MODERN INFORMATION SECURITY POLICIES & PROCEDURES

KYLE HESS

DECEMBER 2008

(Page left intentionally blank)

Introduction

Twenty years ago, very few professionals had practical experience securing a network, as it was a new area of IT and not a well-understood discipline. Only the highest security networks were seen as even needing security; therefore, few professionals existed. Ten years ago, organizations and hiring mangers began to realize the importance of information security as a skill. There were, however, still a very limited number of experienced professionals.

Fast-forward to today:

"The asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. For this reason, the cyber threats need to be addressed at the global level. Given the gravity of the threat and of the interests at stake, it is imperative that the comprehensive use of information technology solutions be supported by a high level of security measures and be embedded also in a broad and sophisticated cyber security culture."[i]

For example, in 2007, T.J. Maxx had data stolen from at least 45.7 million credit cards and debit cards in the largest breach of consumer information ever[ii]. In 2006, the Veterans Administration learned a computer was missing from Unisys, a subcontractor that provides software support to the Pittsburgh and Philadelphia VA Medical Centers. The computer contained insurance claim data for some patients treated in these two facilities or their community clinics. Quote: "It is important to note that we have no reason to believe the computer was stolen for the purpose of gaining veteran information or that the information has been or will be used inappropriately."[iii] Also, entities such as the Russian Business Network (RBN) offer web hosting services and internet access to all kinds of criminal and objectionable activities, with individual activities earning up to $105,000,000 in one year.[iv] Actually, this last statement is not true; technology consultant Valerie McNevin offered this gem up in 2004. The story spread; within two hops, CNN was reporting the $105 billion as an official Treasury Department estimate of global cyber crime profits.[v] However, some $276 million worth of credit cards, bank account info, security exploits and hacker tools were up for sale on online web forums and internet relay chat channels, and IRC that Symantec monitored from July 2007 to June 2008.[vi] Additionally, businesses that take active stands against such attacks are sometimes targeted by denial of service attacks originating in the RBN network. RBN has been known to sell its services to these operations for $600 per month.[vii]

Perimeter security is no longer the main focus of securing a network. For today's organization, it is essential to protect data both at rest and in transit – inside and outside of the organization. Customers expect their data to be protected and have shown that they will leave organizations that violate their trust.

Also, there is an increasing number of compliance initiatives that organizations are required to comply with, such as Sarbanes-Oxley (SOX), a U.S. mandate that applies globally to any company trading on a U.S. exchange; the Payment Card Industry (PCI) Data Security Standard (DSS), covering credit card transactions globally; HIPAA, which refers to the U.S. healthcare sector; and an increasing number of country- and industry-specific standards.

Organizations are finding themselves being required to adhere to two or more compliance standards. Each standard has varying requirements, and information security professionals have to be talented enough to deal with this growing trend. Irrefutably, as the requirement to implement new technologies and security solutions within more restricted budgets becomes more critical, the necessity for specialized training for information security professionals continues to increase.

Overview

Elements of a successful decentralized security program are comprised of strategic (long-term), tactical (short-term), and operational (day-to-day) operatives; with the ultimate goal being the protection of the organization's assets through mitigating risk. The various rings in the diagram below represent the management areas of the security program and relevant activities. This paper will present a detailed discussion of how these rings provide a defense-in-depth security strategy designed to protect the organization against security threats. Several areas of security will be discussed. Others overlap areas of management, and still others are outside the scope of this paper (or might make for a paper in and of themselves).

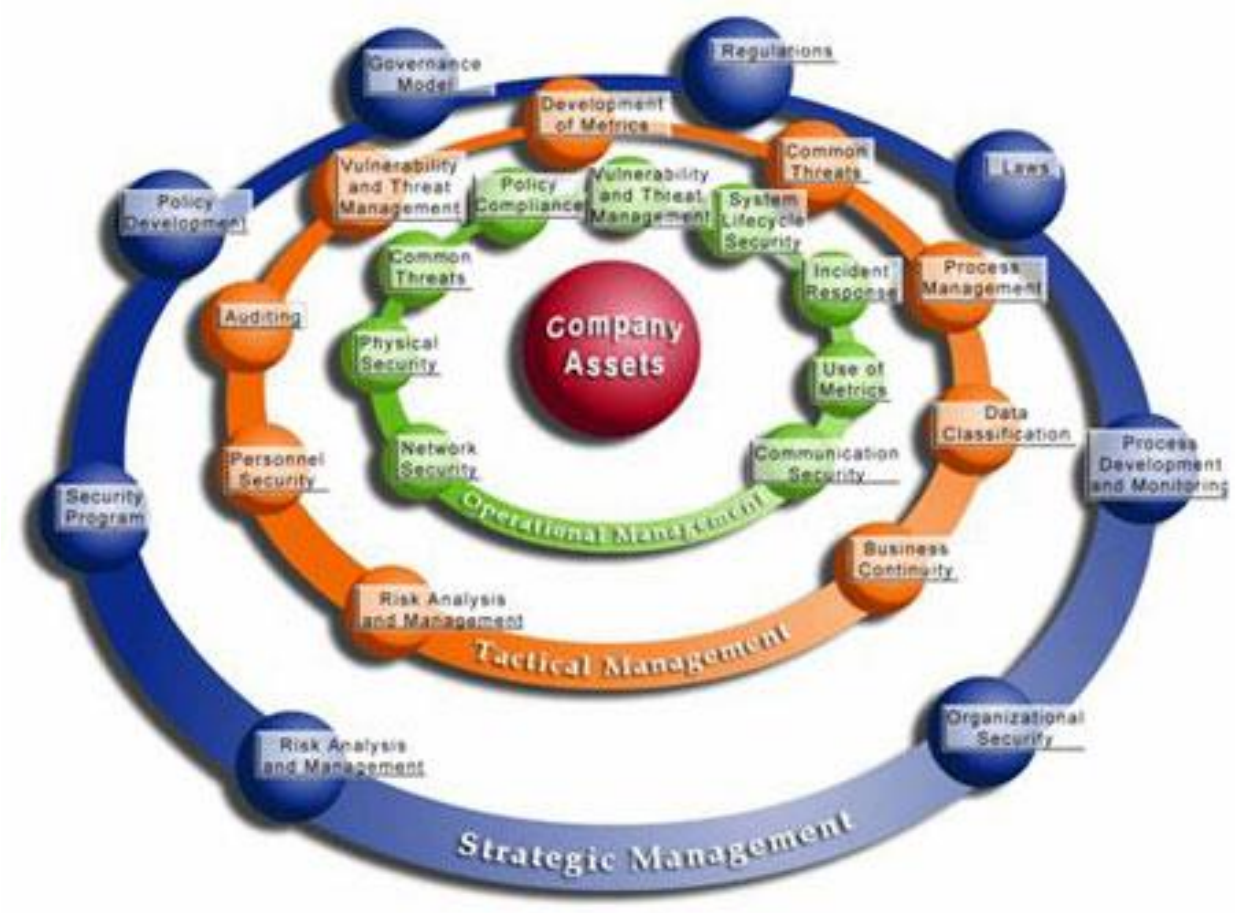

Fig 1. Key elements when building an InfoSec Program[viii]

