UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

Factors for Consideration when Implementing Network Access Control (NAC) Solutions for Small and Medium Sized Businesses (SMBs)

CAPSTONE REPORT

Oscar Hicks
Information Technology Services Director

University of Oregon
Applied Information Management Program

February 2010

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

RUNNING HEAD: IMPLEMENTING NETWORK ACCESS CONTROLS

Factors for Consideration when Implementing Network Access Control (NAC) Solutions for Small and Medium Sized Businesses (SMBs)

Oscar Hicks

Clackamas County Fire District #1

This page intentionally left blank

Abstract

Implementing network access controls (NAC) requires an awareness of various factors pertaining to information authentication, security, and access. Selected literature published between 1990 and 2009 is examined, based on three factors for consideration: assessment, scope of implementation, and costs. The outcome presents guidelines for small and medium sized businesses in the areas of governance, stratagem, and budgetary impacts. Selected annotated references are provided to emphasize best practices and security framework models currently in use.

This page intentionally left blank

Table of Contents

This page intentionally left blank

List of Figures

This page intentionally left blank

Introduction

Problem Area

Research has shown that "malicious attacks on enterprise Information Technology (IT) infrastructures have become a serious threat with the growing importance of the Internet" (Khansa & Liginlal, 2009, p. 113). In addition, "'regulatory frameworks and legislations such as the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act (GLBA), and the Sarbanes-Oxley Act (SOX), require organizations to implement the necessary safeguards to ensure the confidentiality, integrity, and availability of information" (Khansa & Liginlal, 2009). Unfortunately, a connection to the Internet, especially broadband connection that is always on, introduces security threats to small businesses that they may not have the resources or expertise to deal with effectively (Keller, Powell, Horstmann, Predmore & Crawford, 2005)

Keller et al., (2005) posits each new decade introduces new threats to businesses. These threats are increasingly complex and take full advantage of the vulnerabilities within applications and network infrastructure assets. Earlier research conducted by Keller, Powell, Horstmann, Predmore & Crawford (2005), asked respondents to identify the major threats they perceive as likely to cause harm to their business or industry data (see Figure 1).

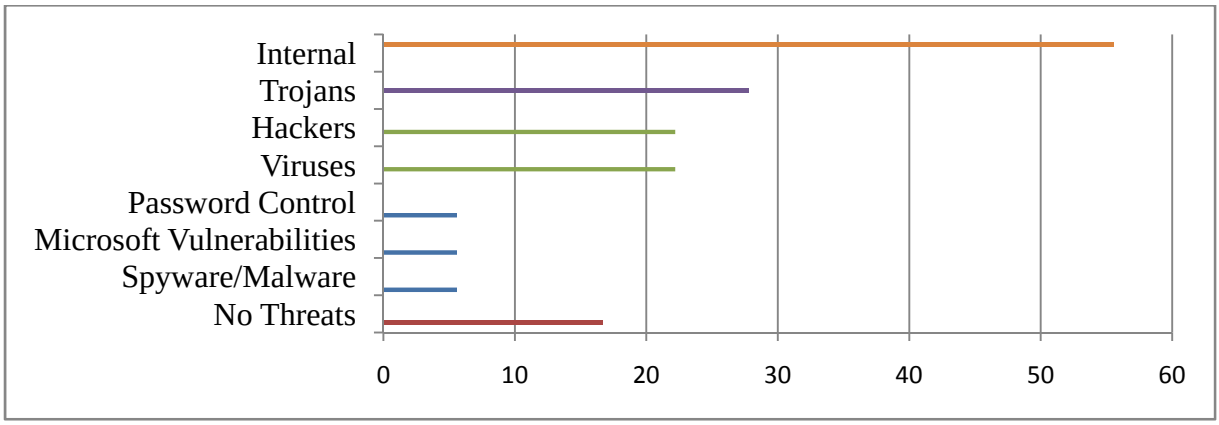

Figure 1 - Perceived Data Security Threats (Keller et al., 2005, p.11)

Over half (55.6 percent) of the respondents felt that primary threats to data come from internal personnel. However, many respondents also indicated that this employee threat could largely be accidental or unintentional. According to Keller et al., (2005), globalization, and information and communication technologies are main issues on organizations and societies, changing the way in which people and organizations interact. Far too many firms take a reactive approach to information security planning (Johnston & Hale, 2009). These issues bring new and more challenges to people, organizations and societies, forcing them to change their perceptions of reality and consequently adopting new business solutions (Peltier, 2005).

Ineffective protection for network infrastructure can often be attributed to the manner in which SMBs go about planning their information security programs (Johnston & Hale, 2009). In addition, a large number of false alarms, even when each is only introducing negligible cost, could escalate into legitimate concerns. Hence, the implementation particulars of NAC configuration choice in a computer network -based problem are more ambiguous than in a nuclear plant problem (Rui, Jinshu & Feng, 2009). For instance, Rui et al., (2009) suggest that managers should determine if systems are configured to detect all the attacks, at the expense of many false alarms. This may be particularly important, because the cost of not detecting all attacks involves potential irreversible damage to human health.

In support of Rui et al., (2009), Saint-Germain (2005), states a number of best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements. According to META Group, companies and institutions affected by such legislation must decide for themselves which security controls are appropriate for their organizations (Saint-Germain, 2005).

Purpose

As noted by Sarrel (2008), proactive network security measures rarely get the attention and commitment from small business owners that they deserve, yet in almost every case an ounce of prevention is worth a pound—or more—of cure (p. 90). In response to this perspective, the purpose of this study is to identify selected factors regarding when and why small and medium sized businesses (SMBs) should consider the implementation of Network Access Control (NAC) into their information enterprise.

There are several forms of NAC solutions, including agent-based, dynamic host control protocol (dhcp)-based, and simple network control protocol (snmp)-based; each with its own set of positive and negative aspects. In this study, focus is on identification of factors for consideration in three key categories: (1) threat assessment; (2) scope of implementation; and (3) costs. For example, preliminary research reveals that a growing number of employees are considering the use of their own personal PCs in their jobs (Brooks, 2006). When considered in relation to threat assessment, this factor might result in concern over potential loss of control by IT departments (Brooks, 2006). Additional questions addressed in the study include:

What are the reported benefits in implementing a NAC solution, related to threat assessment?

In its study of five business sectors, the Council on Competitiveness (Young, 1986), found some are further along than others in recognizing and realizing business benefits from security ("How Companies Capture Business Benefits of Security," 2007). Cost savings, productivity gains, and improved compliance are a few of the benefits highlighted ("How Companies Capture Business Benefits of Security," 2007).

What are the reported drawbacks in implementing a NAC solution, related to threat assessment?

It would be ill fated to think there is a total all in one-security solution without any shortcomings. For example, NAC products that enforce policies via Dynamic Host Configuration Protocol (DHCP) proxy servers do nothing to stop machines that obtain static IP addresses and do not use DHCP to make their network connections. That makes significant portions of corporate networks invisible to the NAC access control products (Greene, 2008).

What are two industry recognized and cost effective NAC security products available for SMBs?

Technology research and advisory firm Gartner defines three NAC common approaches as infrastructure-based, endpoint software-based, and network security appliance-based (Powers, 2008). Research has shown that one recognized product leader in NAC solutions is the Cisco® Network Admission Control (NAC) which helps organizations to achieve these goals (Robinson, 2006).

Significance

It is estimated that more than one million small businesses in the United States connect to the Internet with some form of broadband access (Gercek & Saleem, 2005). Margariti, Meletiou, Stergiou, Vasiliadis, & Rizos (2007) states that security is a fundamental management responsibility of data protection in computers systems and network environments. It is concerned with determining the access control of legitimate entities and also with the protection of assets from threats (Margariti et al., 2007). Research suggests that in many companies, strategies for asset protection are derived from the bottom up, based on incidents at the perimeter of the organization (Johnston & Hale, 2009). As such, these firms segregate information security from their overall strategic directive, thereby creating a divide between the governance of the firm and the management of information security (Johnston & Hale, 2009). The results of such a

disconnect can be disastrous, as management and employees may lose touch with the value of appropriate security actions and as business processes become bogged down with unnecessary or improper controls (Johnston & Hale, 2009). According to Johnston and Hale (2009), in scenarios such as these, a scope of implementation for security planning is highly warranted.

A survey conducted by Visa USA and the National Federation of Independent Business (NFIB) reports that 57 percent of small businesses do not consider securing customer data something that requires formal planning, and 39 percent said they rely on common sense to keep data safe ("Data Security Challenges Small Firms," 2007). As noted by John Oltsik of Enterprise Strategy Group, " Security companies are responding to strong demand from enterprise customers for technology that can help them comply with new federal and state regulations and to counter the threat posed by mobile and remote workers" (Roberts, 2006). Most IT and security departments also face budgetary and personnel resource constraints ("SMBs weigh SECURITY purchases," 2009).

The security of small systems is one of the most difficult challenges faced by management (Bradbard, Norris, & Kahai, 1990). In addition, survey research conducted by Trend Micro (2005) of 1,200 companies in the United States, Germany, and Japan finds that only about 54% of small and medium sized businesses in the U.S. have an IT department. Yet, in 2005 it was reported that phishing encounters increased for about 40% of United States based workers in small and midsize businesses, and spyware became an increasing threat ("SMB networks said at risk," 2005).

Audience/Outcome

This study is aimed at executives and managers responsible for planning information technology security policy within small businesses. Additionally, this review is aimed towards IT consultants as a reference in providing NAC services for SMBs. The outcome is designed as

a guide, based on information derived from real-world cases and peer-reviewed articles. The guide provides a framework for determining the level of acceptable risk of network access security. It is essential to consider potential risks during NAC planning in order to ensure an effective NAC solution implementation within existing network environments. The guide highlights factors for consideration and discussion by SMB executives and management, as a way to aid IT professionals as they collaborate with SMB executives and unit managers to determine potential: (1) threat assessment; (2) scope of implementation; and (3) costs.

Delimitations

Time frame. The literature collected for this study is published between 1989 and 2009. During the past 20 years improved technology has produced ever smaller computers that substantially surpass the processing and data storage capabilities of older machines (Bradbard et al., 1990). The first generation of security threats started in the 1980s (Keller et al., 2005). Typically, these threats were boot viruses that affected individual computers and networks over the course of weeks (Keller et al., 2005). "Although the technologies and some of the threats they raise may be new, enterprises are still well-advised to stick to the tested method for minimizing the risks: a proactive, programmatic approach" (Pironti, 2005).

Selection criteria. The primary sources for the literature are retrieved from ACM Portal, EBSCO Host, Academic Search Premier, Google Scholar, IEEE Digital Library, Summit, and WorldCat. Preference is based on relevance to the topic, depth of analysis, and date published (Leedy & Ormrod, 2005). As a member of UO Libraries, this researcher has access to articles not available to the general public. Limited availability materials are noted in the references list and are available from the Institute of Electrical and Electronics Engineers (IEEE) www.ieee.org.

To ensure the credibility and relevance of the materials selected in the area of network infrastructure security and access controls, the selection of literature is limited to authors who are members of, or associated with international, academic, government, information security, and information technology centered organizations:

- Professional or non-profit organizations: Certified Information Systems Security Professional (CISSP), Cisco Certified Internetwork Expert (CCIE)
- U.S. government agencies: United States Congress, House Committee on Science and Technology, Select Committee on Homeland Security
- Technology focused institutions or organizations
- National Small Business Association (NSBA)

The reasoning behind the selection of these criteria is based on the credibility the institutions have earned in relation to the topic. The selection of literature is limited to the information technology security field in conjunction with small and medium sized business information security practices. Selected sources for this literature review are specifically chosen based on relevancy and focus on factors for consideration in three key categories: (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006), (Bandyopadhyay, Positiv, 2006).

Audience. The target audiences for the literature review are IT managers and consultants who alone or collaboratively create, design, and implement NAC solutions. An effective information security program endeavors to ensure that the organization's information and its processing resources are available when authorized users need them (Peltier, 2005). Security matters have become an integral part of daily life, and organizations need to ensure that they are adequately secured.

