicious activity and misuse of [Company Name] resources will be conducted by organizational units per their established policies.

14. Each organizational unit will report network changes affecting enterprise network security to the Corporate Office.

15. Organizational units will report information security incidents that impact or could impact shared resources to the Corporate Office, following a common response plan developed, implemented and exercised jointly by the Corporate Office and all organizational units.

16. Computer resources and physical information, including but not limited to servers, desktops, laptops, network equipment, firewalls, hardcopies and tapes, have appropriate physical protections in place. Where possible, these resources should also be protected from structural and environmental threats.

17. Organizational units will provide information to the Corporate Office describing all connections from their organizational unit networks to outside resources including private service providers. Updates will be provided as changes occur.

18. Organizational units will develop procedures for implementing system patches, configuration updates, and other measures necessary to protect systems from known vulnerabilities. The procedures will provide for adequate testing prior to implementation to reduce the risk of a negative impact, but also assure the updates are applied quickly enough to assure protection.

19. Requests for exemption from any of the requirements of this policy will be submitted in writing by the organizational unit manager or supervisor to the Corporate Office prior to implementation.

Acceptable Use Policy
For [Company Name]

Overview

[Company Name]'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to [Company Name]'s established culture of openness, trust and integrity. [Company Name] is committed to protecting their employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of [Company Name]. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every [Company Name] employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of the information systems at [Company Name]. These rules are in place to protect the employee and [Company Name]. Inappropriate use exposes [Company Name] to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at [Company Name], including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by [Company Name].

Acceptable Use Policy Guidelines

General Use and Ownership

1. While [Company Name]'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of [Company Name]. Because of the need to protect [Company Name]'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to [Company Name].
2. Personal use of the [Company Name] information systems during work hours is neither fair to other employees nor the employer who is paying for the services and the employees time. Personal use of the [Company Name] information systems must be limited to unpaid time and kept to a reasonable minimum. Authorization must be obtained from the organizational unit supervisor or manager prior to personal use of the information systems. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager. If an employee's personal use of [Company Name] computers or networks becomes excessive, or results in viruses or other harm, the privilege will be rescinded.
3. [Company Name] recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see [Company Name]'s Information Sensitivity Policy. For guidelines on encrypting email and documents, go to [Company Name]'s Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within [Company Name] may monitor equipment, systems and network traffic at any time, per [Company Name]'s Audit Policy.
5. [Company Name] reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with [Company Name]'s Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a [Company Name] email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of [Company Name], unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the [Company Name] Internet/Intranet/Extranet, whether owned by the employee or [Company Name], shall be continually executing approved virus-scanning software with a current virus database unless overridden by organizational unit or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Blogging and Social Networking Policy and Guidelines for [Company Name]

1. Blogging and social networking by employees, whether using [Company Name]'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of [Company Name]'s systems to engage in blogging and social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate [Company Name]'s policy, is not detrimental to [Company Name]'s best interests, and does not interfere with an employee's regular work duties. Blogging and social networking from [Company Name]'s systems is also subject to monitoring.
2. [Company Name]'s Confidential Information policy also applies to blogging and social networking. As such, Employees are prohibited from revealing any [Company Name] confidential or proprietary information, trade secrets or any other material covered by [Company Name]'s Confidential Information policy when engaged in blogging and social networking.
3. Employees shall not engage in any blogging and social networking that may harm or tarnish the image, reputation and/or goodwill of [Company Name] and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging and social networking or otherwise engaging in any conduct prohibited by [Company Name]'s Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to [Company Name] when engaged in blogging and social networking. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of [Company Name]. Employees assume any and all risk associated with blogging and social networking.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, [Company Name]'s trademarks, logos and any other [Company Name] intellectual property may also not be used in connection with any blogging and social networking activity
6. Be transparent and state that you work at [Company Name]. Your honesty will be noted in the Social Media environment. If you are writing about [Company Name] or a competitor, use your real name, identify that you work for [Company Name], and be clear about your role. If you have a vested interest in what you are discussing, be the first to say so.
7. Never represent yourself or [Company Name] in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
8. Post meaningful, respectful comments — in other words, please, no spam and no remarks that are off-topic or offensive.
9. Use common sense and common courtesy: for example, it's best to ask permission to publish or report on conversations that are meant to be private or internal to [Company Name]. Make sure your efforts to be transparent don't violate [Company Name]'s privacy, confidentiality, and legal guidelines for external commercial speech.
10. Stick to your area of expertise and do feel free to provide unique, individual perspectives on non-confidential activities at [Company Name].