Strategic & Tactical Management:

Security Policy

Information is an important business asset and is valuable to an organization. Thus, it needs to be protected to ensure its confidentiality, integrity and availability. The very first thing in information security is to set up policies and procedures on how to protect information. Security policies are the foundation and the bottom line of information security in an organization. A well-written and well-implemented policy contains sufficient information on what must be done to protect information and people in the organization. Security policies also establish computer usage guidelines for staff in the course of their job duties. System administrators and business owners have to acknowledge the fact that security threats exist and how to prevent and respond to them. Identifying and implementing suitable controls requires careful planning and participation of all employees in the organization and is also vital for the success of information security management. Depending on the size, financial resources, and the degree of threat, an organization needs to set up a security policy that finds the right balance between overreacting and the vulnerability of exposing a system to "the bad guys". The objective of a well written and implemented security policy is improved information availability, integrity and confidentiality, from both inside and outside the organization.

An approach to setting security policies and procedures is suggested by the following steps:[ix]

- Identify all the assets that we are trying to protect.
- Identify all the vulnerabilities and threats and the likeliness of the threats happening (risk analysis).
- Decide which measures which will protect the assets in a cost-effective manner.
- Communicate findings and results to the appropriate parties.
- Monitor and review the process continuously for improvement.

To develop a security policy, a thorough understanding of the organization is needed. Consider the goals and direction of the organization. The policy must conform to existing policies, rules, regulations and laws that the organization is subject to. First, a person with enough status to own and implement the policy should be appointed. Getting the right set of people involved from the beginning is critical to the success of the project and acceptance of the policy. It is a joint effort by the technical personnel, process owner and decision makers who have the authority to enforce the policy. The right level of authority on policy decision is required to ensure that the policy is well written and supported as it affects all employees in the organization.

Here is an example of corporate security policy:

1. In order to ensure the integrity of the company's electronic data and systems, all access from external points will be centrally managed by the Information Technology group. For connectivity to and from the public internet, centrally located and managed security firewalls will be utilized. These access points will be set up only with the approval of the VP of information technology and firewall solutions will adhere to the corporate standards approved by the VP of information technology.

2. All connections from the company's network to external networks must be approved by and managed by the perimeter security manager. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures. All connections to approved external networks will pass through company-approved firewalls.

3. E-mail should be primarily used to conduct the business of the company. It is recognized that employees may have a need to use electronic mail for personal reasons. Personal use should be kept to a minimum and should be conducted in a professional manner. All relevant laws and company policies, including those that deal with intellectual property protection, privacy, misuse of company resources, harassment, data security, and confidentiality, apply to use of company E-Mail.

4. Network equipment must be located in a secure location with restricted access. Only employees or a designee should have access to the equipment. In addition, physical access to the network equipment, whether in a secured area or not, must be restricted to authorized individuals who require such access to perform their job responsibilities. For secure access, the local network administrator must maintain a list of authorized personnel. The local network administrator is also responsible for ensuring that, when a person on the access list changes job roles or leaves the company, that access is removed for that person.

5. The company actively monitors all inbound and outbound e-mail. The company reserves the right to retrieve and read any message composed, sent, or received. Please note that even when a message is erased, it may still be possible to re-create the message; therefore, there should be no expectation of privacy of messages.

Laws & Regulations

Information security professionals work within an enterprise to protect it from all non-physical threats to the integrity and availability of its data and systems. Performing this function draws security professionals into simultaneous, ongoing relationships between the organization and the organization's employees and other agents: its customers, suppliers, competitors, government officials and regulators, to say nothing of unidentified and sometimes unidentifiable actors.[x]

A legal perspective on security is valuable in itself, as an aid to defining the assets and interests to be protected and as the source of the prerequisites for and types of recovery available when breaches of security occur. This section will be a discussion of important laws and regulations as they pertain to organizations.

CFAA - Computer Fraud and Abuse Act

The CFAA was originally created solely as a computer crime statute, but in its present form, it imposes both civil and criminal liability for a wide variety of acts that compromise the security of public and private sector computer systems.

The core provisions of the CFAA apply to "protected computer[s]," a term that the act defines in sweeping terms. Under the CFAA, the term "protected computer" means "a computer -

a. "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;" or
b. "which is used in interstate or foreign commerce or communication [.]" [xi]

The first part of the definition reflects the CFAA's origins as a 1984 law enacted to criminalize intrusions to obtain classified information or financial data that were beyond the scope of state computer crime laws then in effect. The second part of the definition, the language that extends the CFAA's protections to any computer "used in interstate of foreign communication," is responsible for the extent of the CFAA's present applicability, because it brings essentially every computer with Internet access within the scope of the statute.

The CFAA imposes liability on anyone who:

1. Intentionally accesses a protected computer without authorization or in excess of authority, and by doing so, steals anything of value, other than the use of the computer itself, where that computer use is worth less than $5,000 in any one year period
2. Knowingly transmits a program, code or instruction, and as a result, intentionally causes damage, without authorization, to a protected computer
3. Intentionally accesses a protected computer without authorization, and as a result, causes damage, recklessly or otherwise
4. Knowingly traffics illegally in passwords or other access credentials that allow unauthorized access to a computer, if that traffic effects interstate or foreign commerce or the computer is used by or for the United States government
5. Threatening to damage a protected computer with intent to extort anything of value or
6. Attempts to do any of the above

DMCA - The Digital Millennium Copyright Act

The Digital Millennium Copyright Act, 17 U.S.C. §1201- 05 (the "DMCA"), provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title [the Copyright Law]," and goes on to prohibit the "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that - (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to [a copyrighted work]; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to [a copyrighted work]; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to [a copyrighted work]."[xii]

Essentially, it criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as Digital Rights Management or DRM) that control access to copyrighted works and it also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.