This literature review is designed to aid IT managers and consultants in determining the level of acceptable risk of network access security, based on the factors for consideration as mentioned in earlier text. Management establishes its goals and objectives for protecting the assets of the enterprise by implementing policies (Peltier, 2005). All too often, security professionals implement the "perfect" security program, and then are surprised that it fails because they forgot to sell their product to their constituents (Peltier, 2005). Organizations often tackle security issues as part of their efforts to comply with a variety of regulatory requirements, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) (Saint-Germain, 2005).

Topic definition. A lack of awareness of computer security is a primary reason that U.S. Congress passed the "Small Business Computer Security and Education Act of 1984." (Bradbard et al., 1990). NAC is one tier of a multi-tiered approach to protect the security and integrity of networks, applications, and data. Bradbury et al., (1990) ask to what extent small businesses are aware of or implementing measures that prevent, detect, or correct possible security exposures? This question underlies the selection of topic definition.

Research focus. Computer security activities by themselves appear to be cumbersome procedures impeding work flow and generating a feeling of mistrust. Financially these activities incur additional operational costs and expertise. However, these activities ultimately protect a vital asset of an organization; business information (Ban & Heng 1995).

NAC implementation has identifiable benefits that are aligned with organizational expectations, business drivers for IT. Drawbacks can include various elements of the selected three factors for consideration. For example, implementation (resources, time, training), threat assessment

(validity, source, probability), cost (hardware, licensing, training). These aspects of NAC implementation form the key concepts used to design the specific conceptual analysis process.

Data Analysis Plan Preview

The intent of this literature review is to identify selected factors regarding when and why small and medium sized businesses (SMBs) should consider the implementation of Network Access Control (NAC) into their information enterprise. The goal is to identify factors related to potential: (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006), (Bandyopadhyay, Positiv, 2006). Data analysis follows the approach to the conceptual analysis process as described by Busch, De Maret, Flynn, Kellum, Le, and Meyers (2005). This process provides a research tool, which can be used to verify the presence of certain words or concepts within texts or sets of texts. Busch et al., (2005) notes that by reducing the text to categories consisting of a word, set of words or phrases, and the researcher can focus on, and code for, specific words or patterns that are indicative of the research question.

Writing Plan Preview

On an enterprise level, planning leads to strategies which provide direction to the firm and touch on all aspects of the organization, including financial, research and development, marketing, human resource, and information technology resources (Johnston & Hale, 2009). The goal of this study is to establish an organized review of information regarding the implementation of NAC literature with an emphasis on (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006), (Bandyopadhyay, Positiv, 2006) identified through the Data Analysis approach

introduced above. By reducing the text during data analysis to categories consisting of a word, set of words or phrases, the focus and coding is on specific words or patterns that are relevant and indicative of the research question (Busch et al., 2005). The information collected from this process is analyzed and synthesized into a set of themes, framed to determine the level of acceptable risk of network access security for successful implementation NAC solutions within an existing enterprise infrastructure. Preliminary themes concern (1) threat assessment; (2) scope of implementation; and (3) costs. Additional themes may emerge.

Definitions

The definitions section presents terms used in the literature review. Definitions are designed to describe concepts, environments, and terms that relate to SMBs network access control planning and implementation as these concepts are utilized in this study. Terms are mined from selected literature, initial concept terms, and key word searches.

- **Acceptable Risk –** is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls (NIST, 2000).
- **Access -** The ability for a user or device to connect to a system or service. An example of access is the requesting and competition of a mobile telephone to get the attention and service access to a cellular radio system (Althos, 2009).
- **Agent**- (1-general) an agent is a person or a device that performs tasks for the benefit of someone or some other device. (2-software) An agent is a program that performs a task in the background and informs the user when the task reaches a certain milestone or is complete. (3-SNMP) An SNMP agent is a program that monitors network traffic. In client-server applications, an agent is a program that mediates between the client and the server (Althos, 2009).
- **Costs -** Cost of implementation of an information security package is usually seen as the sum of all one-time fees incurred at the beginning of executing a lead management program. This typically includes but is not limited to hardware and / or software licensing, setup charges, configuration expenses, and employee training. This is the first piece calculated when determining total cost of ownership (NIST, 2000).
- **Dynamic Host Protocol (DHCP) –** Dynamic host configuration protocol is a process that dynamically assigns an Internet Protocol (IP) address from a server to clients on an

as needed basis. The IP addresses are owned or controlled by the server and are stored in a pool of available addresses. When the DHCP server senses a client needs an IP address (e.g. when a computer boots up in a network), it assigned one of the IP addresses available in the pool (Althos, 2009).

- **Enterprise Network -** The set of Local, Metropolitan, and/or Wide Area Networks and internetworking devices comprising the communications infrastructure for a geographically-distributed organization (Althos, 2009).
- **GLBA -** The Gramm-Leach-Bliley Act (GLB Act), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. The Act consists of three sections: The Financial Privacy Rule, which regulates the collection and disclosure of private financial information; the Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information; and the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses). The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices (Khansa & Liginlal, 2009).
- **HIPPA -** Health Insurance Portability and Accountability Act (HIPAA) for electronic health-care information. HIPAA requires safe electronic data interchange of medical records, also known as protected health information (PHI), by covered entities such as health-care plans and clearinghouses that store and process electronic health-care information. HIPAA security rules guard against unauthorized transmission of PHI only in electronic form--over the Internet, extranet, private networks and leased and dial-up lines (Khansa & Liginlal, 2009).

- **Information Technology –** A broad term that describes the computer hardware, software, and networking industry, including telecommunications and audiovisual equipment (Goleniewski, 2008).
- **Intranet -** An intranet is a private network that is used within a company to provide company information to employees. Intranets may be connected to vendors and customers through private data connections or via public Internet connections. When Intranets are connected to the Internet, they are commonly connected through firewalls to protect the company's internal data (Althos, 2009).
- **Layer-3 routing -** A switching device that operates at OSI network layer 3. Synonymous with router (Althos, 2009).
- **META Group –** Acquired by the Gartner Inc. in April 2005. Gartner, Inc. is the world's leading information technology research and advisory company.
- **Monitoring (Host-based) –** A host-based monitoring system reads all or parts of the dynamic behavior and the state of a computer system. Much as a network-based monitoring system will dynamically inspect network packets, a HIDS might detect which program accesses what resources and discover that, for example, a word processor has suddenly and inexplicably started modifying the system password database (Goleniewski, 2008).
- **Monitoring (Network-based) –** A network-based monitoring system reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. If, for example, a large number of TCP connection requests to a very large number of different ports are observed, one could assume that there is someone conducting a port scan of some or all of the computer(s) in the network (Goleniewski, 2008).

- **Network Access Control –** (NAC), also called network admission control, is defined as a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy (The SANS Institute, 2009).
- **Network Security -** The processes used within a network to validate the identity of users (authentication), access control of services (authorization), and information privacy protection (encryption) (Althos, 2009).
- **National Institute of Standards and Technology (NIST) –** A unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards (The SANS Institute, 2009).
- **Policy Control -** Policy control is the processes that are used to modify the configurations and/or parameters of network elements or devices that control the providing of services to ensure the performance or operation attempts to confirm to defined service levels (Althos, 2009).
- **Remote access -** Remote access is the ability of a device, user or system to communicate or control devices, services or systems at locations outside the boundaries of the device or system they are controlling (Althos, 2009).
- **Rootkit -** A software system that consists of one or more programs designed to obscure the fact that a system has been compromised. Contrary to what its name may imply, a rootkit does not grant user administrator privileges, as it requires prior access to execute and tamper with system files and processes. An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker

has installed, along with the presence of the rootkit. Access to the hardware, *e.g.*, the reset switch, is rarely required, as a rootkit is intended to seize control of the operating system (Althos, 2009).

- **Router –** A router is a device that directs (routes) content (data, voice, or video) from one path to another on a network. Routers base their switching information on one or more parameters contained in the packet of content. These parameters may include availability of a transmission path or communications channel, destination address contained within a packet, maximum allowable amount of transmission delay a packet can accept, along with other key parameters. Routers forward data packets between multiple interfaces based on the network layer. Most modern day routers support one or more of the following protocols: Internet Protocol (IP), Novell IPX, or AppleTalk. Routing occurs at layer 3 of the OSI reference model and can be used to limit the broadcast domain of a bridged network (Althos, 2009).
- **Security (Access) –** Access security is the processes that are used to ensure a system can operate without damage, theft or compromise of its resources from unwanted people or events (Althos, 2009).
- **Security benefits –** Provides a level of network security that allows or restricts clients' access to a LAN or WAN, depending on whether they have the correct security software. A common benefit of NAC is the ability to control guest machine access to a network.
- **Security threat –** Potential people or processes that may allow access to services or information that is not desired or authorized by the owner or controller of the systems or information (Althos, 2009).
- **SMB (Small and medium business) –** is an abbreviation for small and medium-sized business, sometimes seen as small and midsized business. A business with 100 or fewer

employees is generally considered small, while one with 100-999 employees is considered medium sized (SearchCIO-Midmarket.com, 2009).

- **SNMP –** Simple Network Management Protocol (SNMP) is a standard protocol used to communicate management information between the network management stations (NMS) and the agents (ex. routers, switches, network devices) in the network elements. By conforming to this protocol, equipment assemblies that are produced by different manufacturers can be managed by a single program. SNMP protocol is widely used via Internet protocol (IP) and operates over UDP well-known ports of 161 and 162. SNMP was originally defined in RFC1098 and is now obsolete and updated by RFC1157 (Althos, 2009).
- **SOX –** The Sarbanes Oxley Act is a United States law that was passed in 2002 that defines new requirements and responsibilities for company financial reporting. This law was created in response to multiple scandals that resulted from misrepresentative accounting records from companies including Enron and MCI (Althos, 2009).
- **Threat Assessment –** Process of formally evaluating the degree of threat to an information system and describing the nature of the threat (Web Security Glossary, 2005).
- **Wireless Security –** Wireless security is the ability of a wireless system or service to maintain its desired operation without damage, theft, or compromise of its resources from unwanted people or events. Wireless security may use access security, authentication and encryption systems to maintain the security of the system (Althos, 2009).

Research Parameters

Information in the research parameters section of the document provides an overview of the methods used to develop the literature review. There are nine sections including sub-sections, which make up the Search Strategy Report. All sections and sub-sections highlight or detail how the research is conducted and evaluated, and provide an explanation as to how the mined data will be presented. The sections are as follows:

- Search Terms and Subtopic search terms
- Record of Preliminary Searches
- Literature resources
- Search engines
- Databases
- Evaluation criteria
- Data Analysis Plan
- Writing Plan

Search Strategy Report

Search Terms. References for literature review will be collected using the search terms and controlled vocabularies listed below. The search terms chosen are from analysis of noted keywords used in the literature found during initial searches. The literature collected for this study is published between 1986 and 2009. During the past 30 years improved technology has produced ever smaller computers that substantially surpass the processing and data storage capabilities of older machines (Bradbard et al., 1990). One significant barrier to effective use of computers in small business is inattention to computer security (Bradbard et al., 1990). Bryant

(1984) contends that the security of small systems is one of the most difficult challenges faced by management (Bradbard et al., 1990). Key search terms include:

- Access
- Information Technology (IT)
- Network
- Network Access Control
- Security
- SMB (Small and medium business)

Subtopic search terms include:

- IT Consulting
- IT Consulting and SMB security
- Information Security (InfoSec) challenges
- Network Security benefits
- Wireless Security

Record of Preliminary Searches

The spreadsheet below (see Figure 2) illustrates searches to date, along with comments explaining selection process.

