

# **The Application of NIST Special Publication 800-39 for Small Businesses and Organizations**

A Project  
Submitted to the Faculty of the Graduate School of  
The University of Minnesota

By  
Nathaniel L. Hunstad

University of Minnesota  
Technological Leadership Institute

Advisors:

Chair:	Prof. Massoud Amin
Co-Chair:	Prof. Elizabeth Amin
Advisor:	Prof. Alfred Marcus

In Partial Fulfillment of the Requirements for the Degree  
Master of Science in Security Technologies (MSST)

August 2, 2011



## **Executive Summary**

### **– Problem: IT security is vital for small businesses but easy for businesses to overlook**

Since usable IT security can be a complex topic, it can easily be overlooked by small businesses that are short on resources such as money and security-aware personnel. Nevertheless, IT security is just as vital for small businesses as larger businesses. With the increasing number of cybercriminals targeting small businesses, IT security can no longer be ignored.

### **– Possible Solution: NIST Special Publication 800-39**

NIST Special Publication 800-39 is designed to be “the flagship document in the series of information security standards and guidelines” published by NIST. Although implementation is only required by the federal government and contractors, the 800-39 publication can also be used by private businesses as a guideline for security.

### **– Issue: Adapting NIST Special Publication 800-39 to the needs of small businesses**

Because the 800-39 publication is specifically aimed at large government organizations, it has a number of aspects that are not as applicable to small businesses. The focus of this capstone is whether it is possible to use the publication as a foundation for IT security guidance by selectively focusing on those aspects most applicable to small businesses.

### **– Methodology: Survey, literature review, worksheet development, and case studies**

An online survey was conducted, which along with other data shows that small businesses recognize the need for improving their IT security but are not currently achieving the security posture that larger businesses have achieved. With this data and feedback, a worksheet was created based on the 800-39 publication and used in real-life case studies. The case studies show that the worksheet was able to identify and assess IT security-related vulnerabilities in a useful and user-friendly manner, without requiring exorbitant investment in time and other resources.

There are a number of IT security standards available for use by businesses. The 800-39 publication compares favorably to alternative standards, being more comprehensive than some application- and industry-specific standards, as well as being equally or more accessible than other comprehensive standards.

### **– Recommendation: Implementation, with continuous development of the worksheet**

Based on user feedback, this worksheet and the 800-39 publication can be a useful tool for evaluating security. Additional development of the worksheet, possibly branching out to other security realms, can enhance business security in a cost-effective manner.

### **– Delta MSST: Providing the tools for putting a security plan together**

The MSST program provides the tools for putting together a security plan, including the leadership necessary to shepherd the process from beginning to end. Issues such as scenario planning, analysis of complex networks, and evaluation of interdependencies all helped make this project a success.

# Table of Contents

Executive Summary.....	1
Table of Contents.....	2
Introduction.....	3
Problem Statement.....	5
NIST Special Publication 800-39 Implementation Issues.....	5
Project Methodology.....	8
Literature Review.....	8
Online Survey.....	12
Case Studies.....	13
Worksheet Development.....	13
Analysis.....	15
SWOT Analysis.....	15
Online Survey Results.....	16
Case Studies.....	19
Comparisons with Other Standards.....	22
TIM-TIP Analysis.....	33
Alternative Risk Assessment Methodologies.....	34
Recommendations.....	37
Power Zone.....	37
Business Case for Development.....	38
Future Work.....	39
Applicability to Other Types of Security.....	40
Security Implications.....	41
Security Environment for Small Businesses: Security Practice.....	41
Foundation for Future Business Growth.....	42
Security Theory.....	42
Delta MSST.....	44
Scenario Planning.....	44
Trend Forecasting.....	44
Interdependencies.....	45
Complex Adaptive Systems.....	46
Leadership.....	48
Bibliography.....	49
Appendices.....	54
Appendix A: Online Survey Questions and Responses.....	54
Appendix B: First Draft of Worksheet.....	74
Appendix C: Government Organization A Worksheet.....	77
Appendix D: Multimedia Company B Worksheet.....	82

## Introduction

Few topics are as large or as wide-ranging as the topics of small business economics and cybersecurity. Managing a small business, or a small non-profit organization, requires an incredible ability to multitask, covering areas as diverse as start-up capital, accounting, personnel management, marketing, inventory control, payroll, and supply chain management, just to name a few. Cybersecurity also covers a wide array of issues, including malware, botnets, spam, data integrity, firewalls, plus many more topics that change on an almost daily basis. It is little surprise that the intersection of these two realms are nearly as complex as when taken separately, and the answers are not the same for all businesses. Applying security to small businesses and small organizations is an issue that is not always comparable to the implementation of security at larger businesses.

Probably the foremost issue for small businesses trying to improve their security is the problem of determining exactly what a robust, usable security regime would look like that is appropriate for a particular small business's needs. The Department of Homeland Security has determined that creating "Usable Security" is one of the most pressing problems in Cybersecurity Research today: "Typically, as the security of systems increases, the usability of those systems tends to decrease, because security enhancements and commonly introduced in ways that are difficult for users to comprehend and that increase the complexity of user's interactions with systems" [1]. Complexity becomes an even bigger issue when the decision-makers who are in charge of the business may not be technically savvy themselves. A lack of technical know-how can lead to such problems as unclear security risks, as well as "difficulty in capturing and expressing security requirements and relating them to organizational workflows" [1].

A possible solution to this confusion, one that many businesses turn to, is seeking out and utilizing published security standards, of which there are a dizzying array in the marketplace. Some standards are required by law or administrative regulation to be implemented by certain organizations, such as the HIPAA Security Rules that must be followed by those "covered entities" that deal with health records and other personal information [2]. Other standards may not rise to the level of federal statute or rule, but are required by organizations that wish to enter into certain agreements. An example of such a standard would be the Payment Card Industry Data Security Standard (PCI DSS), implemented by businesses that handle payment cards [3]. Still other standards, like COBIT, are meant to be used as flexible frameworks for achieving IT management goals of varying scope. The diversity in standards can cause confusion for organizations looking for help in the area of security, especially when there is no legal or regulatory guidance pointing to which standard they should use. Small businesses, especially ones that do not operate in the fields of health care and finance, likely find that there are no regulatory security standards that they are subject to, and hence have little guidance in determining which standards to use.

For this project, NIST Special Publication 800-39 has been chosen for evaluation as a foundation upon which small businesses and small organizations can build to develop their IT security plans. This particular publication was chosen for several reasons. First, as a publication from the National Institute of Standards and Technology (NIST), it is available to the public free of charge with few limitations placed on its use. Second, the 800-39 publication seeks to be a broad set of guidelines that are not tied to any one particular industry, technology, architecture, or platform,

which ideally makes it applicable to any business sector. The 800-39 publication also seeks to focus on integrating security decisions within all levels of the business, from the top-level decision-makers to the employees who are closest to the actual business processes and products. Not only does this improve security directly through addressing existing vulnerabilities, it encourages everybody involved to make security ingrained into the consciousness of the business itself. Finally, by making security an ongoing process instead of a do-it-and-forget-it singular event, it helps ensure that as both business needs and the technological landscapes change, security considerations will continue to be updated and monitored to address new threats, new vulnerabilities, and new mitigations.

The ultimate goal is to create a worksheet and walk-through based on the 800-39 publication that can be implemented relatively quickly, with some guidance, by people who do not have high technological knowledge. It uses the 800-39 publication as a framework for identifying business processes, vulnerabilities in IT resources that may interfere with those processes, possible threats, edge-case scenarios, and potential mitigations for dealing with the identified threats and vulnerabilities. Although possibly not as comprehensive as other techniques, this method is hopefully more accessible to those who are not already well-versed in IT security issues. Furthermore, it can be used as a foundation to bootstrap to more complete security and assessment methods as the needs arise.

Although the scope of this project is IT security, this approach could be extended to cover other security realms. For example, instead of detailing possible cyber-vulnerabilities that exist which may interfere with business processes, an examination of possible infrastructure vulnerabilities (power, water, transportation) could be undertaken, and a similar process of determining mitigations could be pursued. This may be extended to a number of different risks, such as financial or legal risks. The repeatability of this approach makes this a versatile tool.

Before determining whether the 800-39 publication is a good fit for this problem, however, there are a number of potential roadblocks to identify and address. Because the 800-39 publication was designed for a problem domain different from that of small businesses, there may be hurdles to its implementation. An important step in this project, therefore, is to determine if the 800-39 publication is amenable to being implemented in this manner.

## Problem Statement

### NIST Special Publication 800-39 Implementation Issues

The hurdle of most concern to the implementation of NIST Special Publication 800-39 is the fact that it was developed for implementation by government agencies, and thus may be geared towards larger organizations. Although not always explicit, the 800-39 publication sometimes makes assumptions about the structure of the organization that may not be applicable for small businesses and small organizations, or in other ways pose problems for implementation.

The 800-39 publication puts forward a three-tiered approach to addressing risk: at the organization level, at the business process level, and at the information systems level (these levels are described in more detail later) [4, p. 9]. Small businesses may not have tiers as cleanly differentiated as this model. Depending on the business, there may be no difference at all between the three levels, such as those businesses that deal with information services as a core business process.

In particular, the 800-39 publication states that at the organization level, risks are addressed “by establishing and implementing *governance* structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and mission/business functions” [4, p. 11]. As part of this governance, the role of a “Risk Executive” is defined. This role “serves as the common risk management resource for senior leaders/executives, mission/business owners, chief information officers, chief information security officers, information system owners, common control providers, 25 enterprise architects, information security architects, information systems/security engineers, information system security managers/officers, and any other stakeholders having a vested interest in the mission/business success of organizations” [4, p. 12]. Risk executives have a number of duties in coordinating with leaders and other executives, such as establishing risk management roles and responsibilities, developing a risk management strategy, providing oversight for risk management activities, and ensuring that security decisions are made in line with business missions [4, pp. 12-13].

The risk executive function as defined in the 800-39 publication is meant to be flexible: it “presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization” [4, p. 13]. The risk executive does require expertise in a wide variety of different areas, and could be fulfilled by “a single individual or office (supported by an expert staff) or by a designated group (e.g., a risk board, executive steering committee, executive leadership council)” [4, p. 13-14]. While the 800-39 publication provides flexibility in the manner of defining and staffing the risk executive function, the size of a small business most likely precludes the use of a designated group as the risk executive function. Even designating a single person to fill the risk executive function may not be feasible, as a small business or a small organization may not be able to dedicate one of their employees to this role exclusively. Thus, it is much more likely that a small organization would have one employee, or perhaps a very small number of employees, fill the risk executive position as just one of many tasks that the employee or employee is expected to handle, delivering less than 100% attention to the risk executive role.

The 800-39 publication also talks about trust and trustworthiness, defining trust as “the belief that an entity will behave in a predictable manner in specified circumstances” [4, p. 24]. This entity can be anything from a small hardware or software component to another organization that a business has a working relationship with. Of particular concern to the 800-39 publication is when information system services are contracted out to external organizations: “Trust relationships with external organizations, while generating greater productivity and cost efficiencies, can also bring greater risk to organizations” [4, p. 25]. Given their size, small businesses and organization sometimes have no choice but to contract with other organizations for key services such as information systems. In addition, they may not have the clout, expertise, or resources to be able to negotiate risk management issues in those contracts.

Small businesses and organizations do offer some benefits compared to larger organizations. Since smaller businesses may not have much of a hierarchy or administrative support structure, it is easier to connect the leadership levels of the organization with the lower levels that are more directly involved with business processes and products. This helps avoid a potential problem with larger organizations, where it can be difficult for information to filter both upwards and downwards between different levels, especially with regards to those decision-makers that are tasked with making risk-related decisions.

In addition to the increased diffusion of information, small businesses and small organizations may have more homogenous system architectures than larger businesses. According to the 800-39 publication, “A significant risk-related issue regarding the ability of organizations to successfully carry out missions and business functions is the complexity of the information technology being used in information systems” [4, p. 17]. Larger organizations that are engaged in a large number of business processes are more likely to have heterogeneous systems that are not unified into one architecture. Those organizations that are older may also have a number of legacy systems that were not designed and built with today’s risk and vulnerability environment in mind, further complicating risk management. Smaller organizations that focus on a few key processes will probably have a more unified architecture, making it easier to implement common controls throughout the organization.

One caveat to this, however, may be that smaller organizations introduce new architectures in an “ad hoc” manner as problems arise, without undertaking a decision-making process to investigate and select a solution that works best from a variety of metrics, including security, cost, and effectiveness. In a large organization, the expense required for implementing a new system architecture is so great as to require careful research into all alternatives before implementation. Smaller organizations, since the expense in terms of time and money can be much smaller when implementing new architectures, may go forward with an implementation plan with little checking beforehand aside from availability and cost. This lack of preparation beforehand can complicate risk management in the future.

Organizational culture as defined by the 800-39 publication refers to “the values, beliefs, and norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations” [4, p. 28]. Because risk management strategies can significantly alter the behaviors and actions of all members of an organization, from the top levels to the bottom, the 800-39 publication rightly recognizes that organizational culture can represent a significant issue in terms of the success of a risk management strategy. In small businesses and

organizations, since they are generally more flexible than large organizations with rigid hierarchical structures, organizational culture may not be as significant a barrier to successful risk management. This, however, is only true if the organization is able to match its risk management strategy to its risk tolerance plan.

All of these issues as they relate to small businesses are important to this project, especially those that represent barriers to successfully implementing the 800-39 publication. It is clear that a rigid implementation of the 800-39 publication is likely too difficult for a small business or small organization to pursue, for resource and expertise reasons. However, there are still a number of benefits that even a streamlined implementation of the 800-39 publication would bring to organizations in this position. First and foremost, it would provide a basic framework for these organizations to start thinking about risk management and the threats and vulnerabilities that exist with regards to the use of IT resources in business processes. In addition, if the organization continues to grow and be successful, it would provide a foundation for more expansive implementations of the 800-39 publication, or other standards as they may apply. Finally, it would help change the organizational culture and insert risk management considerations into all future decisions made by the organization.

## **Project Methodology**

### **Literature Review**

Prior to and throughout the project, a review of the relevant literature was completed. NIST Special Publication 800-39 was reviewed in its entirety. In addition, other NIST Special Publications were reviewed in varying levels of detail, including: 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*; 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; 800-30, *Risk Management Guide for Information Technology Systems*; 800-60, Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories*; and 800-60, Volume II: *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. In addition to the NIST Special Publications, FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, were reviewed.

Other standards and sources of IT security information were also investigated for comparison with the 800-39 publication. These standards were chosen based on suggestions from the online survey (discussed below) and represented commonly-used standards and sources of IT security information used in the industry today. The other sources included OWASP (The Open Web Application Security Project), PCI DSS (Payment Card Industry Data Security Standard), the ISO/IEC 27000-series, the Department of Defense's Defense Information Systems Agency (DISA) STIGs (Security Technical Implementation Guide), SANS, COBIT, Microsoft's Security Risk Management Guide, and industry-specific standards such as Sarbanes-Oxley.

### **Federal Information Security Management Act**

Before diving into the 800-39 publication itself, it helps to understand its history and the purposes for which it was created. The Federal Information Security Management Act of 2002 (FISMA) was passed by Congress in recognition of “the importance of information security to the economic and national security interests of the United States” [5]. It requires “each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source” [5]. FISMA does not generally apply to private businesses in the U.S., although it does apply to businesses that provide services under contract to the federal government.

The National Institute of Standards and Technology (NIST) is charged with developing the standards and guidelines necessary for implementing FISMA [6]. NIST has developed a number of Special Publications in the 800 series, as well as Federal Information Processing Standards (FIPS) for the implementation of FISMA. Some of the publications that NIST has created for the implementation of FISMA include [7]:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems
- NIST Special Publication 800-30, Revision 1, Risk Assessment Guideline
- NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective
- NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems
- NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System
- NIST Special Publication 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories

### **NIST Special Publication 800-39**

NIST Special Publication 800-39 is meant to be “the flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA” [4, p. 3]. It is designed to “provide guidance for an integrated, organization-wide program for managing information technology security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems” [4, p. 3]. Like the other publications created by NIST as a result of FISMA, it is mainly aimed at federal agencies, although use by other levels of government and private sector organizations is “encouraged” [4, p. 3].

NIST Special Publication 800-39 begins by describing the risk management process. The risk management process as contained in 800-39 consists of four steps: 1) framing risk; 2) assessing risk; 3) responding to risk; and 4) monitoring risk on an ongoing basis [4, p. 6]. These steps are not carried out just once, but on an ongoing basis as the risk and operational environments change. This process also needs to occur in a holistic manner that runs the gamut from the strategic level to the tactical level, not solely concentrating on any level in particular.

The first step, that of framing risk, is meant to establish a “risk context”, or an “environment in which risk-based decisions are made” [4, p. 6]. It establishes explicit and transparent risk perceptions that organizations use when creating an overall “risk management strategy”. This risk management strategy would include details such as: 1) risk assumptions, or the assumptions about threats and vulnerabilities; 2) risk constraints; 3) risk tolerances; and 4) priorities and trade-offs [4, p. 6]. It would also include “strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives” [4, p. 6].

The second step, that of assessing risk, identifies both the sources of risk as well as the methods for collecting information about risks in general. The information collected in this step consists of: 1) threats to the organization or threats directed through the organization aimed at other entities; 2) existing vulnerabilities; 3) the harm that may occur if those vulnerabilities are exploited; and 4) the likelihood that harm will actually occur [4, p. 7]. The end result is a “determination of risk”. To assist in the collection of this information, organizations also identify: 1) the tools and techniques used for assessing risk; 2) the assumptions that are made during the risk assessments; 3) the constraints that may affect the risk assessment; 4) roles and responsibilities of those involved in the risk assessment process; 5) how risk assessment information is collected, processed, and shared; 6) how risk assessments are to be conducted; 7) the frequency of risk assessments; and 8) how information is obtained about threats [4, p. 7].

The third step in the process is risk response. From the information gathered in the previous steps, organizations will: 1) develop alternatives to responding to the identified risks; 2) evaluate the alternatives; 3) determine the appropriate alternatives to implement based upon the organization’s risk tolerance; and 4) implement the selected courses of action [4, p. 7]. The responses to risk can include risk acceptance, risk avoidance, risk mitigation, risk sharing, or risk transference [4, p. 7]. Creating criteria for the evaluation of risk response alternatives is also an important part of this step.

The fourth step consists of monitoring risk over time. Its purpose is threefold: 1) to verify that the risk response measures chosen in the previous step are actually implemented, and satisfy all information security requirements; 2) determine the effectiveness of the implemented risk response measures; and 3) identify any changes in the threat, operational, technological, or business environments that occur that may impact risk [4, p. 7].

These steps feed into each other, not necessarily in a linear path, according to the 800-39 publication. Information flows in two directions among the various steps, and information used in one step may come from more than one other step. For example, the risk response step may include information that is determined in both the risk assessment step (that of the particular risks that need to be addressed), as well as the risk framing step (that of risk tolerances and priorities/trade-offs). In addition, information gathered may require changing conclusions drawn in other steps: the investigation of a new or previously underestimated threat may require changes to priorities determined in the risk framing process. Figure 1 below, from the 800-39 publication, illustrates the information flows and interplay between the four steps [4, p. 8].

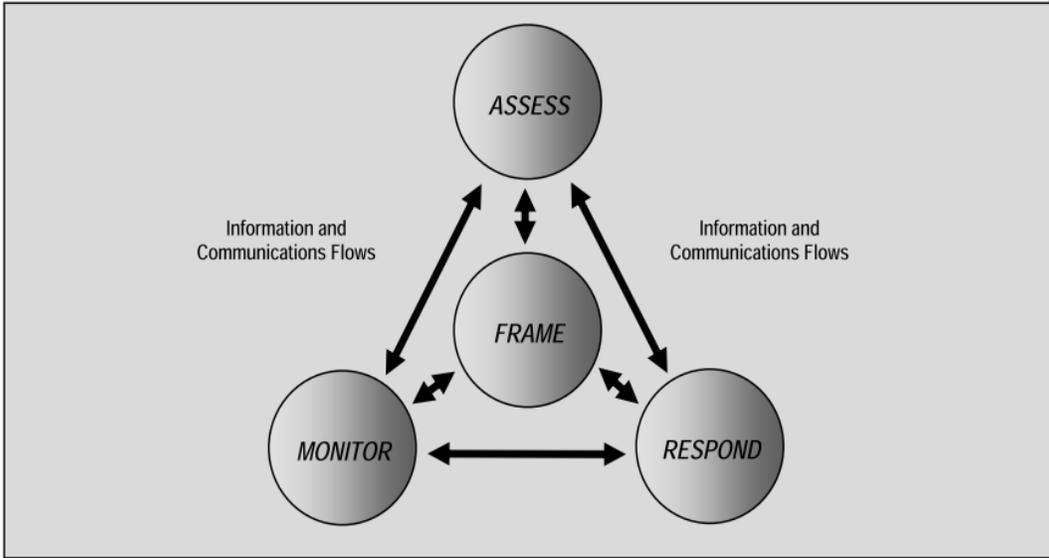


Figure 1 – NIST Special Publication 800-39: Information Flows

NIST Special Publication 800-39 points out that not only do these steps apply within an organization, but also need to be considered for external relationships as necessary. For example, outside suppliers, vendors, or contractors may need to be included in risk assessments if they may communicate or share risk. Risk information should be shared between organizations as appropriate.