Compliance

Controlling risks to personal information through enhanced information security has become the subject of many state and federal laws. The recent upsurge in the number of state and federal laws and regulations represents an emerging legal standard that imposes obligations on organizations to protect the data they collect, store, process, use, and disclose. These laws increasingly affect how higher organizations handle personal information, including sensitive

health and financial data. Many of the new laws require disclosures to victims when there is unauthorized access to systems containing sensitive information. Failure to protect PII (Personally Identifiable Information) will result in public embarrassment and the financial costs associated with managing the response to incidents and may also result in investigations, fines, and other penalties.

Many organizations do not approach information security compliance in an organized and integrated fashion. Some have permitted information security compliance to be handled by more than one department. For example, one department may be tasked with Health Insurance Portability and Accountability Act (HIPAA) compliance, while another office or departments using credit cards may focus on compliance with the Gramm-Leach-Bliley Act (GLBA) or the Payment Card Industry Data Security Standard (PCIDSS). Complicating these efforts are regulatory requirements affecting other departments, such as research facilities, as well as external business partners. As a result, efforts are often incomplete, redundant, or inadequate and expensive.

Sarbanes-Oxley

The SOX legislation was enacted on July 30, 2002 and falls under the umbrella of the U.S. Securities and Exchange Commission. SOX differs from other legislation involving information security and privacy, as it revolves around the protection of financial records and helps ensure the accuracy of financial reports as an indirect means for regulating corporate behavior. The requirements set forth for Sarbanes-Oxley compliance apply to all U.S. public companies, foreign filers in U.S. markets and privately held companies with public debt.[xiii]

Sarbanes-Oxley compliance affects multiple business units across the organization, from the CEO and the CFO to the IT and security departments. However, SOX contains various sections that directly affect the IT and information security functions in today's corporations. To maintain SOX compliance, these departments must implement access and integrity controls on financial information, as well as system monitoring and audit trails – requirements similar to common risk management processes typically present within most public corporations. Section 404 – Management Assessment of Internal Controls, is the one that affects IT and information security the most.

In order to establish SOX compliance, an annual internal control report is required to:

- State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- Contain an assessment, as of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures for the issuer for financial reporting [xiv]

The requirements for SOX compliance are policy driven in areas such as:

- User authentication -- should be based on two-factor authentication: passwords, tokens, biometrics

- Password management – must meet the following requirements: length, complexity, expiration dates
- Access controls -- should be time-specific and/or location-based
- Input validation – accomplished by designing new rules and requirements for existing application code
- Exception handling
- Secure data storage and transmission – data is encrypted in transit or at rest
- Logging – who is accessing what and when?
- Monitoring and alerting – IPS solutions need to be put in place
- System hardening – disable all unnecessary services and remove excessive permissions
- Change management – formal policies and procedures need to be in place
- Application development – testing via a QA department
- Periodic security assessments and audits – e.g. external-yearly, internal-every six months

Gramm-Leach-Bliley Act

The 1999 Gramm-Leach-Bliley Act (GLBA) requires financial institutions to develop, implement, and maintain a comprehensive written information security program that protects the privacy and integrity of customer records. GLBA compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

The GLBA Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. This plan must include:

- Identification of at least one employee to manage the safeguards,
- Construction of a thorough risk management plan on each department handling the nonpublic information,
- Developing, monitoring, and testing a program to secure the information, and
- Changing the safeguards as needed to keep pace with the changes in how information is collected, stored, and used.[xv]

Additionally, GLBA compliance requires both internal and external safeguards. Though the external threat receives the most attention, the improper use of customer information internally is actually an even greater problem. Information leaks are most often caused by employee error or negligence and can result in considerable customer inconvenience or harm, despite the fact that often no malice was intended.[xvi]

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. According to the Centers for Medicare and Medicaid Services (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.[xvii] Title II has two very pertinent pieces as they pertain to information security: The Privacy Rule and The Security Rule.

The Privacy Rule took effect on April 14, 2003. It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.

- Administrative Safeguards - policies and procedures designed to clearly show how the entity will comply with the act
- Physical Safeguards - controlling physical access to protect against inappropriate access to protected data
- Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

The Payment Card Industry Data Security Standard (PCIDSS)

The PCIDSS requires that all merchants that use credit cards comply with a number of technical, physical, and administrative requirements. Non-compliant companies, who maintain a relationship with one or more of the major credit card brands, directly or through an acquirer, risk losing their ability to process credit card payments as well as audits and/or fines. The current version of the standard (1.2) specifies 12 requirements for compliance, organized into 6 logically related groups, which are called "control objectives."[xviii]

A. 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

B. Protect Cardholder Data
   1. Protect stored cardholder data
   2. Encrypt transmission of cardholder data across open, public networks

C. Maintain a Vulnerability Management Program
    1. Use and regularly update anti-virus software
    2. Develop and maintain secure systems and applications

D. Implement Strong Access Control Measures
    1. Restrict access to cardholder data by business need-to-know
    2. Assign a unique ID to each person with computer access
    3. Restrict physical access to cardholder data

E. Regularly Monitor and Test Networks
    1. Track and monitor all access to network resources and cardholder data
    2. Regularly test security systems and processes

F. Maintain an Information Security Policy
    1. Maintain a policy that addresses information security

Risk Analysis and Management

The previous sections were dedicated to the identification and classification of risk. So, what is risk as it pertains to organizations, and how can it be mitigated? The topic of risk analysis is a rich one worthy of a course sequence of its own. The purpose of this section is to introduce the reader to some of the major points of risk analysis.