SEARCH ENGINE / DATABASE	SEARCH TERMS / PHRASES	RESULTS#	QUALITY / RELEVANT	COMMENTS
Academic Search Premier - (BEST)	Network Access Control (NAC)	17	Good / Full text	During latest research session this database provided the most relevant data to my research topic. Search limiter was 20 years and expander was full text or articles with references. EBSCOhost interface w/advanced search
	Information security challenges	1665	Good / Full text, SmartText search	
	Wireless security	10	Good / SmartText search	
	Remote Access best practices	427	Good / Full text, SmartText search	
	Small to Medium-sized business security	624	Good / Fair - not focused on topic	
	Network security benefits	217	Good / found many relvant peer review articles.	
	IT Consulting	25	Good	
	IT Consulting and SMB and security	155	Good / found many relvant peer review articles.	
UO Libraries Catalog - SMMIT /WORLD CAT.ORG databases (TIE for 2nd)	Network Access Control (NAC)	306	Good	During latest research session this database provided the second most relevant data to my research topic. Although there were some results that scored as Poor, mainly because the standard was set.
	Information security challenges	20	Fair	
	Wireless security	310	Good	
	Remote Access best practices	8	Poor	
	Small to Medium-sized business security	2	Poor	
	Network security benefits	14	Fair	
	IT Consulting	12	Fair	
	IT Consulting and SMB and security	0	Poor	
Google Scholar	Network Access Control (NAC)	1900	Good	(Not bad for a free pulblic SE) - could have used a little more on the delimiter/expander options provided.
	Information security challenges	26,200	Good	
	Wireless security	208,200	Fair - too much informaiton with no limiter ability	
	Remote Access best practices	18,400	Fair	
	Small to Medium-sized business security	1,030,000	Fair - vast informaiton with very little relevant content	
	Network security benefits	33,000	Fair	
	IT Consulting	1,700	Fair	
	IT Consulting and SMB and security	1,390	Fair	
UO - MasterFILE (TIE for 2nd)	Network Access Control (NAC)	119	Good	During latest research session this database also provided the second most relevant data to my research topic. Although there were no results that scored as Poor , Academic Search Premier seemed more intuitive.
	Information security challenges	92,418	Fair - was not a narrow limiter that could have been u	
	Wireless security	374	Good	
	Remote Access best practices	28,567	Fair - was not a narrow limiter that could have been u	
	Small to Medium-sized business security	9	Good - new resources as compared to previous week	
	Network security benefits	119	Good	
	IT Consulting	7	Good - very specific	
	IT Consulting and SMB and security	7	Good	
CiteSeer -	Network Access Control (NAC)	78	Fair	(Was expecting much more considering scientific and research nature of the site.)
	Information security challenges	236	Fair	
	Wireless security	62	Fair	
	Remote Access best practices	0	Poor	
	Small to Medium-sized business security	0	Poor	
	Network security benefits	429	Fair	
	IT Consulting	52	Fair	
	IT Consulting and SMB and security	0	Poor	

Figure 2 - Preliminary Search Report

Literature resources. Using the keywords and controlled vocabulary defined above, resources for this literature review are collected using the tools and information sources outlined below. Selected resources chosen for citation are retrieved and cataloged for future reference in portable document format (pdf).

Search engines. Search engines used to collect literature review resources are UO Libraries, Google Scholar, and CiteSeer. These search engines have been effective in providing good sources of information about the topic that will be academic standards (e.g. published works from academic journals or peer-reviewed journals). Ulrich's International Periodicals Directory is used to validate non-academic journals.

Databases. Literature review resources are collected using these databases: UO Libraries Catalog, Summit Union Catalog, WorldCat Index, EBSCO HOST Research Databases, and Academic Search Premier Index. These electronic sources have been effective in locating information relevant to topic.

Evaluation Criteria

Literature is initially evaluated based on relevance to the topic and selected time frame 1995 to 2009. Literature for this study is methodically extracted using the World Wide Web and UO Libraries as the primary source for scholarly texts, references and professional documentation (Leedy & Ormrod, 2005). Article preference is based on relevance to this study, depth of analysis, and date published. Once literature is collected, it is cataloged into three categories: electronically into folders that directly correspond to the three main categories: (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006),

(Bandyopadhyay, Positiv, 2006), the three factors for consideration when implementing NAC by SMBs. The three factors of consideration include potential advantages and disadvantages of each factor before, during, and after the implementation process. Results are presented in a guide that parallels the writing plan section of the literature review.

Article quality is determined based on three criteria: 1) search location – if the literature is published in a scholarly journal, industry trade journal or referenced in a determined scholarly search engine or database, it is deemed credible; 2) if the literature is written for a more advanced audience, for example, IT professionals rather than general audience overviews, it is deemed as a quality piece of literature; and 3) if the article is not a focused advertisement for a specific product, then it is deemed as potentially credible article. Critical evaluation of selected information sources and credibility of the literature is based on the following five criteria (Smith, 2008):

- Authority – What are the author's credentials, reputation among peers, what is the association with a reputable institution or organization?
- Objectivity – Is there bias, does the author state the goals of the publication, and does the information appear valid and well researched?
- Quality – Is it well organized, are there spelling, grammar or typographical errors?
- Coverage – Is other material used and referenced, what facts, statistics, evidence is used and are there gaps?
- Currency – How recently is the research completed?

Evaluations of these criteria are related to the audience needs as well as the goals of the study.

Data Analysis Plan

The references collected for this study are qualitatively analyzed by using the data analysis spiral (Leedy & Ormrod, 2005, p. 151). This spiral has four steps to follow: first the selected reference materials are organized, then they are examined to obtain a sense of what they contain as a whole, next they are identified into groups based on predetermined criteria, and lastly they are synthesized to create the final report. The data analysis process used in this study to support the synthesis step is called 'conceptual analyses'. In conceptual analysis, a concept is chosen for examination, and the analysis involves quantifying and tallying its presence (Busch et al., 2005).

The focus of the conceptual analysis process is on three factors for consideration when implementing a NAC solution, which form three key concepts used for coding: (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006), (Bandyopadhyay, Positiv, 2006). Coding proceeds through a series of eight selective reduction steps (Busch et al., 2005). These steps include:

I. *Level of analysis.* The level of analysis for the coding process is based on sets of words and phrases. These words and phrases are:
    - Securing information assets.
    - Increasing information availability.
    - Implementation.

II. *Major concepts to code for.* The initial different concepts or phrases are:
    - "Cost"

- "Implementation"
- "Security"
- "Assessment"
- "Risk"

III. *Code for existence or frequency of a concept.* The data is coded for existence as well as frequency of concepts and terms. While the number of times the term is used can indicate the relevance as well as importance of the term within the document, in this study the data set for coding is too small for this approach to be viable.

IV. *How to distinguish among concepts.* A narrow level of generalization is applied when mining the data. Search terms and coding for existence should focus enough on the concepts that a wide level of generalization is not necessary.

V. *Rules for coding texts.* Translation rules offer a level of consistency and coherence. Taking the terms and phrases from step 1: level of analysis; articles are coded for the existence of the term or phrase. A translation rule stipulates that only references to the listed terms or phrases will be coded. This ensures consistency in the coding process.

VI. *Decide what to do with irrelevant information.* Conceptual analysis, while extremely useful and effective for providing this type of information when done right, is limited by its focus and the quantitative nature of its examination. Concepts are reviewed throughout the mined text and aligned with one of the major coding concepts, identified in process step 2: Major concepts to code for. Concepts that cannot be aligned with one of the major coding concepts are

rejected as irrelevant data. Information deemed irrelevant is reexamined as a possible direction to relevant data once the initial coding is completed.

VII. *Code the text.* Two methods of coding are used for this literature review. Coding by hand, a manual process of reading the article and writing the concept occurrences, is more time consuming, but more effective to really mine the material collected. The second method is semi-manual with a feature (Search Tool) within Adobe Acrobat Pro. Using this tool speeds the process of mining the data for key words and phrases; however, it takes an added step to tabulate instances of the queried text from downloaded PDFs.

VIII. *Analysis of results.* Words and patterns are collapsed into themes as a way to structure the Review of the Literature section of the study, related initially to the three selected concepts mentioned above. Additional themes may emerge. See below in Writing Plan for details.

Writing Plan

The final set of themes is used to frame a guide for use when determining the level of acceptable risk of network access security for successful implementation NAC solutions within an existing enterprise infrastructure. Preliminary themes concern (1) threat assessment; (2) scope of implementation; and (3) costs.

Theme one - Threat Assessment

Internal. Preliminary research reveals that internal threat assessment risks varies from security breaches, accidental information compromises and other serious incidents

which have overshadowed the focus previously placed on external hacking and caused expensive and embarrassing incidents to disrupt business operations.

External. Preliminary research reveals that clarifying this aspect is important because the kinds of problems that manifest themselves within organizations are very different from the ones that are internal.

Theme two - Scope of Implementation

Policy / Governance. Preliminary research suggests that a key in policy development is to assess the level of risk based on the resources to which access is granted (Desmond, 2007). If the resource is determined to be a rather low, for example, a product list, the use of HTTPS-based authentication may suffice. For more high-value resources, research suggests the use of integrated authentication with something like Microsoft's Active Directory offering.

Knowledge resources. Preliminary research postulates that for users (internal and external) to have access to the various portals of information, whether private or not, "user-friendly" interfaces with complex software and systems are needed (Mayo, 1982). The same kind of careful systems engineering and the same approach to reliability that helped build network infrastructure access, must be applied to the controls and sensors that interact with it.

Physical resources. Preliminary research has shown that the increased dependency on information system resources has resulted in heightened vigilance against security breaches (Wu, 2009). An intrusion detection system (IDS) is one of the many

core security technologies, which firms commonly apply to provide alerts on potential security incidents.

Theme three - Costs

Hard cost. Preliminary research provides empirical evidence that there is a clear correlation between companies' property risk management and their financial performance. Companies that invest in protecting their property tend to create value for the company (IOMA, 2007).

Soft cost. Preliminary research shows that Service Level Agreements (SLAs) have an inherent, but often overlooked soft cost for in-house solutions (Hansen, 2001). Outsource solutions traditionally account for soft cost of an SLA, and naturally use guarantees of service as sales tools. Soft costs is calculated on the pro-rated estimated time that support staff would spend on the project, based upon the assumption that the existing implementation, operations, and support staff have the time to deal with a new security technology project.

Annotated Bibliography

All references used in this literature review are listed in the References section of this study; the references deemed more significant are presented within this section of the literature review. The selected references include an abstract that summarizes the content of the selection for the reader. In addition, comments added by the researcher are also included to describe how the selected reference is used in support of this study and how the credibility of the reference is determined.

Bradbard, D. A., Norris, D. R., & Kahai, P. H. (1990). Computer security in small business: an empirical study. *Computersicherheit im Kleingewerbe: Eine empirische Studie.*, *28*(1), 9-19.

Abstract. Inexpensive hardware and specialized software have significantly increased the use of computers in small businesses, with the result that computer security is a significant concern for these users. This article reports a study of computer security awareness and implementation among small businesses. A security measurement instrument was developed and administered to a large sample of small businesses. The instrument reported in the article provides a comprehensive listing of security measures appropriate for small businesses and informs readers of the appropriate security measures to take. Additionally, owners of small businesses may audit their own security practices through comparisons with the results of the survey

Comments. This study covers some of the many issues small business encounter, which are addressed by a NAC solution. This study is deemed credible because the lead researcher has published over thirty papers that have appeared in scholarly journals or professional meetings. Dr. Bradbard currently teaches courses in management Information Systems and Application Software. Dr. Bradbard maintains professional affiliations with the Association of Computing Machinery, Association of Computing Machinery Special Interest Group on Management Information Systems, National Decision Sciences Institute, Southeast Decision Sciences Institute, and International Association for Computing Systems, and the Association for Information Systems. This article provides an entry point of discussion for SMBs, which address the issue of threat assessment as presented in the Problem Area section of this paper.

Brooks, J. (2006). Matter of trust. *EWeek, 23*(18), 20-20.