11. When disagreeing with others' opinions, keep it appropriate and polite. If you find yourself in a situation online that looks as if it's becoming antagonistic, do not get overly defensive and do not disengage from the conversation abruptly: feel free to ask the PR Director for advice and/or to disengage from the dialogue in a polite manner that reflects well on [Company Name].
12. If you want to write about the competition, make sure you behave diplomatically, have the facts straight and that you have the appropriate permissions.
13. Please never comment on anything related to legal matters, litigation, or any parties [Company Name] may be in litigation with.
14. Never participate in Social Media when the topic being discussed may be considered a crisis situation. Even anonymous comments may be traced back to your or [Company Name]'s IP address. Refer all Social Media activity around crisis topics to PR and/or Legal Affairs Director.
15. Be smart about protecting yourself, your privacy, and [Company Name]'s confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully. Google has a long memory.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Social Networking	Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

Revision History

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of [Company Name] authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing [Company Name]-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Viewing websites with adult or otherwise inappropriate, discriminatory, or derogatory content.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by [Company Name].
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which [Company Name] or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a [Company Name] computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any [Company Name] account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended

recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to [Company Name] is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, [Company Name] employees to parties outside [Company Name].

Email and Communications Activities

The [Company Name] email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any [Company Name] employee should report the matter to their supervisor immediately.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within [Company Name]'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by [Company Name] or connected via [Company Name]'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

[Company Name] employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. [Company Name] may monitor messages without prior notice. [Company Name] is not obliged to monitor email messages.

Acceptable Encryption Policy
For [Company Name]

Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Scope

This policy applies to all [Company Name] employees and affiliates.

Policy

Proven, standard algorithms such as Triple DES, Blowfish, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. [Company Name]'s key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Corporate. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Revision History

Extranet Policy
For [Company Name]

Purpose

This document describes the policy under which third party organizations connect to networks for the purpose of transacting business related to [Company Name].

Scope

Connections between third parties that require access to non-public [Company Name] resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for [Company Name] or to the Public Switched Telephone Network does NOT fall under this policy.

Policy

Pre-Requisites

Security Review

All new extranet connectivity will go through a security review. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

Third Party Connection Agreement

All new connection requests between third parties and [Company Name] require that the third party and [Company Name] representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the [Company Name] Corporate Office as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into [Company Name] are to be kept on file with the [Company Name]'s Corporate Office.

Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by the Corporate Office. Typically this function is handled as part of the *Third Party Agreement*.

Point Of Contact

The Corporate Office must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the [Company Name], and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the POC changes, the relevant extranet organizational unit must be informed promptly.

Establishing Connectivity

Organizational units within [Company Name] that wish to establish connectivity to a third party are to file a new site request with the Corporate Office. The Corporate Office will address security issues inherent in the project. If the proposed connection is to terminate within [Company Name], the organizational unit must engage the [Company Name]'s Corporate Office. The organizational unit must provide full and complete information as to the nature of the proposed access to the Corporate Office, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will [Company Name] rely upon the third party to protect [Company Name]'s network or resources.

Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The organizational unit is responsible for notifying the Corporate Office when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

Terminating Access

When access is no longer required, the organizational unit within [Company Name] must notify the team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranets must be audited on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct [Company Name] business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct [Company Name] business necessitate a modification of existing permissions, or termination of connectivity, the Corporate Office will notify the POC or the organizational unit of the change prior to taking any action.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Terms	Definitions
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
Organizational unit	The [Company Name] organization who requested that the third party have access into [Company Name].
Third Party	A business that is not a formal or subsidiary part of Wells Family Dentistry.