A *risk* to the organization is something that can, in some way, cause harm or reduce the operational utility of a system. *Threats* are those things which may occur independently of the system under consideration and which may pose the risk. Three aspects associated with a risk can be identified: the loss associated with the event; the likelihood that the event will occur; and the degree to which event consequences may be changed. Risks can be generic or project–specific. Generic risks are those common to all projects, such as requirements misunderstanding, key personnel loss, or insufficient time for testing. Project specific risks are threats that result from the particular vulnerabilities of the given project and organization. The lack of documentation on the success or failure of past experiences is one of the reasons for inefficient risk management utilization or non-utilization in many organizations. Besides risk management knowledge, the past experiences analysis is fundamental to help managers plan and control risks[xix]. Potential risks to an organization may include:

- Power Loss - The loss of the electrical power supply to the information systems.
- Communication Loss - The inability to transfer information to and from the organization through the defined system parameter.
- Data Integrity Loss - A realized, or perceived possible, alteration of the data and/or information maintained by or consisting of the specified asset.
- Accidental Errors - Improper use of information technology not due to malicious intent but solely through mistaken incorrect use
- Computer Virus - A program which spreads by attaching itself to "healthy" programs. After infection, the program may perform a variety of non-desirable functions.
- Abuse of Access Privileges by Employees - Employees are authorized by the security policy of the organization and further narrowed by their job responsibilities to perform a small selection of functions with the information system. This category covers those acts which may be performed but which are not authorized.
- Natural Disasters - Those occurrences which degrade some aspect of the information system other than fire and earthquake and are not manmade. Examples would be flooding, a tornado, etc…
- Attempted Unauthorized System Access by Outsider - Non-employees, or personnel not contracted to perform work on the information system that are not appropriately authorized yet are attempting, but not succeeding, in gaining access to the information system.
- Theft or Destruction of Computing Resource - A primary resource of the organization is the computing capability of its information systems. This threat addresses the unauthorized use of this resource and the destruction of this resource - through physical or other means.
- Destruction of Data - Information held by an organization is not only that used by their business applications, but includes that used by the systems to operate, manuals, personal experience and other forms. This threat may destroy that information, or simply prevent the organization from using it.
- Abuse of Access Privileges by Other Authorized User - While an employee is authorized to perform, and may be required, to perform many actions using the information system, he or she is limited to what may be done through organizational policy, job restrictions and technological controls. But an authorized user - whether an employee or contractor - may attempt to perform operations which are denied them.
- Successful Unauthorized System Access by Outsider - This covers non-employees and non-contractors using, and possibly destroying, information system resources. "Crackers" fit within this threat description.
- Non-Disaster Downtime - This covers those times when the information system is unavailable for use not caused by disaster. Examples of this would be maintenance, component failure and a system 'crashing'.
- Fire - This includes both major fires that destroy resources to those which prevent assets from being used for any reason.
- Earthquake - This includes both directly destructive and influences of lesser and distant earthquakes.

Risk Analysis

Risk analysis is a technique used to identify and assess factors that may jeopardize the success of a project or achieving a goal. This practice also helps to define preventive measures to reduce the probability of these factors from occurring and to identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the organization.

There are two primary methods and one hybrid method of risk analysis:

- Qualitative - Improve awareness of information systems security problems and the posture of the system being analyzed.
- Quantitative - Identify where security controls should be implemented and the cost envelope within which they should be implemented.
- Hybrid method- A selected combination of these two methods can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.[xx]

The first, qualitative analysis, is simpler and more widely used. Qualitative analysis helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and procedures (see fig.2) for which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls. Simply put, an organization determines the severity of an established risk by multiplying likelihood (y-axis) by potential impact (x-axis). The subsequent placement of the threat on the matrix determines the course of action that should be taken.

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Fig 2. Qualitative Risk Analysis Matrix[xxi]

Quantitative analysis does this as well as identifies the specific areas in which the losses and safeguards exist. It is based on independently objective processes and metrics and requires that an increased degree of effort be placed in deterring the cost values and that a greater amount of effort be placed into the calculations.[xxii] It presents its results in a management-friendly form of monetary values, percentages, and probabilities.

Taken from Ding Tan's Quantitative Risk Analysis Step-By-Step:

"The importance of presenting a quantitative risk analysis in a manner similar to a well-managed engineering capital project cannot be underestimated. Uncertainty, ambiguity, risk, and subjectivity make management nervous about spending money; therefore, it is imperative to present a well-prepared quantitative risk analysis to soothe management's anxiety about the unknown. By doing due diligence to collect enough corroborating data, the chance of success for project approval is greatly increased."[xxiii]

Risk Management and Governance

Risk management requires risk awareness (achieved through risk analysis) by senior corporate officers, a clear understanding of the enterprise's appetite for risk (accept, mitigate, etc…), an understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

Similar to implementing security policy, a senior officer (CEO, CIO, CSO, etc…) should be the champion of any risk management-related initiative. Buy-in is crucial: he or she has the power to accept or veto any project because they have the final authority over the budget.

Risk appetite, at the organizational level, is the amount of risk exposure, or potential adverse impact from an event, that the organization is willing to accept/retain. Once the risk appetite threshold has been breached, risk management treatments and business controls are implemented to bring the exposure level back within the accepted range.[xxiv] Any risk analysis technique can be helpful in determining an organization's risk appetite, coupled with the organizations past risk exposure and what type of business the organization is in.

To use my company as an example (see table 1), the Internal Audit department's IT risk management methodology is based on Control OBjectives for Information and related Technology (COBIT)[xxv] Framework in which IT risk falls in to the Plan & Organize domain of the COBIT framework. IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. The adoption of the COBIT guidelines and practices as a de facto standard is common because they are platform independent[xxvi]. COBIT supports IT governance (see fig. 3) by providing a framework to ensure that the following exists:

- Strategic alignment - focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- Value delivery - is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
- Resource management - is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
- Risk management - requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.
- Performance measurement - tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.[xxvii]

Fig 3. COBIT 4.1 Framework

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains are called:

- Plan and Organize (PO) -Provides direction to solution delivery (AI) and service delivery (DS)
- Acquire and Implement (AI) -Provides the solutions and passes them to be turned into services
- Deliver and Support (DS) - Receives the solutions and makes them usable for end users
- Monitor and Evaluate (ME) - Monitors all processes to ensure that the direction provided is followed[xxviii]

Table 1. Sample Risk Management Assessment:

COBIT Objectives		Risk Assessment Categories	Notes / Comments
PO1	Define a strategic IT plan	IT Governance	
PO2	Define the information architecture	Privacy & Confidentiality of Data, Data Retention	Includes data classification; propose Privacy / Location of Data Review
PO4	Define IT processes, organization and relationships	IT Governance, IT Asset Management & Procurement	
PO10	Manage projects	Global Project System, In-House Software Development, Opportunity Management System	Tested via SOX and implementation reviews; could test PMO function
AI2	Acquire and maintain application software	PeopleSoft Security, Hyperion Security, JDE Security, Lotus Notes Security, Engineering (CAD) Systems, Global Project System, In-House Software Development, Opportunity Management System	Tested via SOX and implementation reviews; could test PMO function; proposing Effectiveness of Application Usage review
AI3	Acquire and maintain technology infrastructure	Windows Active Directory, UNIX Security, Enterprise Voice Network, Oracle Database, AS400, NA Firewall, Raptor (telnet software for JDE), Remote Network Access, Desktop & Technical Support	Tested via SOX and implementation reviews; could test PMO function

Please take note that many of the COBIT objectives are tested using SOX controls. Many governance frameworks (COBIT, ISO27001) can map to different compliance models (SOX, PCIDSS, GLBA), the organization must determine which tools to use and how to use them. SOX and COBIT work well together because together they can define the following[xxix]:

- Performance indicators (e.g., benchmarks) from both internal and external sources are defined, and data are collected and reported regarding achievement of these benchmarks.
- IT management monitors its delivery of services to identify shortfalls and responds with actionable plans to improve.
- IT management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, and benchmarks.
- Serious deviations in the operation of internal control, including major security, availability, and processing integrity events, are reported to senior management.
- Internal control assessments are performed periodically, using self-assessment or independent audit, to examine whether internal controls are operating satisfactorily.
- IT management obtains independent internal control reviews of third-party service providers

Operational Management

The (network, or security) operations department has responsibilities that pertain to everything that takes place to keep a network, computer system, applications and environment up and running in a secure and protected manner. After the network is setup is when operations kicks in, which includes the continual day-to-day maintenance of an environment. These activities are routine in nature and enable the environment, systems and applications to continue to run correctly and securely.[xxx]

Whether it's an "Army of One" position in a two-hundred seat company, or a team of a dozen Security Analysts staffing a 24x7x365 SOC (Security Operations Center) facility protecting a 200,000 seat, globally networked organization; the constant barrage of cyber threats today demands a well orchestrated, diligently maintained, and extremely nimble posture. It is no longer sensible to simply dole out security responsibilities to system administrators and "hope for the best". Disparately applied processes, unilateral prioritizations, and daunting system administrator workloads, lead to an uneven (and oftentimes negligent) execution of security measures across the enterprise. [xxxi]

Here are but a few of the challenges facing security professionals today:

- As organizations continue to allow business partners and customers access to critical corporate data, security professionals cannot tell the difference between insiders and outsiders anymore – putting private data and intellectual property at risk.
- The multiple point products in use today don't share information, which increases the cost and complexity of security management, limiting end-to-end visibility, and resulting in false positives and undetected attacks.
- Operations teams (security, network, data center, and audit) are not working together, duplicating efforts and impacting response time.
- Organizations lack an understanding of its security posture both within business divisions and from an enterprise-wide perspective because there is no central aggregation of relevant data. [xxxii]

Operational management is the day-to-day application and execution of the planned overall organizational security strategy (strategic and tactical). Operational management makes use of hardware and software solutions as well as technical and organizational know-how. If planned correctly, the strategy will provide defense-in-depth security across the entire organization, no matter how big or small. Some day-to-day activities may include:

- Monitoring network traffic for anomalies
- Reviewing the logs of antivirus and endpoint servers
- Scanning the network for rogue PCs using an asset discovery tool
- Properly securing backup media
- Checking to make sure that all privileges are removed from termed employees

Antivirus Software

Antivirus software are computer programs that attempt to identify, neutralize or eliminate malicious software. The term antivirus is used because the earliest examples were designed exclusively to combat computer viruses; however most modern antivirus software is now designed to combat a wide range of threats including: worms, spyware, phishing attacks, rootkits, and Trojans, which are often described collectively as malware.

A quick overview of malware:

- A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive. Also, viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer.
- A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other computers and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through.
- Spyware programs can collect various types of personal information, such as Internet surfing habits, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party.[xxxiii] Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.
- Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization.
- A rootkit is malware which consists of a program (or combination of several programs) designed to take fundamental control (in Unix terms "root" access, in Windows terms, "Administrator" or "Admin" access) of a computer system, without authorization by the system's owners and legitimate managers.[xxxiv] Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms.

- A Trojan is malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. They are used to circumvent protection systems in effect creating a vulnerable system to allow unauthorized access to the user's computer.

My company uses Symantec Corporate antivirus (SAV) and Symantec Endpoint Protection (SEP) to combat malware. We are in the process of moving all servers and PCs over to Endpoint Protection exclusively, so the focus of this section will be on SEP. So far, SEP seems to be an excellent product; there is an entire suite of products wrapped up into the one package, much of the execution is automated, and many of the functions can be controlled centrally. Virus definitions are pushed out automatically on a daily basis, or can be deployed manually via the Live Update server (see fig. 4).

Fig 4. Symantec Endpoint Protection Screenshot

All policies and packages can be deployed from the central SEP server. In addition, all reporting servers and PCs can be monitored centrally. There is comprehensive monitoring and reporting tools built into the dashboard (see fig. 5). I have it configured to include: Action Summaries, Risks per Hour, Status Summaries, Definition Distribution, and Unacknowledged Notifications. In addition, I have set up email notifications for myself and several local IT administrators for several types of noteworthy events (new risks, virus defs out-of-date, and server changes).