Abstract. The article focuses on the importance of trust in a computer network server operating system. The feature of trusted operating system, such as mandatory access controls, can help in ensuring a security protection to the system. The author commented that even if there was this tight system control, he was able to evaluate several trusted operating system developments in commonly used network providers such as SELinux implementations, Core Linux distributions, AppArmor software, and Process Rights Management in Solaris 10 of Sun Microsystems Inc.

Comments. Part of a NAC solution for IT administrators, and one of the toughest and trying jobs, is securing a server that will run vital enterprise applications. No matter what operating system the server is running, effectively hardening the server requires long hours and painstaking effort. This article highlights many of those efforts. The credibility of the article is based on the specialties of the author which consist of writing and editing; technical knowledge of IT products and services; close familiarity with tech media people and practices; expertise around open source software, licensing, and development processes. The article is part of the data set for coding, and supports the development of the Review of the Literature section of this paper.

Data Security Challenges Small Firms. (2007). *Information Management Journal, 41*(5), 19-19.

Abstract. The article discusses a survey conducted by Visa USA and the National Federation of Independent Business (NFIB) on the data security challenges faced by small businesses in the U.S. The survey indicated that 57 percent of small firms do not consider securing customer data as something that requires formal planning, and 39 percent rely on common sense to keep data safe. Michael E. Smith of Visa USA noted that data security breaches involving payment card information occur more frequently at small businesses. Visa announced a program to help small firms improve their security by urging them to reduce the data they store.

Comments. This article covers some of the reasons for implementing an NAC solution, regardless of the industry. This article is deemed credible because it is produced by a well-known journal in the information security industry. In addition, there is extensive coverage on the study and the material is technical in nature and relevancy. Information from this article is used to develop the Significance section of this literature review.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x.

Abstract. Information system (IS) security continues to present a challenge for executives and professionals. A large part of IS security research is technical in nature with limited consideration of people and organizational issues. The study presented in this paper adopts a broader perspective and presents an understanding of IS security in terms of the values of people from an organizational perspective. It uses the value-focused thinking approach to identify 'fundamental' objectives for IS security and 'means' of achieving them in an organization. Data for the studies were collected through in-depth interviews with 103 managers about their values in managing IS security. Interview results suggest there are 86 objectives that are essential in managing IS security. The 86 objectives are organized into 25 clusters of nine fundamental and 16 means categories. These results are validated by a panel of seven IS security experts. The findings suggest that for maintaining IS security in organizations, it is necessary

to go beyond technical considerations and adopt organizationally grounded principles and values.

Comments. This article covers issues that arise in the assessment phase of NAC implementation for executives and IS professionals. This article is deemed credible because it is produced by a well-known journal in the information security industry. In addition, there is extensive coverage on the study and the material is technical in nature and relevancy. The article is part of the data set for coding, and supports the highlighted need for policy and governance as factor for consideration in the scope of implementation theme, presented in the Review of the Literature section of the paper.

Falk, A. & Kosfeld, M. (2006). The Hidden Costs of Control. *The American Economic Review 96*(5): 1611-1630.

Abstract. We analyze the consequences of control on motivation in an experimental principal- agent game, where the principal can control the agent by implementing a minimum performance requirement before the agent chooses a productive activity. Our results show that control entails hidden costs since most agents reduce their performance as a response to the principal's controlling decision. Overall, the effect of control on the principal's payoff is no monotonic. When asked for their emotional perception of control, most agents who react negatively say that they perceive the controlling decision as a signal of distrust and a limitation of their choice autonomy.

Comments. The analogy presented by this article expands on the culture and how it is perceived and managed within an organization. This article is deemed credible because it addresses the element of security many SMBs overlook; perceptions of the end user. Falk is a member of the Institute for the Study of Labor (IZA) at the University of Bonn. Both authors have authored several dozen working papers and articles in the fields of labor, economics and microeconomics. Kosfeld is currently a member of the Department of Management and Applied Microeconomics and Faculty of Economics and Business Administration at Goethe University Frankfurt. This article presents the economic impact that enhanced security may have on an organization. This article is part of the data set for coding, and is used to address the theme of costs, presented in the Review of the Literature section of the paper.

Gercek, G., & Saleem, N. (2005). Securing small business computer networks: An examination of primary security threats and their solutions. *Information Systems Security, 14*(3), 18-28.

Abstract. This article addresses the primary threats to computer networks that a small business might encounter and provides strategies to counter these threats. It emphasizes the key characteristics associated with each category of security threat and provides approaches to eliminate or alleviate these threats. The article also presents a case study of a small insurance company for which the authors helped design, implement, and secure computer networks.

Comments. This article should be particularly informative and helpful to businesses where a non-technical professional or an IT professional with inadequate background in network computing is responsible for administrating computer networks, an environment that is quite prevalent among small businesses. This article is deemed credible because it is produced by a well-known journal in the information security industry. In addition, there is extensive coverage on the study and the material is technical in nature and relevancy. This article is part of the data set for coding, and supports discussion of the drawbacks and benefits of a NAC solution as presented within the three main themes in the Review of the Literature section of this paper.

Greene, T. (2008). Software-based NAC security useful despite drawbacks. *Network World.* Retrieved from http://www.cso.com.au/article/267164/software-based_nac_security_useful_despite_drawbacks . DOI: 14 001 592 650

Abstract. Despite some shortcomings, software-based network access control technology that enforces policies on network endpoints is often the first choice of customers who adopt the technology.

Comments. This article covers some of the pros and cons of NAC implementation within an existing telecommunications infrastructure. This article is deemed credible because the author is a senior editor at Network World, covering network access control, virtual private networking gear, remote access, WAN acceleration and aspects of VoIP technology. He has also published over twenty IT industry recognized papers in the NAC and information security environments. This article

is part of the data set for coding, and supports the discussion of the cons of NAC implementation as presented within the themes in the Review of the Literature and in the Conclusion sections of this paper..

Hsin Hsin, C. (2006). Technical and management perceptions of enterprise information system importance, implementation and benefits. *Information Systems Journal*, *16*(3), 263-292. doi:10.1111/j.1365-2575.2006.00217.x.

Abstract. This paper compares information systems (IS) integration in high-tech organizations from the information technology (IT) and general management perspectives. All the organizations studied have experience of integrated Enterprise Resource Planning systems, and some with their extension to Supply Chain Management and Customer Relationship Management systems. The operational scope of the sample systems, and senior IT and general management perceptions of the importance of their functions, benefits and implementation success factors, obtained by qualitative interviews with 49 senior managers and a quantitative survey of 219 high-tech companies, are described and compared. Although the opinions expressed indicate some mutual hostility, IT and general management perceptions of IS implementation were very similar. The significance of these findings is discussed and some suggestions for further investigation, placing them in a wider context, are made. Arguably, the similarities found are more important than the differences.

Comments. This article covers some of the business impacts that NAC solution implementation which must be addressed by an organization. Research has shown

that overall assessments of business functions are strongly correlated with overall levels of implementation, and tend to rate system benefits and system reliability more highly. This article is deemed credible because it is produced by a well-known journal in the information security industry. In addition, there is extensive coverage on the study and the material is technical in nature and relevancy. Various levels of an organization play key roles in the success or lack of success obtained by a security solution. This article is part of the data set for coding, and supports the Conclusion section of this paper, as part of a checklist of discussion items to take away from this study.

Johnston, A. C., & Hale, R. O. N. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129.

Abstract. The article discusses information security management as practiced by organizations, examining its strategic implementation and maintenance as well as the empirical value added to an organization by such programs. The computer systems of businesses are constantly under attack, the article states, attacks that include insider abuse and the theft of intellectual property. Other topics include information security planning, a survey of security professionals, and security programs implemented on an enterprise-level governance process.

Comments. This article is deemed credible because it is produced by the *Communications of the ACM*, a leading print and online publication for the computing and information technology fields. It is recognized as the most trusted and knowledgeable source of broad scope in information technology. There is

wide-ranging coverage of NAC solutions from policy implementation to appliance comparisons. In addition, the authors have been peer reviewed in various journals and cited numerous times for their recognition of information security as one of the most important management challenges that SMBs and public sector organizations face. As this report-highlights, lack of standards thwarts enterprise-wide scalability, even more so interoperability. NAC is drowning in standards and consortiums—to name a few; Trusted Network Connect (TNC), Cisco's Network Admission Control, and Microsoft NAP. Unfortunately, these only address a low level of NAC interoperability; none yet enables building an extensible policy framework that works fluidly with any vendor. The bottom line presented in this reference is that either government should take the lead in mandating standards requirements, or organizations need to manually attach NAC components together, or just use a completely proprietary solution. This article is used to address issues of interoperability of NAC applications when planning a security solution implementation, as presented in the Problem Area of this paper. This article is used as a key component of the discussion of NAC policy and governance.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2), 7-19.

Abstract. This article focuses on how small businesses (fewer than 500 employees) are managing information security and the associated risks. Findings

indicate that the businesses interviewed for this study are taking many of the typical steps that are indicative of best security practices. However, there are also several areas of concern that could potentially leave their systems open to threats

Comments. Computer crime surveys are important inputs to management and authorities, providing information on the national IT security status. Such measurement instruments are increasingly valuable as more and more enterprises become critically dependent on IT and the Internet. Finally, recommendations for improvements regarding access control and data protection are provided. The paper is part of a comprehensive study on information security and measurement. The article is deemed credible because of the coverage of security practices and solutions provided that are vendor neutral. The article is not predisposed to any particular solution and offers several feasible options for SMBs. This article is used in support of the development of the Problem Area and Delimitations in this paper.

Khansa, L., & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM, 52*(11), 113-117. doi: 10.1145/1592761.1592789

Abstract. Malicious attacks on enterprise IT infrastructures have become a serious threat with the growing Importance of the Internet. Regulatory frameworks and legislations such as HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), and SOX (Sarbanes-Oxley Act) require organizations to implement the necessary safeguards to ensure the confidentiality,

integrity, and availability of information. Failure to do so makes them vulnerable to heavy monetary penalties and loss of customer base and goodwill. Several quantitative models have been proposed in the literature to justify information security investments at the firm level. Risk-driven decision models are limited by the difficulty of reliably estimating the potential losses from security breaches and the probability of such breaches

Comments. In quantifying the benefits of investing in Information Security, the researchers proceeded to explore the current developments of Information Security investments over the past few years. These developments showed paradigm shifts ranging from a purely technical approach towards Information Security, towards a more managerial way of protecting information by investing in an Information Security culture within organizations. Being in IT management, this researcher has firsthand experience in gaining capital dollars for IT initiatives. This article is deemed credible because it presents options for IT executives to use as a guide in obtaining funding for security projects and initiatives. The coverage the article includes graphs and charts, which allow the reader to better understand the material. The article is used to support development of the Problem Area and Definitions in this paper.

Loch, K., Carr, H., & Warkentin, M. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186. Retrieved from Business Source Premier Database. http://www.jstor.org/pss/249574

Abstract. Information systems security remains high on the list of key issues facing information systems executives. Traditional concerns range from forced entry into computer and storage rooms to destruction by fire, earthquake, flood, and hurricane. Recent attention focuses on protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction. The consequences of these events can range from degraded or disrupted service to customers to corporate failure. This article reports on a study investigating MIS executives' concern about a variety of threats. A relatively new threat, computer viruses, was found to be a particular concern. The results highlight a gap between the use of modern technology and the understanding of the security implications inherent in its use. Many of responding information systems managers have migrated their organizations into the highly interconnected environment of modern technology but continue to view threats from a perspective of a pre-connectivity era. They expose theft firms to unfamiliar risks of which they are unaware, refuse to acknowledge, or are often poorly equipped to manage.