Revision History

Guidelines on Anti-Virus Process
For [Company Name]

Recommended processes to prevent virus problems:

- If using a personally owned device to access [Company Name]'s servers or data, always run the Corporate standard, supported anti-virus software. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with [Company Name]'s *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette or flash drive from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check the *Anti-Virus Policy* and this Recommended Processes list for updates.

Proposed Firewall Policy
For [Company Name]

The firewall must be a part of a consistent overall organizational security architecture. Firewall policies must be realistic, and reflect the level of security in the entire network.

Firewalls are only as sound as their supporting firewall policies. It is imperative that the rules concerning the configuration of every component in the firewall (Internet router, firewall, proxy server, virus software) are properly understood, fully documented and carefully implemented.

Independent testing of the firewall on a regular basis, and especially immediately after installation, is essential. The majority of successful hacking attempts are due to inadequate or faulty configuration of one or more firewall components. Attacks on the firewall by a firm specializing in such services, using reputable testing software, should be carried out immediately after implementation and on a regular (preferably monthly) basis thereafter.

Implement an alerting system to warn of attempted attacks. Ideally, alerts should be generated by the firewall and by the proxy servers. Penetration tests should trigger these alerts. Careful screening of anyone who is to have physical or logical access to the firewall components or their documentation must be conducted. This should include at least two references (one business, one character), an identity check (passport or driving license) and a credit check.

Anyone who is to have physical or logical access to the firewall components or their documentation must sign a non-disclosure and confidentiality agreement.

Policies and procedures must be applied to contractors and third-party employees as thoroughly as to permanent staff. Third-party organizations must be asked to sign “like measures” contracts to ensure that they apply similar controls to [Company Name]’s.

All firewall components should be located in a secure room with controlled and limited access.

Remote management of any component in the firewall must not be permitted, unless via an encrypted and authenticated dial-up connection.

A duplexed installation should be considered to prevent a single point of failure. Bear in mind that the opportunity for configuration error is also doubled in this situation and extra care should be taken in documenting, implementing and testing such an installation.

The bottleneck effect of each firewall component must be carefully measured to ensure that future traffic volumes are not constrained by today’s choice of product. Performance is as important as security in each of these components.

Implement in stages.

Business plan and "plain English" requirements documentation – **who** needs **which** service, **when** and **why**!

"Shopping list" of components to implement the requirements. Includes routers, firewalls, proxy servers, mail relays, virus control, content management, log monitoring and alerting software.

Technical configuration documentation for each firewall component. Includes descriptions of how each component achieves its control objectives.

Documentation of responsibilities and procedures for installation, maintenance, patching and updates, rule changes and incident response.

Implementation and test of pilot.

Roll out

Regular configuration and penetration tests

The firewall documentation must be regarded as a **controlled system**. The firewall documentation will comprise:

- the *Security Requirements of [Company Name]*
- the *Firewall Policy and Specification for [Company Name]*
- the *[Company Name] Firewall Change Log*
- the printed configuration of the firewall operating system (including all user accounts)
- the configuration of the firewall software and its rules

When a controlled document is updated, the obsolete document must be recalled and the updated document issued. All old copies must be destroyed except one, which must be marked "Obsolete" and retained in the Document Change file.

"Changes" means any changes in the firewall system **whatsoever**, including (but not limited to):

- hardware
- operating system
- firewall software
- proxy software
- firewall rules
- use or number of administrative accounts
- physical location of the firewall components

Any changes to the firewall configuration **whatsoever** must be validated against the Requirements Document and the Firewall Policy and Specification (this document). If necessary these documents must be updated and re-approved to reflect the changes.

Any changes to the firewall configuration **whatsoever** must be recorded in the firewall change log.

Each controlled document shall contain the following information:

- Document name and location (in the header)
- Issue date (in the header)
- Issue number (in the footer)
- Page number and total number of pages (in the footer)

Document change records must be retained for a period of 5 years.

[Company Name] Firewall Overview

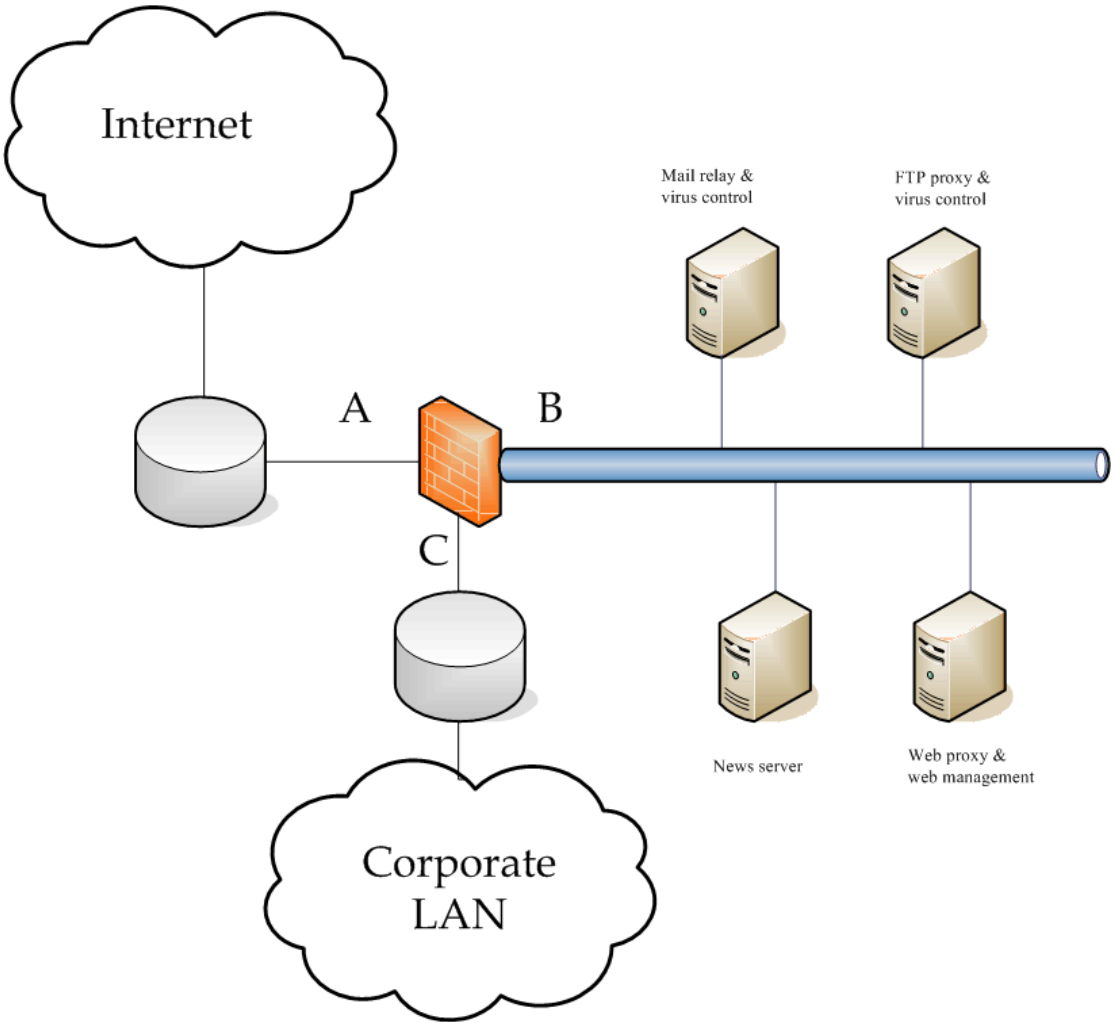

Figure 5. Firewall Diagram

The firewall box ("the [Company Name] Firewall"), controls the traffic between [Company Name] users (interface "C"), the demilitarized zone (interface "B") and the Internet (interface "A").