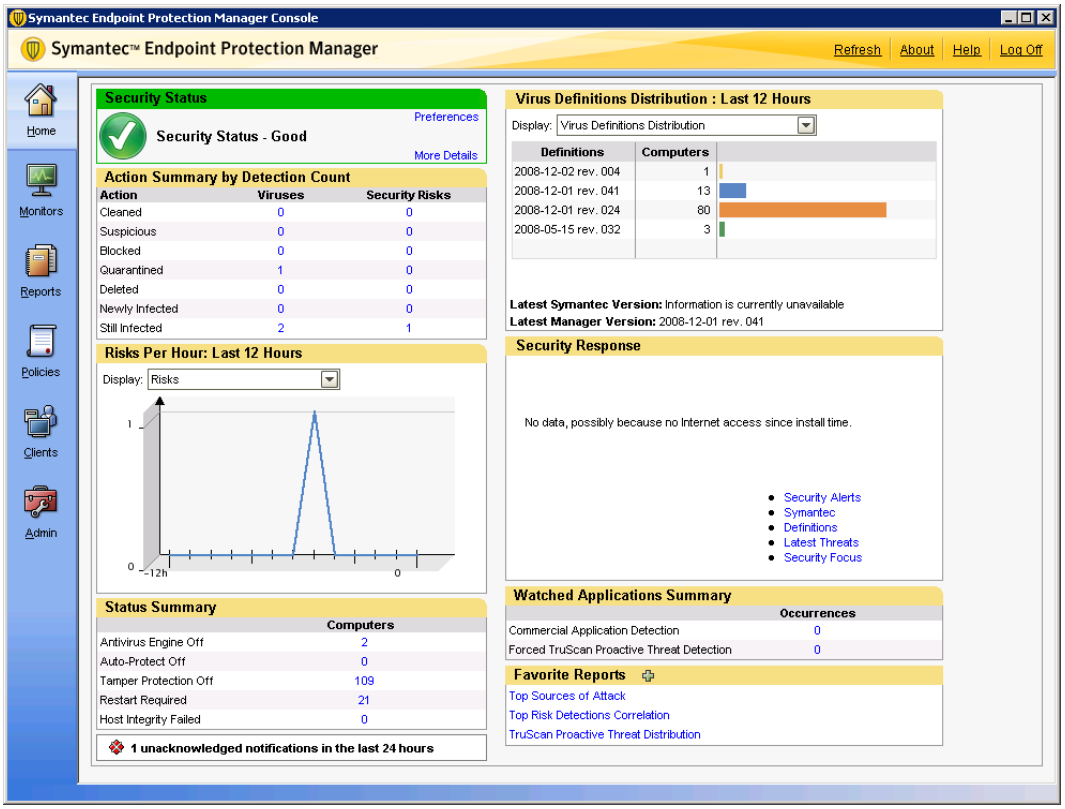

Fig 5. Symantec Endpoint Protection Server Dashboard

IPS

An intrusion-prevention system (IPS) is an inline security device that performs deep-packet inspection to identify and block malicious traffic. IPSs are considered an improvement over intrusion-detection systems (IDS), which are passive devices that simply identify an attack but take no action to block it. IPSs are designed to respond in real time to attacks by dropping packets deemed malicious, all the way up to the application layer.

IPS devices protect networks in a variety of ways. First, IPSs look for signatures of known viruses and worms, and block that traffic when an attack is identified. IPSs also have a rate-limiting feature that allows a network administrator to set a threshold of traffic that is allowed to pass at any one time. This technique thwarts distributed denial-of-service attacks, in which an attacker floods the network with otherwise legitimate traffic. IPS devices also use behavior analysis to build a baseline of normal network activity and to raise alerts when abnormal behavior is occurring on the network. Most IPS devices offer all three types of protection.[xxxv] My company purchased and implemented Tipping Point's IPS solution about 9 months ago. A typical network-wide TippingPoint deployment consists of SMS Clients, a centralized Security Management System (SMS), and multiple TippingPoint systems (see fig 6).

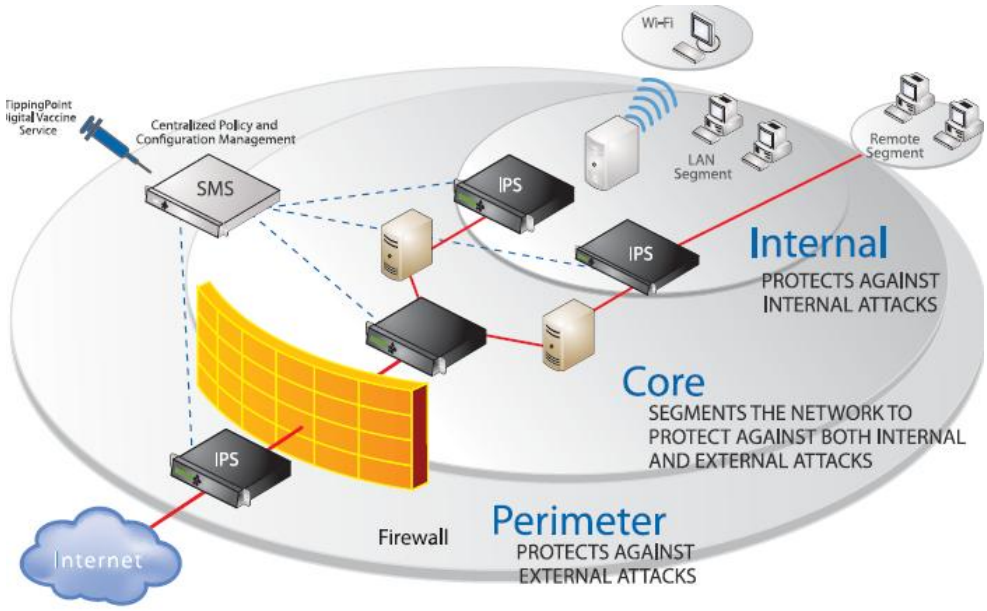

Fig 6. Tipping Point IPS deployment[xxxvi]

I also wanted to mention the dashboard. The SMS dashboard displays an overview of current performance for all TippingPoint systems in the network, including notifications of updates and potential problems that may need attention (see fig 7).