A major part of NIST Special Publication 800-39 is the concept of “Multitiered Risk Management”. This breaks risk management into three levels: 1) the “Organizational” level, situated at the top; 2) the “Mission/Business Process” level, situated in the middle; and 3) the “Information System” level, situated at the bottom [4, p. 9]. Each level has a different role in risk management, but all three levels work together to ensure the success of the risk management plan. Figure 2 below illustrates the multitiered risk management system [4, p. 9].

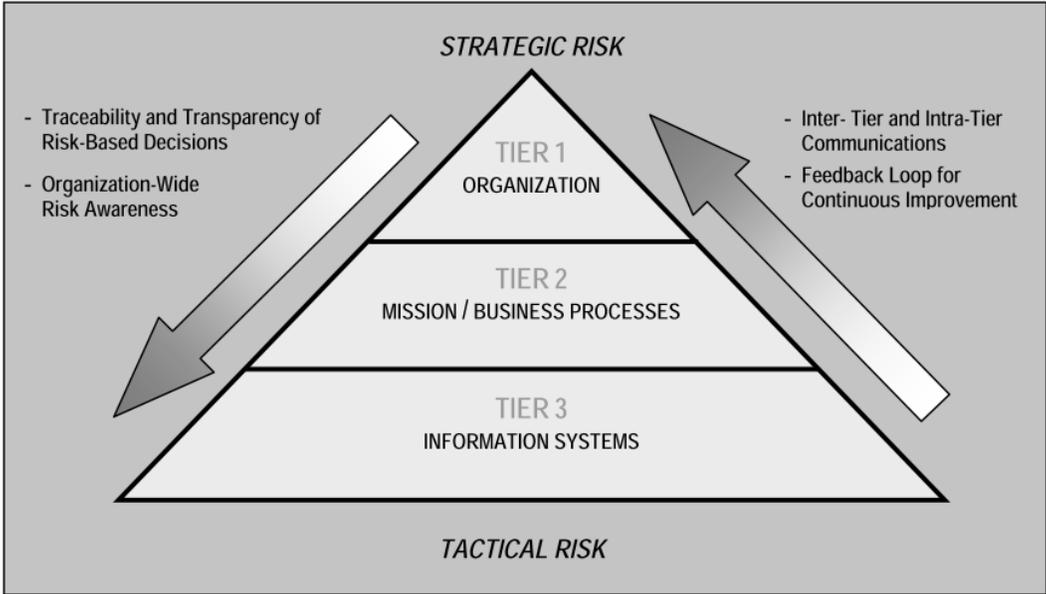


Figure 2 – NIST Special Publication 800-39: Multitiered Risk Management

The top tier, the “Organizational” level, is mainly charged with risk framing. At this level, context is provided for the other risk management activities carried out at the other levels [4, p. 9]. The middle tier, the “Mission/Business Process” tier, is primarily concerned with carrying out the business processes that are dictated by the top tier. As such, it carries out such activities as prioritizing the mission/business processes of the organization, determining the information needed to successfully carry out the goals of the organization, and creating an enterprise architectures that meet the security and operational goals and objectives of the organization [4, p. 10]. The lowest tier, the “Information System” tier, is closest the day-to-day functions of the organization. This tier is mainly concerned with implementing the security controls chosen by the other tiers, as well as providing feedback back up the hierarchy to Tiers 1 and 2 as to the effectiveness of the implemented security control. The “Information Systems” level also monitors any new vulnerabilities discovered as the threat, technological, and operational environments change [4, pp. 10-11].

## **Online Survey**

To collect data about the current IT practices of businesses, both small and large, an online survey was created using Survey Monkey. Links to the survey were posted to one online forum dealing with computers, one online “social media” site devoted to network security, and on the author’s personal blog. Links were also emailed out for further distribution to organizations that met the target audience of small businesses and organizations. The full list of survey questions and responses is located in [Appendix A](#). The survey was opened to responses on 19 April 2011, and closed to responses on 3 May 2011, providing two weeks worth of data.

The survey was designed to collect data on several areas. The first section of the survey asked questions about the basic data of the business in question: size, IT deployment, and the formality of the IT role in question. These questions were included so that it would be later possible to analyze the results based on organization size, for the purpose of analyzing the differences between large and small organizations.

The next sections, making up the bulk of the survey, ask about various IT security practices. These were generally simple “yes/no” questions, and most of them were modeled after IT security practices discussed in several NIST Special Publications. The questions ranged from more simple IT security “best practices” questions to specific questions about such areas of IT security as mobile device policies. The questions were not designed to probe deeply into any one particular aspect of IT security, but rather to get a sense of the differences between large and small organizations in the formality and extensiveness of their IT security practices.

The final section of the survey asked if the respondent was concerned about IT security, if they had heard of any publications or standards for IT security, and whether they had heard of NIST Special Publication 800-39 specifically and were using it in their organization. Those respondents who were amenable to answering follow-up questions could leave an email address.

Since survey respondents were largely self-selected, the results of the survey can’t be used statistically to model the business community as a whole. Rather, it was commissioned for two purposes. First, it was used to get a general sense of the different attitudes brought to bear on IT security in businesses of varying sizes, with a special focus on small businesses. Second, it provided a pool of contacts for follow-up questions that were used in the creation of the case

studies and worksheet feedback. Despite the fact that there was no attempt to make the survey a representative sample of the business community, the number of responses does allow for some conclusions to be drawn that can probably be applied to the business community at large.

## **Case Studies**

From the survey responses, several respondents were selected for additional questions in order to create “case studies” looking into the specific IT security practices of their organizations. They were selected based on a number of factors, including business size, survey answers that were deemed either very representative or very unrepresentative of survey responses, willingness to cooperate with the data collection process, and familiarity with the author. One case study was chosen due to the fact that it was the author’s organization, and so afforded a high level of access.

## **Worksheet Development**

The main goal of this project is to create a deliverable product based on NIST Special Publication 800-39 in the form of a worksheet that can be used by small businesses and small organizations to best assess their IT security needs. While using the 800-39 publication as a base, it also simplifies it to remove those parts that are not as applicable in the realm of small businesses and small organizations and to make it more approachable and usable.

The worksheet was created by reviewing NIST Special Publication 800-39 and other NIST documents, transferring what was believed to be most important, and downplaying, minimizing, or omitting the rest. The initial design of the worksheet was five spreadsheet “sheets” as described in [Appendix B](#). These sheets were Risk Assessment (corresponding to task 2-1 of the 800-39 publication), Risk Determination (corresponding to task 2-2 of the 800-39 publication), Risk Framing (corresponding to task 1-1 of the 800-39 publication), Resources (corresponding to tasks 1-2, 1-3, and 1-4 of the 800-39 publication), and Risk Responses (corresponding to tasks 3-1, 3-2, 3-3, 3-4, 4-1, and 4-2 of the 800-39 publication).

One significant change from the 800-39 publication was to put the Risk Assessment step ahead of Risk Framing step. This was done with the belief that small businesses would be more comfortable starting with an assessment of existing processes and resources rather than “identifying, characterizing, and providing representative examples of threat sources, vulnerabilities, consequences/impacts, and likelihood determinations” that are called for in task 1-1. By moving this step until after the identification of resources and possible vulnerabilities, these threat sources and consequences can be determined with the already identified data in mind. It should be noted that the 800-39 publication acknowledges that the risk management process is not linear, so reordering the sequence of steps should not have a marked impact on the final product.

On the Risk Responses sheet, the “Implementation Details” column was pre-filled with a number of security controls from NIST Special Publication 800-53. These are possible starting points for dealing with certain vulnerabilities, and could be helpful to those people who are unfamiliar with some currently available security controls. If necessary, other controls could be used in addition to the suggested controls.

Macros and formulas were used to copy information from one sheet to another, reducing the amount of data entry necessary. It should be noted with some irony, however, that the use of macros in a spreadsheet itself represents a security vulnerability. For reasons of platform independence, the worksheet was created in both XLS (Excel) and ODS (OpenDocument) formats.

The worksheet was then initially used in this “first draft” form with several of the case study organizations to determine the functionality of the worksheet. Specifically, issues such as usability, completeness, and technical issues with implementation were evaluated. Based on feedback from users, the worksheet was revised. As feedback was obtained, changes were made to improved the worksheet for future users.

# Analysis

## SWOT Analysis

Table 1 below shows a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis of the of NIST Special Publication 800-39 and the developed worksheet.

Table 1 – SWOT Analysis

SWOT Analysis	
Strengths	Weaknesses
Readily available	Generalized
Flexible	Requires technical knowledge
Applicable to many organizational types	
Increasing use of technology	Better assessment tools
Large number of small businesses	More secure software
Interdependencies between technologies	Economic weakness
Changes in liability	
High-visibility security failures	
Opportunities	Threats

The SWOT analysis shows a number of strengths, mainly its availability, flexibility, and its ability to be applied to many different organizations types. Weaknesses include the fact that it is rather generalized view of risk assessment and risk management that doesn't specifically dictate precise solutions to problems (this is a consequence of the flexibility of the 800-39 publication). It also requires a certain level of existing technical knowledge to be applied well: an employee not already fairly well-versed in IT issues would not be able to use it effectively.

There are many opportunities for using this worksheet with small businesses to improve IT security. First, there is the ever-increasing use of technology that creates a need for improved security. The large number of existing small businesses and the fact that they tend to have unmet IT security needs is another opportunity. Interdependencies between different technologies, such as the connection between portable devices and "back office" IT infrastructure creates additional security vulnerabilities that need to be addressed by risk management processes such as this. Potential changes in liability law that could increase the costs of a security breach for an affected business represent another opportunity for the use of this worksheet. Finally, high-visibility security failures may compel businesses to put more resources into IT security.

Some threats to the use of this worksheet for risk assessment include the development of better assessment tools that are cheap and easy to use, more secure software that does not require extensive risk mitigation, as well as continued economic weakness that may prevent small businesses from investing in IT security. The first two, while threats to the use of this worksheet specifically, would be beneficial overall to the security environment that businesses face.

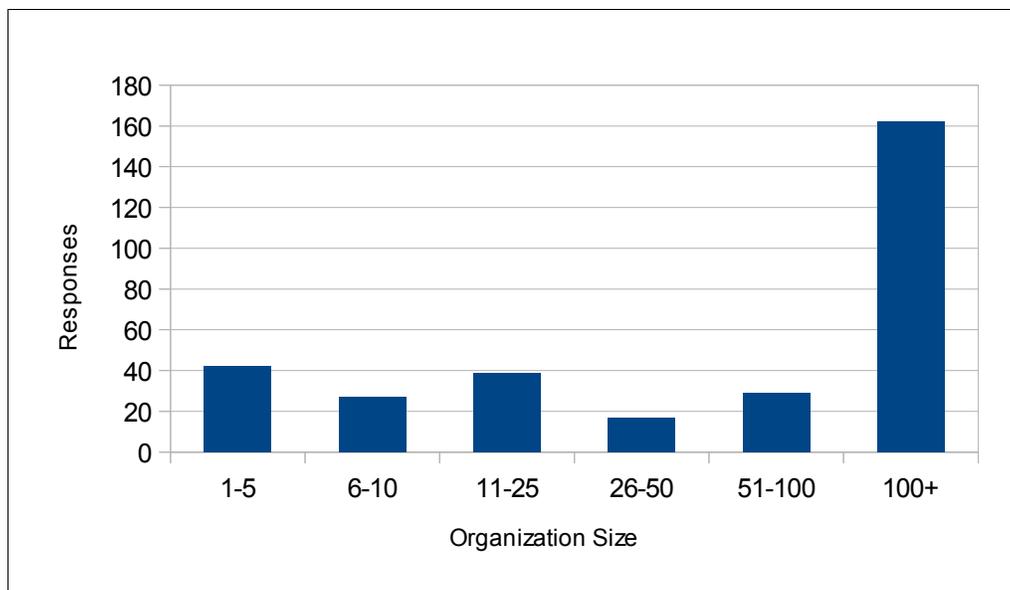
Many of these issues are further dealt with later in the analysis.

## Online Survey Results

During the time period that the online survey was available to the public, between 19 April 2011 and 3 May 2011, a total of 316 responses were collected. Since no attempt was made to ensure that the respondents were statistically representative of the business community at large, the results can't be used to draw statistically valid conclusions about the beliefs and practices of the overall business community. The data can be used, however, to get an indication of the practices and beliefs of those that responded to the survey.

Question #1 of the the survey asked respondents to select the size of their organization. Since the main goal of this project is to see how IT security is handled by smaller organizations, particular attention was paid to those respondents from smaller organizations. For analysis, data is presented with crosstabs by organization size, to best illustrate the differences in IT security beliefs and practices between smaller organizations and larger organizations.

Of the total 316 responses to the survey, the breakdown of organization size is shown below in Figure 3:



*Figure 3 – Number of responses per size of organization*

Although a majority of the responses came from respondents working at an organization with over 100 employees, approximately one third came from organizations with 25 employees or less. About 13% of responses came from organizations with five or fewer employees, the smallest size category in the survey.

Concerns about IT security in the workplace did vary by organization size, with smaller organizations less likely than larger organizations to say that they were “Extremely” or “Very” concerned with IT security in the workplace (Question #33), as shown below in Figure 4. However, even the size grouping that had the lowest percentage of “Extremely” or “Very” concerned responses, that of an organization size of 11-25 employees, had a response rate of

45% “Extremely” or “Very” concerned. Few people answered “Not at all concerned” in any organization size.

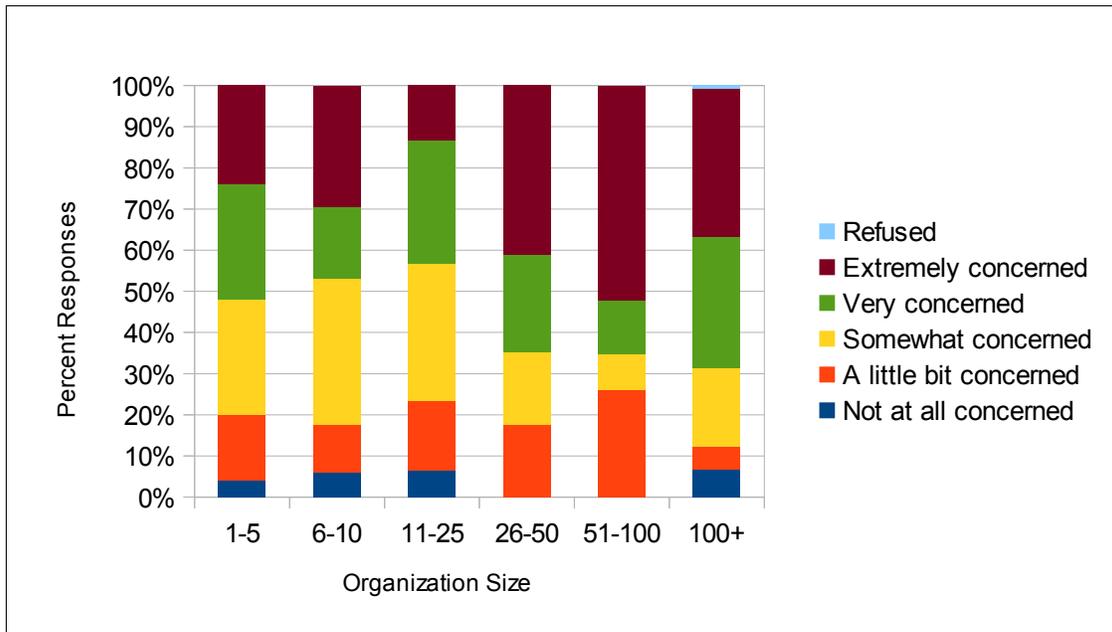


Figure 4 – Responses, by organization size, to Question #33: “How concerned about you about IT security in the workplace? Please limit your answer to the workplace only”

One manner in which large organizations differ from smaller organizations is in their security practices. In general, the survey responses show that smaller organizations are less likely to follow IT security “best practices”. As one example, the following is the response to Question #5 regarding the physical lockdown of critical computer equipment, such as servers. Respondents from smaller organizations were less likely to say that they physically locked access to servers than respondents from larger organizations.

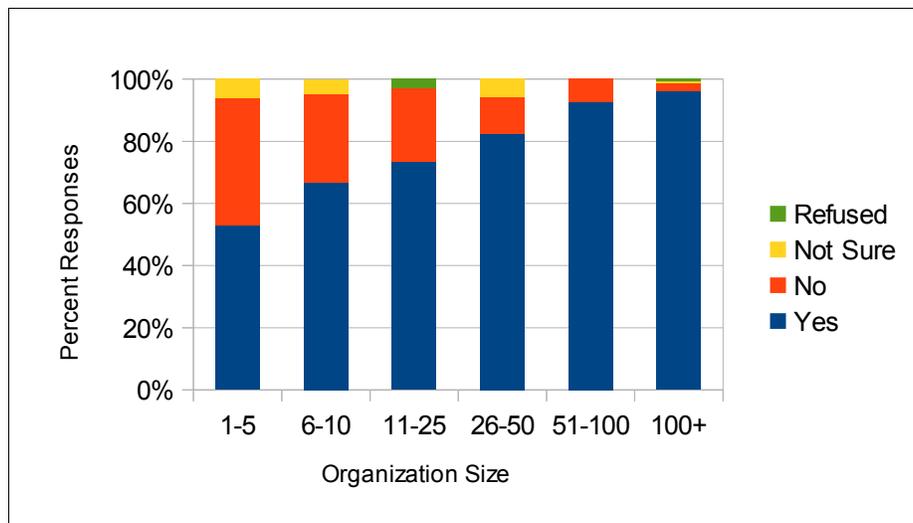


Figure 5 – Responses, by organization size, to Question #5: “Does your organization physically lock down critical hardware such as servers by placing them in a locked room, using access control, etc.?”

When it comes to more complex IT security practices, respondents from smaller organizations were also much more likely to answer that they did not have a formal IT policy in a specific realm. Question #13 asked about smartphone security, a relatively new aspect of IT security that is becoming increasingly important as more and more work is done via portable devices. No more than 15% of respondents from organizations with less than ten employees answered that there was a formal security policy with regards to smartphone and other portable devices, compared with almost 70% of those respondents from organizations with more than 100 employees. This is shown below in Figure 6.

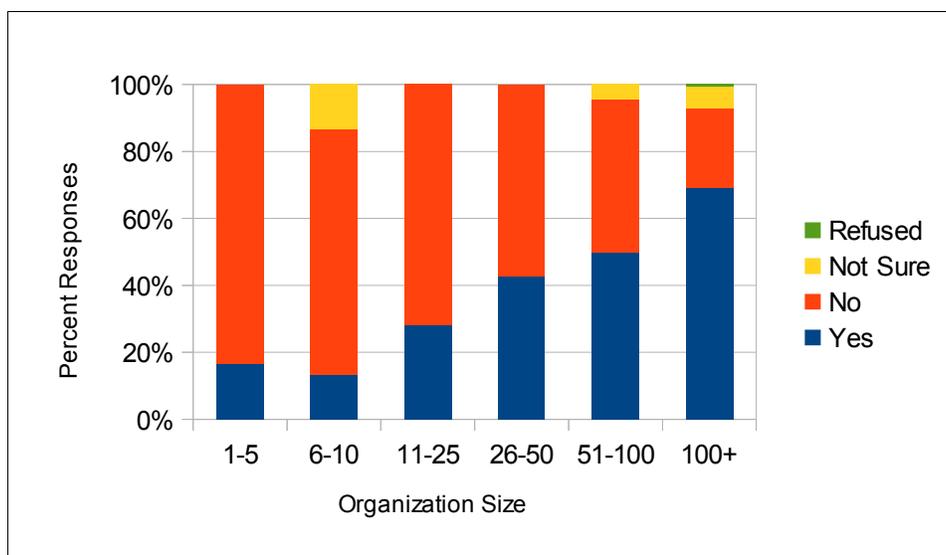


Figure 6 – Responses, by organization size, to Question #13: “Regarding the last question, does your organization have a security policy that covers the use of portable wireless devices, such as banning the installation of apps or enabling remote wipe capabilities?”

The survey also demonstrated relatively low awareness of NIST Special Publication 800-39, particularly at smaller organizations, shown below in Figure 7. The majority of organizations, regardless of size, were not aware of NIST Special Publication 800-39. However, for the most part respondents from larger organizations were more likely to answer that they had heard of it or use it in their organization than respondents from smaller organizations. In particular, no respondent from organizations with between 11 and 25 employees said that NIST Special Publication indicated that it was in use in their organization. This represents that NIST Special Publication 800-39 has a potential use in these organizations.

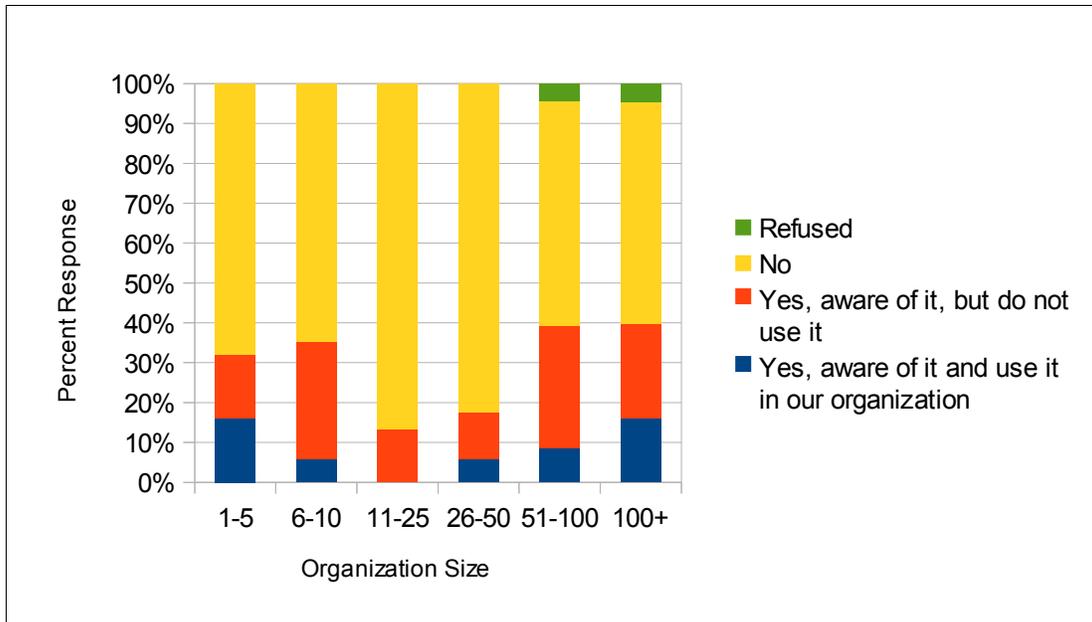


Figure 7 – Responses, by organization size, to Question #32: “Are you aware of NIST Special Publication 800-39?”

Question #31 of the survey was an open-ended question, asking respondents to comment on any other standards that they are aware of and use in their organizations. Being an open-ended question, a wide variety of responses were encountered, in varying formats. The most frequent responses offered were:

- FISMA-related documents
- ISO 27000-series
- Department of Defense Security Technical Implementation Guides (STIGs)
- PCI DSS
- The SANS (SysAdmin, Audit, Network, Security) Institute
- The Open Web Application Security Project (OWASP)
- CISSP (Certified Information Security Systems Professional)

A number of respondents indicated that they use information available on the internet via search engines or websites devoted to security issues. Given the great number of such websites in existence, no particular website stood out as a go-to source for information. Interestingly, ISO 31000 was not mentioned by any respondents; Chapter 3 of the 800-39 publication “attempted to align with the risk management process in ISO 31000” [8].

## Case Studies

The final question of the survey asked respondents for their email addresses for follow-up contact. As this question was not required, not all respondents left an email address: the final number of addresses left, 28, represented a sub-10% response rate. From those email addresses, several respondents were selected for further communication, with a preference shown towards respondents from smaller organizations. In addition to the contacts made as a result of the

survey, several personal contacts were made with people employed by small organizations to get their input.

The collected responses from these individuals were condensed into the following case studies.

### **Case Study #1: Government Agency A**

Government Agency A is a unit of state government in the legislative branch. The organization is broken up into three broad departments: non-partisan offices that are staffed by officially non-partisan staffs, and two departments run by each of the major political parties, referred to as the DFL and Republican caucuses. The overall staffing level is approximately 220 FTEs (Full Time Equivalents). The staffing levels for the respective partisan caucuses fluctuates depending on the number of elected members of each political caucus; the partisan caucus holding the majority of elected seats has more staff than the minority caucus.

There are three IT departments in the agency, mirroring the makeup of the rest of the agency. The non-partisan IT staff handle centralized IT resources, such as the network infrastructure, the public website, purchasing decisions, and some policy decisions. Each partisan caucus also has an IT department, which is mainly concerned with end-user support.

IT security is handled at several levels. At the end-user level, partisan IT staff deal with issues such as computer configuration, software installation, and user requests including password resets. Non-partisan IT staff handle security issues such as configuration of the web filter, email spam filter, wireless network, and server hardware. [REDACTED]

The 800-39-based worksheet was filled out for one of the partisan IT departments, and is available in [Appendix C](#). Since the agency is not a business, but more similar to a non-profit agency, the business processes were broken down into the constituent pieces necessary for the agency to carry out its constitutionally-dictated duties, such as crafting legislation. The worksheet was used to identify key IT resources used in those processes, and potential vulnerabilities.

Through the use of the worksheet, it was determined that the highest priority vulnerabilities were [REDACTED]

[REDACTED] Resource limitations were noted, which helped frame the responses to the vulnerabilities and risks.

Most of the risks were proposed to be mitigated in some way, although some of the lowest-priority risks were simply accepted at the present. Given the resources available, mitigations concentrated on better implementation of existing tools and policies. Many of the mitigations were taken from NIST Special Publication 800-53, with appropriate details filled in. These served as a useful starting point for many of the mitigations.

At present, due to procedural and budgetary constraints, these proposed mitigations have not yet been addressed by decision-makers. The ultimate plan of this organization is to work with key stakeholders to implement many of the proposed mitigations, after considering user input and resource constraints.

By explicitly forcing users to list business processes and the IT resources used, the worksheet made it clear which potential vulnerabilities were most likely to interfere with business processes if exploited, helping with the prioritization of those vulnerabilities. The suggested mitigation implementations were also helpful in narrowing down the choices for possible mitigation techniques. Prompting for scenarios proved helpful in determining relative risk as well.

### **Case Study #2: Multimedia Company B**

Multimedia Company B is a company based in Minneapolis that offers video production, editing, duplication, and transfer services to businesses and the general public [9]. It has six full-time employees and three part-time employees, putting it squarely in the small business category. One employee handles most of the IT troubleshooting in addition to his normal work; there is no dedicated full-time IT staff person. Procedures are not consistent between staff people, as each employee is mainly responsible for managing their own work products. [REDACTED]

The 800-39-based worksheet was filled out on a Macintosh, and is available in [Appendix D](#). The fact that a Macintosh computer was used created an issue not seen previously: the worksheet itself worked correctly on a Macintosh computer, but the underlying code that transferred data from one sheet to another did not function. This was determined to be caused by the fact that the code requires the Windows Scripting Engine, not present on Macintosh computers. This issue was only cosmetic, however, and could be solved by simply manually copying data from sheet to sheet. Other issues peculiar to Microsoft Excel also made filling out the sheet less user-friendly than hoped for, such as difficulty in inserting rows for additional data.

Based on the responses in the worksheet, [REDACTED]

Some risks that are currently accepted may need to be readdressed as facts and technology change. The worksheet can help with this process by ensuring that all relevant data is in one place, speeding up future review. [REDACTED]

[REDACTED] Should the business switch to a different application in the future, this redundancy may no longer be in place, and thus the decision whether to accept or mitigate the risk will need to be revisited.

As with the previous case, breaking down business processes into individual components and ranking the vulnerabilities present in the various IT resources made it easier to determine which items needed to be addressed and which risks could be accepted as-is. As the business changes in the future, the worksheet can be revisited as necessary to incorporate new business process, IT resources, vulnerabilities, and threats.

### **Other Feedback**

A number of survey respondents declined to participate fully as case studies, but still offered feedback on the worksheet, as well as how they currently deal with security issues.

One respondent does IT work for a digital marketing company located in [REDACTED], with a number of local and international business clients. In his informal role as the IT provider in the office, he has found that security issues have no sense of urgency, making it hard to convince coworkers to make security a priority, especially in their products [11]. Upon reviewing the worksheet, he found it to be “a clean way for someone somewhat knowledgeable to determine security risks” [12]. Possible problems with the worksheet include its usefulness without outside guidance for those who are not already knowledgeable about IT security, as well as the overall issue of getting an organization to commit to improving security without a person in charge of that particular issue area [11].

Another respondent works for an IT service provider, mainly focusing on providing IT services to small businesses. As a service provider to businesses that are not in the IT field, clients generally do not have a good sense of IT security risks. Culture and expectations on behalf of the client are problems that can lead to security breaches [13]. Security assessments are basic and customized for the client; the main tool for assessment is the Microsoft Security Assessment Tool [13].

Demonstrating that IT security is much more institutionalized in larger companies than smaller companies, an IT expert working for a large corporation states that security is handled by several dedicated personnel, as well as structured IT security management processes and assessments. Nevertheless, culture is still described as an impediment to security, as many in the business still believe that security is a non-issue [14].

This feedback generally reinforced what the online survey and case studies described: that IT security is more often overlooked in small businesses than large businesses, and that small businesses do not often use sophisticated IT security assessment and management practices. The worksheet could help fulfill those needs, although it does require an existing level of technological understanding to use well.

### **Comparisons with Other Standards**

When NIST Special Publication 800-39 was chosen for this project, it was chosen with the knowledge that other standards for IT security exist, and are in fact used by large numbers of businesses and organizations of all sizes. While there are far too many standards to be able to do a comparison of each with the 800-39 publication, comparing the 800-39 publication with several of the more widely-used and popular standards can show the strengths and weaknesses of both. Many of these standards were mentioned by respondents to the online survey.

## ISO/IEC 27000-series

The ISO/IEC 27000-series is a series of standards that has been set aside by the International Organization for Standardization (ISO) for information security matters [15]. They are a relatively new series of standards, being conceived of only in 2005, although many of the standards that the 27000-series are derived from predate this time period [16]. The main documents in the series currently are *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements*, which specifies an information security management system, and *ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management*, which specifies information security management best practices. Other documents in the series include *ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management – Measurement*, which describes a methodology for measuring the effectiveness of an ISMS, and *ISO/IEC 27005 – Information technology – Security techniques – Information security risk management*, which deals with the overall risk management process. Like all ISO standards, the 27000-series documentation can be purchased and downloaded online at some expense to the end user.

In lieu of purchasing the individual ISO standards, it is possible to download free of charge an ISO 27k Toolkit that has been created by an online community of ISO 27000-series users [17]. This toolkit contains flowcharts describing the implementation process for the standards, sample asset registers and business cases, guidelines for activities such as asset valuation and risk assessment, security checklists, security policy templates, and other supporting documentation. This toolkit can help with the implementation of the ISO 27000-series standards, but it is not a replacement for the standards themselves.

There are a number of companies that provide auditing capabilities for hire against the ISO 27000-series standards, which at this time essentially means certification of compliance with the ISO/IEC 27001 standard [18]. Only certifications that are issued by an Accredited Certification Body are recognized as official [19]. The cost in money and time of being certified can vary depending on the size of the company, but it's common to see a time span of several months and a cost of professional auditing of several thousand dollars [20]. Self-assessment is possible, but is generally not viewed as highly and as comprehensively as certification by an Accredited Certification Body.

The ISO 27000-series is meant to be an all-encompassing set of standards relating to information security management systems, and it is much broader than the other alternative standards discussed here. As such, it is an alternative standard that is very comparable to NIST Special Publication 800-39. At the same time, some of the associated ISO 27000-series documents go into great detail as to the methodologies that are to be used, defining key terms very specifically and going into minute detail over measurement processes. Thus, the scope of the full series can be overwhelming in its complexity, especially for businesses that are new to the area of IT security. Certification of compliance with the ISO/IEC 27001 standard requires the inclusion of all requirements laid out in the standard; exclusion of any requirements, even due to type or size of the business, is “not acceptable when an organization claims conformity” to the standard [21, p. 4]. The ISO/IEC 27002 standard, which deals with practices for information security

management, is most similar to NIST Special Publication 800-53, as they both contain lists of specific security controls for implementation.

Although there are many similarities between NIST Special Publication 800-30 and the ISO 27000-series, there are some difference. One obvious difference that the 800-39 publication has is that it is available free of charge to the public, whereas the ISO 27000-series documents can cost in excess of \$100 apiece to purchase; certification is even more expensive and time-consuming. The lower cost of obtaining the 800-39 publication is something that could benefit small businesses with fewer resources that can be devoted to IT security. The 800-39 publication also does not go into as much detail as some of the ISO 27000-series documents, especially with regards to methodologies that must be implemented for compliance with the standard. The ISO 27000-series can sometimes read as a checklist of specific procedures that must be implemented, even going to far as to require such things as ensuring that “documents remain legible and readily identifiable” [21, p. 8]. Such details, while important for certification, are likely less critical for small businesses where one person at most may be tasked with IT security.

As an ISO standard, the ISO 27000-series is well-recognized and used by a number of businesses and organizations for information security management systems. However, given its complexity and its cost, it seems unlikely that a small business or organization would find it necessary or cost-effective to be certified against the standard without some external business need, such as a requirement for contracting with other businesses. The 800-39 publication is more accessible to small businesses and other organizations that do not have a need for the full ISO/IEC 27001 certification. It seems unlikely that a business would choose to implement both of the sets of guidelines given the cost and the large overlap between the two.

### **COBIT**

COBIT, an “IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks” [22], is a publication of ISACA, formerly known as the Information Systems Audit and Control Association. COBIT’s most current version is version 4.1, with work currently proceeding on a new revision that will ultimately be COBIT 5 [23]. The COBIT framework is available for download at no monetary cost, with additional services available for purchase.

Currently, the COBIT framework is broken down into 34 IT processes, broadly grouped into “Plan and Organise”, “Acquire and Implement”, “Deliver and Support”, and “Monitor and Evaluate” domains [24]. Many of these IT processes are related to IT governance in general; only one, “Ensure Systems Security” under the Deliver and Support domain, directly addresses security issues. In this process, the focus is put on “maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents” by “defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents” [24]. Metrics are a key part of COBIT, and the metrics for this process include the number of incidents that damage the organization’s reputation with the public, and the number of non-conforming systems [24]. A number of control objectives are described, such as Identity Management and Security Testing, Surveillance, and Monitoring.

COBIT is a commonly used IT framework: it is the framework most frequently used for compliance with the Sarbanes-Oxley Act, which applies to all publicly-traded companies in the U.S. [25]. Nevertheless, there are some criticisms of the COBIT framework. One criticism is that it is too broad, never describing how goals are to be met, but instead simply directing that they must be met [26]. Another criticism is directed at the metrics, arguing that the security metrics are of low utility and ignore necessary context. For example, one major non-conforming IT system may be of greater security concern than a larger number of specialized systems that are not facing the outside world.

Because COBIT is a generalized IT framework, and does not deal just with security, it is not directly comparable to NIST Special Publication 800-39. Thus, they do not represent interchangeable guidelines: COBIT is much broader in overall scope than the 800-39 publication. When dealing specifically with the issue of IT security, both COBIT and the 800-39 publication do share a common characteristic that is seen as a flaw by some critics in COBIT, namely that there are no specific mitigations described for security issues in either document. Of interest is the fact that ISACA makes available for purchase a guide mapping the controls in NIST Special Publication 800-53 with COBIT 4.1.

Given the broad, comprehensive nature of COBIT, it seems that a business would likely choose either COBIT or another set of guidelines such as the 800-39 publication, but not necessarily both simultaneously.

### **Microsoft Security Risk Management Guide**

Microsoft's Security Risk Management Guide is designed to be a vendor- and technology-neutral guide on "how to plan, establish, and maintain a successful security risk management process in organizations of all sizes and types" [27, p. 3]. It incorporates both qualitative and quantitative approaches to risk management, and is broken down into four phases: risk assessment, decision evaluation, implementation, and verification of control effectiveness [27, p. 21]. Included with the guide are templates for data gathering, scheduling, and estimating the impacts and probabilities of potential threats. It also includes a walkthrough of the implementation for a fictional business. The guide is available for download free of charge from Microsoft's website.

The Security Risk Management Guide is a fairly complete package, which gives step-by-step instructions for implementing a complete risk management system. It is quite similar in its approach to NIST Special Publication 800-39, often using the same terminology and processes. For example, Figure 8 below from the guide is quite similar to Figure 9, the multi-tiered organization-wide risk management diagram in the 800-39 publication, showing the interactions between different levels of governance when it comes to risk management.

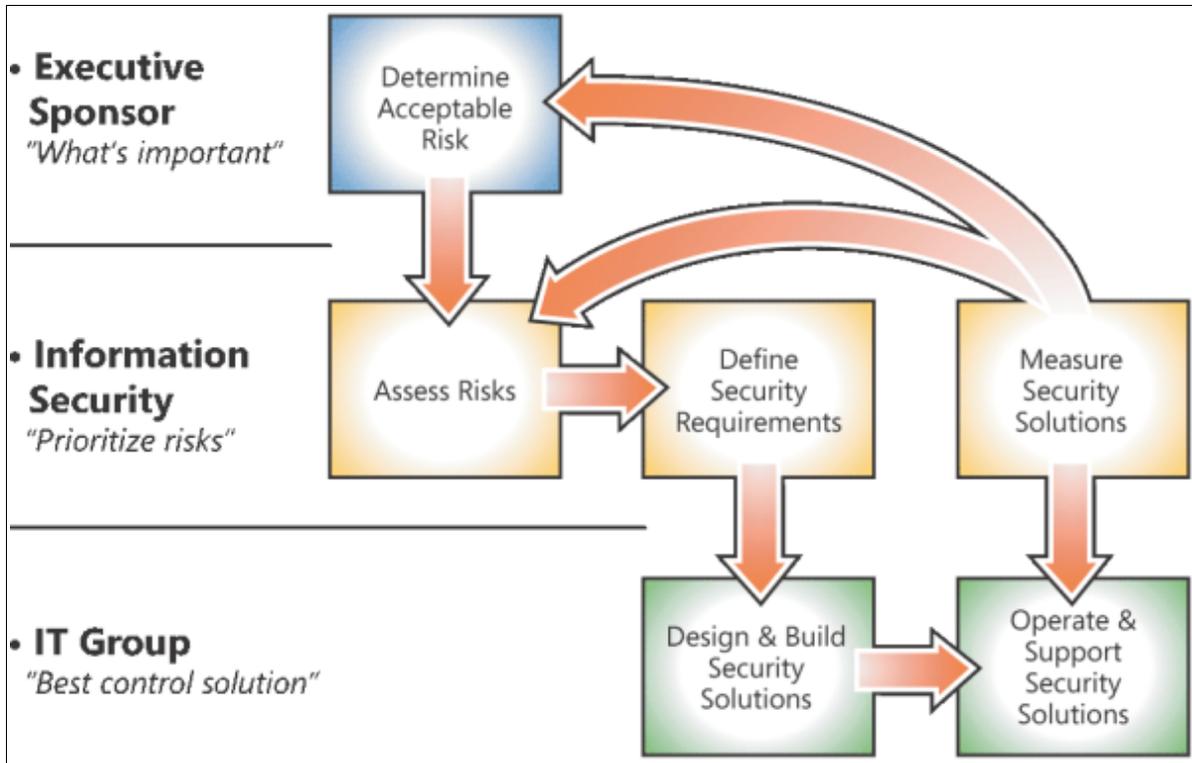


Figure 8 – from the Microsoft Security Risk Management Guide

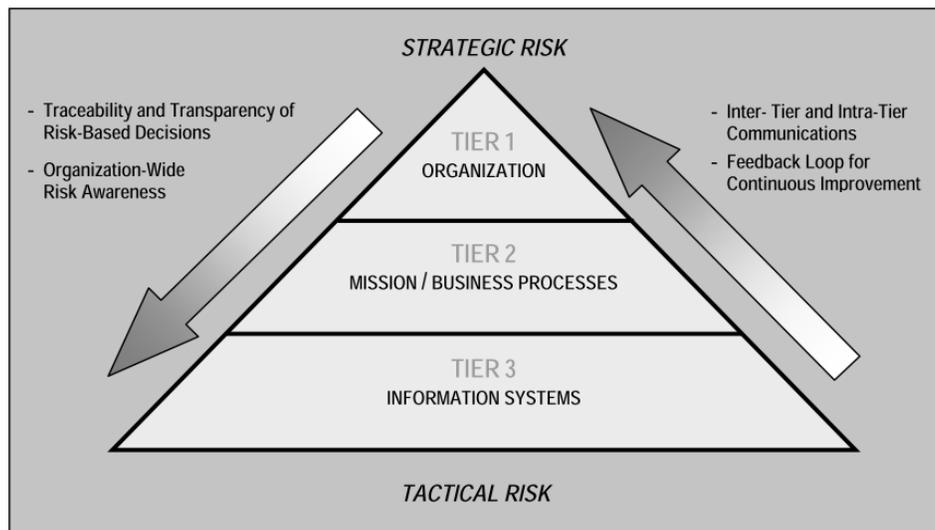


Figure 9 – NIST Special Publication 800-39: Multitiered Risk Management

The Security Risk Management Guide also includes a number of possible security controls, much like NIST Special Publication 800-53.

Considering its free cost, comprehensive nature, and step-by-step instructions, the Security Risk Management Guide is a viable alternative for businesses looking for risk management tools. It could be used side-by-side with the 800-39 publication, allowing businesses to take the best practices from each document.

## OWASP

Another frequently-mentioned and cited source for security information is OWASP. OWASP, or the Open Web Application Security Project, is “an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted” [28]. OWASP has a number of projects that are run and maintained by members on a variety of security-related topics, such as protection against software flaws when programming software, detection of software flaws in existing applications, and managing security within software life cycle development [29]. There are a large number of projects, ranging from inactive, orphaned projects to stable quality projects that represent professional-level documentation and tools.

Several of the OWASP projects are widely used and cited in the IT security industry. One of the most popular projects is known as the OWASP Top Ten Project, which details what are considered to be the ten most critical web application security flaws. The specific flaws are described, examples of vulnerabilities are discussed, and potential mitigation actions are put forward [30]. Another popular OWASP project is the OWASP Guide Project, which is a lengthy guide designed to “help businesses, developers, designers and solution architects to build secure web applications” [31]. The guide covers a number of sections of development, from pre-development planning to adding security controls and APIs to applications to mitigating specific vulnerabilities.

OWASP has also recently ventured into the realm of standards with their publication of the OWASP Application Security Verification Standards (ASVS). The goal of the standard is to create an open standard that will normalize security verification of web applications, and “provide a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection” [32]. Various levels are defined in terms of increasing rigor of testing, from automated testing at the lowest level of rigor to internal verification at the highest level [32].

The most immediately visible difference that the OWASP Projects have when compared to NIST Special Publication 800-39 is that OWASP focuses almost entirely on web application security, especially web applications that are built as a key part of the business. Thus, the OWASP Projects, individually and even collectively, are not nearly as comprehensive as the 800-39 publication. For those businesses that engage in web application development, or extensively use web applications as part of their business, then the OWASP Projects would contain a good deal of information for dealing specifically with web application security. Outside of this scope, however, it is hard to see where the OWASP Projects would be helpful for overall IT security.

Despite the fact that the OWASP Projects focus on web application security, there are some similarities between the information put out by OWASP and the 800-39 publication. For example, the OWASP Development Guide, much like the 800-39 publication, talks about identifying key business risks and performing threat modeling, although mainly within the context of how business processes interact with web applications.

The OWASP Projects represent a very useful and thorough documentation set for web application security. For businesses that use web applications as an integral part of their business

processes, the OWASP Projects could provide a more detailed extension of the concepts encompassed by the 800-39 publication. The OWASP ASVS standard could be particularly helpful for businesses that outsource their web application development, providing a set of verification levels to help determine how secure a web application truly is: such a standard could be written into a development contract, for example.

## **PCI DSS**

PCI DSS (Payment Card Industry Data Security Standard) is a security standard that is used by organizations and businesses that handle debit card, credit cards, and similar payment methods. According to the PCI Security Standards Council (SSC), they are designed to “provide an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents” [33]. The standard was born when security standards put forward by Visa, MasterCard, and other card holders were aligned and refined. The most latest standard revision is PCI DSS version 2.0, made effective 1 January 2011, with merchants required to use the latest revision no later than 31 December 2011 [34]. All merchants that handle debit and credit cards have to be compliant with the standard; compliance is enforced by the individual card issuers [35].

The standard sets out 12 requirements that are divided into six separate logical groupings: Build and Maintain a Secure Network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Measure and Test Networks, and Maintain an Information Security Policy [36]. Each of these groups has requirements and sub-requirements spelled out in the standard: under “Protect Cardholder Data” is the requirement to “Encrypt transmission of cardholder data across open, public network”, with sub-requirements detailing the use of strong cryptography, wireless encryption, and not using insecure modes of communication like unencrypted instant messaging [36]. The standard thus essentially acts as a requirements checklist, all of which must be met to ensure compliance. Compliance is measured either through the use of a Self-Assessment Questionnaire for smaller organizations, or auditing by a Qualified Assessor for larger organizations [37].

PCI DSS has come under some criticism for being little more than a checklist that ignores significant security threats. As a “point in time” assessment, PCI compliance is not set in stone: “Things can change in the network, and elsewhere in the systems and procedures that cause the company to ‘fall out of’ compliance” [38]. Michael Jones, the CIO of Michaels Stores, testified in front of Congress that the standards are “very expensive to implement, confusing to comply with, and ultimately subjective, both in their interpretation and in their enforcement” [39]. Others counter that the PCI DSS standard is “better than nothing” [38].

Since PCI DSS deals exclusively with protecting credit and debit card information, the standard is not nearly as comprehensive as NIST Special Publication 800-39; this is a similarity shared with the OWASP Projects. Businesses can use PCI DSS as a checklist for securing payment processing (and, in fact, they generally must do so per agreements with the card issuers), but it can’t be used beyond that realm to deal with securing other assets. Conversely, using the 800-39 publication as a broad framework for assessing IT security, and then using PCI DSS as a tool for securing those realms that deal with card payments, could work well as a viable IT security implementation plan. Since the 800-39 publication doesn’t generally require particular

mitigations for dealing with security risks, there is no reason why the mitigations required by PCI DSS could not be implemented within the security framework.

### **Security Technical Information Guides (STIGs)**

A STIG (Security Technical Implementation Guide) contains “technical guidance to ‘lock down’ information systems/software that might otherwise be vulnerable to a malicious computer attack” [40]. They have been created by the Department of Defense’s Defense Information Systems Agency (DISA) Field Security Operations division. STIGs are updated by the agency as needed to correct errors, omissions, and incorporate new CTO guidance [41].

STIGs are highly specialized and deal with a wide variety of both software and hardware applications. There are STIGs for operating systems, software applications, and networking infrastructure to name a few. A specific STIG, such as the STIG for the Windows 7 OS, consists of a list of requirements for properly configuring the software, including installing the latest service pack, using an approved anti-virus system, updating Access Control Lists (ACLs), and configuring services [42]. STIGs can have dozens or hundreds of individual components that must be verified for compliance, and tools are available for some STIGs that can automatically configure software and devices to comply with the STIG, as well as later test that compliance [43].

Even more so than the OWASP Projects and the PCI DSS standard, STIGs are highly specialized and individually cover one very narrow security realm, in some cases as granular as a specific application running on a specific operating system. In the IT security forest, STIGs are some of the individual trees. Given the flexibility of NIST Special Publication 800-39 when it comes to specific mitigations, however, STIGs can easily be used as part of the larger security framework, similar to the PCI DSS standard. Where an assessment using the 800-39 publication sees some vulnerabilities that need to be mitigated, STIGs represent a workable mitigation strategy for some situations.

### **SANS**

The SANS Institute (deriving from SysAdmin, Audit, Network, Security) was established in 1989 as a research and education organization [44]. SANS provides a wide variety of IT security certifications and training materials aimed at security professionals. They also maintain the “Information Security Reading Room”, consisting of approximately 1,900 security-focused white papers on a variety of topics [45]. Many of the papers were written by students seeking the Global Information Assurance Certification (GIAC) to fulfill a portion of the certification requirements. These documents can be used as reference materials for a number of security-related topics; however, as they are usually white papers by students that are not updated, the information contained within them may be out of date.

Another security resource provided by SANS is a set of Computer Security Policy Templates. Many of these templates are sanitized versions of security policies from large organizations [46]. The templates cover a number of different issues, such as email security, internet security, mobile security, and physical security [46]. They are meant as a “starting point” and can be customized as necessary to deal with the specifics of any individual business or organization.

Since SANS does not put out any standards themselves, there is no direct comparison with NIST Special Publication 800-39. However, as with previous alternative standards, the SANS security policy templates can be used along with the 800-39 publication in order to implement some of the mitigations that are decided upon. These security templates would be especially useful for those organizations that have little previous experience in IT security and need assistance with creating basic security guidelines. As the business grows and the needs change, these templates can be amended as reviews of the security landscape under the 800-39 publication are undertaken and new issues are addressed.

### **Industry-Specific Regulations**

Several security standards are mandated by law for organizations that conduct business in certain economic sectors. For example, HIPAA (Health Insurance Portability and Accountability Act) is a law passed by Congress in 1996 that mandates the Department of Health and Human Services to promulgate rules for the protection of patient health records [47]. Any covered entity as defined by the regulations must follow these rules for protecting data [48]. FERPA (The Family Educational Rights and Privacy Act) is a law that covers the privacy of student education records [49]. Sarbanes-Oxley, also referred to as SOX, applies to all publicly-held companies in the U.S. and covers the protection and storage of financial information, among its other requirements [50].

These specific sets of regulations apply only to a certain subset of businesses and organizations, and thus can't be used as general, overarching guidelines for security. However, as with the other highly-specific IT security-related documents and standards, they can be integrated within the broad framework of NIST Special Publication 800-39. Most of the businesses that must deal with these regulations, however, are already well aware of the fact they need to comply with regulations, and thus are probably less likely than other businesses to completely lack an IT security plan. In addition, as previously noted COBIT is currently the most popular method of complying with Sarbanes-Oxley.

### **NSA Security Configuration Guides**

The National Security Agency (NSA) Information Assurance Directorate's focus is on "protecting National Security Information and Information Systems, in accordance with National Security Directive 42" [51]. In support of this goal, the NSA develops and distributes guides for securing software, similar to STIGs [52]. These guides are available free to the public and cover a wide array of operating systems, applications, and hardware devices such as switches [52].

As with STIGs, the NSA Security Configuration Guides can be used with the 800-39 publication as specific mitigation techniques for dealing with vulnerabilities that are uncovered during the assessment process. Especially for those small businesses that may not know where to start when searching for mitigation, these guides can provide a good starting point for securing IT resources. Since the guides cover many of the most popular software applications and operating systems available, businesses that typically use off-the-shelf software solutions, instead of proprietary custom software, would likely find guides from the NSA that are directly applicable.

## Enterprise Risk Management Processes

Many different guidelines for enterprise risk management have quite similar processes at their core. For example, Figure 10 below from the 800-39 publication shows the interplay between the assessment, monitoring, response, and framing steps [4, p. 32]:

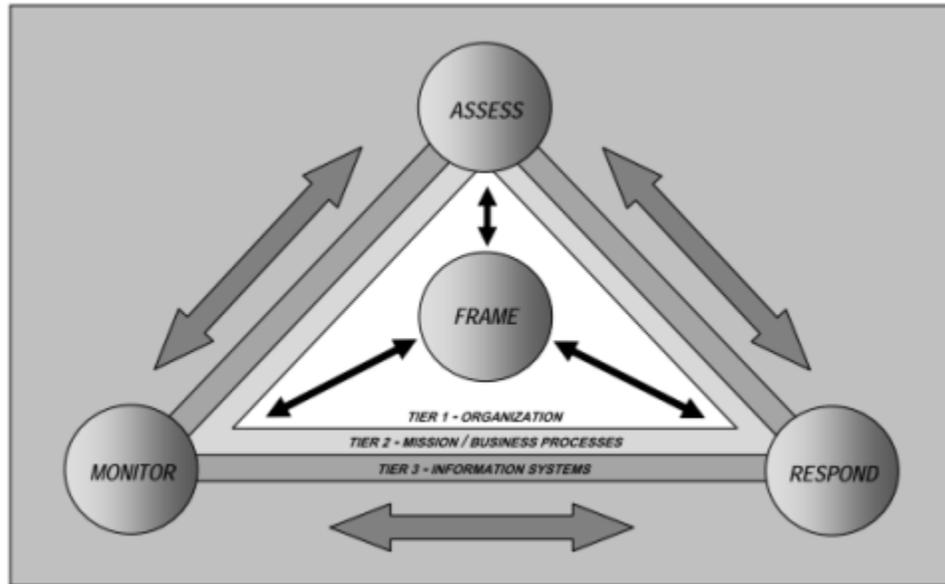


Figure 10 – NIST Special Publication 800-39: Risk Management Processes Applied Across the Tiers

In Figure 11 below, a similar process is laid out by Gartner Research in this slide from Professor Alok Gupta's presentation in ST8330, showing defining risk management, planning, management, and reporting [53]:

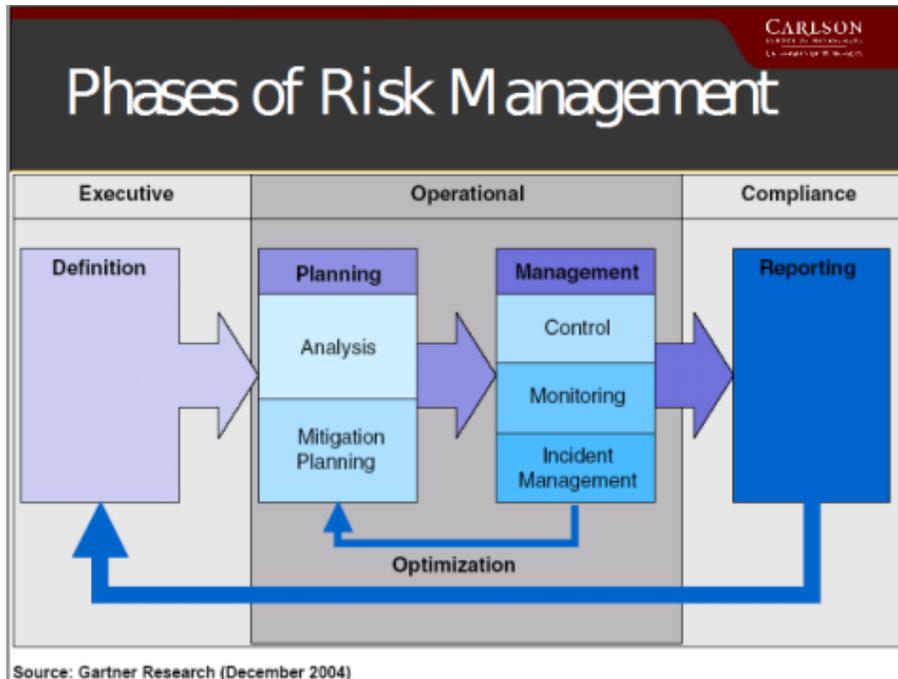


Figure 11 – “Phases of Risk Management” slide from Session Nine slides, MSST 8330, Professor Alok Gupta

COBIT has four interrelated domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate, as shown in Figure 12 below [24, p. 12]:

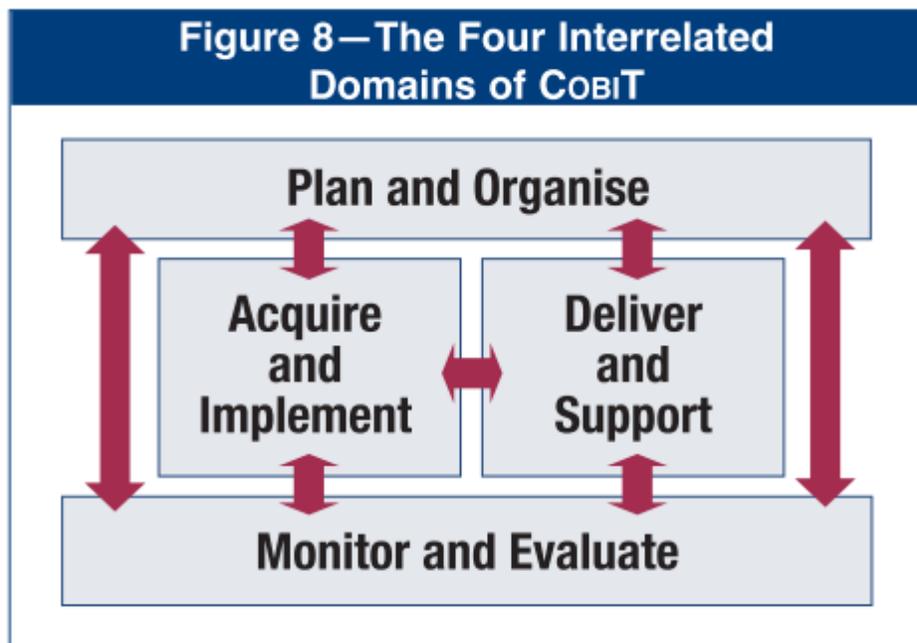


Figure 12 – “The Four Interrelated Domains of COBIT”, Figure 8 of COBIT v4.1

The ISO27k Toolkit explicitly refers to a PDCA (Plan-Do-Check-Act) framework, shown below in Figure 13:

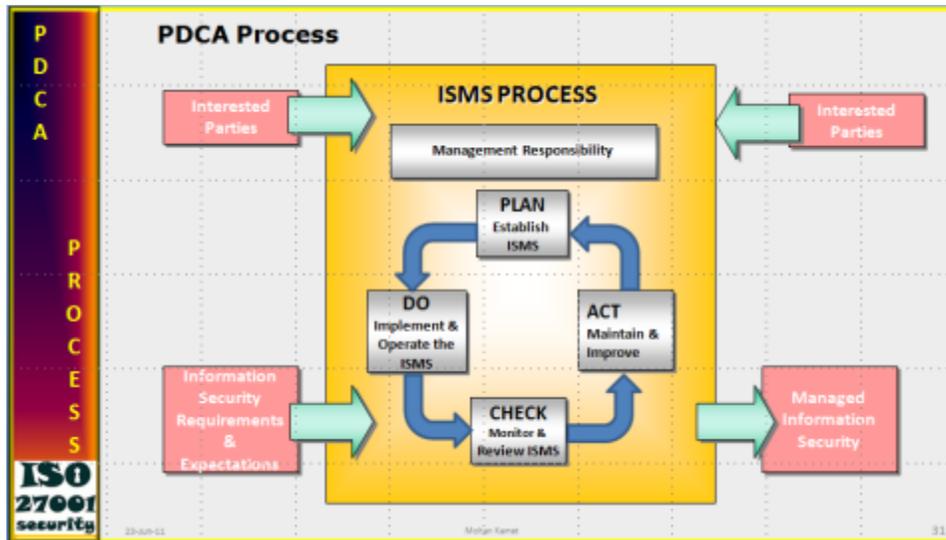


Figure 13 – Plan-Do-Check-Act Process, ISO27k Toolkit

All of these processes are similar, based (in the case of the ISO27k Toolkit, explicitly) on the “Deming Cycle” or “Shewhart Cycle” [54], a four-step process of planning the change, implementing the change, studying the results, and acting as necessary to ensure that improvements continue. No matter what guidelines or standards are ultimately used, the same cycle can use followed to ensure effective implementation and timely monitoring.

### TIM-TIP Analysis

A TIM-TIP (Technology Interaction Matrix™ – Technology Interaction Plot™) Analysis, created by Professor Lockwood Carlson, is a tool used for investigating interactions between different types of technologies. This aids in determining which combinations of technologies have the most potential for synergistic development. A sample Technology Interaction Matrix is below in Figure 14:

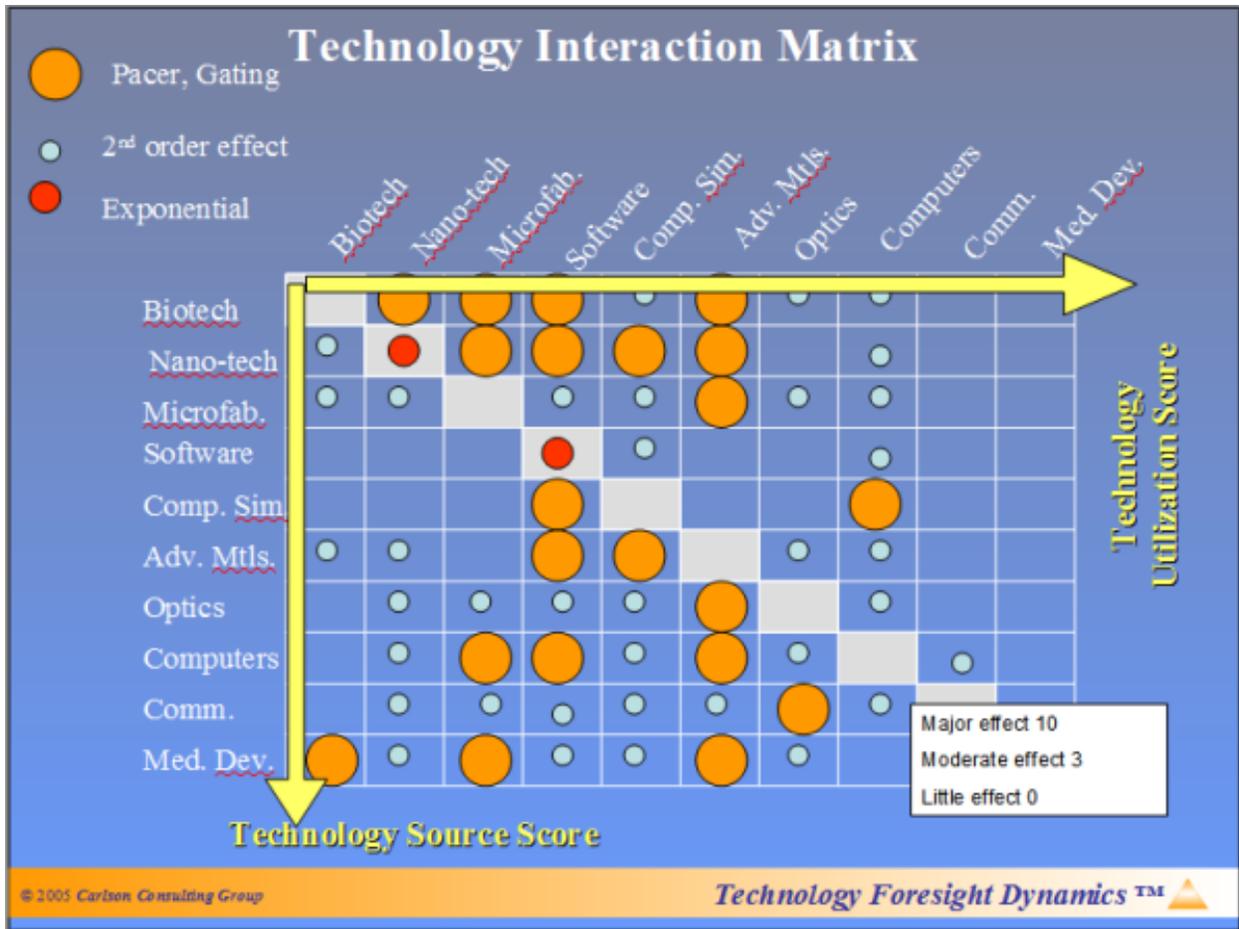


Figure 14 – Technology Interaction Matrix™, Professor Lockwood Carlson, MSST 8112 Session 2 Slides

Since NIST Special Publication 800-39 is technology-independent, there are no specific technologies that can be analyzed using the TIM-TIP analysis. In addition, the TIM-TIP analysis is geared more towards technology and product development than methodologies. Although the worksheet created in this project is a possible product, it is not amenable to a TIM-TIP analysis for determining synergies.

### Alternative Risk Assessment Methodologies

Other risk assessment methodologies would likely be less useful than using this worksheet based on the 800-39 publication. To demonstrate this, two alternative risk analyses were conducted for the IT infrastructure of case study #1: a CARVER analysis and a DSHARP analysis

#### CARVER Analysis

**Criticality:** the IT infrastructure has varying levels of criticality, depending on the particular infrastructure in question. Core infrastructure, such as the network backbone, would be the most disruptive to service if it were made unavailable in some manner. Other infrastructure, like the VoIP service, are less critical due to redundancies and alternative methods of communication. Overall, however, the long-term, complete loss of IT infrastructure would be a very unlikely

event. Thus, although IT infrastructure is critical for the normal, daily operation of the organization, it is not critical in a broader sense.

**Accessibility:** Hardware IT infrastructure is mainly readily available, with computer stations in the open and accessible to the public. Core IT infrastructure is behind locked doors, although some cabling runs are in the open. From a software standpoint, there are several web servers that face the the publicly-accessible internet, and users are allowed to install their own software and use removable media devices. These vulnerabilities are partially mitigated by the deployment of anti-malware software.

**Recoverability:** Data on centralized servers are backed up on a nightly basis. Email servers are mirrored to a separate disk array. Computers and other hardware that malfunction are replaced with spare devices. Power is supplied via Uninterruptible Power Supplies (UPS) and an emergency generator during power outages to core switches and servers, allowing for a graceful shutdown that preserves data.

**Vulnerability:** The IT infrastructure is vulnerable to various threats such as data loss, denial of service, malware, account hijacking, data theft, and physical theft.

**Effect:** Accidental data loss and physical theft of devices that do not have data on them would have little effect due to redundant data and replacement devices; the only significant loss would be monetary. More critical vulnerabilities are data theft and account hijacking, which could lead to the loss of confidential data or to identity theft. Depending on the type of theft, the effects could be limited to just one person (in the case of an identity theft), or it could lead to more serious, system-wide effects (such as a person misrepresenting themselves through a compromised email account to achieve a particular goal).

**Recognizability:** The recognizability of the IT infrastructure to the general public is very low, although certain threats, if realized, may get some media coverage (such as a widespread identity theft as a result of data theft). Overall, however, the broader recognizability of this infrastructure is non-existent most of the time, and therefore would probably make it a less appealing target than some other, more high-profile organizations and infrastructures.

The CARVER analysis does a poorer job of systematically finding and describing vulnerabilities than the worksheet. CARVER analyses are much more useful for big-picture overviews of a specific target; they are much less useful for detailing individual vulnerabilities. In addition, since CARVER analyses work best for major targets, not minor targets or even sub-targets, small businesses would probably find that doing a CARVER analysis would not produce much actionable information.

### **DSHARP Analysis**

**Demographics:** Not applicable to the IT infrastructure

**Symbology:** IT infrastructure is of no symbolic value, other than as a part of the greater government infrastructure

**Historical:** Attacks against IT infrastructure in general are routine; however, attacks singling out this particular infrastructure are not known to have been promulgated to date.

**Accessibility:** Hardware IT infrastructure is mainly readily available, with computer stations in the open and accessible to the public. Core IT infrastructure is behind locked doors, although some cabling runs are in the open. From a software standpoint, there are several web servers that face the the publicly-accessible internet, and users are allowed to install their own software and use removable media devices. These vulnerabilities are mitigated by the deployment of anti-malware software.

**Recuperability:** Data on centralized servers are backed up on a nightly basis. Email servers are mirrored to a separate disk array. Computers and other hardware that malfunction are replaced with spare devices. Power is supplied via Uninterruptible Power Supplies (UPS) and an emergency generator during power outages to core switches and servers, allowing for a graceful shutdown that preserves data.

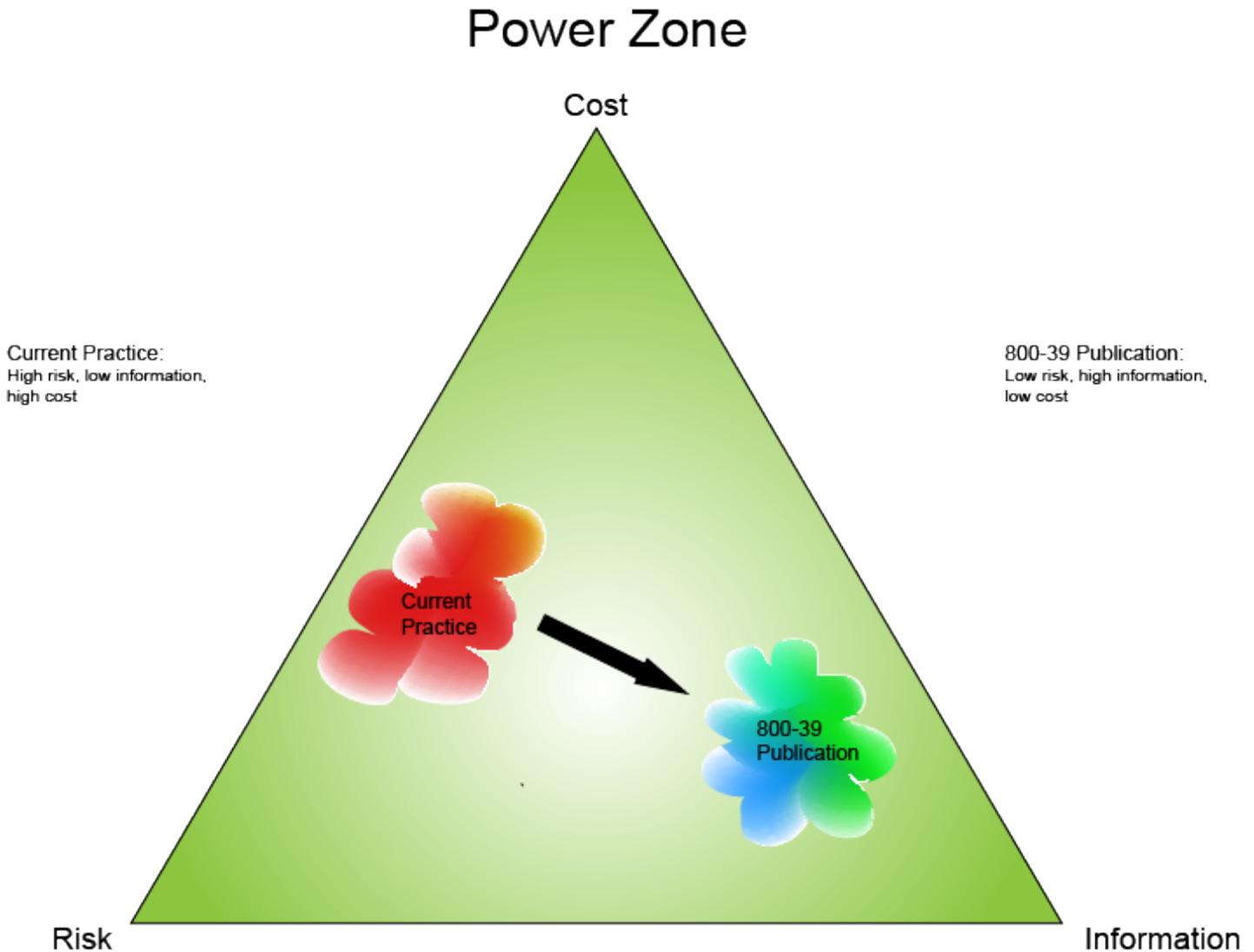
**Population:** Not directly applicable to the IT infrastructure. Approximately 350-400 individuals inside the organization use the IT infrastructure regularly, with an unknown number of members of the public accessing websites.

The DSHARP analysis is even poorer than the CARVER analysis for analyzing IT infrastructure. It partially duplicates the CARVER analysis (Accessibility, Recuperability), while the other categories add little of practical value to the analysis. As with the CARVER analysis, it is unlikely that a small business or other small organization would find a DSHARP analysis to be worthwhile.

## Recommendations

### Power Zone

A Power Zone diagram, Figure 15, shows the current state of IT security practice for small businesses, along with the desired location via implementation of the process.



*Figure 15 – 800-39 Publication Power Zone*

Currently, small businesses face a relatively high-risk, low-information, high-cost situation when it comes to IT security. Risks are undefined, information is not readily accessible, and costs are undefined, leading to a potential large cost when vulnerabilities are exploited. With the NIST Special Publication 800-39, risks can be reduced and information can be increased, all while keeping overall costs low. The result is a risk assessment methodology that is as extensive as necessary, tailored for the needs of the business.

## **Business Case for Development**

Both statistics and lessons learned throughout the undertaking of this project lend credence to the idea that this product could prove to be viable in the marketplace, especially as aimed at small businesses. In the U.S., there are a number of definitions of what constitutes a “small business”. According to the Small Business Administration (SBA), a “small business” is a business that has less than 500 employees; by this measure, approximately 50% of jobs in the U.S. are in small businesses [55, p. 18]. The U.S. Census Bureau does not have a definition of a “small business”, but does collect statistics on business size. By these measures, in 2004 there were over 5.7 million firms with less than 100 employees, with a combined payroll of almost 42 million employees [56]. This represents about 40% of the payroll of all U.S. firms. Clearly, small businesses make up a significant proportion of all businesses in this country.

The online survey commenced for this project lays out evidence that small businesses need assistance with IT security services. Although the survey was not conducted scientifically and thus is not a representative portrait of the business community at large, the number of sample respondents and the consistency of survey answers can be used to draw some conclusions that are likely to apply generally. Specifically, the survey shows that there is a correlation between business size and the implementation of various IT security mitigations: the smaller the business, the less likely that IT security had been given much thought. This reinforces the hypothesis that prompted investigation into this issue, that being small business IT departments, over-tasked and under-resourced, are likely to spend most of their time on the day-to-day operation of a business’s IT resources, and not thinking about less immediate issues like security. It is only when a security crisis has occurred that attention is given to this area.

Nevertheless, the survey also indicates that a large number of people who provide IT services to small businesses are at least somewhat concerned about security vulnerabilities. Specifically, question #33 shows that, on average, about half of people who provide IT security for small business are “Extremely” or “Very” concerned about security. While these numbers are not necessarily extendable to all small businesses, it does show that in general, small businesses are at least somewhat aware that they may have vulnerabilities in their IT infrastructures that could result in risks to their business processes from outside threats. These are precisely the people who would be most likely to be interested in any products that would enhance security at an affordable price in terms of money and manpower required.

Although there is evidence that this sector is ripe for development, there are some issues that face security experts wishing to target this market. The very issue that makes IT security so important in small businesses, namely the fact that many small businesses do not spend much thought or money on it, makes it difficult to convince small businesses that such investment is necessary. One local IT security company that targets small- and medium-sized businesses has found breaking into this market sector harder than anticipated, even though its current customers are quite happy with the product and results [57]. Emphasizing the dangers that a business can face, especially a business that may not have the resources that larger businesses have to weather an IT-related security incident, is probably the best way to encourage small businesses and organizations to invest. However, such a pitch must also not dwell too far into the realm of hyperbole and simply be about spreading fear. Using statistics and solid data keeps discussions about risk management grounded in reality without venturing into alarmism.

History has shown that, with few exceptions, complexity tends to increase in the IT realm as technology advances. Some of the more recent developments include ubiquitous wireless capabilities, virtual networks, and virtual servers [58]. In the words of Bruce Schneier, “Complexity is the worst enemy of security” [59]. As technologies get more complex, the number of bugs increase, fewer people understand the underlying parts of the system, systems get more difficult to analyze, and individual components can interact in unforeseen and frightening ways [59]. At the same time, prices go down even as complexity goes up. What were once prohibitively expensive technologies that only the largest of companies could afford are now being made available to smaller businesses. These trends make it clear that IT security for small businesses will become even more of an issue in the future, not less, creating an expanding market.

### Future Work

Short- and long-term moves (also known as “Alfie tables” in recognition of Professor Alfred Marcus) are shown below in Table 2.

Table 2 – Future Work

Short-Term and Long-Term Moves					
Move	Why	Who	How	When	Cost
Add “Alfie Tables”	Provide usable summary for customer		Extend worksheet	Short term	Minimal
Risk Assessment Grid	Provide usable summary for customer		Extend worksheet	Short term	Minimal
Mac Compatibility	Improve system compatibility		Change worksheet coding	Short term	Minimal
Branch out to other security domains	Extend the applicability of product		Create new worksheets	Long term	Time to customize, learn about other standards
Add Security Controls	Provide immediate options for mitigations		Add to worksheet	Long term	Research controls, add and update as needed

The most immediate work that must be done with this worksheet and process is to continually improve it based on user feedback. More effort must be made to get user feedback, and once obtained the worksheet will be changed as needed to make it more usable and improve its utility.

Other possible future actions include adding specific suggested mitigations to some common vulnerabilities, and possibly integrating other standards into the worksheet. This integration would make it easier for those businesses and organizations that fall under a specific regulatory purview to more quickly assess compliance.

Another possible avenue of development for this worksheet would be to flesh out the scenario planning stage more fully. Instead of just a cursory investigation of “edge case” scenarios, more

time could be expended on putting together a thorough set of scenarios, including assigning realistic probabilities to certain outcomes, as well as estimates of cost. This would allow for a more quantitative analysis of assessing security priorities.

The worksheet in its current form contains a lot of information, but not necessarily in a user-friendly summary format. Reports could be added along the lines of “Alfie tables” a risk probability/severity grid, expressing the information in a more visual format. This would allow for more easily determining priorities at a glance, without dealing with pages of text.

### **Applicability to Other Types of Security**

This project has focused on IT security. However, the worksheet is flexible enough to be able to encompass other areas of security if necessary. For example, if one were to wish to do an assessment of infrastructure security, a similar process could be undertaken with the worksheet, replacing “IT Resources Used” with “Infrastructure Resources Used” and detailing power, water, and transportation requirements for specific business processes. From there, the risk assessment would proceed similarly to the one done for IT security, identifying risks and determining mitigations as necessary, such as redundant communication lines.

## Security Implications

### Security Environment for Small Businesses: Security Practice

Given the number of small businesses in this country, as well as increasing dependence on technology, interest groups from the FCC [60] to the U.S. Chamber of Commerce [61] to the National Cyber Security Alliance [62] advocate for more awareness of cybersecurity in small businesses. Data on cyber attacks aimed at small businesses show that 74% of small- and mid-sized businesses had been affected by a cyber-attack in the past year, with the average cost of an attack being approximately \$188,000 [63]. Another survey puts the number of affected businesses at 90% [64]. Large numbers of small and medium businesses have also reported losing confidential data on the customers [63]. Such numbers may need to be taken with a grain of salt given that the source of the statistics, Symantec, would stand to benefit from increased spending on cybersecurity products.

Many small business owners believe that they are less of a target than larger businesses, leading to dangerous levels of complacency. A recent case of cybercrime in Ukraine specifically targeted small- and medium-sized businesses in the U.S., stealing \$70 million from bank accounts [65]. One researcher likens targeting small businesses to “robbing a small bank [versus] robbing a large bank. The smaller bank might have less guards and just as much money to steal” [66]. As long as small businesses have information that is of value to somebody, they will be targeted by criminals; business size is mostly orthogonal to risk.

With regards to the nation’s critical infrastructures as designated by the Critical Infrastructure Protection Program, small businesses are present in a number of the designated categories. While they generally would not be present in the government, national monuments, or nuclear categories, there are small businesses in many, if not all of the remaining critical infrastructure categories. Because they are small businesses, however, attacks against any one organization, or even a small number of organizations, would probably not have the critical infrastructure impacts that an attack against a larger organization or an infrastructure like an airport.

Nevertheless, cybersecurity attacks can certainly cause real and permanent harm to those small businesses that are subject to attack, even if they do not rise to the level of an attack against critical infrastructure of the nation. Attacks can lead to direct loss of money via loss of or damage to products, theft of money, and lawsuits. They can also lead to more intangible losses such as the loss of customer goodwill and reputation. A recent *Los Angeles Times* article described the ease with which a four-person accounting firm was compromised by a pen tester, as well as the reaction by one of the partners: “I thought we had good security. I thought we were safe” [67]. Another firm lost \$465,000 from a business bank account due to hackers [67]. Such losses can be devastating to the businesses involved.

Another security issue to consider is that attacks upon businesses can be used to further attack other targets. One key example of this phenomenon is the use of botnets to engage in criminal activity such as spamming or harvesting user login credentials. Small business IT assets can be compromised and added to botnets: a survey by Trend Micro, an IT security corporation focusing on anti-virus and anti-malware products, found that out of 100 million compromised IP addresses, 25 percent were business computers [68]. Not only does this kind of malware pose a

threat directly to a business via stealing of important data, but these compromised computers can be used to launch attacks at other targets, possibly causing additional damage to the company. For example, an ISP could block spam traffic from an infected computer, causing other connectivity problems with a business's website. Although businesses whose computers are made members of botnets are not now saddled with legal liability stemming from attacks, this may change if groups that favor stronger liability controls on IT security breaches are able to pass laws to achieve their goals.

All businesses, large or small, have data that need protecting from outside threats. The size of a business does not necessarily diminish the threats, vulnerabilities, risks, or value of what is being protected. Small businesses will need to be vigilant about IT security going forward not only to protect their own assets and business continuity, but also because they are part of the fabric of the broader economic and security realm in this nation.

### **Foundation for Future Business Growth**

One key part of any risk assessment and management plan is ensuring that it is not just a one-time event, but an ongoing process that is continuously revised and updated as business needs, vulnerabilities, threats, and resources change. Because the worksheet provides documentation that covers all of these areas, when the security or business environments change and the risk management plan needs to be updated, previous worksheets can serve as a foundation for future iterations. This cuts down on the amount of time and other resources that need to be spent on managing risk.

Broadly speaking, risk management cycles are pretty similar. As previously discussed, most systems use the PDCA (Plan-Do-Check-Act) framework, where risk management is iteratively improved with each trip through the cycle, and new information is incorporated into existing plans. The 800-39 publication also uses this method [4, p. 32]. As a business grows, this general method can be implemented whether the business continues to use the 800-39 publication, or another set of standards and guidelines. What matters most is that the business gets into the habit of doing repeated risk assessment, and that this becomes a habit.

It is the goal of any small business to succeed, and in many cases success means growing the business. As a business grows and more assets need to be protected against, again this worksheet can provide the foundation for more complete assessment methodologies, so there is no need to "start from scratch" and start a risk assessment process completely anew. Since the 800-39 publication is geared towards larger organizations, as a business grows more and more of the standard as-is can be added to the risk assessment process, such as specifically designating a risk executive once the business is large enough to merit it. With this approach, security would be constantly and consistently improved.

### **Security Theory**

A common thread throughout the MSST program has been the difficulty in convincing businesses and organizations that have not seriously thought about security to start doing so. For reasons of cost, expertise, time, and the fact that security is viewed as a cost-center, not a product that creates revenue for the business, security is often overlooked and ignored by businesses. Several possible solutions have been put forward to encourage businesses to take security

seriously, such as communicating the need for risk management in a manner that business executives can understand, providing hard numbers in terms of return on investment and other metrics that show that security is a cost-saver, not a cost-center, and positioning security in a customer-service manner, providing value to the rest of the business as a whole.

Information sharing is also an important part of good security practice. Since security threats often target more than just a single entity or infrastructure, sharing security-related information between similar organizations and infrastructures allows for greater overall security. As explained during an MSST Security Practicum discussion, even businesses that directly compete with each other in the marketplace will share security information with each other on common threats. Although there are always limits to the amount of sharing that is possible, such as when it comes to competitive advantage or national security issues, information sharing is a net benefit to improving security.

This project, by using a low-cost, non-proprietary guideline for implementing IT security, shows the benefits of less resource-intensive security practices. These can better integrate with existing business practices and thus lower the barriers to implementing sound security practices. In addition, the open nature of the guidelines can serve to enhance information sharing. The nature of the reports, as well as the repeatability of the process, also serve to creating more meaningful information and enhance sharing. Ideally, this project demonstrates the feasibility of a more widespread, low-cost, information-rich approach to security and risk management, one that does not require large investments in time and other resources to reap the benefits.

## **Delta MSST**

### **Scenario Planning**

One issue that was repeatedly visited in the MSST program, most frequently in the course on Futuring, was the usefulness of scenario planning. “What if?” scenarios that assume that some policy or event has occurred, and then investigate the consequences of such an event, are very useful within the security realm for determining the best- and worst-case consequences of making security decisions. Although scenarios do not always come to pass as planned, and in fact may never occur, they are still very useful for ensuring that possible outcomes have been thoroughly investigated, even low-probability events.

Scenarios are used within the context of this project for exactly that purpose: to investigate the “edge-cases” when security vulnerabilities are exploited to their fullest extent. It is quite unlikely that all, or even many, of the scenarios would come to pass at any one time, let alone simultaneously. The likelihood of a scenario coming to pass decreases as the number of variables increase: a scenarios with 20 variables, even if each variable was assigned a value that was 90% certain, would only have a 12% chance of coming to pass exactly as described [69]. However, by investigating possible consequences of security decisions, even if they are improbable, a business or organization can make a more informed decision about where to direct their security resources.

### **Trend Forecasting**

Also discussed most thoroughly in our Futuring course, the concept of trend forecasting is another very useful tool for risk assessment. In trend forecasting, the focus is not so much on analyzing specific possible events as with scenario planning, but determining in broad terms where technologies, economies, and human thinking is heading. One example is this oft-used slide from Professor Lockwood Carlson’s Futuring course, Figure 16:

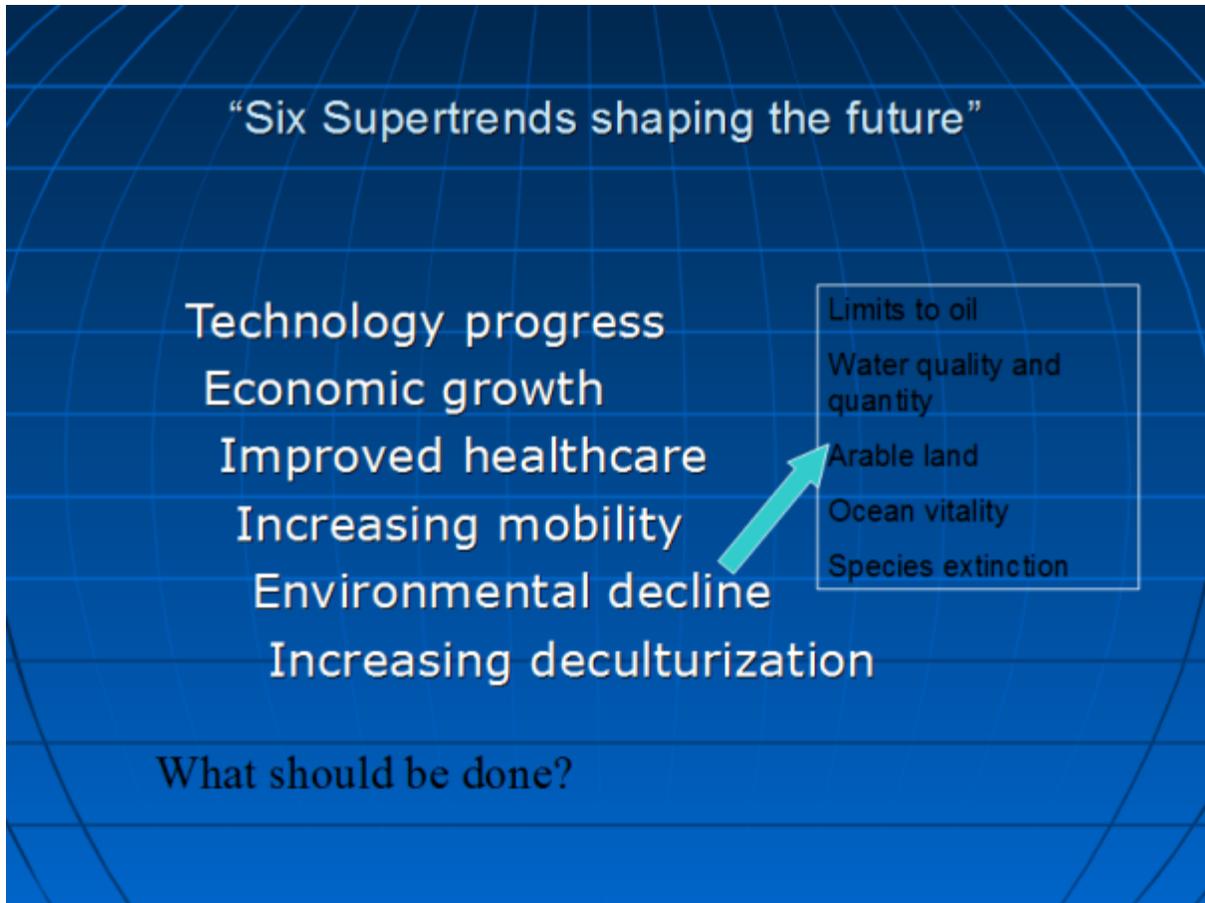


Figure 16 – “Supertrends” slide from Session Two slides, MSST 8112, Professor Lockwood Carlson

In the realm of IT security, a number of trends are important to keep in mind. One trend is the fact that attacks are getting more complex and more automated as time goes on. Another trend, especially in the developing world, is the large number of mobile devices that are going online and represent both a target of attacks as well as a source for attacks. The rising complexity of software is another trend that has a significant effect on IT security. These trends are important to keep in mind when making decisions about how best to implement an IT security policy that is secure not only now, but going forward.

### **Interdependencies**

A key concept mentioned in several MSST courses was that of interdependencies. Although we may have a tendency to analyze the security of systems in isolation, it is of utmost importance to remember that very few systems exist in a vacuum, and that the interplay between various systems is itself an issue that must be addressed from a security standpoint. The following slide from Brian Isle, Figure 17, is just one of many that emphasizes the importance of system interdependencies:



# Interdependency



Figure 17 – “Interdependency” slide from Scenario Development slides, MSST 8111, Brian Isle

Although this project focuses on IT security, it is important to remember that IT security is not the only security issue that must be faced by small businesses and organizations. Anything that interferes with business processes can have a devastating impact on the very existence of a business, so IT security must be addressed within the realm of all security issues, including infrastructure security, physical security, and supply chain security, just to name a few. As IT security will likely be a part of each of these other realms, analyzing the interdependencies between IT systems and other systems used by the business is critical to making sure all vulnerabilities are adequately addressed.

## Complex Adaptive Systems

Unanticipated, emergent behaviors of complex systems was also discussed in several MSST courses. Whether it was the emergent properties of the nation’s electric grid that have, in several cases, turned local instabilities into widespread outages, or the interactions between terrorist cells as shown in Figure 18 below from MSST 8112, understanding the precursors and warning signs for emergent behavior from complex systems is a key security concept:

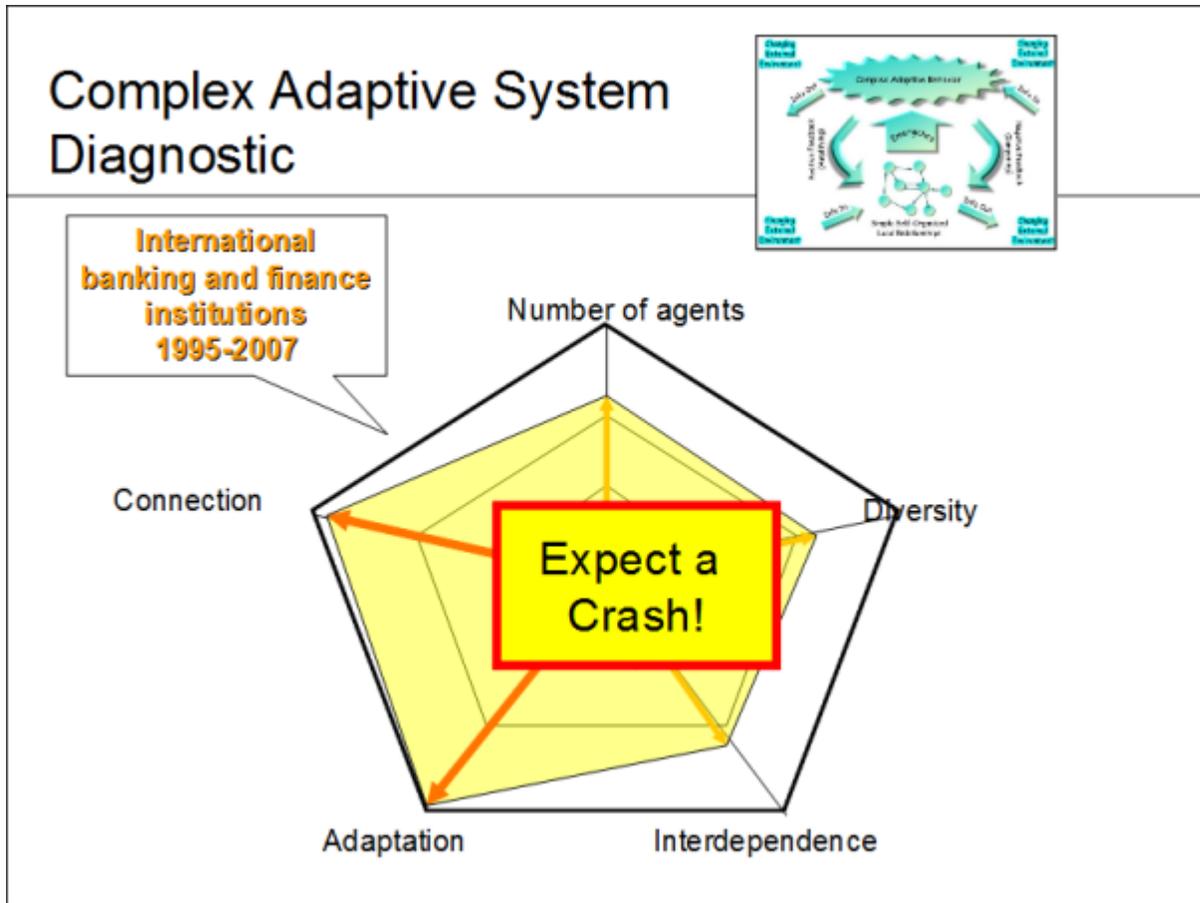


Figure 18 – “Complex Adaptive System Diagnostic” slide from Session Three slides, MSST 8112, Professor Lockwood Carlson

Technological systems can have some of the most complex emergent behaviors, something that must be taken into account when assessing IT security. For example, take the combination of two common IT resources, email and wireless communications. Conventional email systems over a wired network have relatively few, well-known failure modes: denial of service and hijacking of credentials being two of the most common. When you add a wireless network, this creates several new vulnerabilities, such as data leakage over unencrypted wireless networks. You may have strong encryption on the server coupled with strong passwords to help prevent account hijacking, but if the transmission between the server and the client device is over an unencrypted wireless network, those protections are all for naught. Similarly, the unencrypted wireless network possibly becomes the most vulnerable point of entry for a denial-of-service attack.

Another example of two technologies interacting in previously unexpected ways is the prevalence of mobile devices, and automation systems that tie into infrastructures such as power and water. Products are being delivered to market that allow for the control of electrical appliances via smartphone devices [70]. At the same time, smartphone devices are increasingly being subject to malware attacks [71]. As more people take advantage of home automation systems, this provides a new vector for attacks upon the electric infrastructure via smartphone applications.

Especially when combined with interdependency modeling, complex adaptive system considerations is vital when analyzing how different systems can fail, and how those failures can spread to other, connected resources.

## **Leadership**

Above all else, the MSST program has emphasized the need for leadership in the realm of security. Security is a tough problem, one that is too frequently swept under the rug due to cost, complexity, and the notion that “nothing bad has ever happened, so why bother addressing security” that is often prevalent in organizations, especially among the smaller businesses this project focuses on. Making security a priority on the level of other key business practices takes leadership above all else. Presenting the case for investment in security, rationally discussing the consequences of investing in security (as well as dis-investing in security) without resorting to fear and hyperbole, getting buy-in from all levels of an organization, and seeing a security project to completion all require leadership.

Without a future cadre of security leaders, important security needs will go unmet, affecting everything from a business just starting up to the critical infrastructures of this nation. With leadership, however, we can address security in a mature, rational, cost-effective manner that will ensure the strength of our community, our economy, and our nation. The MSST program has given us the tools necessary to make security a priority in whatever endeavors we may undertake now and in the future.

## Bibliography

- [1] U.S. Department of Homeland Security. “A Roadmap for Cybersecurity Research”. November 2009.
- [2] U.S. Department of Health and Human Services. “Health Information Privacy”. Internet: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html> [12 June 2011].
- [3] Fritz Young. “Is PCI Compliance a Law? Should it be?” Internet: <http://www.pcicomplianceguide.org/> [12 June 2011].
- [4] Nation Institute of Standards and Technology. “NIST Special Publication 800-39: Managing Information Security Risk”. March 2011.
- [5] National Institute of Standards and Technology. “FISMA: Detailed Overview”. Internet: <http://csrc.nist.gov/groups/SMA/fisma/overview.html>, 17 August 2010 [12 June 2011].
- [6] “Responsibilities for Federal information systems standards”, Title 40 U.S. Code, §11331.
- [7] National Institute of Standards and Technology. “FISMA Frequently Asked Questions”. Internet: <http://csrc.nist.gov/groups/SMA/fisma/faqs.html>, 10 June 2010 [12 June 2011].
- [8] Ron Ross. “MSST Capstone project on 800-39”. Personal Email (28 June 2011).
- [9] ██████████. “email questions”. Personal email (8 July 2011).
- [10] Elinor Mills. “In their words: Experts weigh in on Mac vs. PC security.” *CNet News* (1 February 2010). [On-line]. Available: [http://news.cnet.com/8301-27080\\_3-10444561-245.html](http://news.cnet.com/8301-27080_3-10444561-245.html) [11 July 2011].
- [11] ██████████. “IT Security Survey”. Personal email (25 April 2011).
- [12] ██████████. “IT Security Survey”. Personal email (17 June 2011).
- [13] ██████████. “IT Security Survey”. Personal email (17 May 2011).
- [14] ██████████. “IT Security Survey”. Personal email (24 April 2011).
- [15] The ISO 27000 Directory. “An Introduction to ISO 27001, ISO 27002....ISO 27008”. Internet: <http://www.27000.org/index.htm> [12 June 2011].
- [16] The ISO 27000 Directory. “A Short History of the ISO 27000 Standards”. Internet: <http://www.27000.org/thepast.htm> [12 June 2011].
- [17] ISO 27001 Security. “The FREE ISO27k Toolkit”. Internet: [http://www.iso27001security.com/html/iso27k\\_toolkit.html](http://www.iso27001security.com/html/iso27k_toolkit.html) [12 June 2011].
- [18] The ISO 27000 Directory. “Directory of Consultants Support The ISO27000 Series”. Internet: <http://www.27000.org/consultants.htm> [12 June 2011].

- [19] ISO17799 FAQ. “Frequently Asked Questions about ISO27002 (ISO17799)”. Internet: [http://iso-17799.safemode.org/index.php?page=ISO17799\\_FAQ](http://iso-17799.safemode.org/index.php?page=ISO17799_FAQ) [12 June 2011].
- [20] ITEXPERT Magazine. “Getting ISO27001 Certification” Internet: <http://www.itexpertmag.com/the-business/getting-iso27001-certification>, 10 October 2009 [12 June 2011].
- [21] ISO/IEC IS 27001:2005(E) – Information technology – Security techniques – Information security management systems – Requirements.
- [22] ISACA. “COBIT Framework for IT Governance and Control”. Internet: <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx> [12 June 2011].
- [23] ISACA. “COBIT 5 Initiative – Status Update”. Internet: <http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx> [12 June 2011].
- [24] ISACA. (May 2007). *COBIT® v4.1*. [On-line]. Available: [http://www.isaca.org/Knowledge-Center/cobit/Documents/CobIT\\_4.1.pdf](http://www.isaca.org/Knowledge-Center/cobit/Documents/CobIT_4.1.pdf) [12 June 2011].
- [25] Sarbanes-Oxley Compliance Journal. “COBIT + DLP = SOX Compliance”. Internet: [http://www.s-ox.com/dsp\\_getFeaturesDetails.cfm?CID=2456](http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=2456) [12 June 2011].
- [26] Skyview Partners. “What is COBIT Security and When Might You Need to Apply It?” Internet: [http://www.skyviewpartners.com/pdf/COBIT\\_Security.pdf](http://www.skyviewpartners.com/pdf/COBIT_Security.pdf) [12 June 2011].
- [27] Microsoft TechNet. (2006). *The Security Risk Management Guide*. [On-line]. Available: <http://technet.microsoft.com/en-us/library/cc163143.aspx> [13 July 2011].
- [28] The Open Web Application Security Project. “About The Open Web Application Security Project”. Internet: [https://www.owasp.org/index.php/About\\_OWASP](https://www.owasp.org/index.php/About_OWASP) [12 June 2011].
- [29] The Open Web Application Security Project. “Category:OWASP Project”. Internet: [https://www.owasp.org/index.php/Category:OWASP\\_Project](https://www.owasp.org/index.php/Category:OWASP_Project) [12 June 2011].
- [30] The Open Web Application Security Project. (October 2010). *OWASP Top 10 – 2010*. [On-line]. Available: <http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf> [12 June 2011].
- [31] Owasp-development-guide. “Introduction”. Internet: <http://code.google.com/p/owasp-development-guide/wiki/Introduction> [12 June 2011].
- [32] The Open Web Application Security Project. (June 2009). *OWASP Application Security Verification Standard 2009 – Web Application Standard*. [On-line]. Available: [http://www.owasp.org/images/4/4e/OWASP\\_ASVS\\_2009\\_Web\\_App\\_Std\\_Release.pdf](http://www.owasp.org/images/4/4e/OWASP_ASVS_2009_Web_App_Std_Release.pdf) [12 June 2011].
- [33] PCI Security Standards Council. “For Merchants”. Internet: <https://www.pcisecuritystandards.org/merchants/> [12 June 2011].

- [34] PCI Security Standards Council. “PCI Security Standards Council Enters Next Phase of Data Security Standards Development”. Internet: [https://www.pcisecuritystandards.org/pdfs/pr\\_110105\\_jan1\\_effective\\_date.pdf](https://www.pcisecuritystandards.org/pdfs/pr_110105_jan1_effective_date.pdf) [12 June 2011].
- [35] PCI Security Standards Council. “PCI Quick Reference Guide”. Internet: [https://www.pcisecuritystandards.org/documents/pci\\_ssc\\_quick\\_guide.pdf](https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf) [12 June 2011].
- [36] PCI Security Standards Council. “Navigating PCI DSS”. Internet: [https://www.pcisecuritystandards.org/documents/navigating\\_dss\\_v20.pdf](https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf) [12 June 2011].
- [37] PCI Security Standards Council. “Getting Started with the PCI Data Security Standard”. Internet: [https://www.pcisecuritystandards.org/security\\_standards/getting\\_started.php](https://www.pcisecuritystandards.org/security_standards/getting_started.php) [12 June 2011].
- [38] Anthony Bettini. (Summer 2009). “PCI DSS: Better Than Nothing”. *McAfee Security Journal*. [On-line]. Available: <http://www.mcafee.com/us/resources/reports/rp-security-journal-summer-2009.pdf> [12 June 2011].
- [39] U.S. Congress. Hearing of the Emerging Threats, Cybersecurity, and Science and Technology Subcommittee. 31 March 2009. [On-line]. Available: <http://www.homeland.house.gov/SiteDocuments/20090331142012-77196.pdf> [12 June 2011].
- [40] Information Assurance Support Environment, Defense Information Systems Agency. “STIGs”. Internet: <http://iase.disa.mil/stigs/>, 10 June 2011 [12 June 2011].
- [41] Defense Information Systems Agency. “Memorandum for Distribution”. Internet: <http://iase.disa.mil/stigs/downloads/stig-dev-and-bimonthly-memo.pdf>, 25 March 2011 [12 June 2011].
- [42] Information Assurance Support Environment, Defense Information Systems Agency. *Windows 7 STIG – Version 1, Release 4*. [On-line]. Available: [http://iase.disa.mil/stigs/downloads/zip/u\\_windows\\_7\\_v1r4\\_stig\\_20110429.zip](http://iase.disa.mil/stigs/downloads/zip/u_windows_7_v1r4_stig_20110429.zip) [12 June 2011].
- [43] Raytheon. “Security Blanket®”. Internet: <http://www.trustedcs.com/SecurityBlanket/SecurityBlanket.html> [12 June 2011].
- [44] SANS. “SANS Frequently Asked Questions (faq): Security Training”. Internet: <http://www.sans.org/faq/> [12 June 2011].
- [45] SANS. “Welcome to SANS Information Security Reading Room”. Internet: [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/) [12 June 2011].
- [46] SANS. “Information Security Policy Templates”. Internet: <http://www.sans.org/security-resources/policies/#template> [12 June 2011].

- [47] “Fraud and abuse control program”, Title 42 U.S. Code, Chapter 7, Subchapter XI, Part A, §1320a-7c.
- [48] 45CFR164.501 (2010).
- [49] U.S. Department of Education. “Family Education Rights and Privacy Act”. Internet: <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>, 8 April 2011 [12 June 2011].
- [50] SOX-online. “Information and Security”. Internet: <http://www.sox-online.com/security.html> [12 June 2011].
- [51] U.S. National Security Agency. “About IA at NSA”. Internet: [http://www.nsa.gov/ia/ia\\_at\\_nsa/index.shtml](http://www.nsa.gov/ia/ia_at_nsa/index.shtml), 23 May 2011 [17 June 2011].
- [52] U.S. National Security Agency. “Security Configuration Guides”. Internet: [http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml), 15 January 2009 [17 June 2011].
- [53] Alok Gupta. “Security Planning and Controls”. Slides for ST8330 Class (29 July 2010).
- [54] American Society for Quality. “Project Planning and Implementing Tools: Plan-Do-Check-Act Cycle”. Internet: <http://asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html> [23 June 2011].
- [55] Office of Advocacy, Small Business Administration. (2010). *The Small Business Economy, A Report to the President*. [On-line]. Available: [http://www.sba.gov/sites/default/files/sb\\_econ2010.pdf](http://www.sba.gov/sites/default/files/sb_econ2010.pdf) [12 June 2011].
- [56] U.S. Census Bureau. “Statistics about Business Size (including Small Business) from the U.S. Census Bureau”. Internet: <http://www.census.gov/epcd/www/smallbus.html> [12 June 2011].
- [57] Steve Alexander. “Ramsey-based security firm finds success, not riches”. *Star Tribune* (5 June 2011). [On-line]. Available: <http://www.startribune.com/business/123143688.html> [12 June 2011].
- [58] John Pallatto. “IT Managers See No End to Technology Complexity”. *CIO Insight* (19 May 2005). [On-line]. Available: <http://www.cioinsight.com/c/a/Trends/IT-Managers-See-No-End-to-Technology-Complexity/> [12 June 2011].
- [59] Bruce Schneier. “Crypto-Gram Newsletter”. 15 March 2000. [On-line]. Available: <http://www.schneier.com/crypto-gram-0003.html#8> [12 June 2011].
- [60] Federal Communications Commission. “Cybersecurity Roundtable: Protecting Small Businesses”. Internet: <http://www.fcc.gov/events/cybersecurity-roundtable-protecting-small-businesses> [12 June 2011].
- [61] U.S. Chamber of Commerce. “Commonsense Guide to Cyber Security for Small Businesses”. Internet: <http://www.uschamber.com/reports/commonsense-guide-cyber->

- [security-small-businesses](#), September 2004 [12 June 2011].
- [62] National Cyber Security Alliance. “Small business needs to focus on cybersecurity”. Internet: <http://www.staysafeonline.org/blog/small-business-needs-focus-cybersecurity>, 27 October 2009 [12 June 2011].
- [63] Federal Communications Commission. “Cybersecurity Roundtable: Securing and Empowering Small Businesses With Technology”. Internet: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-306596A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306596A1.pdf), 16 May 2011 [12 June 2011].
- [64] Jaikumar Vijayan. “90% of companies say they've been hacked: Survey”. *Network World* (22 June 2011). [On-line]. Available: <http://www.networkworld.com/news/2011/062211-90-of-companies-say-theyve.html?hpg1=bn> [24 June 2011].
- [65] Herb Weisbaum. “Cybercrooks target vulnerable small businesses”. *ConsumerMan on MSNBC* (25 February 2011). [On-line]. Available: [http://www.msnbc.msn.com/id/41742303/ns/business-consumer\\_news/t/cybercrooks-target-vulnerable-small-businesses/](http://www.msnbc.msn.com/id/41742303/ns/business-consumer_news/t/cybercrooks-target-vulnerable-small-businesses/) [12 June 2011].
- [66] Peter Suci. “Businesses most at risk from Web hackers”. *USA Today* (25 May 2011). [On-line]. Available: [http://www.usatoday.com/money/industries/technology/2011-05-22-cNBC-businesses-at-risk-of-hacking\\_n.htm](http://www.usatoday.com/money/industries/technology/2011-05-22-cNBC-businesses-at-risk-of-hacking_n.htm) [12 June 2011].
- [67] Cyndia Zwahlen. “Small firms learn size doesn’t matter to hackers”. *Los Angeles Times* (23 May 2011). [On-line]. Available: <http://articles.latimes.com/2011/may/23/business/la-fi-smallbiz-security-20110523> [12 June 2011].
- [68] Trend Micro. “Security Spotlight: The Evolution of Botnets”. Internet: [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the\\_evolution\\_of\\_botnets\\_april\\_26\\_2010\\_.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_evolution_of_botnets_april_26_2010_.pdf) [12 June 2011].
- [69] Joesph Coates. “Scenario Planning”. 26 January 1999.
- [70] SmartHome. “SmartLinc – INSTEON Central Controller”. Internet: <http://www.smarthome.com/2412N/SmartLinc-INSTEON-Central-Controller/p.aspx> [8 July 2011].
- [71] Info Security Magazine. “Mobile malware report predicts tough times ahead for smartphone users” (13 June 2011). [On-line]. Available: <http://www.infosecurity-magazine.com/view/18631/mobile-malware-report-predicts-tough-times-ahead-for-smartphone-users/> [8 July 2011].

## Appendices

### Appendix A: Online Survey Questions and Responses

This survey was posted online using Survey Monkey (<http://www.surveymonkey.com>) between 19 April 2011 and 3 May 2011, during which time a total of 316 responses were collected. Links to this survey were sent to several online forums and blogs. No attempt was made to create this survey in such a way as to make the respondents a representative sample of the business community at large. Rather, the purpose was to get a general sense of the diversity in what organizations are doing now, as well as to find organizations for further questioning.

The survey consisted of the following questions and responses. All questions were required and used radio buttons to limit responses to one response only unless otherwise noted. Results for all questions other than question #1 are shown with crosstabs for the size of the organization.

**Question 1: How many employees are in your organization? Please use your best estimate if you are unsure.**

Q1	1-5	6-10	11-25	26-50	51-100	100+	Total
Responses	42	27	39	17	29	162	<b>316</b>

**Question 2: How many employees use computers and other IT resources as a major part of their job? Again, use your best estimate.**

Q2	1-5	6-10	11-25	26-50	51-100	100+	Total
Just a few	4	1	2	0	1	2	<b>10</b>
More than a few, but less than half	0	0	1	1	0	4	<b>6</b>
Half to a bit more than half	0	1	0	1	0	7	<b>9</b>
Almost everybody	8	4	13	2	5	65	<b>97</b>
All employees use IT resources in their work	30	21	23	13	23	84	<b>194</b>
<b>Total</b>	<b>42</b>	<b>27</b>	<b>39</b>	<b>17</b>	<b>29</b>	<b>162</b>	<b>316</b>

**Question 3: Do you have an IT role in your organization? This could include anything IT-related, such as creating IT policies, purchasing hardware or software, or providing end-user support.**

Q3	1-5	6-10	11-25	26-50	51-100	100+	Total
Yes	39	22	35	17	28	148	<b>289</b>
No	3	5	4	0	1	14	<b>27</b>
Total	<b>42</b>	<b>27</b>	<b>39</b>	<b>17</b>	<b>29</b>	<b>162</b>	<b>316</b>

If the answer to #3 was “Yes”, then the following question was presented. Otherwise, it was skipped:

**Question 4: With regards to the last question, is this a formal or informal IT role?**

Q4	1-5	6-10	11-25	26-50	51-100	100+	Total
Formal	28	18	30	15	27	137	<b>255</b>
Informal	9	4	5	2	1	10	<b>31</b>
Total	<b>37</b>	<b>22</b>	<b>35</b>	<b>17</b>	<b>28</b>	<b>147</b>	<b>286</b>

**Question 5: Does your organization physically lock down critical hardware such as servers by placing them in a locked room, using access control, etc.?**

Q5	1-5	6-10	11-25	26-50	51-100	100+	Total
Yes	17	14	25	14	25	145	<b>240</b>
No	13	6	8	2	2	4	<b>35</b>
Not Sure	2	1	0	1	0	1	<b>5</b>
Refused	0	0	1	0	0	1	<b>2</b>
Total	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>151</b>	<b>282</b>

**Question 6: Does your organization have a policy that limits access to shared resources (files, printers, etc.) on a "need to know"/"need to use" basis, or are resources shared without limitation?**

<b>Q6</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Access is limited	20	18	24	15	23	140	<b>240</b>
No limits on access, everything is open	10	3	10	2	4	8	<b>37</b>
Not Sure	1	0	0	0	0	2	<b>3</b>
Refused	1	0	0	0	0	1	<b>2</b>
<b>Total</b>	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>151</b>	<b>282</b>

**Question 7: Does your organization track and audit your IT infrastructure, including both hardware and software?**

<b>Q7</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	21	10	17	11	23	133	<b>215</b>
No	8	6	17	6	4	10	<b>51</b>
Not Sure	2	4	0	0	0	6	<b>12</b>
Refused	1	1	0	0	0	2	<b>4</b>
<b>Total</b>	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>151</b>	<b>282</b>

**Question 8: Does your organization make changes to out-of-the-box software for security reasons? This could include enabling or disabling services, uninstalling components, or changing policies to disallow making changes to the operating system.**

<b>Q8</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	21	17	25	12	21	132	<b>228</b>
No	8	3	8	4	4	11	<b>38</b>
Not Sure	2	1	1	1	2	7	<b>14</b>
Refused	1	0	0	0	0	1	<b>2</b>
<b>Total</b>	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>151</b>	<b>282</b>

**Question 9: Does your organization have a policy for the sanitization and disposal of old or obsolete hardware?**

<b>Q9</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	18	13	19	10	16	116	<b>192</b>
No	14	6	12	6	7	15	<b>60</b>
Not Sure	0	2	3	1	4	18	<b>28</b>
Refused	0	0	0	0	0	2	<b>2</b>
<b>Total</b>	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>151</b>	<b>282</b>

**Question 10: Does your organization have VPN or other remote-access capabilities?**

<b>Q10</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	25	17	30	14	22	140	<b>248</b>
No	7	3	3	3	5	7	<b>28</b>
Not Sure	0	1	1	0	0	1	<b>3</b>
Refused	0	0	0	0	0	2	<b>2</b>
<b>Total</b>	<b>32</b>	<b>21</b>	<b>34</b>	<b>17</b>	<b>27</b>	<b>150</b>	<b>281</b>

If the answer to #10 was “Yes”, then the following question was presented. Otherwise, it was skipped:

**Question 11: Regarding the last question, does your organization have a written policy on using your VPN, such as policies on where and how you may connect to it?**

<b>Q11</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	8	4	9	5	15	90	<b>131</b>
No	17	8	19	9	5	36	<b>94</b>
Not Sure	0	3	1	0	2	10	<b>16</b>
Refused	0	0	0	0	0	3	<b>3</b>
<b>Total</b>	<b>25</b>	<b>15</b>	<b>29</b>	<b>14</b>	<b>22</b>	<b>139</b>	<b>244</b>

**Question 12: Do employees in your organization ever use portable wireless devices, such as smartphones, for business use?**

<b>Q12</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	25	15	25	14	22	142	<b>243</b>
No	7	4	7	3	4	3	<b>28</b>
Not Sure	0	0	1	0	1	1	<b>3</b>
Refused	0	0	0	0	0	3	<b>3</b>
<b>Total</b>	<b>32</b>	<b>19</b>	<b>33</b>	<b>17</b>	<b>27</b>	<b>149</b>	<b>277</b>

If the answer to #12 was “Yes”, then the following question was presented. Otherwise, it was skipped:

**Question 13: Regarding the last question, does your organization have a security policy that covers the use of portable wireless devices, such as banning the installation of apps or enabling remote wipe capabilities?**

<b>Q13</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	4	2	7	6	11	98	<b>128</b>
No	20	11	18	8	10	34	<b>101</b>
Not Sure	0	2	0	0	1	9	<b>12</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>24</b>	<b>15</b>	<b>25</b>	<b>14</b>	<b>22</b>	<b>142</b>	<b>242</b>

**Question 14: Does your organization have a policy covering the use of removable media such as flash drives?**

<b>Q14</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, removable media is banned entirely	2	1	1	1	0	14	<b>19</b>
Yes, removable media use is restricted	6	2	7	4	8	59	<b>86</b>
No, there are no restrictions on removable media	23	15	25	12	16	63	<b>154</b>
Not Sure	0	1	0	0	1	7	<b>9</b>
Refused	0	0	0	0	0	3	<b>3</b>
<b>Total</b>	<b>31</b>	<b>19</b>	<b>33</b>	<b>17</b>	<b>25</b>	<b>146</b>	<b>271</b>

**Question 15: Does your organization have a public website?**

<b>Q15</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	28	17	32	15	24	142	<b>258</b>
No	3	2	1	2	1	3	<b>12</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>31</b>	<b>19</b>	<b>33</b>	<b>17</b>	<b>25</b>	<b>146</b>	<b>271</b>

If the answer to #15 was “Yes”, then the following question was presented. Otherwise, it was skipped:

**Question 16: Regarding the last question, does your organization have a policy that dictates the content of the website, as well as who can change it?**

<b>Q16</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, access is limited to certain employees and content only	25	16	31	15	24	135	<b>246</b>
No, everybody can change the website and put any content on it	3	1	0	0	0	0	<b>4</b>
Not Sure	0	0	1	0	0	4	<b>5</b>
Refused	0	0	0	0	0	2	<b>2</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>32</b>	<b>15</b>	<b>24</b>	<b>141</b>	<b>257</b>

**Question 17: Does your organization sell software services to other companies?**

<b>Q17</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	14	9	11	8	8	49	<b>99</b>
No	14	10	21	9	15	92	<b>161</b>
Not Sure	0	0	0	0	0	1	<b>1</b>
Refused	2	0	1	0	2	3	<b>8</b>
<b>Total</b>	<b>30</b>	<b>19</b>	<b>33</b>	<b>17</b>	<b>25</b>	<b>145</b>	<b>269</b>

If the answer to #17 was “Yes”, then the following question was presented. Otherwise, it was skipped:

**Question 18: Regarding the last question, is security part of your development process from the beginning, or is it added on at the end of development?**

<b>Q18</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Security requirements are set before development begins	5	2	2	2	4	20	<b>35</b>
Security requirements are incorporated during development	9	5	6	4	2	18	<b>44</b>
Security requirements are added on after most development is complete	0	1	0	2	0	2	<b>5</b>
Security requirements are not addressed at all	0	0	2	0	0	1	<b>3</b>
Not Sure	0	0	0	0	2	6	<b>8</b>
Refused	0	0	0	0	0	2	<b>2</b>
<b>Total</b>	<b>14</b>	<b>8</b>	<b>10</b>	<b>8</b>	<b>8</b>	<b>49</b>	<b>97</b>

**Question 19: Does your organization clearly address the responsibilities and duties regarding security vulnerabilities and mitigations for all involved parties in contracts with outside vendors?**

<b>Q19</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	15	10	15	6	11	83	<b>140</b>
No	7	5	11	7	10	26	<b>66</b>
Not Sure	8	3	4	4	3	31	<b>53</b>
Refused	0	0	2	0	1	3	<b>6</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>143</b>	<b>265</b>

**Question 20: Does your organization have contingency plans, backup sites, or backup communications links? Select all that apply. If there are none, click on the "Next" button.**  
*(Note: This question allowed multiple responses)*

<b>Q20</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Physical Backup Sites	19	12	27	11	19	121	<b>209</b>
Backup Virtualization (Cloud servers, etc.)	15	5	8	7	9	71	<b>115</b>
Backup Communications Links	8	7	10	8	14	101	<b>148</b>
Backup Power Generation	12	10	16	7	15	112	<b>172</b>
Disaster Plans	10	7	13	7	16	120	<b>173</b>
Other (please specify)	3	2	0	0	4	5	<b>14</b>

**Other Responses:**

- We run a datacentre, and DR is a huge component of our budget
- WAN replication to co-location
- Sucession of authority (in case someone gets hit by a bus)
- Shotgun taped to the server chassis in case the AI decides to throw another fit.
- quarterly drills
- offsite tape backup storage (x2)
- Multiple data centers, completely highly available.
- Geographically Load-balanced Services (x2)
- backup HSM key recovery, escrow
- A bunch of DVD's in a locked fireproof safe in some dude's cabin, under the floor boards. Seriously.
- A backup site ("cold site") in case of an event that would render our primary location unusable.

**Question 21: Does your organization have a web filter or other web content blocking mechanism?**

<b>Q21</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	5	7	11	10	13	106	<b>152</b>
No	22	11	20	7	10	30	<b>100</b>
Not Sure	3	0	1	0	1	1	<b>6</b>
Refused	0	0	0	0	1	2	<b>3</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>139</b>	<b>261</b>

**Question 22: Does your organization have a spam filter or other email filter to block spam and malicious attachments?**

<b>Q22</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	27	18	27	17	24	131	<b>244</b>
No	1	0	5	0	1	4	<b>11</b>
Not Sure	2	0	0	0	0	3	<b>5</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>139</b>	<b>261</b>

**Question 23: Does your organization deploy anti-virus or anti-malware software and keep it up to date?**

<b>Q23</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, deployed and updated regularly	22	15	24	13	22	131	<b>227</b>
Yes, deployed but not up to date	1	1	2	3	1	3	<b>11</b>
No	7	2	4	1	1	3	<b>18</b>
Not Sure	0	0	2	0	1	1	<b>4</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>139</b>	<b>261</b>

**Question 24: Is cryptography used in your organization to protect data at rest (by encrypting files or disks) or in transit (by encrypting email, using SSL/TLS on your website, etc.)?**

<b>Q24</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, both data at rest and in transit is encrypted	14	8	11	5	12	75	<b>125</b>
Only data in transit is encrypted	7	2	12	8	6	27	<b>62</b>
Only data at rest is encrypted	1	1	1	1	1	9	<b>14</b>
No, neither data at rest or in transit is encrypted	5	5	6	2	4	13	<b>35</b>
Not Sure	3	2	2	1	1	6	<b>15</b>
Refused	0	0	0	0	1	9	<b>10</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>139</b>	<b>261</b>

**Question 25: Does your organization engage in vulnerability scanning, penetration testing, or other kinds of testing for vulnerabilities?**

<b>Q25</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	15	6	11	7	13	88	<b>140</b>
No	13	8	19	9	8	24	<b>81</b>
Not Sure	1	3	2	1	3	22	<b>32</b>
Refused	1	1	0	0	1	5	<b>8</b>
<b>Total</b>	<b>30</b>	<b>18</b>	<b>32</b>	<b>17</b>	<b>25</b>	<b>139</b>	<b>261</b>

**Question 26: Does your organization have a formal, written policy on the creation and deletion of user accounts?**

<b>Q26</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	7	6	9	7	15	108	<b>152</b>
No	19	11	19	10	9	20	<b>88</b>
Not Sure	1	0	3	0	0	9	<b>13</b>
Refused	1	0	0	0	1	0	<b>2</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>31</b>	<b>17</b>	<b>25</b>	<b>137</b>	<b>255</b>

**Question 27: Does your organization have a formal, written policy for the termination of IT access upon termination of employment?**

<b>Q27</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes	9	8	11	7	17	111	<b>163</b>
No	16	7	17	10	6	15	<b>71</b>
Not Sure	2	2	3	0	2	11	<b>20</b>
Refused	1	0	0	0	0	0	<b>1</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>31</b>	<b>17</b>	<b>25</b>	<b>137</b>	<b>255</b>

**Question 28: Does your organization have a formal, written policy on software installation by employees?**

<b>Q28</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, installation of all software by employees is banned	1	2	7	6	2	36	<b>54</b>
Yes, only approved software can be installed by employees	6	5	9	5	10	72	<b>107</b>
No, employees can install any software they want	19	8	14	5	11	22	<b>79</b>
Not Sure	0	1	1	1	1	4	<b>8</b>
Refused	2	1	0	0	1	3	<b>7</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>31</b>	<b>17</b>	<b>25</b>	<b>137</b>	<b>255</b>

**Question 29: Does your organization reprimand or sanction employees who do not follow IT policies or procedures?**

<b>Q29</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, with a formal record in their employment file	2	3	3	2	5	42	<b>57</b>
Yes, but only informally with no documentation	15	7	17	7	9	39	<b>94</b>
No	8	4	11	5	7	22	<b>57</b>
Not Sure	3	2	0	2	4	29	<b>40</b>
Refused	0	1	0	1	0	5	<b>7</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>31</b>	<b>17</b>	<b>25</b>	<b>137</b>	<b>255</b>

**Question 30: Does your organization ever talk with employees about cybersecurity, either through seminars, training, or memos?**

<b>Q30</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, through formal training, seminars, or memos	6	3	6	4	9	70	<b>98</b>
Yes, but only informally	13	4	12	7	8	37	<b>81</b>
No	9	9	13	6	7	27	<b>71</b>
Not Sure	0	0	0	0	0	2	<b>2</b>
Refused	0	1	0	0	1	1	<b>3</b>
<b>Total</b>	<b>28</b>	<b>17</b>	<b>31</b>	<b>17</b>	<b>25</b>	<b>137</b>	<b>255</b>

**Question 31: Are you aware of any publications or standards for "best practices" when it comes to IT security? Please list all that you are aware of, even if you do not use them in your organization. If you can't think of any, please type "None". (Note: this is an open-ended question)**

- Yes. NIST 800 documents ISO 27000
- yes - too many to list
- yes
- What

- "we have a significant Infosec intranet site that details what you can and cannot do as well as ""ask the subject matter experts"" if you have specific questions. we also have a hotline for pressing matters that cannot wait for the resolution of an opened I"
- "Use of the term ""best practice(s)"" should be banned unless proof is provided that something is the best. Very often the term is used as an excuse for something that may in fact not be productive. books ""Security Engineering"" ""The New School of Info"
- Unknown
- Too much work for a survey, sorry.
- Too many to list. Figure out what Kevin Mitnick did and go from there.
- Too many to list
- The Standard of Good Practice for Information Security
- The Department of Defense Security Technical Implementation Guides (DoD STIGs). Some are publicly available. Check out the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD) for a whole collection of Secur
- Techrepublic
- SSLF
- Short on time atm
- Seriously?! The only strict rule (with consequences) in our company is that no one leaves a logged in pc without locking it. This is our main ongoing in-house battle. Further we assume everybody is stupid.
- Security Guidance for Critical Areas of Focus in Cloud Computing, BS7799, ISO27001, etc.
- SAS70 PCI:DSS SOX
- SANS, NIST, NSA
- SANs
- Restrict access to only those who need it, when in doubt, document
- Phrack?
- PCI-DSS whatever NIST has Otherwise only informally - although we have an FCESP and a couple of CSSPs floating around
- PCI-DSS
- PCI, SOX, HIPAA
- PCI, PKI, IPSEC
- PCI DSS
- PCI complaine
- PCI applies. We use CIS standards for hardening servers, and follow OWASP/OSSTMM for penetration testing.
- PCI
- password security browsing security
- OWASP, EAL, PADSS, CC
- Our own internal publications, but to remain anonymous I won't be saying which they are. Microsoft Tech Net
- NSA Guidelines, DoD STIGs
- nsa guidelines

- Not sure what you are asking.
- Not off the top of my head, although if I were at work I could probably get a list.
- Nope (lazy)
- None.
- No.
- No comment.
- No
- NIST, FISMA, COBIT, ISO, OWASP, ISACA, Secure 360 conference
- NIST, DOD
- NIST, CERT, CIS, Cobit, coso
- NIST S.P. 800-39
- NIST Pubs
- Nist Iso27002 Owasp Pci
- NIST
- Networkworld.com computerworld.com
- na
- n/a
- n
- Mr Google, my research assistant, keeps me up to date.
- Microsoft
- many different online & published resources.
- lots of awesome
- lmgfy :)
- Length passwords. Restricted internal network access. Public keys instead of passwords.
- JIS Q 27001 (ISO/IEC 27001) and JIS Q 27002 (ISO/IEC 27002) JIS Q 15001 (Privacy Protection System in Japan) Guideline for IT farms, by Japan Government: [http://www.meti.go.jp/policy/netsecurity/law\\_guidelines.htm](http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm)
- its called google
- ITIL, COBIT.
- ITIL <http://it.wikipedia.org/wiki/ITIL>
- itil
- ISO27002
- ISO27001/2, RiskIT, CobiT
- ISO27000, though that's more of an Information Security standard.
- ISO 27001 NIST SP 800-53 Actually, the entire NIST SP 800 series. COBIT ITIL
- I'm acutely aware of ITIL and MOF and am currently in the process of implementing both methodologies at our company. With these in place, I will then be moving to a much more strict IT policy that will encompass nearly all of the items you brought up in
- IEEE privacy and security
- I have compiled them all into a list: <http://tinyurl.com/45xeh9y>
- "I am a CISSP and each environment has its own challenges. There are many different circumstances and we all generally try to do what is best or ""best practice"". Mostly this is driven by standards from organizations such as NIST, or product vendors. This i"

- <http://www.google.com/search?q=publications+or+standards+for+best+practices+IT+security>
- HIPPA, SOX, PCI-DSS, OH SO MANY MORE.
- Google. Also whatever HR will sign off on.
- Generally, common sense. Confirm everybody's identity, don't plug in the thumb drive you found in the parking lot, etc
- For the most part, Highland Computer Solutions generally finds out the needs of a company and then researches the most efficient way to accomplish what needs to be done both security wise and software wise. For the most part we use websites like toms hard
- FISMA NIST 800-53 FERPA HIPAA OSSTMM OWASP Testing Guide CISSP ITIL
- FISMA FIPS HIPPA to many to list
- FISMA
- FIPS PCI-DSS
- Don't share passwords.
- DoD 8570, SP 800, OWASP
- DISA STIGS, NSA Guides, DOD 8570
- DISA STIGs
- disa gold disk retina scan cert advisories sign up for patches for each vendor.
- Depends on product or policy, too many to list.
- Defense in Depth Principle of Least Privilege Schneier on Security =P
- CSO, SC. Access Control
- COBIT, ISO 27001
- CISSP official books
- CISSP manuals Cisco security best practice guides Juniper Networks best practice guides etc...
- CISSP All-in-One Exam Guide, Fifth Edition
- CIS, SANS, ISACA, (ISC)2, ISO27000
- CIS Benchmarks NIST Special Publications Generally Accepted Information Security Principles
- CIS benchmarks
- Best practices are often published by security firms, research partners, software vendors, and many others.
- Best practices are bunk.
- BCP34 ISF Standard ISO 17799 Microsoft TechNet SANS USENIX/LISA
- Aware, but management doesn't care.
- Availability vs Integrity vs
- 2600
- 1
- 0
- /r/netsec
- ---

**Question 32: Are you aware of NIST Special Publication 800-39?**

<b>Q32</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Yes, aware of it and use it in our organization	4	1	0	1	2	21	<b>29</b>
Yes, aware of it, but do not use it	4	5	4	2	7	31	<b>53</b>
No	17	11	26	14	13	73	<b>154</b>
Refused	0	0	0	0	1	6	<b>7</b>
<b>Total</b>	<b>25</b>	<b>17</b>	<b>30</b>	<b>17</b>	<b>23</b>	<b>131</b>	<b>243</b>

**Question 33: How concerned about you about IT security in the workplace? Please limit your answer to the workplace only.**

<b>Q33</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Not at all concerned	1	1	2	0	0	9	<b>13</b>
A little bit concerned	4	2	5	3	6	7	<b>27</b>
Somewhat concerned	7	6	10	3	2	25	<b>53</b>
Very concerned	7	3	9	4	3	42	<b>68</b>
Extremely concerned	6	5	4	7	12	47	<b>81</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>25</b>	<b>17</b>	<b>30</b>	<b>17</b>	<b>23</b>	<b>131</b>	<b>243</b>

**Question 34: How concerned about you about IT security at home? Please limit your answer to your home only.**

<b>Q34</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
Not at all concerned	2	1	2	3	1	4	<b>13</b>
A little bit concerned	2	3	6	2	3	18	<b>34</b>
Somewhat concerned	9	5	9	3	4	34	<b>64</b>
Very concerned	8	3	9	4	7	43	<b>74</b>
Extremely concerned	4	5	4	5	8	31	<b>57</b>
Refused	0	0	0	0	0	1	<b>1</b>
<b>Total</b>	<b>25</b>	<b>17</b>	<b>30</b>	<b>17</b>	<b>23</b>	<b>131</b>	<b>243</b>

**Question 35: Have you ever been a victim of an IT security breach? This could be anything from a virus infection to identity theft. You may leave this question blank if neither apply. (Note: this question allowed multiple responses)**

<b>Q35</b>	<b>1-5</b>	<b>6-10</b>	<b>11-25</b>	<b>26-50</b>	<b>51-100</b>	<b>100+</b>	<b>Total</b>
At work	6	5	10	8	6	43	<b>78</b>
At home	9	5	9	4	8	45	<b>80</b>

**Question 36: If you are interested in being contacted for a follow-up interview, please enter your email address here. All communications will be held strictly confidential. All company names, details, and identifying information will be anonymized if necessary. No data will be shared with anybody outside of myself and the three members of the graduate school evaluation committee.**

**In addition, those contacted for follow-up may be asked to test and comment on a security-enhancement consulting product free of charge. (Note, this was a non-required question)**

*Answers Redacted*

## Appendix B: First Draft of Worksheet

### Sheet 1: Risk Assessment

#### 800-39 Worksheet for Small Organizations

##### Risk Assessment (Task 2-1)

Business Process	Sub Process	IT Resources Used	Possible Vulnerabilities	Notes
------------------	-------------	-------------------	--------------------------	-------

---

### Sheet 2: Risk Determination

#### 800-39 Worksheet for Small Organizations

##### Risk Determination (Task 2-2)

Vulnerabilities	Edge-Case Scenarios	Relative Risk (1 low-5 high)	Notes
-----------------	---------------------	------------------------------	-------

---

### Sheet 3: Risk Framing

## 800-39 Worksheet for Small Organizations

**Risk Framing/Trends**

(Task 1-1)

**Common Threat Sources**

**Notes**

---

**Common Vulnerabilities**

**Notes**

---

**Scenario Consequences**

**Notes**

---

## Sheet 4: Resources

### 800-39 Worksheet for Small Organizations

**Resources/Priorities** (Task 1-2, 1-3, 1-4)

<b>Available Resources</b>	<b>Notes</b>
----------------------------	--------------

---

<b>Priorities</b>	<b>Notes</b>
-------------------	--------------

---

## Sheet 5: Risk Responses

### 800-39 Worksheet for Small Organizations

**Risk Responses** (Task 3-1, 3-2, 3-3, 3-4, 4-1,4-2)

<b>Vulnerability/Risk</b>	<b>Priority</b>	<b>Risk Response</b>	<b>Implementation Details</b>	<b>Responsible Party</b>	<b>Policy Changes</b>	<b>Followup Monitoring</b>
	#N/A					
	#N/A					

**Appendix C: Government Organization A Worksheet**

**Sheet 1: Risk Assessment**

**Information Redacted**

**Sheet 2: Risk Determination**

**Information Redacted**

**Sheet 3: Risk Framing**

**Information Redacted**

**Sheet 4: Resources**

**Information Redacted**

**Sheet 5: Risk Response**

**Information Redacted**

**Appendix D: Multimedia Company B Worksheet**

**Sheet 1: Risk Assessment**

**Information Redacted**

**Sheet 2: Risk Determination**

**Information Redacted**

**Sheet 3: Risk Framing**

**Information Redacted**

**Sheet 4: Resources**

**Information Redacted**

**Sheet 5: Risk Response**

**Information Redacted**



## The Application of NIST Special Publication 800-39 for Small Businesses and Organizations

MSST Capstone Presentation  
Nathan Hunstad  
2 August 2011



## Executive Summary

- **Problem:** IT security is vital for small businesses but easy for businesses to overlook
- **Possible Solution:** NIST Special Publication 800-39
- **Issue:** Adapting NIST Special Publication 800-39 to the needs of small businesses
- **Methodology:** Survey, literature review, worksheet development, and case studies
- **Recommendation:** Continuous development of the adapted worksheet
- **Delta MSST:** Providing the tools for putting a security plan together



## Introduction

- IT Security for Small Businesses
  - Lack of resources
  - Lack of IT awareness
  - Lack of urgency
  - Too many standards
- Can NIST Special Publication 800-39 be the answer?



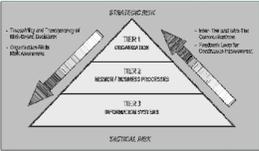
## Problem Statement

- Possible NIST Special Publication 800-39 Issues
  - Assumptions about organization size
  - Assumptions about organization structure
  - Scope of business practices
- Possible NIST Special Publication 800-39 Benefits
  - Less ingrained culture
  - Uniformity



## Problem Statement

**From This**



**To This**

800-39 Worksheet for Small Organizations				
Risk Assessment	(Task 2-1)			
Business Process	Sub Process	IT Resources Used	Possible Vulnerabilities	Notes



## Project Methodology

- Literature review
  - NIST Special Publications: 800-39, 800-37, 800-53, 800-53A, 800-30, 800-60
  - FIPS Publication 199, FIPS Publication 200
  - ISO 27000-series
  - COBIT
  - Industry-specific standards
- Online Survey
- Worksheet Development
- Case Studies

### Analysis: Literature Review and Survey

- FISMA
- NIST Special Publication 800-39

Organization Size	Not at all concerned	Somewhat concerned	Very concerned	Extremely concerned	Refused
1-5	~10%	~20%	~30%	~20%	~10%
6-10	~10%	~20%	~30%	~20%	~10%
11-25	~10%	~20%	~30%	~20%	~10%
26-50	~10%	~20%	~30%	~20%	~10%
51-100	~10%	~20%	~30%	~20%	~10%
100+	~10%	~20%	~30%	~20%	~10%

- Two weeks of data, n=316
- Widespread concern about security

### Analysis: Worksheet Use

### Analysis: Case Studies

- Case Study 1: Government Agency A
  - Several IT departments
  - Lack of uniform controls
  - Worksheet identified vulnerabilities, helped prioritize risk
- Case Study 2: Media Company B
  - No IT department
  - Every employee for themselves
  - Worksheet identified vulnerabilities, risks that were acceptable

### Analysis: Other Standards

- Generalized Standards (ISO 27000, COBIT, Microsoft)
- Specific Standards (OWASP, STIGs, NSA)
- Industry Standards

### Analysis: SWOT

SWOT Analysis	
Strengths	Weaknesses
Readily available	Generalized
Flexible	Requires technical knowledge
Applicable to many organizational types	
Increasing use of technology	Better assessment tools
Large number of small businesses	More secure software
Interdependencies between technologies	Economic weakness
Changes in liability	
High-visibility security failures	
Opportunities	Threats

### Recommendations

- Power Zone
- Business Case for Development
- Applicability to Other Security Areas

### Future Moves

Short-Term and Long-Term Moves					
Move	Why	Who	How	When	Cost
Add "Affile Tables"	Provide usable summary for customer		Extend worksheet	Short term	Minimal
Risk Assessment Grid	Provide usable summary for customer		Extend worksheet	Short term	Minimal
Mac Compatibility	Improve system compatibility		Change worksheet coding	Short term	Minimal
<hr/>					
Branch out to other security domains	Extend the applicability of product		Create new worksheets	Long term	Time to customize, learn about other standards
Add Security Controls	Provide immediate options for mitigations		Add to worksheet	Long term	Research controls, add and update as needed

- ### Security Implications
- Security Environment for Small Businesses
    - Cyber attacks constant
    - Thousands of dollars of losses
  - Critical Infrastructure
    - Small businesses present in many CIP areas
  - Changing Threats
    - Framework to build from

### Δ MSST

- Scenarios
- Trend Forecasting
- Interdependencies
- Complex Systems
- Leadership

Complex Adaptive System Diagnostic

"Six Superrends shaping the Future"

Interdependency