Proxy hosts are located on the demilitarized zone (DMZ). ***Although each proxy is shown as a separate computer, proxy functions may be combined where product compatibility, performance and traffic volume permit.***

The firewall will be configured to block all traffic, with the exception of the rules in the table shown in this document.

Only the following traffic will be permitted in the [Company Name] firewall.

Table 4

Ref No	From	To	Protocol	Restrictions
1	A	B	HTTP/HTTPS	To web proxy only (by IP address)
2	B	A	HTTP/HTTPS	From web proxy only (by IP address)
3	C	B	HTTP/HTTPS	To web proxy only (by IP address)
4	B	C	HTTP/HTTPS	From web proxy only (by IP address)
5	A	B	FTP	To FTP proxy only (by IP address)
6	B	A	FTP	From FTP proxy only (by IP address)
7	C	B	FTP	To FTP proxy only (by IP address)
8	B	C	FTP	From FTP proxy only (by IP address) (download B to C only)
9	A	B	NNTP	From news server only (by IP address)
10	B	A	NNTP	To news server only (by IP address)
11	C	B	NNTP	From news server only (by IP address)
12	B	C	NNTP	To news server only (by IP address)
13	A	B	SMTP	To mail relay only (by IP address)
14	B	A	SMTP	From mail relay only (by IP address)
15	C	B	SMTP	To mail relay only (by IP address)
16	B	C	SMTP	From mail relay only (by IP address)

Table 4. Access Control List

The mail relay will be configured to log all mail traffic and to virus scan (and quarantine where appropriate) all e-mail attachments.

The web proxy will utilize web management software to block access to libelous, offensive or pornographic material and to non-business sites. The web management software will also be configured to monitor web use.

The FTP proxy will be configured to monitor all FTP traffic and to virus scan (and quarantine where appropriate) all file transfers.

The news server will be configured to block access to non-business sites and to monitor newsgroup use.

An alerting and reporting system should be implemented to manage the logs of all the firewall components.

Use the following check list to determine that users are correctly prepared for use of the firewalled service:

Are there written guidelines for the use of firewalled services?
□ No □ Draft □ Finalized (not issued) □ Issued (not trained) □ Issued & trained

Are all users of firewalled services formally authorized to do so by their management?
□ No □ Some □ Yes

Does each user have a dedicated username and password for access to services?
□ No □ Some □ Yes

Use the following check list to determine that the firewall is properly implemented:

Is there a business plan, containing “plain English” requirements documentation? (detailing who needs which service, when and why)
□ No □ Yes

Is there a “shopping list” of components required to implement the requirements of the business plan? (detailing routers, firewalls, proxy servers, mail relays, virus control, content management, log monitoring and alerting software)
□ No □ Yes

Is there thorough technical configuration documentation for each firewall component? (detailing descriptions of how each component achieves its control objectives)
□ No □ Yes

Is there documentation of responsibilities and procedures for:
installation?
□ No □ Yes

maintenance?
□ No □ Yes

patching and updates?
□ No □ Yes

rule changes?
□ No □ Yes

incident response?
□ No □ Yes

Are there regular configuration and penetration tests of all firewall components?
□ No □ Yes

Are there configuration and penetration tests of all firewall components after each change of configuration or update?
□ No □ Yes

Appendix D

Information Security Checklist

- Risk management plan
  - Security strategy
  - Security Plan
- Risk Assessment
  - Assets (Location & Value)
  - Compliance
  - Threats & Vulnerabilities (external and internal)
- Policies, procedures and guidelines.
  - Enterprise Security Policy
  - Acceptable Use Policy
  - Acceptable Encryption Policies
  - E-mail use Policy
  - Extranet Policy
  - Anti-virus Guidelines
  - Firewall Configuration Policy
  - Mobile Device Use Policies
  - Social Networking/Social Media/Web 2.0 Acceptable Use Guidelines
- Security and Policy Awareness/ Training Plan
- Incident Response Plan
- Disaster Recovery/Business Continuity Plan
- Change Management Plan