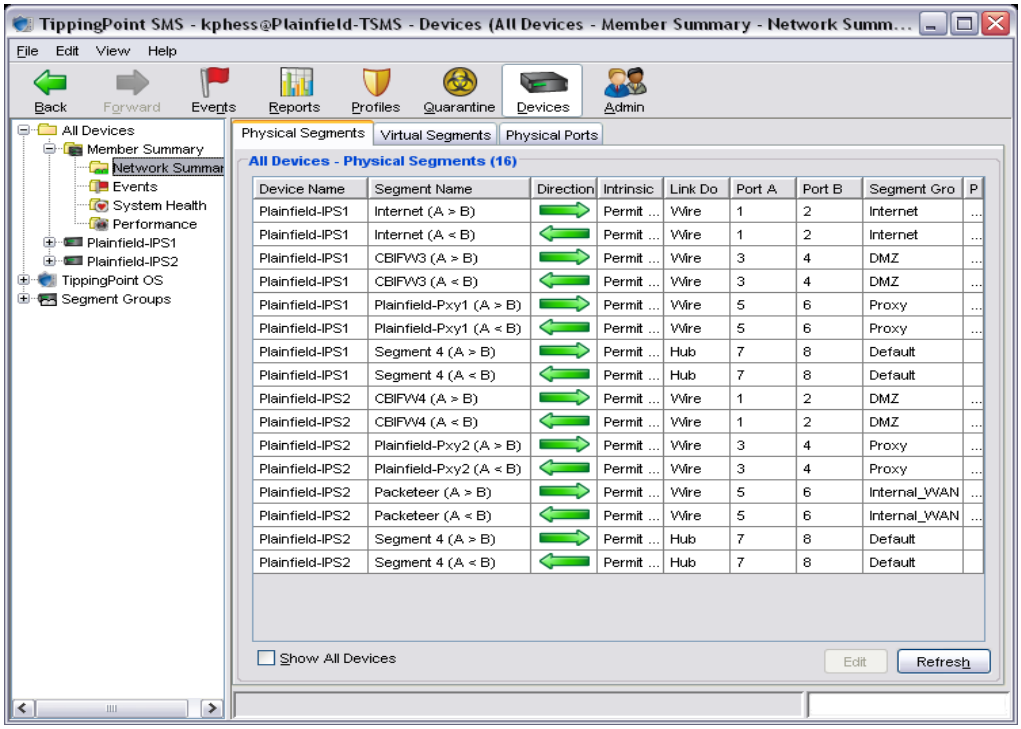

Fig 7. TippingPoint Dashboard

SIEM

Many systems and applications which run on a network generate events which are kept in event logs. These logs are essentially lists of events, with records of new events being appended to the end of the logs as they occur. Well-defined protocols, such as syslog and SNMP, can be used to transport these events, as they occur, to logging software that is not on the same host on which the events are generated. A SIEM (Security Information and Event Manager) is a piece of software (or a hardware appliance) which takes as input logs and alerts from a variety of systems, such as firewalls, routers, and servers, and attempts to inform the engineer of unusual occurrences which warrant further investigation.[xxxvii]

It is beneficial to send all events to a centralized SIEM system for the following reasons:

- Access to all logs can be provided through a consistent central interface (fig. 8)
- The SIEM can provide secure, forensically sound storage and archival of event logs
- Powerful reporting tools can be run on the SIEM to mine the logs for useful information
- Events can be parsed as they hit the SIEM for significance, and alerts and notifications can be immediately sent out to interested parties as warranted
- Related events which occur on multiple systems can be detected which would be impossible to detect if each system had a separate log
- Events which are sent from a system to a SIEM remain on the SIEM even if the sending system fails or the logs on it are accidentally or intentionally erased[xxxviii]

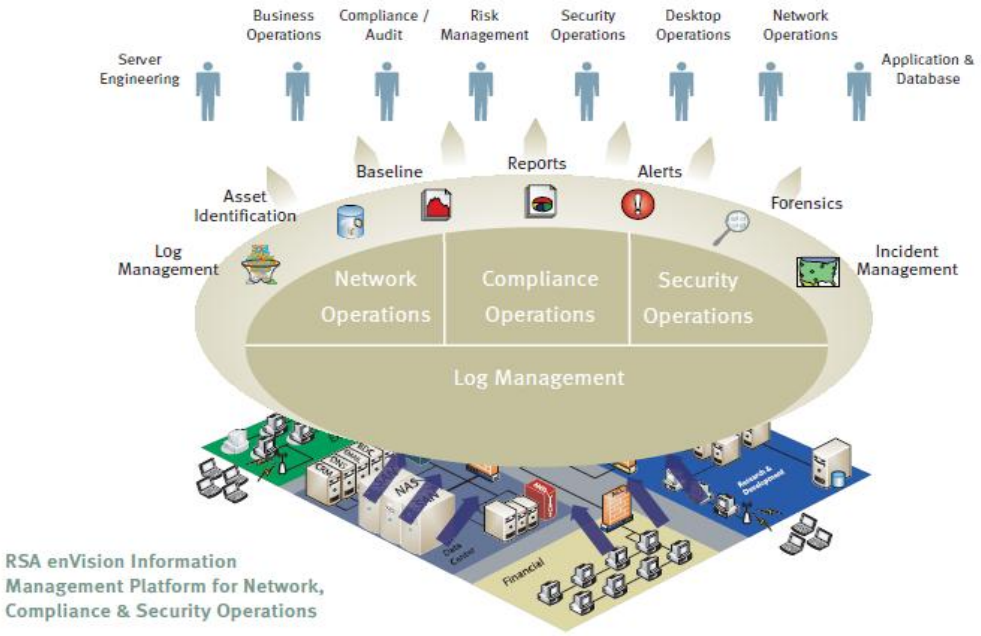

Fig 8. RSA enVision SIEM Log Management Solution[xxxix]

No SIEM tool is an island. To function effectively, a SIEM tool will require pre-deployment and integration with several security devices. For optimum effectiveness, reporting data from a firewall, an IPS/IDS sensor, an authentication service (AAA, LDAP, AD, etc...), and vulnerability scan data will need to be integrated during the incident handling preparation phase. In addition, for forensic identification and prosecution the data capture and correlation can be invaluable. For auditing and compliance, proper reporting can go a long way towards proving compliance. A good SIEM tool can provide the analytics and knowledge of a good security engineer and can be automated and repeated against a mountain of events from a range of devices. Instead of 1,000 events per day, an engineer using a SIEM can handle 100,000 events per day (or more). And a SIEM doesn't leave at night, find another job, or take vacations. [xl]

My company implemented the RSA enVision SIEM around 6 months ago. It offers all of the above-mentioned features; the reporting functionality is fantastic. Also, it allows us to centrally manage much of the malicious activity that occurs globally. As shown somewhat loosely in fig. 4, daily reports are generated to designated local IT administrators around the globe. All network segments report up through the SEIM with any alerts, incidents, etc… If anything is amiss (see fig. 9), the problem gets fixed in a timely fashion, without me having to track anyone down.