Comments. This article is deemed credible because it is published by a peer-reviewed publication of which is highly recognized in the Information Security sector. This paper considers several important issues related to security risk management, the presence of network externalities in security risks, and the distinction of general (network) and system-specific protection measures. The results show that the consideration of network externalities and layered protection changes the risk mitigation decisions significantly. In addition, accurate

estimation of system risk plays a critical role in the success of risk management. Otherwise, the use of a uniform baseline protection approach may be more desirable when the misjudgment of relative system risks is likely to occur. This article is part of the data set for coding, and is used in the Review of the Literature section of the paper, in addressing why SMB should consider a NAC solution, not only for risk management, but also for asset and information security management.

Margariti, S. V., Meletiou, G., Stergiou, E., Vasiliadis, D. C., & Rizos, G. E. (2007). Security systems consideration: A total security approach. *AIP Conference Proceedings, 963*(2), 954-958. DOI: 10.1063/1.2836250

Abstract. The safety problem for protection systems is to determine in a given situation whether a subject can acquire a particular right to an object. Security and audit operation face the process of securing the application on computing and network environment; however, storage security has been somewhat overlooked due to other security solutions. This paper identifies issues for data security, threats, and attacks, summarizes security concepts and relationships, and describes storage security strategies. It concludes with recommended storage security plan for a total security solution.

Comments. This report is deemed credible because it is published by a peer-reviewed publication of which is highly recognized in the Information Security sector. The report focuses on the security of data, computer networks, and digital storage, which are all parts of a total NAC solution. Inherently, “NAC” describes

network access systems that deliver a broad range of features focused on coupling user identity, host posture assessment, threat remediation and policy-based access controls for enterprise networks. This report is used as a supporting reference to establish the Significance of this study, and presents how to plan a total approach to security, rather than a piece-meal approach. The report highlights some of the sub questions in this study, thus broadening the reader's scope of understanding of NAC as a part of a total security approach.

(NIST), N. I., & Division, C. S. (2000). Federal information technology security assessment framework. Retrieved from http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf.

Abstract. Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to 1) determine the current

status of their security programs relative to existing policy and 2) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets. These assets include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs, or operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all asset security controls and all interconnected systems that the asset depends on produces a picture of both the security condition of an agency component and of the entire agency.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policy. At level 2, the asset also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At level 5, the asset has procedures and controls fully integrated into a comprehensive program.

Comments. This assessment provides a detailed framework from which IT consultants or senior network engineers can present to executive management for purposes of establishing or reassessing current information security policies and methods. This report is deemed credible because it is published by a peer-reviewed publication of which is highly recognized in the Information Security sector. This assessment is part of the data set for coding, and is presented as a

guideline throughout the study. It is used in support of the development of themes, presented in the Conclusions section of the paper.

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, *14*(2), 37-48.

Abstract. This article addresses the elements that make up a successful information security awareness program. It addresses the role that organization personnel play in the information security program and how to use this information to one's benefit. It also discusses how to establish awareness program scope, how to segment the audience, and how to ensure that the content is effective in getting the message to the user community.

Comments. This report is deemed credible because it is published by a peer-reviewed publication of which is highly recognized in the Information Security sector. This article discusses that there are more than 245 million malware attacks each month. In the explanation of the trend, it's stated that most of these attacks are newly developed variants, not seen before and used for a very brief time. The rapid evolution of malware is partially possible because of widely available malware development toolkits and large cooperative networks of hackers sharing development efforts and profits. Rather, it is the lack of awareness by the end user to the realism of these types of threats. This article is part of the data set for coding, and supports the discussion of the theme titled “scope of implementation” in the Conclusions section of the paper. This article serves as support for this

section because of the currency of research, and because the topic of user awareness is a highly discussed issue within the security realm.

Pironti, J. (2005). Minimizing New Risks the Old-Fashioned Way. *Wireless Week, 11*(8), 31.

Abstract. Focuses on the information security challenges posed by smart phones and personal digital assistants. Mobile device features that increase the risk of information leakage; Solutions that can minimize the risk posed by information accessibility.

Comments. This article is deemed credible because it addresses some of the new issues that are facing organizations, as end users demand more mobility and flexibility. The author is an enterprise solutions architect and security consultant with 15 years of security experience. He has created and implemented wired and wireless NAC solutions for several fortune 500 companies. This article supports the discussion of why NAC is not just for security on the visible portions of a network, but more so, a gatekeeper for access, authentication and authorization into an organization information infrastructure, presented in Delimitations.

Powers, V. (2008). Keeping an eye on the network. (cover story). *University Business, 11*(3), 54-58.

Abstract. The article focuses on the increasing number of universities and colleges taking the Network Access Control (NAC) approach to protect information resources in the U.S. The three common types of NAC approaches

are discussed and include the infrastructure-based, endpoint software-based and network security. Juniper Networks Inc. engineer Steve Hanna explained that universities are also integrating other security functions with the NAC approach.

Comments. As universities focus on facilitating quality education and academic research, they are faced with the difficult task of maintaining an open door policy for massive loads of network traffic despite the growing demands of providing a stable and secure network environment. Universities must safeguard the integrity and availability of their campus data network, reduce threats to computer systems connected to the network and reduce the likelihood that computers on campus are used to attack other organizations. This article is part of the data set for coding, and highlights a heterogeneous environment that many SMBs do not have to deal with, as presented in the Review of the Literature section of the paper. The author posits the need for open standards to allow for maturity and broader endpoint inspection by NAC solutions. This article is deemed credible because it presents a current case study of NAC in a college environment that has tested several options prior to the NAC implementation. This article will be used to highlight some of the implementation issues as well as pros of a NAC solution.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60-66.

Abstract. This article provides information on various best practice frameworks that exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy

and information security regulations. Of the various best practice frameworks available, the most comprehensive approach is based on the implementation of the international information security management standard, International Organization for Standardization (ISO)/IEC 17799, and subsequent certification against the British standard for information security, BS 7799. This ISO 17799/BS 7799 framework is the only one that allows organizations to undergo a third-party audit. Organizations are faced with a multitude of information security risks. Theft of trade secrets and the loss of information due to unexpected computer shutdowns can cause businesses to lose their commercial advantage. It is becoming increasingly clear, however, that to address all aspects of security, organizations need to implement a more comprehensive approach using a methodical compliance framework.

Comments. This report is deemed credible because it is published by a peer-reviewed publication of which is highly recognized in the Information Security Management sector. In addition, this article highlights the needs for standardization of framework and security methodologies. An increasing number of businesses, moreover, are seeking to obtain security certification from third-party organizations, given that certification guarantees that the controls implemented meet information security requirements. Some best practices that facilitate the implementation of security controls include Control Objectives for Information and Related Technology (COI/RT), ISO/IEC 17799/BS 7799, Information Technology Infrastructure Library and Operationally Critical Threat, Asset and Vulnerability Evaluation (ITIL/OcT/Ave). This article is used in the

Problem Area and Delimitations sections of the study, in support of discussion of best practices that are standards based, ideal for SMBs with limited resources.

SMB networks said at risk. (2005). *Communications News*, *42*(12), 6-9.

Abstract. This article offers news briefs related to network security. According to Steve Quane, general manager of Trend Micro's small and medium business operations, smaller organizations experience security threats due to restricted time and cost in scaling IT resources to provide technical advice among employees. Consultant Scott Bradner criticized an editorial about Internet governance.

Comments. Network security is an issue for all businesses. The challenges faced by SMBs are unique and significant. Taken together, the ongoing threat to network security and myriad challenges to SMBs necessitates a unique and comprehensive approach to risk management, auditing and best practices. This brief, yet concise article is intended as a guide for IT management, service providers and consultants seeking to enhance the security posture of SMBs, which acknowledges the unique challenges that SMBs face. This article is deemed relevant because it focuses the SMB security issues that are most common; cost, time, and resources. This article is deemed credible because of the study conducted by Trend Micro**,** a global leader with over two decades of expertise in endpoint, messaging and Web security, which are key components to a NAC solution (Trend Micro, 2009). The study highlighted the challenges SMBs face in manipulating IT resources to provide technical advice, conduct system scans, clean machines manually, deploy patches and security policies, and educate staff

in order to enable a secure working environment. This article is part of the data set for coding, and is used to lead into themes one and three as presented in the Review of the Literature and Conclusions sections of this paper.

SMBs weigh security purchases. (2009). *Communications News, 46*(3), 8-8.

Abstract. SECURITY Small and midsize businesses (SMBs) are aligning their own concerns with key security threats this year, and spending where it hurts, according to research conducted by Chadwick Martin Bailey. Among the findings: Companies are focusing security spending on the most important and likely threats to their businesses. IT professionals identified the least-critical threats, and lowest budget priorities, to most SMBs as: storage encryption, security solutions for teleworkers and networking/unified threat management.

Comments. Chadwick Martin Bailey (CMB) a leading research company that specialize in advanced analytics research, from a conjoint design method, regression model, and data mining techniques. This article is deemed credible because of the level of experienced research used to obtain and present the data. CMB is noted as one of the top 50 US-based research and consulting firms. This article is part of the data set for coding, and is used in support of this researchers findings in regards to the hard and soft costs of NAC solutions for SMBs, as presented in the Review of the Literature and Conclusions sections of this paper.

Review of Literature

This study is designed to recognize selected factors regarding when and why SMBs should consider the implementation of NAC into their information enterprise. Twenty references, composing the set of literature selected for coding, are mined for key words using two methods: manually by reading the material and, using the Search Tool within Adobe Acrobat Professional 9. Appendix A shows the results of these two coding processes.

The following review consolidates and summarizes information collected from these references in relation to the three factors for consideration when implementing a NAC solution: (1) threat assessment (Young, 1986), (Greene, 2008); (2) scope of implementation (Falk & Kosfeld, 2006); and (3) costs (Brooks, 2006), (Bandyopadhyay, Positiv, 2006). The review begins with a brief overview of NAC, followed by collected data presented as themes covering the three selected factors for consideration when implementing a NAC solution. Additional sub-themes are presented as they emerged during data analysis.

NAC Overview

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to a network by devices, when initially attempting to access the network (NIST, 2002). For example, NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back office

servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed (Goleniewski, 2008).

NAC is different from other control systems such as firewalls and layer 3 routing devices, because NAC allows user-focused access control (NIST, 2002). NAC aims to do exactly what the name implies -- control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls, which determine where users and devices can go on a network and what they can do (Goleniewski, 2008).

Research has shown that NAC is ideal for corporations and agencies where the user environment can be tightly controlled. However, Khansa and Liginlal (2009), state that even though NAC may seem ideal, some administrators have expressed doubt about the practicality of NAC deployment in networks with large numbers of diverse users and devices, the nature of which constantly change. In union with Khansa and Liginlal (2009), Powers (2008) provides several case studies of NAC implementations for a large university with multiple departments, numerous access points and thousands of users with various backgrounds and objectives, with a fully integrated NAC solution. These case studies demonstrate the potential offered by a successful NAC solution. In addition, the case studies highlight three different scenarios of NAC solutions, as defined by technology research and advisory firm Gartner, including those that are: (a) infrastructure-based, (b) endpoint software-based, and (c) network security appliance-based (Powers, 2008).

In previous years, network administrators created their own tools for information security. Today IT administrators can purchase off -the-shelf products from various

vendors with support, which makes the deployment much easier from an administrative standpoint (Powers, 2008). One emerging trend in NAC for application on college campuses, noted by Steve Hanna (p. 55), distinguished engineer at Juniper Networks and co-chair of the Trusted Network Connect Work Group says, is integrating other security functions with NAC. As noted by Powers (2008), this type of combination of technologies is designed to increase the level of control.

The case is especially noteworthy and deserving of further analysis, because, unlike corporations, higher education institutions face unique challenges with IT security as students arrive each semester with their own computers; many times their security devices are off, their anti-virus software is gone or simply outdated and odd configurations abound (Powers, 2008). "The challenge has always been how to take student laptops and bring them to a certain minimum level of health," says Hanna (Powers, 2008, p. 55). In addition, Hanna says, rather than maintaining isolated silos for intrusion detection, firewalls, and such, the trend is integrating the security component by moving to open standards (p. 56). Increased network security development and broader endpoint integration are two other trends affecting the future of NAC in education (Powers, 2008).

Protecting IT networks used to be a straightforward case of encircling computers and servers with a firewall and ensuring that all traffic passed through just one gateway. However, the increase in mobile workers, number and type of device and the amount of non-employees requiring network access, has led to a dissolving of that network

perimeter. Access requests can come from anyone and anywhere, which is why academic and non-academic organizations are turning to NAC technologies (Powers, 2008).

It is not the intent of this study to present a view of doom, if a NAC solution is not in place. For example, network traffic may not all be harmful within a small independent bank, but some type of security is crucial. Financial institutions are governed by legislation, such as the Gramm-Leach-Bliley Act, that states banks, brokerage companies, and insurance companies must securely store personal financial information (Khansa & Liginlal, 2009).

However, not all types of organizations are governed in this manner. According to Herold (2002), the growing trend requiring businesses to ensure the security and retention of certain types of information is apparent through the increasing use of electronic records in court cases and during the legal discovery process, and by reviewing some of the current laws (Herold, 2002). For example, U.S. federal regulations require that some employee records be maintained for one year, some require retention for five years, some for 30 years, and some indefinitely (Herold, 2002). In addition, the IEEE (2004), states that 48 percent of public companies say they will spend more than US$500,000 per year complying with the Sarbanes-Oxley Act (IEEE, 2004). According to Herold (2002), HIPPA is another regulation that affects organizations in that covered entities must not only ensure the security and appropriate access to health information while in transit through networks, but also while the information is in storage (Herold, 2002). Additionally, such information must be maintained for six years from the date of its creation or six years from the date for which it was last in effect, whichever is later (Herold, 2002).

Information security implementation companies are responding to strong demand from enterprise customers for technology that can help them comply with new federal and state regulations and to counter the threat posed by mobile and remote workers (Roberts, 2006). Non-compliance with these regulations brings risks of fines, jail, and lawsuits that can affect either individuals or corporate entities. According to Herold (2002), Keller et al., (2005), and others, any industry whose computer systems store and process data such as a patient's medical records number, a Social Security Number, a patient's home address or diagnosis code, are subject to HIPAA's security regulations. Therefore, whether the SMB is a not-for-profit organization or a for-profit competitor, its computer network may be responsible for many processes crucial to central and back-office operations. It therefore makes sense to secure these systems and their data from an operational and legal standpoint (Keller et al., 2005).

Theme One – Threat Assessment

Risk assessment deals with the probability of being exposed to a danger, as compared to threat assessment, which deals with the consequences of that danger (NIST, 2002). According to Keller et al., (2005) the threat environment has changed drastically in recent years; threats are more complicated and attackers are part of organized groups seeking profit rather than fame. Of the many possible threats facing information technology, this section addresses only two: internal and external threats.

Internal threats. Routine self-assessments are an important means of identifying inappropriate or ineffective security procedures and controls, including reminding employees of their security-related responsibilities, and demonstrating management's

commitment to security (Peltier, 2005). Typically, an intrusion detection device sits on a mirrored network switch port and inspects traffic between switches in search of malicious bit patterns. However, this does little to ensure that employees are following security policies and procedures. Unfortunately, training and security awareness are generally the first areas cut in times of budget reductions, largely because the direct benefit of security training is difficult to determine (Keller et al., 2005).

While companies have for years invested in intrusion-detection systems and firewalls to create a shell around their networks, according to Peltier (2005) that is not enough. Internal networks provide fertile ground for attacks on data and systems when threats manage to crack the shell or are introduced by employees or others with access rights (Peltier, 2005).

A number of technologies and services are just hitting the market with the goal of firming up internal network defenses. Some inject intelligence into network security appliances in an attempt to stay a step ahead of security threats, while others aim to limit access to users. For example, Juniper Networks Inc. offers two Intranet Controller appliances and Intranet Agent software that evaluates personal computers, user identity, and network information to ensure users are accessing the network properly and not introducing security threats (Brooks, 2006).

David Langston, CIO of Allied Home Mortgage Capital Corp. says, “Anybody who's been involved in security knows that the vast majority of compromise events are generated internally” (as cited in Sarrel, 2008, p.89). Sarrel (2008) reports that at Allied Home, internal network threats usually result from poor judgment, such as employees opening spam. The goal with these network-security measures is to equip administrators

with tools to shore up internal defenses (Sarrel, 2008). It is a problem that many companies may not want to recognize. Again, as noted by Langston, "When companies protect themselves at the network perimeter, it's because there are bad people out there" (as cited in Sarrel, 2008, p. 90).

External threats. Organizations today must deal with a multitude of external information security risks. Terrorist attacks, fires, floods, earthquakes, and other disasters can destroy information processing facilities and critical documents. In many cases in the past, before sophisticated computer networking, security threats such as viruses, worms, Trojan horses, and denial-of-service attacks were viewed as little more than an annoyance. However, external security threats to an enterprise are much higher today because of network interconnectivity and mobility. Sarrel (2008) states that the explosion of wireless and mobile devices, cell phones, air cards, and pagers has created a mobile society consisting of millions of telecommuters, field workers, traveling sales personnel, and home-office workers . Users can connect to their office networks from hotels, airports, and other remote locations, as well as from home (SMB, 2005). The very features of connectivity and accessibility that make networks and the Internet so indispensable to contemporary society, however, create dangerous and unforeseen consequences (Sarrel, 2008).

Cisco Systems, a leading provider of security services, maintains that remote users accessing corporate networks are more exposed than ever to attack from the outside (Gercek & Saleem, 2005). A personal computer on a network is a common point of attack. A user's laptop can also become infected through a remote Internet connection,

and then infect the entire network. In August 2004, a computer worm called Blaster, shut down 120,000 systems in three minutes and eventually shut down businesses around the world (Gercek & Saleem, 2005). Slammer, another worm, spread worldwide in 11 minutes and infected 55 million hosts per second. According to Cisco, the cost of viruses and worms is approximately $13 billion a year (Gercek & Saleem, 2005).

Theme Two – Scope of Implementation

Intrusion detection systems can determine if an organization is under attack or if unauthorized activity is occurring. Network-based systems monitor all activity on the network itself. Host-based systems, on the other hand, monitor a specific server or computer, and can determine if a hacker is attempting to access files or surreptitiously use the computer (Peltier, 2005). However, as noted by Khansa and Liginlal (2009), NIST (200), and others, an organizational endorsed security policy is a must when setting the framework for a NAC solution.

Research has shown that a documented security policy is necessary to ensure adequate and cost effective organizational and system security controls. A sound policy delineates the information security access structure and assigns defined security responsibilities (Johnston & Hale, 2009). Research conducted by Keller et al., (2005), shows that employees and those internal to the company generate a significant risk to the business. It would seem logical to assume that an organization would address this risk to information security through development of policies that address employee awareness and training. Ironically, research indicates that this is not the case (Johnston & Hale, 2009).

Policy /Governance. The organizational makeup and size of SMBs present a unique set of security policy concerns. According to Desmond (2007), any enterprise adopting a security risk assessment program should consider its objectives and measure its benefits carefully. It should determine and plan its implementation to ensure that full value is obtained. Keller et al., (2005) state the development of a policy to govern the use of hardware, the Internet, and e-mail is only effective if users have a strong belief that they will be detected for improper use of the system and that the punishment will be severe.

, Kabay (2002) adds that security policies challenge users to change the way they think and address their own responsibility with regard to the protection of organizational information, while the strict imposing of any policies may drive users to resist them. As a result, the method of policy implementation may be very important, since users may tend to assume that rigid security policies and procedures make their job harder and in general do not enjoy being told what to do.

Most organizations are still basing their information authentication and access methodologies on old security standards that were developed several decades ago, and are struggling to cope with the increase in threats and vulnerabilities not addressed by current security standards (Saint-Germain, 2005). While there is a new ISO/IEC 27000 series of security standards, they are not that much more advanced (Dhillon & Mishra, 2007). ISO/IEC 270001 adds a security policy life-cycle approach to security management, in the hope that a more mature information security management will lead to a better information security. However, Dhillon and Mishra (2007) state that in the current rapidly changing information security environment, just implementing state-of-

the-art security is no longer adequate. Standards work well in a more static environment, but in today's dynamic security environment, it is necessary to be innovative in security management approach, and go beyond what standards prescribe (Moulton & Coles 2003). Dhillon and Mishra (2007) go so far as to suggest that sometimes standards must be ignored and information security must be adjusted to the latest developments in security research.

Knowledge resources. Research reveals that small businesses are seeking opportunity wherever they can find it, and most believe it exists in the greater exchange of information with other small businesses (Bradbard, Norris, & Kahai, 1990). Sharing and integrating information across the global enterprise and with customers, partners, and suppliers is perceived as a way to survive in lean times (IOMA, 2007).

The issue that becomes apparent is that although addressing IS security at a technical and organizational level is important, "its implementation must also take cognizance of ethical and human considerations" (Dhillon & Torkzadeh, 2006, p. 2). The universal argument, supported by many earlier researchers (Baskerville, 1993; Straub & Welke, 1998; Dhillon & Backhouse, 2001), is that IS security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources, and addresses the values of people and identifies `fundamental' objectives for IS security and `means' of achieving them in an organization (Dhillon & Torkzadeh, 2006).

Most organizations have a number of information security controls. Without a solid NAC solution in place, the controls tend to be somewhat disorganized and disjointed, having been implemented often as solutions to specific situations or simply as

a matter of convention (Germain, 2005). The security controls in operation typically address certain aspects of IT or data security, specifically, leaving non-IT knowledge resources such as documentation and proprietary knowledge less protected overall. Business continuity planning and physical security, for examples, may be managed independently of IT or information security, while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization (Dhillon & Torkzadeh, 2006).

Physical resources. In any true NAC solution, the physical systems should be robust and comply with regulatory standards such as Sarbanes-Oxley and HIPPA (Koebbe, 2007). IT applications are business centric, because they allow the business to operate as efficiently as possible and to exchange data between employees, customers, and suppliers. Koebbe (2007) states that IT departments often carefully secure the physical location of network equipment to protect it from unauthorized access. Ideally, the staff is directed by policy to turn off unused network ports with network switch control software to prevent unauthorized connection to the network. The control of open ports, however, tends to erode over time, as the staff unintentionally leaves ports enabled during network reconfiguration.

Research suggests that every product, whether software or hardware, has vulnerabilities that, when exploited, can lead to extensive damage (Keller et al., 2005). One of the components of a NAC solution hardware make up is the storage device or entity that is storing information assets. Researchers Margariti et al., (2007) contend a common theme that arises for many SMBs is the lack of awareness and total consideration of security plans. For example, secure storage management demands a

complete knowledge of all information that resides on a system and includes management of the traffic to and from the storage device (Margariti et al., 2007).

Theme Three – Costs

One of the potential most cost-effective approaches to securing assets is based on a general usage restriction of an asset or a system containing assets. According to Solms (2001), the two most well known examples of this approach are (a) the trading off availability of an asset for confidentiality, for instance by removing internet access or USB ports on a system, and (b) hardening a system for one single application. In addition, ensuring that restricting the usage of an asset is considered before costly security mechanisms are added can improve the cost-effectiveness of information security dramatically (Solms, 2001). A policy that restricts the use of email for certain highly sensitive documents is an example of a low-cost solution. As another example, having a shared directory (or a document management system) for such documents and monitoring access to that directory is often to be preferred over having such documents dispersed throughout the organization (NIST, 2000).

When it comes to cost pertaining to NAC, research has presented various outlooks on what cost is and what it should be. Researchers Lye and Wing (2005) state that there are costs (negative values) and rewards (positive values) associated with the actions of the security administrator and attacker. The attacker's actions have mostly rewards and such rewards are often framed in terms of the amount of damage done to the network. Research by Jrad, Morawski, and Spergel (2004) shows that cost can be described in terms of potential costs, administrative costs, or capital costs. In this study, the differing terms are Hard and Soft costs in relation to a NAC solution.

Hard costs. Cost is the total cost of the impact of a particular threat experienced by a vulnerable target. Hard-dollar costs are measured in terms of real damages to hardware or software, as well as quantifiable IT staff time and resources spent repairing these damages (Khansa & Liginlal, 2009). Semi-hard costs might include such things as lost business or transaction time during a period of downtime (Khansa & Liginlal, 2009).

According to the 2006 CSI/FBI Computer Crime and Security survey, total losses caused by various types of computer security incidents amounted to $54,494,290 for the 313 respondents that were willing and able to estimate (Koebbe, 2007). Previous research has shown that while many types of security breaches are on the decline, losses from laptop or mobile hardware theft actually increased from $19,562 per respondent in 2005 to $30,057 per respondent in 2006. According to the CSI/FBI survey, total losses among the 313 respondents amounted to $6,642,660 (Koebbe, 2007).

According to Solms (2001), dependent upon the type of organization, financial consequences may range from fines levied by regulatory authorities to brand erosion. Although the focus on this study is on SMBs, Solms (2001), states that as the global business eco-system becomes ever more inter-connected, and small businesses become more and more electronically linked to larger supply chains, their lack of information security readiness will spread the risk through all levels of the economy.

Soft costs. Soft costs include such things as lost end user productivity, public relations damage control, a decrease in user or public confidence or lost business opportunities. For example, in terms of one particular NAC feature, intrusion detection, organizations can categorize soft costs in several ways: (1) accuracy of the detection

system, (2) the response cost, and (3) the costs associated with correctly or incorrectly detecting benign and malicious events (Yue & Çakanyildirmim, 2007).

Whether it is collecting forensic data, notifying affected customers or responding to employee concerns, cleaning up after a security breach can drain IT resources and greatly affect employee productivity (Khansa & Liginlal, 2009). “The cost of that forensic analysis can certainly add up in addition to the lost time and lost productivity as a result,” warns Oliver Friedrichs, a Symantec Security Response Director (Khansa & Liginlal, 2009, p. 114). If critical systems have been compromised, certainly the risk to bottom line could be fairly substantial (Keller et al., 2005). In fact, according to a Ponemon Institute survey, the cost of diverting employees from everyday tasks to managing a data breach increased 100 percent last year, from $15 per record in 2005 to $30 a record (Yue & Çakanyildirmim, 2007).

Conclusion

The NIST (2002) recommends that agencies must plan for security, and ensure that the appropriate officials are assigned security responsibility to authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively influence their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level (NIST, 2002).

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to a) determine the current status of their security programs relative to existing policy and b) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets (NIST, 2002). These assets include information, individual systems, or a logically related grouping of systems that support operational programs, or operational programs. Assessing all asset security controls and all interconnected systems on which the asset depends produces a picture of both the security condition of an agency component and of the entire agency (NIST, 2002).

Ultimately, before a security administrator can put together a program to sell information security to upper management and fellow employees, the first sell of the product must be to him or herself (Peltier, 2005). According to Peltier (2005), Keller et al., (2005) and others, many information security professionals hear either directly or

indirectly that the role they are performing is classified internally as “overhead”, and that it inhibits the other employees from meeting their assigned objectives. Peltier (2005) adds while the classification as overhead may be true, the same can be said for other “C” level employees, including the CEO, CFO, CTO, CISO, etc. However, “C” level employees have a charter that establishes their legitimacy and describes their function in support of the business objectives and mission of the organization (Peltier, 2005). Publishing a charter is important for a security professional, however perhaps more important is that the security professional believes in the value that is added to an organization by his or her efforts.

An effective information security program endeavors to ensure that the organization’s information and its processing resources are available when authorized users need them. A careful, planned deployment of a comprehensive security system can help avoid unwittingly denying access to users or devices that may not have been known to be out of compliance. The choices of a NAC solution are either a hardware-based or framework-based or combination of both. Regardless of the NAC solution chosen, this researcher believes the key will be an understanding of the factors for consideration when implementing a NAC solution.

Arguments may be proposed or countered for a NAC solution. The level of security and security measures to be adopted within an organization is ultimately a management decision. However, for the SMB environment, this decision will have to be undertaken within a defined set of factors for consideration. The above discussion briefly examines some of the factors and suggests some key factors and components, which can be used in addressing a NAC solution in the SMB environment.

In summary, key factors for consideration when considering a NAC solution within a small or medium sized business, as revealed in this study are:

1) Complete a thorough assessment of information security both internally and externally. Research has shown that many security breaches could have been avoided if reasonable security controls had been in place at the time of the breach (Verizon, 2008).

2) Be cognizant of possible implementation hurdles, (i.e. training and awareness), organizational culture in regards to change, product integration and scalability.

3) Examine budgetary considerations, both implicit and explicit. Garner a fiscal understanding of the mission of the organization, based on the information security assessment.

4) Integrate security awareness training across the enterprise. If delivered effectively and with proper incentives, security awareness training can provide basic knowledge across the organization on issues applicable to data protection. A common focus that is unclear in many organizations is integrating security across the enterprise, which requires a culture that includes workers as a first line of defense and engages them in securing the enterprise. The key to that is training. A workforce that receives training is also more likely to report an incident, which provides the data, that security departments require (IOMA, 2007). IOMA (2007) states the benefits of acknowledging soft costs for an organization are: lower insurance costs, improved crisis response, and recovery, streamlining processes, improved workflow, reduced losses from fraud, and fewer service disruptions.

According to Peltier (2005), by implementing a required awareness program, an organization can effectively educate employees about the risks of data compromise, their

role in preventing it, and how to respond when incidents do occur. Creating and maintaining a secure network can cost a lot of money. Buying firewalls, proxy servers, intrusion detection systems, and anti-virus and anti-spam software can add up rather quickly (Peltier, 2005). In addition, the costs of training system administrators how to operate and configure these systems and others in a secure manner add to the financial burden. A security solution will be useless to an organization if those guarding the information infrastructure do not have sufficient knowledge or training to properly use it (Keller et al., 2005). There are several reputable vendors and institutions to choose from for information security training (see Figure 3). In addition to training resources, Appendix B provides additional NAC solution resources. This researcher is not providing an endorsement of these institutions; rather merely suggesting that an effort should be made to increase the information security knowledge resource pool within an organization.

NIST The Computer Security Division (CSD) - (893) www.nist.gov	The E-Government Act [Public Law 107-347] passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 “National Institute of Standards and Technology

SANS www.sans.org	The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.
(ISC)² www.isc2.org	Security Certification Consortium, Inc., (ISC)²®, is the global, not-for-profit leader in educating and certifying information security professionals throughout their careers. We are recognized for Gold Standard certifications and world class education programs

Figure 3 – Information security training organizations

References

Althos. (2009). *TeleCom Dictionary Publication*. Althos Publishing. Retrieved from http://telecomdictionary.com/

Ban, L. Y., & Heng, G. M. (1995). Computer security issues in small and medium-sized enterprises. *Singapore Management Review, 17*(1), 15.

Bandyopadhyay, R., & Positiv, P. (2006). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 7. doi: 10.1145/1592761.1592780.

Baskerville, R. (1993) Information systems security design methods: implications for information systems development, ACM *Computing Surveys*, *25*, 375–414.

Bradbard, D. A., Norris, D. R., & Kahai, P. H. (1990). Computer security in small business: An empirical study, *28*(1), 9-19.

Brooks, J. (2006). Matter of trust. *EWeek*, *23*(18), 20-20.

Busch, C., De Maret, P. S., Flynn, T., Kellum R., Le, S., Meyers, B., Saunders, M., White, R., & Palmquist, M. (2005). *Content analysis.* Writing@CSU. Colorado State University Department of English.

Cisco Systems, Inc.(2010), *Corporate Overview*, Retrieved from http://newsroom.cisco.com/dlls/corpinfo/corporate_overview.html

Data security challenges small firms. (2007) *Information Management Journal, 41*(5), 19-19.

Desmond, P. (2007). Good policy makes for good security. *Network World*, *Network World*, *24*, 44-46.

Dhillon, G. & Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*, 127–153.

Dhillon, G. & Mishra, S. (2007) Information systems security governance research: a behavioral perspective. *2nd Annual Symposium on Information Assurance*. New York State.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x.

Falk, A. & Kosfeld, M. (2006). The hidden costs of control. *The American Economic Review 96*(5): 1611-1630.

Gercek, G., & Saleem, N. (2005). Securing small business computer networks: An examination of primary security threats and their solutions. *Information Systems Security*, *14*(3), 18-28.

Goleniewski, L. (2008). *Telecommunications essentials : the complete global source* (Second ed.). Boston: Pearson Education, Inc.

Gramm-Leach-Bliley Act. (1999). In *Wikipedia*, *the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act.

Greene, T. (2008). Software-based NAC security useful despite drawbacks. *CSO* Retrieved from http://www.cso.com.au/article/267164/softwarebased_nac_security_useful_despite_drawbacks.

Hansen, E. (2001) Internal SLA (Service Level Agreements) for information security. SANS Institute InfoSec Reading Room 8

http://www.sans.org/reading_room/whitepapers/standards/internal_sla_service_level_agreements_for_information_security_548?show=548.php&cat=standards

Health Insurance Portability and Accountability Act. (1996). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

Herold, R. (2002). Records retention and security regulations… Think about it! *Data Security Management, 82-02-54*. Retrieved from http://www.informationshield.com/papers/Records%20Retention%20and%20Security%20Regulations.pdf

Hsin Hsin, C. (2006). Technical and management perceptions of enterprise information system importance, implementation and benefits. *Information Systems Journal*, *16*(3), 263-292. doi:10.1111/j.1365-2575.2006.00217.x.

IEEE, (2004) Regulation and information security, *On the Horizon,* Retrieved from *http://www.cigital.com/papers/download/j2oth-qxd.pdf*

IOMA. (2007) How companies capture business benefits of security. . *Security Director's Report, 7*(11), 1-13.

IOMA. (2009) Company cuts could mean new approach to info security. *Security Director's Report, 9*(9), 1.

Jenkins, W. O. (2003, November 6). Homeland security: *challenges in achieving interoperable communications for first responders.* Washington, D.C., USA: Government Accountability Office. http://www.gao.gov/products/GAO-04-231T

Johnston, A. C., & Hale, R. O. N. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129.

Jrad, A., Morawski, T., & Spergel, L. (2004). A model for quantifying business continuity preparedness risks for telecommunications networks [Electronic version]. *Bell Labs Technical Journal*, 107-123.

Kabay, M. (2002). Developing security policies. *Computer security handbook*, 4th Ed, (46), John Wiley & Sons.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2), 7-19.

Khansa, L., & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM, 52*(11), 113-117.

Koebbe, P. (2007). A case for separate networks. Communications News, November 2007, 34-35

Leedy, P. D., & Ormrod, J. E. (2005). Practical research. Upper Saddle River, NJ: Pearson
Education.

Literature Reviews. (n.d.) *The writing center*. Retrieved from University of North Carolina at Chapel Hill: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Loch, K.D., Carr, H. H., & Warkentin, M. E. (1992), *MIS Quarterly, 16* (2), 173-186. Retrieved from Management Information Systems Research Center, University of Minnesota http://www.jstor.org/stable/249574.

Lye, K.-w., & Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security, 4*(1/2), 71. (DOI) 10.1007/s10207-004-0060-x

Margariti, S. V., Meletiou, G., Stergiou, E., Vasiliadis, D. C., & Rizos, G. E. (2007). Security systems consideration: A total security approach. *AIP Conference Proceedings, 963*(2), 954-958.

Mayo, J. (1982). Evolution of the intelligent telecommunications network. *Science, New Series, 215*(4534) 831-837

McKeon, D. (2001, August 8). The real value of the Internet. eR*esources*, Retreived from: http://www.eresources.com/news/the-real-value-of-the-internet

Moulton, R. & Coles, R. S. (2003) Applying information security governance. *Computers and Security* (22:7) 580-584

Nagarajan, R. (2008). Next-generation access network architectures for video, voice, interactive gaming, and other emerging applications. *Challenges and directions, 13*(1), 69-86.

(NIST), N. I., & Division, C. S. (2000). Federal information technology security assessment framework. Retrieved from http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf.

(NIST), Technology Administration, C. S. (2002). Risk management guide for information technology systems. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security, 14*(2), 37-48.

Pironti, J. (2005). Minimizing new risks the old-fashioned way. *Wireless Week, 11*(8), 31.

Powers, V. (2008). Keeping an eye on the network. (Cover story). *University Business, 11*(3), 54-58.

Roberts, P. F. (2006). Missing the NAC boat. *EWeek, 23*(7), 13-14.

Robinson, C. W. (2006). Network gatekeeper. *Network Computing, 17*(16), ES8-ES8

Rui, T., Jinshu, S., & Feng, C. (2009). *Network access control mechanism based on locator/identifier split*. University of Oregon Libraries. Retrieved from http://doi.ieeecomputersociety.org/10.1109/NAS.2009.34

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Sarbanes-Oxley Act. (2002). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

Sarrel, M. D. (2008). How secure is your company? *PC Magazine, 27*(8), 90-90. University of Oregon Libraries. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=32546500&loginpage=Login.asp&site=ehost-live&scope=site

SearchCIO-Midmarket.com . SMB Definition retrieved January 7, 2010 fromWeb site: http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci1005201,00.html#

Security Solitions. (2007, 04 24). *New study reveals password vulnerabilities and concerns.* Retrieved from http://securitysolutions.com/news/password-concerns-study

SMB (Small and medium business). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Small_and_medium_enterprises

SMB networks said at risk. (2005). *Communications News*, *42*(12), 6-9. University of Oregon Libraries. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=19165247&loginpage=Login.asp&site=ehost-live&scope=site

SMBs weigh security purchases. (2009). *Communications News*, *46*(3), 8-8.

Smith, T. (2008). Critical evaluation of information sources. University of Oregon Libraries. Retrieved from http://libweb.uoregon.edu/guides/findarticles/credibility.html

Solms, B. (2001) Corporate governance and information security. *Computers and Security* (20:3) 215-218.

Straub, D.W. & Welke, R.J. (1998) Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, *22*, 441–469.

The SANS Institute. (2009). *About SANS*. Retrieved from http://www.sans.org/security-resources/glossary.php

Trend Micro, (2009*) About Trend Micro.*, Retrieved from http://us.trendmicro.com/us/about/index.html

Web Security Glossary. (2005). Retrieved from Digital Guards: http://www.digitalguards.com/glossary.php

Verizon. (2008). 2008 Data breach investigations report. *Data Breach Investigations: 29.* Retrieved from http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Young, J. (1986). Council on Competitiveness. *Where America Stands*. Retrieved from http://www.compete.org.

Yue, W. & Çakanyildirmim, M., (2007) *Journal of Management Information Systems, 24*, (1), 329–353.

Appendix A

Data Analysis - Coding Results

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
Bradbard, D. A., Norris, D. R., & Kahai, P. H. (1990). Computer security in small business: An empirical study. , *28*(1), 9-19.	Costs	0	
	Implementation	20	T2 - Measures, processes, associations
	Security	93	T1 - Evidence, strategies, considerations, effectiveness
	Assessment	0	
	Risk	2	T1 - Perception, association, exposure
Brooks, J. (2006). Matter of trust. *EWeek*, *23*(18), 20-20.	Costs	0	
	Implementation	0	
	Security	14	T1 - Attacks, concerns, multilevel, framework, context
	Assessment	0	
	Risk	1	T2 - Incompatibilities
Data security challenges small firms. (2007). *Information Management Journal*, *41*(5), 19-19.	Costs	0	
	Implementation	0	
	Security	9	T1 / T2 - Standards, threats, challenges, breaches
	Assessment	0	
	Risk	2	T1 - Existence, manage
Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system	Costs	3	T3 - Proposed, associated, objective, management
	Implementation	4	T1 /T2 - Socio-ethical,

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
security in organizations. *Information Systems Journal, 16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x.			technological, cognizance, controls
	Security	196	T1 / T2 / T3 - Specifications, associations, critical, measures, management, perception, objectives
	Assessment	5	T1 / T3 - Focused, threats, costs, merits
	Risk	25	T2 / T3 - Analysis, association, methods, inadequacy, evolution
Falk, A. & Kosfeld, M. (2006). The hidden costs of control. *The American Economic Review 96*(5): 1611-1630. The hidden costs of control cont.	Costs	52	T1 / T3 - Psychological, intuition, control, rationale, cumulative distribution, benefits, autonomy
	Implementation	3	T2 - Principals, average
	Security	1	T1 - Guarding,
	Assessment	0	
	Risk	0	
Gercek, G., & Saleem, N. (2005). Securing small business computer networks: An examination of primary security threats and their solutions. *Information Systems Security, 14*(3), 18-28.	Costs	5	T2 - Setup, administration, prohibitive
	Implementation	0	
	Security	87	T1 / T2 - Challenges, emerging, implications, measures, categorization
	Assessment	0	

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
	Risk	9	T1 - Internal, functionalities, perpetuation
Greene, T. (2008). Software-based NAC security useful despite drawbacks. *Network World.* Retrieved from http://www.cso.com.au/article/267164/software-based_nac_security_useful_despite_drawbacks . DOI: 14 001 592 650	Costs	4	T1 /T3 - Incremental, overruling
	Implementation	0	
	Security	9	T1 - Scalability, reporting,
	Assessment	0	
	Risk	0	
Hsin Hsin, C. (2006). Technical and management perceptions of enterprise information system importance, implementation and benefits. *Information Systems Journal*, *16*(3), 263-292. doi:10.1111/j.1365-2575.2006.00217.x.	Costs	22	T1 / T3 - Objectives, capacity, profitability, reduction, overruns, performance measures
	Implementation	68	T2 - Influences, qualitative interviews, reliability, reengineering, benefits, pilot-tested
	Security	2	T2 - Data quality
	Assessment	4	T1 / T2 - Business function, correlations
	Risk	2	T2 - Survey, success
Johnston, A. C., & Hale, R. O. N. (2009). Improved security through information	Costs	2	T1 - Association
	Implementation	5	T1 / T2 - Classification, contrasting, influences

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
security governance. *Communications of the ACM, 52*(1), 126-129. Johnston, A. C., & Hale, R. O. N. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129. Cont.	Security	94	T2 - Culture, investments, optimization, implications, facilitation
	Assessment	0	
	Risk	5	T1 / T2 - Potential impacts, ameliorating risk, models, management planning
Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management, 22*(2), 7-19. businesses	Costs	3	T1 / T2 - Tools, downtime, response time
	Implementation	0	
	Security	115	T1 / T2 - Effectiveness, legal, ethics, damages, breaches, losses, implications, measures, incidents
	Assessment	0	
	Risk	20	T1 / T2 - Attitude, awareness, development, assumptions, target
Khansa, L., & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM, 52*(11), 113-	Costs	0	
	Implementation	0	
	Security	77	T2 / T3 - Aggregated revenues, market segments, effective reduction,

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
117. doi: 10.1145/1592761.1592789			measurement, quantifying
	Assessment	1	T1 - Damage
	Risk	2	T2 - Driven decision-models
Loch, K., Carr, H., & Warkentin, M. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*(2), 173-186. Retrieved from Business Source Premier Database. http://www.jstor.org/pss/249574	Costs	0	
	Implementation	0	
	Security	67	T2 - Implications, resources, policy, budget, regulations
	Assessment	1	T2 - processing
	Risk	52	T1 / T2 - Environment, disruption, recognizable, employees
Margariti, S. V., Meletiou, G., Stergiou, E., Vasiliadis, D. C., & Rizos, G. E. (2007). Security systems consideration: A total security approach. *AIP Conference Proceedings*, *963*(2), 954-958. DOI: 10.1063/1.2836250	Costs	1	T3 - Encryption, decryption, training, knowledge-share
	Implementation	0	
	Security	50	T2 - Authentication, schema, approach, framework
	Assessment	0	
	Risk	0	
(NIST), N. I., & Division, C. S. (2000). Federal	Costs	13	T1 / T3 - Organizational, mission impact,

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
information technology security assessment framework. Retrieved from http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf.			effectiveness, low-risk, alternatives
	Implementation	12	T2 - Tools, operations, maximum-mission effectiveness
	Security	154	T2 - Controls, management structure, responsibilities, procedures, compliance, policies, plans, criteria
	Assessment	16	T2 - Process, framework, development
	Risk	45	T1 / T2 - Implementation, vulnerability management, authorization, sensitivity
Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, *14*(2), 37-48.	Costs	4	T1 - Analysis, in-house, incorporation
	Implementation	2	T2 - Sensitivity, management, employees
	Security	167	T2 - Compliance, objectives, awareness, incorporation, customization
	Assessment	4	T1 - Performance, determining factors of risk
	Risk	9	T1 / T2 - Analysis techniques, acceptable level, infrastructure, priorities
Pironti, J. (2005). Minimizing new risks the old-	Costs	0	

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
fashioned way. *Wireless Week, 11*(8), 31.	Implementation	0	
	Security	14	T1 / T2 - Integrity, controls, capability, capacity
	Assessment	1	T1 - Business importance
	Risk	9	T1 / T2 - Proactive, pragmatic, classification, mobility
Pironti, J. (2005). Minimizing new risks the old-fashioned way. *Wireless Week, 11*(8), 31. *Cont.*			
Powers, V. (2008). Keeping an eye on the network. (cover story). *University Business, 11*(3), 54-58.	Costs	6	T1 / T3 - Recoup, complexity, installation, potential
	Implementation	2	T1 / T2 - Increased efficiencies, reduction in complaints
	Security	17	T2 - Endpoints, enforcement, infrastructure, appliance-based
	Assessment	0	
	Risk	2	T2 - Control, policies
Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.	Costs	2	T1 / T2 - Compliance, effective execution
	Implementation	10	T2 - Standards, controls, access, security audits, maintenance
	Security	124	T1 / T2 - Certification, management controls,

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66. Cont.			regulation, preservation of information
	Assessment	6	T2 - Management process, contingency planning, methodology
	Risk	28	T1 / T2 - Confidentiality, governance, consequences, controlled objectives
SMB networks said at risk. (2005). *Communications News, 42*(12), 6-9.	Costs	3	T2 / T3 - Ownership, security measures
	Implementation	0	
	Security	14	T1 / T2 - Protection, prevention, evolving security landscape
	Assessment	0	
	Risk	2	
SMBs weigh security purchases. (2009). *Communications News, 46*(3), 8-8.	Costs	2	T1 / T2 - Leased equipment, managed services, amortization
	Implementation	2	T2 - Integration, monitoring, management
	Security	6	T2 / T3 - Budget priority, improvements, integration
	Assessment	0	

Article	Coding Terms	Adobe Count	Related to Theme (One, Two, Three) noted as T1, T2, or T3
SMBs weigh security purchases. (2009). *Communications News*, *46*(3), 8-8 cont.	Risk	0	

Appendix B

NAC Resources

Company	Web link
Bradford Networks	*www.bradfordnetworks.com*
Cisco	*www.cisco.com*
Enterasys	*www.enterasys.com*
ForeScout	*www.forescout.com*
Identity Engines	*www.idengines.com*
Juniper Networks	*www.juniper.net*
Lockdown Networks	*www.lockdownnetworks.com*
Microsoft	*www.microsoft.com*
Mirage Networks	*www.miragenetworks.com*
Nortel Networks	*www.nortel.com*
StillSecure	*www.stillsecure.com*
Sophos	*www.sophos.com*
Symantec	*www.symantec.com*
Trusted Computing Group	*www.trustedcomputinggroup.org*
Vernier Networks	*www.verniernetworks.com*