	A	B	C	D	E	F	G
1	Date/Time	"ComputerName"	"UserName"	"VirusName"	"FileName"	"Action"	
2	54:55.0	00051871-XPD	squintero	<Virus Name>	E:\\RECYCLER\\S-1-	Risk Repaired	
3	54:56.0	00051871-XPD	squintero	<Virus Name>	E:\\RECYCLER\\S-1-	Risk Repaired	
4	54:56.0	00051871-XPD	squintero	W32.Ircbrute	E:\\RECYCLER\\S-1-	Virus Found	
5	34:25.0	00013484-XPD	SYSTEM	<Virus Name>	E:\\autorun.inf	Risk Repaired	
6	34:25.0	00013484-XPD	SYSTEM	W32.SillyFDC	E:\\autorun.inf	Virus Found	
7	35:51.0	00013484-XPD	SYSTEM	<Virus Name>	c:\\documents and	Risk Repair Failed	
8	36:13.0	00013484-XPD	SYSTEM	<Virus Name>	c:\\documents and	Risk Repair Failed	
9	37:10.0	00013484-XPD	psodaprom	Trojan Horse	E:\\RECYCLER\\S-1-	Virus Found	
10	37:10.0	00013484-XPD	SYSTEM	<Virus Name>	E:\\autorun.inf	Risk Repaired	
11	22:56.0	00051871-XPD	squintero	<Virus Name>	E:\\RECYCLER\\S-1-	Risk Repaired	
12	22:56.0	00051871-XPD	squintero	<Virus Name>	E:\\RECYCLER\\S-1-	Risk Repaired	
13	22:56.0	00051871-XPD	squintero	W32.Ircbrute	E:\\RECYCLER\\S-1-	Virus Found	
14	51:33.0	00009066-XPL	radabrx	<Virus Name>	C:\\Documents and	Risk Repaired	
15	51:33.0	00009066-XPL	radabrx	<Virus Name>	C:\\Documents and	Risk Repaired	
16	51:33.0	00009066-XPL	radabrx	VBS.Redlof.A	C:\\Documents and	Virus Found	
17	59:23.0	00050382-XPL	JREILLY	Infostealer.Gampass	D:\\Music\\go hard	Virus Found	
18	59:23.0	00050382-XPL	JREILLY	Trojan.Wimad	D:\\Music\\kanye v	Virus Found	
19	59:24.0	00050382-XPL	JREILLY	Infostealer.Gampass	D:\\Music\\go hard	Virus Found	
20	59:24.0	00050382-XPL	JREILLY	Trojan.Wimad	D:\\Music\\kanye v	Virus Found	
21	07:39.0	00007292-XPD	EBGUTIERREZ	<Virus Name>	Unavailable	Risk Repaired	
22	07:44.0	00007292-XPD	EBGUTIERREZ	<Virus Name>	Unavailable	Risk Repaired	
23	55:20.0	00050589-XPD	SYSTEM	<Virus Name>	C:\\Program Files\\	Risk Repaired	
24	55:20.0	00050589-XPD	SYSTEM	Trojan.Zlob	c:\\program files\\a	Virus Found	
25	55:21.0	00050589-XPD	SYSTEM	<Virus Name>	C:\\Program Files\\	Risk Repaired	
26	03:08.0	00050589-XPD	SYSTEM	<Virus Name>	C:\\System Volume	Risk Repaired	
27	03:08.0	00050589-XPD	SYSTEM	Trojan.Zlob	c:\\system volume	Virus Found	

Fig 9. Sample RSA enVision Report

Conclusion

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.[xli] Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. It is achieved by implementing a suitable set of controls, including policies, procedures, organizational structures, software and hardware. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

Finally, I believe that the content of this paper is not only accurate in describing the myriad of challenges the information security professional faces today, but also thought-provoking enough to open the eyes of an unconvinced executive who is teetering on the fence of whether or not to take modern security policies and procedures seriously.

[i] http://www.circleid.com/posts/estonian_cyber_security_strategy/
[ii] http://www.msnbc.msn.com/id/17871485/
[iii] http://www.usa.gov/veteransinfo.shtml
[iv] http://en.wikipedia.org/wiki/Russian_Business_Network
[v] http://blog.wired.com/27bstroke6/2007/09/cybercrime-more.html
[vi] http://blog.wired.com/27bstroke6/2008/11/the-nets-underg.html#more
[vii] http://en.wikipedia.org/wiki/Russian_Business_Network
[viii] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210562,00.html?bcsi_scan_04EACAFF688FDA04=vjCYQwF6dF6sQ5wrQ7PQZAUAAACPxF0D&bcsi_scan_filename=0,289483,sid14_gci1210562,00.html%20#
[ix] http://www.sans.org/reading_room/whitepapers/policyissues/494.php
[x] http://www.securityfocus.com/infocus/1669
[xi] 18 U.S.C.§ 1030 (e)(2).
[xii] 17 U.S.C. §1201 (b)
[xiii] http://h20427.www2.hp.com/program/taw/ap/en/200802/4005.htm
[xiv] http://h20427.www2.hp.com/program/taw/ap/en/200802/4005.htm
[xv] http://banking.senate.gov/conf/
[xvi] http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act
[xvii] http://www.hhs.gov/ocr/hipaa/
[xviii] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
[xix] http://www.jucs.org/jucs_9_7/managing_organizational_risk_knowledge/de_Landa_Farias_L.pdf
[xx] http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf
[xxi] http://www.pmc.gov.au/implementation/images/risk_matrix.gif
[xxii] http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf
[xxiii] http://www.sans.org/reading_room/whitepapers/auditing/849.php
[xxiv] http://www.continuitycentral.com/feature0170.htm
[xxv] http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
[xxvi] http://searchsecurity.techtarget.com/searchSecurity/downloads/Lahti_Ch02.pdf
[xxvii] http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39073
[xxviii] http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39073
[xxix] http://searchsecurity.techtarget.com/searchSecurity/downloads/Lahti_Ch02.pdf
[xxx] http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1064650,00.html
[xxxi] http://www.csoonline.com/article/453484/Centralizing_Enterprise_Security_Operations_and_Management
[xxxii] http://www.eiqnetworks.com/solutions/Security_Operations.shtml
[xxxiii] http://www.onguardonline.gov/topics/spyware.aspx
[xxxiv] http://www.usenix.org/publications/login/1999-9/features/rootkits.html
[xxxv] http://www.networkworld.com/buyersguides/guide.php?cat=865474
[xxxvi] http://www.tippingpoint.com/pdf/resources/datasheets/400917-007_TippingPointIPS.pdf
[xxxvii] http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf
[xxxviii] http://en.wikipedia.org/wiki/Siem
[xxxix] http://www.rsa.com/node.aspx?id=3170
[xl] http://www.sans.org/reading_room/whitepapers/logging/1781.php
[xli] http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm