

Spring 2011

Information Assurance; Small Business and the Basics

William Samuel Fleming IV
Regis University

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Fleming, William Samuel IV, "Information Assurance; Small Business and the Basics" (2011). *All Regis University Theses*. 476.
<https://epublications.regis.edu/theses/476>

This Thesis - Open Access is brought to you for free and open access by ePublications at Regis University. It has been accepted for inclusion in All Regis University Theses by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

INFORMATION ASSURANCE; SMALL BUSINESS AND THE BASICS

A THESIS

SUBMITTED ON 31 OF JANUARY, 2011

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY
OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN
INFORMATION ASSURANCE

BY

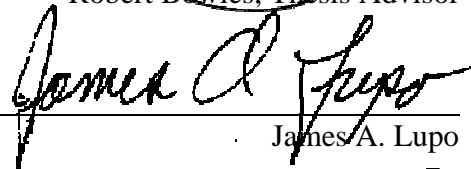
W. Samuel Fleming IV

William Samuel Fleming IV

APPROVALS



Robert Bowles, Thesis Advisor



James A. Lupo



Daniel M. Likarish

Abstract

Business is increasingly dependent on information systems to allow decision makers to gather process and disseminate information. As the information landscape becomes more interconnected, the threats to computing resources also increase. While the Internet has allowed information to flow, it has also exposed businesses to vulnerabilities. Whereas large businesses have information technology (IT) departments to support their security, small businesses are at risk because they lack personnel dedicated to addressing, controlling and evaluating their information security efforts. Further complicating this situation, most small businesses IT capabilities have evolved in an ad hoc fashion where few employees understand the scope of the network and fewer if any sat down and envisioned a secure architecture as capabilities were added. This paper examines the problem from the perspective that IT professionals struggle to bring adequate Information Assurance (IA) to smaller organizations where the tools are well known, but the organizational intent of the information security stance lacks a cohesive structure for system development and enforcement. This paper focuses on a process that will allow IT professionals to rapidly improve their organizations' security stance with few changes using tools already in place or available at little or no cost. Starting with an initial risk assessment research provides the groundwork for the introduction of a secure system development life cycle (SSLDC) where continual evaluation improves the security stance and operation of a networked computer system.

Acknowledgements

This thesis would not have been possible without the help of the many great people I have come in contact with. I would first like to thank my Advisor, Robert Bowles, who is passionate about Information Assurance and truly devoted to his students understanding of its impact on business. Second, John Lockett, of Ricoh Business Solutions; without his constant suggestions and technical expertise I might have shied away from this project. The sole intent was to prove that this type of undertaking isn't insurmountable, thank you for keeping me moving. Third, the Colorado Convention Center management and staff; their support of my educational journey offered me the perfect platform for discovery.

Finally, I could not have done this without the support of my wife Susan and our fantastic family who have endured three years of late nights and constant work. To Ryan, at two years old, we found out about your arrival the same week I started this process and to Jack, whose arrival, four months ago, coincided with the completion of this project, I say daddy is done. Often ten minutes at dinner was the only time you all saw me as I descended the stairs to my desk in the basement. Through all of life's demands, you all stuck with me, even when I didn't make it easy, knowing that this experience was a rewarding one for myself and our family.

William Samuel Fleming IV

(Sam)

Table of Contents

Abstract ii

Acknowledgements iii

Table of Contents iv

List of Figures viii

List of Tables ix

Chapter 1 – Introduction 1

 Background 1

 Problem Statement 3

 Information System under Study 4

 Importance of Project 4

 Research Approach 6

 Thesis Overview 7

Chapter 2 – Review of Literature and Research 8

 Department of Defense Doctrine and Corporate Reality 8

 Risk Assessment 10

 Governance 14

 Written policy 16

 Documentation 19

 Operations 21

 Patch management 22

 Backup and Disaster Recovery 23

 Compliance 24

 System Development Lifecycle 25

 Methodology 31

 Conclusion 33

Chapter 3 – Methodology 35

 Process 35

 Statement of Work 36

 Policy and Procedure development 37

 Inventory 38

Documentation..... 39

Network Management..... 40

Risk Analysis..... 41

PCI compliance 42

Tool Development 43

Secure System Development Lifecycle..... 44

Conclusion..... 45

Chapter 4 – Results 47

Inventory and Network Documentation..... 47

Baseline of the Existing Network..... 50

Threat Analysis 55

Asset Definition 55

Threat Assessment 56

Hardware and Infrastructure 56

Logical Controls..... 59

Risk Assessment 61

Recommendations 62

Threat Scenario: Technical Software Failures or Errors 63

Threat Scenario: Deliberate software attack..... 63

Threat Scenario: Technical Hardware Failures or Errors 64

Threat Scenario: Deliberate Acts of Information Extortion 65

Threat Scenario: Deliberate Acts of Trespass 66

Threat Scenario: Compromises of Intellectual Property 66

Threat Scenario: Acts of Human Error or failure 67

Secure System Development Lifecycle..... 70

Putting It All Together 71

Chapter 5 – Project Conclusions..... 73

Summary of the Previous Chapters 73

Project Objectives 75

Future Research..... 76

Conclusion..... 77

References..... 79

Appendix A. Statement of Work 84

1. Background 84

2. Objectives..... 85

3. Scope 85

4. Specific Tasks 86

5. Period of Performance..... 89

6. Inspection and Acceptance Criteria..... 91

Appendix B. Sample Artifacts 92

 Threat Assessment Matrix..... 92

 Sample Switch Configuration 94

 Current CCC Architecture..... 96

 Physical Network Map 97

 Sample New Employee Access Memo 98

Group Policy Screenshots 100

 Logical Computer Audit..... 101

Appendix C. PCI Assessment Tool 103

Appendix D. Project timeline 122

 November 2009 122

 December 2009 122

 January 2010 122

 February 2010 122

 March 2010 122

 March 10, 2010 123

 April 2010 123

 May 2010..... 123

 May 1-2, 2010 124

 June 2010..... 124

 July 2010 124

 August 2010 125

 September 2010..... 125

 September 28, 2010..... 125

 October 2010 126

 November 2010 126

December 2010 126

January 2011 127

Appendix E. Policies and Procedures 128

 Topic: Information Governance Policy..... 128

 Topic: Misuse and Abuse of Information Technology Assets 132

 Topic: Application Service Provider Security Standards..... 136

 Topic: SDLC and Change Management Policy 142

 Topic: Physical Access Control 150

 Topic: Technology Asset Inventory 152

 Topic: Technology Disposal Policy 155

 Topic: Laptop Computer Checkout..... 159

 Topic: Network Documentation..... 163

 Topic: Network Management Policy 168

 Topic: Employee Internet Use Monitoring and Filtering Policy..... 172

 Topic: Network Router Policy 176

 Topic: Password Policy..... 178

 Topic: Technology Risk Assessment Policy..... 184

 Topic: Acceptable Use Policy..... 186

 Topic: Information Sensitivity 194

 Topic: Email Use Policy 199

 Topic: Guidelines on Anti-Virus Process..... 202

 Topic: Support Policy and Procedure..... 203

List of Figures

Figure 1. The NIST risk assessment methodology (Stoneburner et al., 2002) 13

Figure 2. Data breaches: a time span of events (Baker et al., 2008)..... 22

Figure 3. PCI-DSS requirements 24

Figure 4. The characteristics of each SDLC phase and the risk management activities that support them. (Stoneburner et al., 2002)..... 26

Figure 5. The disciplines and phases of RUP and their associated timeframes. (Ambler, 2005). 29

Figure 6. The iterative nature of RUP releases. (Ambler, 2005) 30

Figure 7. Organizational and design activities showing alignment patterns. (Hevner et al., 2004) 32

Figure 8. Main server room condition pre-project..... 49

Figure 9. Original logical architecture 51

Figure 10. Post project logical architecture 96

Figure 11. Current Network Topology showing the relationship between the ISP network and CCC supplied equipment crucial for understanding network bottlenecks..... 97

Figure 12. Group Policy settings enforcing password strength and 90 day reset. 100

Figure 13. Windows update disabled by Group Policy allows WinINSTALL to manage..... 100

Logical Computer Audit 101

Figure 14. Manual audit of Active Directory, WinINSTALL and Kaspersky 101

List of Tables

Table 1: Definitions of Information Assurance Objectives 8

Table 2. Best Practices for Vulnerability Assessment..... 12

Table 3. Information Security Dimensions..... 15

Table 4. Character of Information Technology Problems addressed by Design Science..... 35

Table 5: Probability Rating System 41

Table 6: Consequence Rating System..... 42

Table 8. Probability X Consequence = Risk; used to prioritize the threat assessment matrix. 61

Table 9. Critical Threat Matrix weighted for prioritization..... 62

Table 10. Switch Configuration..... 94

Table 11. PCI compliance tool..... 106

Chapter 1 – Introduction

Background

Like many great leaps of progress, the unending growth of information technology (IT) in the workplace has created new businesses, areas of commerce for existing businesses, and unfortunately new problems. Indeed, the Internet as we know it, growing out of the ARPNET's policy of open and flexible design, was never intended for secure communication. (Longstaff et al., 1997) As the volume of financial and other data transactions increase over the Internet, the potential for harm from network threats also increases. As a consequence, complex security measures that were once required by only Fortune 500 companies, such as regular security audits, are increasingly a necessity even for the smallest of companies. As we continue to become an ever more networked society the financial benefits attainable by hacking a network grow. As a result, it should come as no surprise that the number of attacks and the creativity spent in trying to breach a network continue to increase.

Small businesses are particularly susceptible to attack because they tend to be extremely homogenous; Gartner estimates that “90 percent of small to medium sized businesses (SMB)s are running Windows on their servers, 80 percent are using Outlook and Exchange for e-mail, and 70 percent are using SQL databases” (Browning & Pescatore, 2003). Gartner research further indicates that more than 60% of midsize businesses in North America do not have a dedicated resource to manage security (Brown & Browning, 2003). The situation in small businesses is likely worse; where security is lumped into a myriad of other responsibilities for someone on the IT staff or even the sole IT professional. In fact, many organizations are too small to even warrant a full-time IT professional relying instead on vendors or even retail establishments to guide their IT efforts.

Adding to this, smaller organization's information systems (IS) projects generally grow from basic implementations on simple networks; as users realize the capabilities available to them, more features are added and the complexity of the processes used to secure them evolves. As this ad hoc development accelerates, tools are added to secure the environment, but few employees understand the scope of the network and fewer participate in designing the infrastructure in a secure fashion. The attacks on the World Trade Center and the Pentagon on September 11, 2001 exposed numerous organizations to the glaring reality that their networks were not positioned to survive all out assault. However "many of the technology-related problems that emerged from the September attacks have less to do with the capabilities of the technology itself than with how it was implemented" (Seifert, 2002).

While an operational system can never be 100% secure, completely vulnerability free, the more specific vulnerabilities are understood, the better prepared a business will be to face an attack. The goal of this study therefore is to identify a process that will aid system administrators as they move forward in their security efforts in the face of largely undocumented and unregulated environments. For this approach to work, Information Security (IS) is replaced with the broader discipline of Information Assurance (IA). The US Government's National Information Assurance Glossary defines Information Assurance (IA) as:

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection and reaction capabilities. (Committee on National Security Systems, 2006)

While IA includes the practice of applying security applications and devices it is broader than IS because it brings together disciplines that emphasize risk management, reliability and

governance over deployment and tactic. Where IS relies on computer science, IA is not just about computer security but rather a holistic approach to management that forces the business to quantify its systems in terms of the value to the business, address the threats computerized or otherwise that could compromise these systems and identify the steps necessary for business continuity if and when a negative event occurs.

The difficult part of system administration at small businesses in light of IA practice is that organic growth and ad hoc development have resulted in systems that are undocumented, unregulated and unreliable. The IT professional is at a loss when challenged with where to begin because increasing the level of IA most often brings associated increases in costs and reductions in operational capabilities; adding a web filter is expensive and the users can't openly navigate the areas they have become accustomed to.

While every IA strategy will consume resource costs, identified as any cost associated with developing and launching an IA strategy, smaller businesses have already demonstrated their lack of resources through their inability to hire IT personnel in sufficient numbers to support their operation. For the IT professional, the challenge then is to implement IA to improve an organization's security stance and in the process increase operational reliability without creating a program that is too expensive using tools already in place or available at little or no cost. Implementation of IA then lays the groundwork for the introduction of a secure system development life cycle (SSLDC) to continually improve the security situation, along with the operational capabilities of the company's information systems through managed development.

Problem Statement

The organic nature of system development and the lack of dedicated IT security personnel along with the increasing frequency of information attacks have left many small

businesses acutely exposed to security vulnerabilities. While the IT professional has a myriad of tools available to draw from, too few companies have systematically developed the organizational policies, controls and processes necessary to evaluate and optimize information security efforts while balancing their associated costs. It is therefore necessary to establish a path for the IT professional to introduce IA into the organization in a way that quickly improves the security position of the organization while optimizing operational capability mindful of costs and introducing a process to guide further development and security improvement.

Information System under Study

The Colorado Convention Center in Denver Colorado provided the network for this research based on the criteria that the system in question contained valuable information, was increasingly problematic, and the organization lacked any type of IS policy, control or development goals. The IT team consisting of three individuals was constantly in a state of crisis management; no future planning or optimization was occurring due to the high number of support calls and system outages being experienced. While all too common in small business, the need for this study was crucial to the organization's ability to gain control of the system and provide the company with planning and development tools to insure its ongoing security and competitiveness.

Importance of Project

Information systems have grown in complexity over the past decade; as businesses employ more Software as a Service (SaaS) their systems require enterprise style measures to ensure security. Small businesses are just as sophisticated as the Fortune 500 in their use of technology and the organic development they have experienced coupled with small or non-existent IT staffing has increased their exposure to vulnerabilities to an unacceptable level.

In 2008 the Verizon Business Risk Team published a comprehensive study compiling the history of four years of research across 500 separate data breach investigations and found that “most breaches resulted from a combination of events rather than a single action” (Baker, Hylender, & Valentine, 2008). The combination of events could include employees opening suspicious emails that then insert malware on unprotected systems, poorly written applications that allow a user to exploit known vulnerabilities left unpatched, a security device configured to fail by fully allowing access or any number of similar combinations. The challenge, especially in smaller organizations, is to adequately identify and address the vulnerabilities that reduce the significance of any combination of events.

The fundamental principle is that you can’t protect what you don’t know about. This is where IA enters the equation. Through its interdisciplinary approach, the fundamentals of well run businesses are applied to the context of IT. By addressing IT as a function of business management begins to apply the same level of scrutiny, planning and governance applied to other areas of business such as sales or accounting where documented processes and metrics determine how the business functions.

According to the Ponemon Institute’s, fourth annual *U.S. Cost of a Data Breach Study* “data breach incidents cost U.S. companies \$202 per compromised customer record in 2008, compared to \$197 in 2007. Within that number, the largest cost increase in 2008 concerns lost business created by abnormal churn, meaning turnover of customers” (Ponemon, 2009) The traditional view of IT as strictly a cost center with little inherent value, a must-do because others are, is quickly being replaced by the view that IT is one part of the information systems that function as a critical component of overall enterprise governance. Increasingly, businesses are threatened with loss or theft of sensitive data; brand erosion, increased operating expenses and

near-term profit declines, all of which are consequences of these occurrences that require intense public relations efforts. In light of this and the real dollar threats to the bottom line, effective IA can mean the difference between a having a thriving company or a bankrupt one. Smaller organizations have until recently operated as though only the large corporations are at risk however, “as consumers see big companies ramp up security, they’ll expect it at all levels” (Smith, 2009)

Research Approach

As previously mentioned, the problem contains four objectives crucial to the introduction of IA into a small business; Information Governance, Risk Management, Network Operations, and the creation of an SSDLC. Because each organization will place different values on costs or capabilities, a universal approach is not warranted. While Frameworks such as COBIT and IT-VAL exist, the overhead associated with them is far too great for consideration by small business when first implementing a comprehensive IA effort where none existed before. Different strategies are beneficial to IT professionals based on their needs, but all administrators can follow the process as they introduce IA to their organizations.

Too often security professionals express the same level of concern for all vulnerabilities that come to their attention. The focus of this research is to help qualify the various threats and categorize them through effective risk assessment enabling the proper controls to be put in place and establishing a pattern for continual improvement. The source citations aid in channeling this discussion, pointing out the necessary components, their importance, and how to most effectively address vulnerabilities.

Depending on an organization’s managerial buy-in and the value they might place on process or capability, five organizations might come up with five solutions; all of which fit their

specific goals. Looking at the “fundamental aspects of information security can help an organization rapidly improve its security stance generally without major procedural, architectural, or technical changes to its environment.” (SANS Institute, 2009) While each IT professional will have a different approach, the study brings clarity to the complicated process of securing a network and the SSDLC introduces a framework to streamline the process as the network evolves.

Thesis Overview

A literature review of Information Assurance, risk management, computer security, and systems development will follow in Chapter 2. Descriptions of the design science methodology including the creation of artifacts created for the study are detailed in Chapter 3. Chapter 4 presents the results of the project including the artifacts that bring understanding to the challenges and aid development of a SSDLC. Finally in Chapter 5, a discussion of the conclusions drawn from the study and potential opportunities for further development of the study system will be presented. Appendix A is a statement of work prepared by the researcher and authorized by the general manager to act as a guide for the project. Appendix B is a sample of the artifacts that bring clarity to high level concepts. Appendix C discusses a spread sheet tool created to understand PCI compliance and how the CCC will meet these requirements. Appendix D is a timeline of how the project progressed including major milestones and discussion of the roadblocks encountered. Finally, in Appendix E, the complete set of policies and procedures under review by legal counsel area presented. Appendix E represents the culmination of this process which was to engage management where once only the IT professional struggled.

Chapter 2 – Review of Literature and Research

This chapter examines Department of Defense (DOD) doctrine to provide a basis for the importance of Information Assurance (IA) in today’s small business information systems. The chapter then focuses on previous work in the field of IA including risk analysis; Governance, operations and the concept of a system development lifecycle to provide the foundation for the project undertaken. Finally a discussion of the research methodology known as design science, will demonstrate the value of the artifact based research conducted in this study leading into a broader discussion of its application in Chapter 3.

Department of Defense Doctrine and Corporate Reality

IA is largely a concept of the DOD. The definition of IA given in the National Information Assurance Glossary is that:

Information assurance is defined as Information Operations (IO) that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protections, detection and reaction capabilities. (Committee on National Security Systems, 2006)

Availability, integrity, authentication, confidentiality and non-repudiation as objectives of IA are further laid out and defined in Table 1.

Table 1: Definitions of Information Assurance Objectives

Definitions of IA objectives	
Availability	Assured access by authorized users
Integrity	Protection from unauthorized change
Authentication	Verification of originator
Confidentiality	Protection from unauthorized disclosure
Non-Repudiation	Undeniable proof of participation

(Joint Chiefs of Staff, 1998)

In DOD terms, IO is any action that occurs using IS as a weapon while at the same time safeguarding the information contained on one's own system. "IO apply across all phases of an operation, the range of military operations, and at every level of war (Joint Chiefs of Staff, 1998) In effect, IA is an operation that specifically focuses on protecting valuable military IS in order to maintain the flow of information during battle while at the same time maintaining IS connectivity with enemy combatants in order to attempt to disrupt the flow of their information.

The DOD cannot focus on IA only during a time of crisis; the fact that the United States is constantly at threat of an information attack demands continual vigilance. IA as a portion of US defense is a continual process where:

- 1) Access to the system by authorized users is maintained
- 2) Access is denied to unauthorized users
- 3) The information contained in the IS is safeguarded from loss, theft and corruption
- 4) Information transmissions can and are monitored
- 5) Early detection of intrusion is possible
- 6) Necessary action can be taken during and post intrusion to maintain communication and recover fully afterward.

On September 11, 2001, the business world awoke to the terrifying reality that it too was a target of hostilities. Like the DOD, most corporate organizations use their IS not only to support their business, but also to extend their reach to potential customers and to share information and services with existing customers. Prior to 9/11, the most obvious forms of compromise led to the loss of personally identifiable information (PII) like credit cards or social security numbers and the defacement of corporate websites. In the minds of most Americans, this

form of hacking, while serious, was considered a minor inconvenience in light of the ease of shopping and volumes of information available at the click of a button.

What is important about the DOD and IA that (Baker & Wallace, 2007) discuss is that “given security controls’ technical origins, we suspect that many security programs still focus on the technical and operational practices and overlook management controls such as policy development”. IA seeks to bridge the organizational gap by concentrating not only on computer science solutions but rather all the other business disciplines utilized by well run organizations to effect policy creation, employee training, discipline, and risk management. The DOD has taken the approach that all information is an operation and therefore should be managed as well as any other aspect of the organization. In the wake of the 9/11 attacks, business are realizing that now more than ever their operation is impacted by information and IA is gaining importance in businesses looking for comprehensive security improvements.

Risk Assessment

A business threat is defined as “an event or condition that has not happened yet but could potentially occur; the presence of these events or conditions increases risk” (Weaver, 2007) to the business. All companies regardless of size will encounter threats. Some will be physical such as a hurricane or fire; some will be financial like supply chain interruption or financing difficulties; and some will be technical like viruses or cyber attack. Risk can be defined as “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization” (Stoneburner, Goguen, & Feringa, 2002). Risk management is a function of business security planning. It is important to know what needs to be protected from what, as poorly documented threats and improperly prioritized risks lead to the creation of unnecessary policies which can create the

potential for other greater risks to be completely missed. The objectives of Risk Management are Risk Assessment (RA) to recognize risk, and Risk Control (RC) to manage the exposure to risk on a continuous basis.

RA, as a process includes identifying exposure to risks; analyzing the risks, and prioritizing the risks to be compensated for or mitigated. In the world of information technology (IT), RA looks in great detail at system characterization, threat and vulnerability identification, control analysis, and the determination of risk impact. In addition to the obvious - facilities, staff, hardware and software - asset identification must include mundane and often overlooked items like network cabling, uninterruptible power supplies (UPS), physical security and facility integrity. While often overlooked, these factors can critically affect systems. An historic building may lack the structural support to carry the weight of a data center located on the third floor. Without an understanding of this critical flaw the entire system could quite literally tumble down. Threat assessment, therefore, is the root of RA. Identifying critical assets and developing policies to manage threats to those assets allows management to focus on specific instances of risk. RC picks up where RA ends, considering risk determination, putting the risk in appropriate context; control recommendations, how does an organization respond to the risk; and results documentation, were the risks appropriately prioritized and did the controls do what they were designed to do.

To effectively measure the success of any security program, it is first important to understand what needs to be secured and why. Acquiring this level of understanding is not an easy task. Indeed, “at the 2001 RSA conference in San Francisco, Microsoft Vice President Dave Thompson said: “Security is a journey, not a destination.”” (Mercuri, 2002) Where security personnel will often place the same level of importance on all threats, “most organizations have

tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.”(Stoneburner et al., 2002)

Influencing security professionals’ tendency towards technical controls is the fact that many of the best practices included in vulnerability assessment are mundane and not related to technology. Table 2 focuses heavily on the physical and procedural aspects of running a business, almost completely ignoring the technical aspects of the information system. Indeed in small business, where the Systems Administrator (SA) was most likely hired for technical expertise, the argument is too often made that vulnerability planning is within the scope of the SA’s job description and that such policy decision aren’t really necessary because the risks to the business are too small to be measurable. Unfortunately this mindset leads to compromise.

Table 2. Best Practices for Vulnerability Assessment

Best Practices for Vulnerability Assessment
• Identify the assets and processes at risk.
• Focus on business risk, not technology.
• Look beyond the IT turf (consider security impact of facility and human resource policies).
• Use available automated tools for technical vulnerability scans.
• Anticipate legal obligations to ward off intruders and prevent involvement in distributed attacks.
• Consider nonelectronic information (shred sensitive input and output forms; evaluate nonmagnetic backups, for example, microfiche).
• Measure what really matters (lost time, not success rate in blocking attacks; intrinsic value of lost or acquired data after a violation).

(Mercuri, 2002)

While many tools and frameworks exist to help organizations uncover their vulnerabilities, the purpose of any assessment ultimately is to provide measures that mitigate the risks associated with the company’s information assets. NIST (Figure 1) has developed a risk assessment methodology that details the nine primary steps along with the myriad of technical

and business related requirements that must be considered to effectively manage a risk assessment. As (von Solms & von Solms, 2004) discuss, the typical questions that business need to address include:

- Against which risks must our assets be protected
- What countermeasures will provide the most efficient against these risks

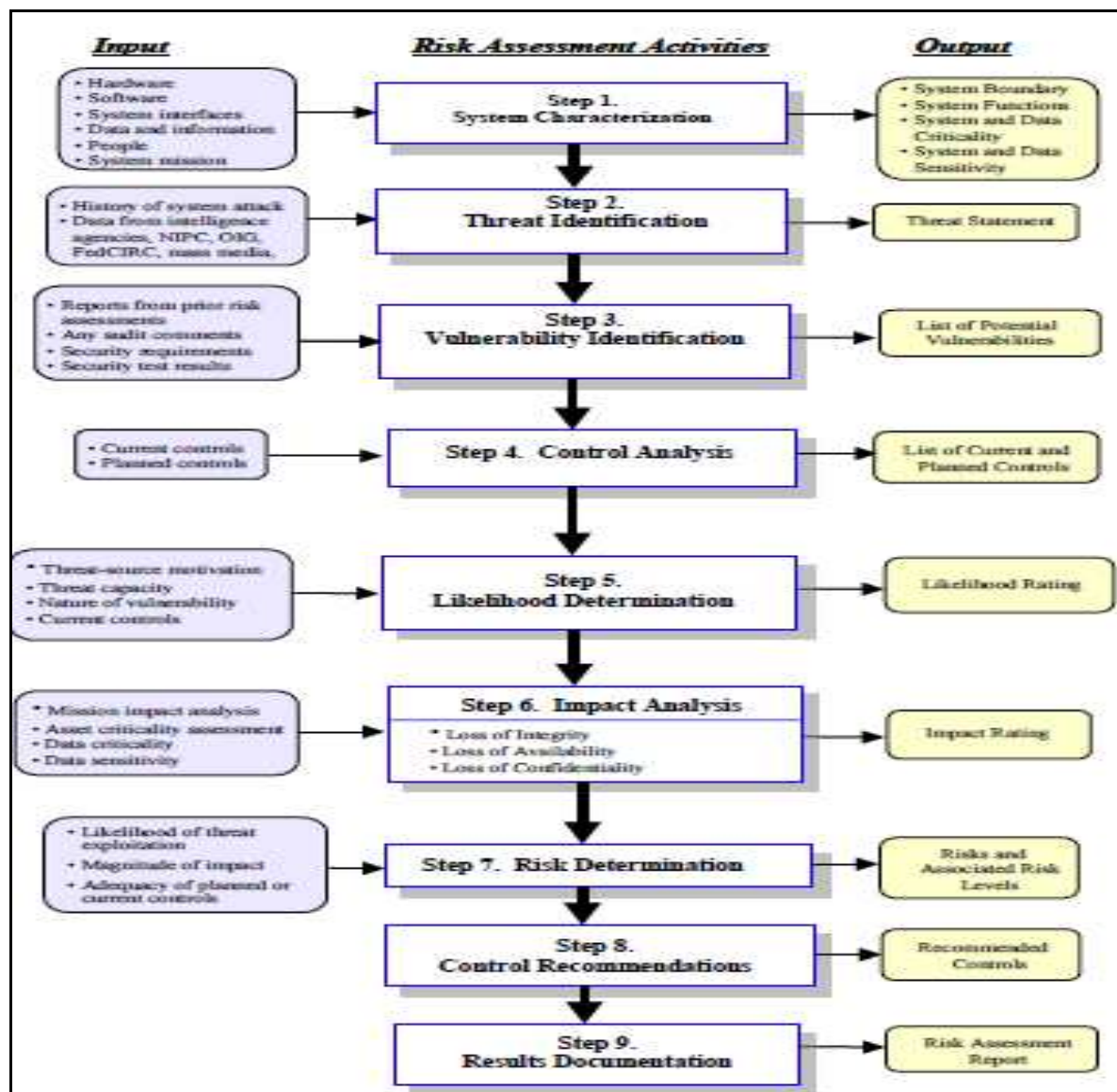


Figure 1. The NIST risk assessment methodology (Stoneburner et al., 2002)

The emphasis of the NIST risk assessment process is to identify a risk from all angles not just the technical or system related aspects, and that the processes much like a system development lifecycle, be ongoing and iterative so that the organization's security stance is ever evolving. Because risk analysis is not a one-time activity, the initial report used to formulate a security policy also sets the stage for information system governance. The initial policy is applied, then as the policy is enforced and monitoring occurs, the discovery of new threats and intrusion attempts create the need for reassessment, which in turn results in further refinement of the security stance of the organization.

Governance

Executive management in many companies continues to view information security as if technology alone will secure the organization. The current practice, viewing security as a technical challenge includes the layering of firewalls, intrusion detection systems (IDS), spam filters and virus protection. IA complements this approach through the application of management philosophy. "The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission."(Stoneburner et al., 2002)

Information security is multi-dimensional with easily identifiable dimensions as shown in Table 3. This list is long on business decisions and conspicuously brief regarding technology solutions. Very often management of a small business hires one individual as a System Administrator (SA) to run their information systems and to whom all these other policy decisions are delegated. Unfortunately progress in all these areas is slow due to the overwhelming amount of work and the complexity of the decisions required. Consequently the SA soon comes to realize that they can't perform their job effectively while also securing the company and thus security concerns take a back seat to day-to-day operations. Eventually, the SA will "either move

on, or out...This opens the company to severe risks because no continuity exists as well as the fact that the security plan never gets fully implemented”.(von Solms & von Solms, 2004)

Table 3. Information Security Dimensions

The Corporate Governance Dimension
The Organizational Dimension
The Policy Dimension
The Best Practices Dimension
The Ethical Dimension
The Certification Dimension
The Legal Dimension
The Insurance Dimension
The Personnel/Human Dimension
The Awareness Dimension
The Technical Dimension
The Measurement/Metrics Dimension
The Audit Dimension

(von Solms & von Solms, 2004)

In an article written for the Harvard Business Review, (Ross & Weill, 2004) were widely been quoted as having found that firms with superior IT governance have over 20% higher levels of profitability than firms with poor governance, given the same strategic objectives. This would seem to state that better IT governance makes any company more profitable than those with lower levels of governance. What the article actually found was that companies with mature governance enjoyed 20% higher profits than companies with less mature governance when following identical business strategies. The important takeaway of this article is not that increased profitability comes from increase governance maturity, but rather that achieving mature levels of governance is extremely resource intensive and as a result particularly smaller organizations will attempt governance in an ad-hoc manner (just as they do with system development), but that accomplishing higher levels of governance proves a strong strategic differentiator in competitive business environments. Adding to this finding, Ross and Weill state

that “top performing enterprises generate a return on their investment that is 40%+ better than their competitors”.

As highlighted in Chapter 1, the cost to business of security incidents is rising. Foremost in the minds of most companies is the ability to secure their sensitive data including credit card accounts, employee records, corporate performance data, audit results and security related capabilities. Security incidents affect not only the confidentiality of sensitive data, but can also hamper the integrity and availability of IT resources, disrupt compliance and ultimately threaten the financial health of an organization.

In 2009, HSBC a financial holding company headquartered in London England, and ranked as the sixth largest bank in the world, was fined \$5.2 Million USD for losing CD media containing unencrypted personal data for over 180,000 customers. (Kennedy, 2009) The fine breaks down to roughly \$29.00 USD per customer account and when added to the Poenemon Institute estimate from Chapter 1 of \$202 USD per account for recovery purposes, means that this incident will likely cost HSBC \$41.5 Million ($\{ \$29 + \$202 \} \times 180,000 = \$41,580,000$).

For HSBC the loss was not a technical compromise, but rather a physical oversight; too often a breach is the result of personnel negligence whether by leaving a laptop in the back of a cab or improperly disposing of abandoned media. If nothing else, the HSBC case highlights the fact that governance is needed to keep these incidents to a minimum. While the cost of properly implementing a governance strategy is high, HSBC is a clear lesson that it is far less expensive to move a governance strategy forward than not.

Written policy

“Most...technological threats require help from unwitting human accomplices on the receiving end in order to do their damage” (Miller, 2006).

The development of policies – as important and time consuming as they are – leave many IT security professionals struggling. The policies they craft are met with resistance, intentionally ignored or simply ineffective. While frustrating, these issues are easily avoided if acceptance, simplicity and staff training are considered as part of developing the overall program.

Like any corporate initiative, acceptance starts from the top. As an IT security professional, belief in the need for a policy will only go as far the CEO allows. Over inflated risks and cost will not win acceptance; facts and loss projections present a more reasonable approach. Once the CEO and management agree to the development of an IT security plan, the focus turns to the employees. Unveiling the program on zero-day is the quickest way to a failed policy. Informing the staff of changes and briefing them on progress while the program is being developed will help ease the transition and may even create converts who understand the reasons behind the initiative.

Well defined corporate strategy should begin with an Acceptable Use Policy. While different users may have access to different parts of a company's system, all users are exposed to some parts; therefore, the Acceptable Use Policy must be comprehensive and include statements regarding the uses of all technology available within the organization. The policy should spell out unauthorized activities such as harassment via email or blogs, the viewing of offensive or illegal content, the use of company resources such as email or the Internet for personal business, how to handle unsolicited email that might contain viruses and how to avoid infecting the network with imported hardware, software or files. The Acceptable Use Policy must also be vague enough to cover technology and uses not specifically identified or yet to be developed that nonetheless would prove disruptive. The Acceptable Use Policy must also detail what constitutes a violation of the policy and the penalties for such violations. Companies are regularly advised to

obtain the employee's signature on the policy so they cannot refute knowledge of it if a violation occurs.

The second part of a good security policy is user accounts, which dictate how assets are utilized. Access control, authentication and network security are located in this portion of a policy. Users may come from many different populations such as employees, partner businesses and consumers. It is important that the user policy spells out access for all to be inclusive of each audience. Multiple logins, including screen saver passwords, should be utilized. "Authentication is the methodology used to determine that a user is who they state they are and that they have the required credentials to access certain areas" (Reyes, 2005). Authentication can utilize usernames, passwords, and biometrics, which authorize different users to varying levels of access. An administrator may have access to add and delete software while a general user may only have access to functions and software pre-existing on the machine. Each user must understand that it is their responsibility to protect the technology from unauthorized access.

Finally, user accounts should enhance network security by partitioning users to specific parts of the system in order to increase security. User Account types should rarely be cross-platform- for example, an employee product representative should only have access to a service order platform, a partner should only have access to an intranet behind a firewall on a VPN to determine what parts to supply, and a consumer should only have access to a public-facing website where they may purchase and pay for a product. Opening systems up beyond their user requirements can create problems. If the partner can access the service order platform, what stops them from falsifying orders to increase their sales?

As with user accounts, each organization has different software platforms and process modules within each platform. A manufacturing organization may have a production platform, a

fulfillment platform and an accounting platform. An enterprise management system like SAP may include multiple modules like Accounts Payable, Accounts Receivable, and Shipping. In each instance, the different platforms and modules should only be accessed by employees whose specific job requires access to them. Each department of an operation requiring various platforms may require its own management policies, which then become part of the governance of the business. “Governance is actually a catch-all role for the idea of important business management disciplines. It’s not just IT, it’s really a business function” (Desmond, 2007). A member of the production team does not need to understand the fulfillment team’s policies and vice-versa. Only the parties involved should be required to understand platform specific policies or general users may become overwhelmed.

Accepted use policies, user accounts and platform specific policies intend to inform the users of general company policies as well as specific platform policies that govern the way a company conducts itself. While each is important, the focus of a good security policy should be on limiting the amount of information each employee must assimilate based on their function and responsibility to the organization. Well-written policies do not by themselves guarantee security, in fact the organization must work hard to enforce what they have written, and therefore the policies should be organized, brief and specific regarding what occurs when they are not followed.

Documentation

Every project begins with planning which means paperwork. Accurate documentation of the physical makeup of the network is essential to both risk analysis and governance because it’s hard to analyze or measure unknown elements. In addition, “the increased scope of design and levels of complexity of information systems implementations are forcing the use of some logical

construct (or architecture) for defining and controlling the interfaces and the integration of all of the components of the system” (Zachman, 1987). Documentation should include the physical network, servers and server apps, and Active Directory configuration and then move into the application structure specific to each process used.

Documentation is paramount to governance because “leaders of the organization must have a clear vision of the desired future state of the entire system...for both diagnosing the need for changes and for managing the process of change” (Beckhard & Pritchard, 1992).

Documentation allows the IA practitioner to identify vulnerabilities in the physical as well as logical construct of the information system that would otherwise remain obscured. The ad-hoc nature of system development as mentioned elsewhere has many hidden pitfalls that are only truly understood when the architecture, similar to the architectural drawings necessary for the creation of a new building, is formally laid out and examined.

Documentation and enterprise architecture go hand in hand with the secure development of a small businesses’ network. Architecture and documentation assist in policy development, technical control and governance leading towards strategic differentiation. Indeed information technology is a tool that businesses use every day to extend their position in a competitive market. Consider Wal-Mart who consistently proves that what all business in mass retail needs to do, master distribution and inventory management, can be achieved to a degree that creates an extremely powerful advantage that competitors, even with similar tools available, can’t beat. Of course the downside of this technology is the threat of unintended disruption.

Fault tolerance through increased systems understanding may be the most important role documentation plays in the network. In December 1998, Ingram Micro’s main data center in Tucson Arizona, was taken offline for an entire day by a short ultimately traced to a fire alarm

panel that resulted in a power outage disabling the telephone and computing systems, erasing the short-term memory in their online sales main frames forcing some of Ingram's customers to seek other retailers to meet their immediate needs. The incident, which lasted six hours, and was resolved by bypassing the offensive circuit, cost Ingram \$3.2 Million dollars. While Ingram sought compensatory relief from their insurance provider documentation could have prevented this outage or at minimum led to much faster discovery (Salkever, 2000). This incident also highlights management's need to shift to a more holistic view of information security through governance. The cause was not an attack or data related issue it was the result of a physical security system that interacted with mission critical systems in ways Ingram did not initially understand. Each department responsible for their various systems most likely understood their role within Ingram, but governance above the departmental level might have prevented this incident completely.

Operations

While most system administrators (SA) understand that operations involve the processes which keep the network and services running, the overall demands of this position often mean that the SA and his/her staff spend more of their time and effort addressing immediate business requirements creating solutions with no consideration for scalability, fostering a patch and run short-term mentality that maintains system functionality but obscures the notion that there is "a timeframe in which major transformation (needs) to occur" (Cerny, 2009).

Administration, maintenance and provisioning are all vital functions that fall within the realm of operational management, however in the highly time sensitive world of system availability, these functions are often overlooked beyond the immediacy of keeping the wheels turning. Contrary to Hollywood depictions of high skilled programmers working for weeks to

infiltrate an organization’s network, the reality according to the Verizon Business Risk Team is that 55 percent of all attacks required little or no skill to perpetrate and that 85 percent of all attacks were not targeted, but rather opportunistic because the hacker either, discovered known vulnerabilities such as cross side scripting present in a particular company’s website, or knew of vulnerabilities in a particular application and then sought to discover and exploit many organizations utilizing these applications in rapid succession (Baker et al., 2008). Most surprising, Baker and his team, Figure 2, found that the length of time taken by the hacker to perpetrate the compromise was much faster, often measuring in hours or days, than the time it took the subject corporations to discover the compromise, which typically ranged weeks to months, and worse, their mitigation timeframe stretched into weeks after the long discovery phase during which the vulnerability continued to remain exposed to exploit.

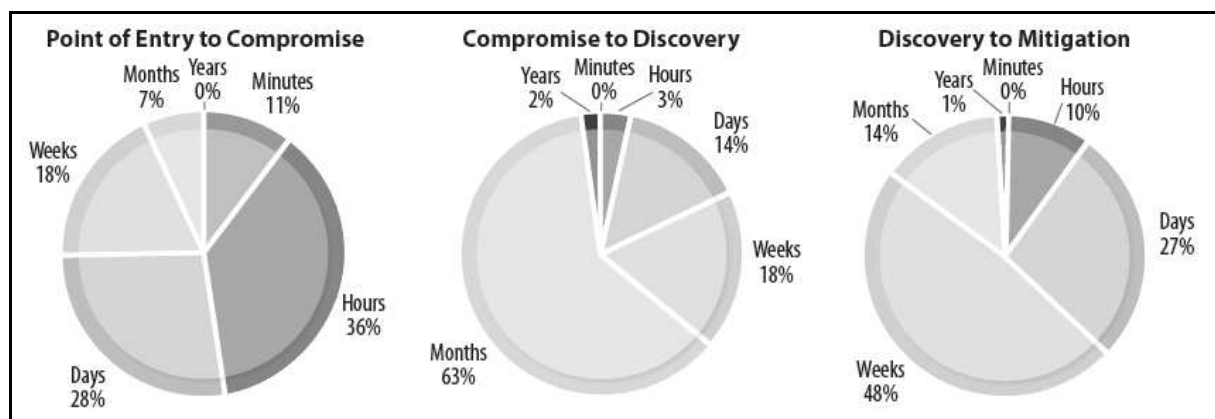


Figure 2. Data breaches: a time span of events (Baker et al., 2008)

Patch management.

While patch management should be viewed as part of a systems configuration and overall change management programs, it has become increasingly important to network administrators and security professionals to consider in their overall operation. In 2003, “within 10 minutes, 90% of all vulnerable machines had been infected” with the Slammer worm even though the

patch had been available from Microsoft for six months (Andrew, 2005). In 2004, CERT published 4000+ vulnerabilities which demanded that business respond even though “only 27 new vulnerabilities were reported as having been exploited” (Heiser, 2005). Clearly more vulnerabilities are recognized than are exploited. While effective patch management protects the availability of the system, “it is practical to manually install a patch on one or several highly-exposed systems...updating a complete enterprise requires” management (Heiser, 2005). The Slammer worm is estimated to have cost businesses over \$500 million to fix. This cost is associated with the downtime and labor required to clean infected systems.

Backup and Disaster Recovery

While IS professionals have been focusing on business continuity planning and disaster recovery planning (BCP/DRP) since the Y2K, 9/11 highlighted the reality that a large percentage of organizations did not have a BCP/DRP in place and as *Contingency Planning and Management Magazine* found, 40% of companies forced to shut down for 3 days or more failed within 36 months (CDW, 2007). While the costs to an organization resulting from network outages is difficult to estimate we know that it can run from thousands to millions of dollars per hour depending on the business and its technology exposure. Organizations need to understand that lost revenue is but one component of this cost which can also include “related late charges, regulatory noncompliance penalties, loss of customer goodwill, and the cost of public relations to repair any damaged reputations”(CDW, 2007).

With complex systems integration leading to the transformation of business processes, BCP/DRP have often been viewed as part of the IS process rather than the overall business process when in fact, BCP/DRP is a management function that is as important to delivering continued value to stakeholders as any sales or manufacturing operation is.

Compliance

PCI-DSS addresses over 200 controls within the information technology (IT) and payment processing environment. As a general guideline, any company that accepts credit or debit card payments must comply with the PCI standard. Companies that fail to comply are subject to fines and penalties or complete disconnection from payment card programs. PCI-DSS has become the de facto framework for the protection of payment card information and related data. “Because of anti-trust regulations, all of the major card brands still maintain their own data protection programs, but the brands mandate that their merchants and service providers comply with the PCI-DSS” (Price-Waterhouse-Coopers, 2008).

<p>Build and Maintain a Secure Network</p> <p><i>Requirement 1:</i> Install and maintain a firewall configuration to protect cardholder data</p> <p><i>Requirement 2:</i> Do not use vendor-supplied defaults for system passwords and other security parameters</p> <p>Protect Cardholder Data</p> <p><i>Requirement 3:</i> Protect stored cardholder data</p> <p><i>Requirement 4:</i> Encrypt transmission of cardholder data across open, public networks</p> <p>Maintain a Vulnerability Management Program</p> <p><i>Requirement 5:</i> Use and regularly update anti-virus software</p> <p><i>Requirement 6:</i> Develop and maintain secure systems and applications</p>	<p>Implement Strong Access Control Measures</p> <p><i>Requirement 7:</i> Restrict access to cardholder data by business need-to-know</p> <p><i>Requirement 8:</i> Assign a unique ID to each person with computer access</p> <p><i>Requirement 9:</i> Restrict physical access to cardholder data</p> <p>Regularly Monitor and Test Networks</p> <p><i>Requirement 10:</i> Track and monitor all access to network resources and cardholder data</p> <p><i>Requirement 11:</i> Regularly test security systems and processes</p> <p>Maintain an Information Security Policy</p> <p><i>Requirement 12:</i> Maintain a policy that addresses information security</p> <p>(PCI Standards Council, 2008)</p>
---	--

Figure 3. PCI-DSS requirements

PCI-DSS consists of 12 requirements in six categories, Figure 3, that address security management, policies, procedures, network architecture, and software design with regard to the protection of payment card data. On October 1, 2008, the PCI Security Standards Committee (PCI-SSC) released version 1.2 of the standard that provides enhancements and clarifications to earlier requirements, which all currently certified merchants are required to validate against by January 1, 2010.

Despite the penalties associated with information breach addressed by PCI-DSS, companies are struggling to comply with the requirements. In general auditing firm Price Waterhouse Coopers (PWC) has found that companies view compliance as an IT problem, lack clear definition as to the scope of the processing environment covered in the certification and underestimate the complexity of PCI compliance (Price-Waterhouse-Coopers, 2008). Many frameworks, tools and software have been developed to assist companies with their PCI efforts. A quick Google search for PCI reveals over 144,000,000 entries, each promising to painlessly assist companies in reaching compliant status. The simple fact is that PCI-DSS compliance is a path riddled with conflicting information that can lead a company astray.

System Development Lifecycle

All organizations have a mission. Whether explicitly defined in a mission statement or implicitly understood by the industry they operate within an understanding that the organization's mission is critical to the implementation of IA within a system structure. Striking a balance between the level of IA and its impact on system operations and resource costs is growing increasingly difficult and thus requires a disciplined approach. As pointed out in NIST

800-30, integrating IA through risk management into the System Development Life Cycle (SDLC) can have an immediate impact on IA integration.

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	<ul style="list-style-type: none"> Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	<ul style="list-style-type: none"> The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	<ul style="list-style-type: none"> The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	<ul style="list-style-type: none"> Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	<ul style="list-style-type: none"> Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Figure 4. The characteristics of each SDLC phase and the risk management activities that support them. (Stoneburner et al., 2002)

While eliminating all risk from an information system is impractical and therefore impossible, one of the most effective ways of introducing security is through the introduction of a system development lifecycle (SDLC). Figure 4 correlates the phases of an SDLC to the risk management activities that support each. Businesses have many tools to choose from when implementing an SDLC. Control Objectives for Information and Related Technology (COBIT) is one such framework that defines an SDLC that implements “control objectives to develop policies, procedures, and organizational structures designed to provide reasonable assurance that business objectives are achieved” (IT Governance Institute, 2007) Further, the goal of COBIT is to produce a “control framework for enterprise governance and risk management” (IT Governance Institute, 2007). While extremely detailed, small business is challenged to implement such a large framework due to its lack of resources and though consultants can be hired to guide the process, a secure system can be maintained initially without such large frameworks as long as security is built into the SDLC process before damage occurs.

Big up-front design methodologies like Waterfall or Rapid Application Development (RAD) take an enormous amount of time, are extremely expensive and lack the flexibility to respond quickly to changes in requirements and for this reason more agile frameworks have been created. Agilest are convinced that an evolutionary iterative approach to system development will overcome the major faults of traditional methods. There are three major issues with traditional development that the Agilest work to overcome; a communication gap between the client and the developer, an overabundance of documentation and inability to incorporate change gracefully.

Many large system development initiatives have failed because the developer and the client did not view the project in the same way. In a traditional development scheme, the

architects do an analysis with the client and then leave to undertake the remaining steps of the software development lifecycle without the client; agilest look to involve the client at every level. This “tacit knowledge” as described by (Boehm, 2002) keeps the developer and the client on an even footing. There are no misinterpreted requirements waiting to derail the project.

Boehm goes on to distinguish Agile methods from “heavy” methods as those that follow the YAGNI precept; that is You Aren’t Going to Need It, so why do it? Traditional methods produce multiple artifacts that may or may not be needed in the end. While this is a way of avoiding the pitfalls associated with gaps in tacit knowledge, it is time consuming and expensive to document every possible item before beginning development.

“A Manager’s Intro to the Rational Unified Process (RUP)” (Ambler, 2005) describes an agile framework for Information System (IS) development. RUP is a comprehensive process for streamlining the system development lifecycle. The lifecycle RUP describes is easily recognizable to managers accustomed to having multiple projects in various stages of development regardless of their specific business concentration. RUP practitioners are encouraged to tailor the product to an organization’s implementation needs. RUP is a full lifecycle development consisting of four phases and nine areas of work referred to as disciplines. Figure 5, demonstrates the amount of time required to implement each discipline in a particular stage is graphically represented by a hump. For example there is little or no time given to testing in the inception and elaboration phases, but as a project moves through the construction and transition phases it becomes more involved.

1. There are five critical observations that differentiate RUP from other development methods: Work products - the business model, the source code, and project documentation - will be created and changed at every stage of the development.

2. The project will progress in “waves.”
3. Risk management is imperative to a positive outcome. The time needed to document risk to a project is valuable and cannot be ignored
4. Each phase will end with a go/no-go decision. The client has the opportunity to decide whether to proceed or cancel for any reason as circumstance allows.

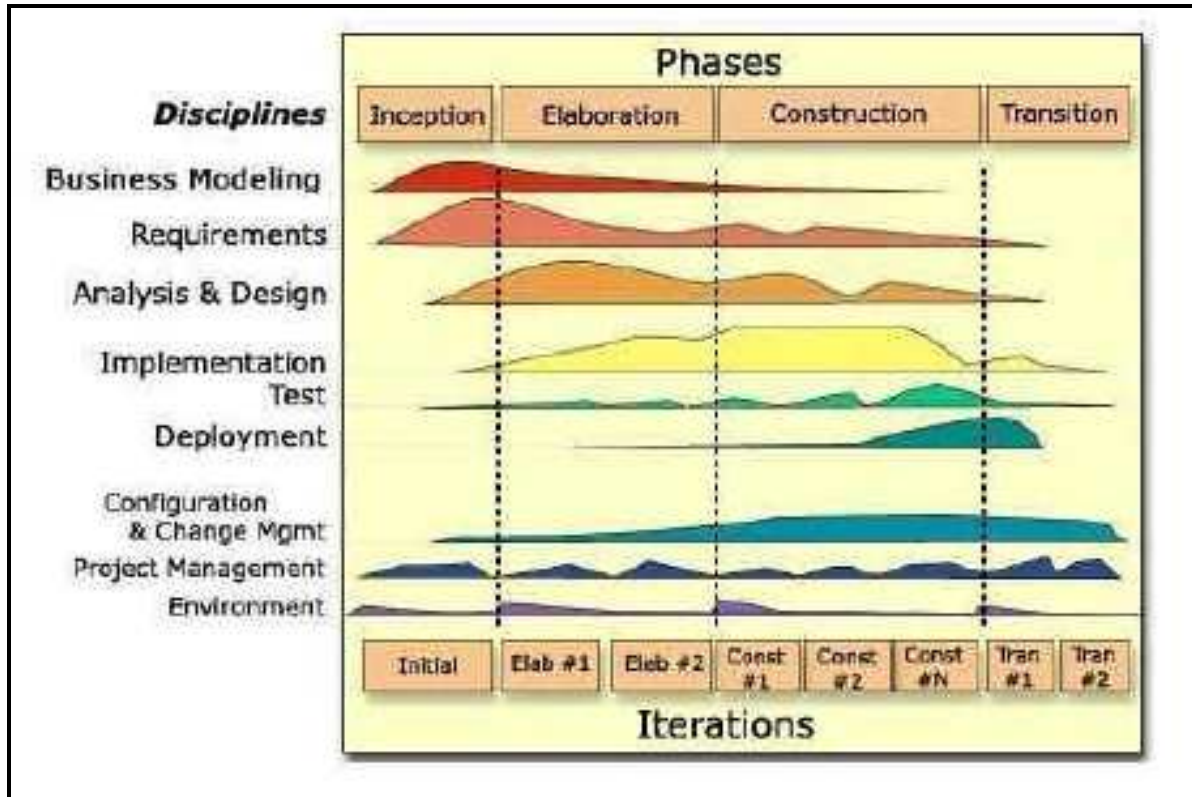


Figure 5. The disciplines and phases of RUP and their associated timeframes. (Ambler, 2005)

The view taken by traditional developers is that each discipline occurs substantially in one phase. Viewing the hump chart, Figure 5, reveals that all disciplines are in motion throughout the RUP lifecycle.

Essential to the successful implementation of a project is “early and intense involvement by the customer” (Hirsch, 2002). At the Inception Stage, a comprehensive use case study is

undertaken. This involves interviewing all stakeholders regarding their needs, their current usage and what they expect of the new system. During the Elaboration Stage, the stakeholders are re-interviewed as the requirements are drawn up. This process, coupled with rapid testing, gives the stakeholders and developers the opportunity to refine artifacts continually as the larger view of the IS evolves. Through the Construction and Transition Phases it is essential to maintain collaboration between developers and stakeholders through effective communication. At the conclusion of each part of the lifecycle, the client is allowed to decide whether or not to proceed. Feedback is critical to this decision. If expectations have been managed effectively, the risks have been addressed, the cost benefit is apparent and the IS functions as required, the decision to proceed to the next phase or to begin the next iteration will be simplified.

Much like a day-to-day business operation, multiple iterations are released sequentially, so the work may be in multiple phases at any given time. Figure 6 shows the incremental release of an IS into production over time. RUP practitioners place a great value on this incremental process as it allows them to begin testing even as the business modeling, requirements and IS analysis progress.

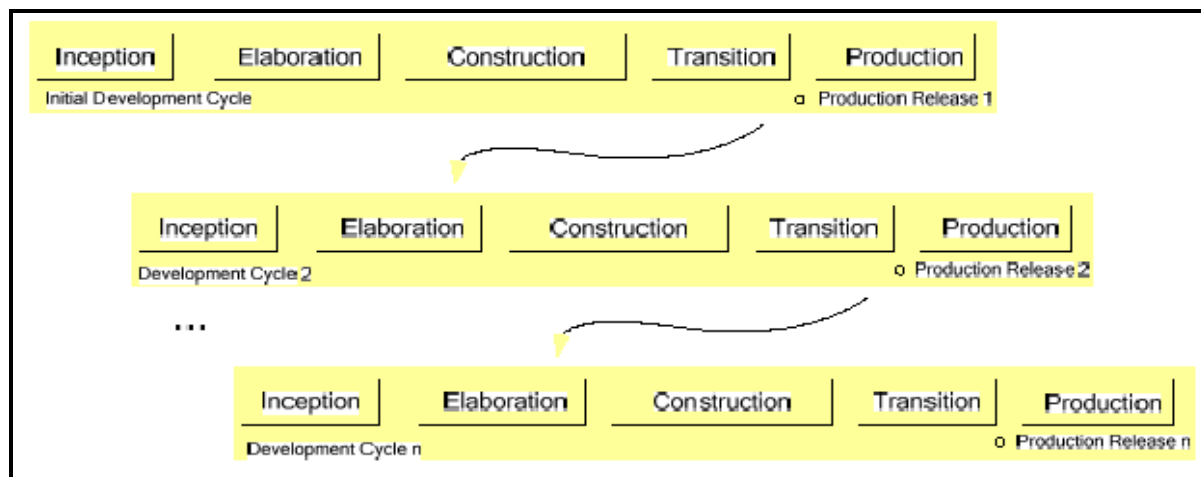


Figure 6. The iterative nature of RUP releases. (Ambler, 2005)

Consider the experience of Zuhlke Engineering AG: “Daily builds are the rule... We are incorporating minor change requests... into a running iteration” (Hirsch, 2002). Problems are identified early on thus the value this approach brings to the team. Debugging is less time consuming and issues related to how multiple components interact arise and are addressed before they are incorporated.

Methodology

In their seminal work on Design Science, Alan Hevner and his associates point out that that in order for a study to be considered design-science research it must not simply be a routine design or system building effort; utilizing a checklist developed by another party is not in and of itself Design Science. Further, they conclude that the key differentiator between routine design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies (Hevner, March, Park, & Ram, 2004). However the unabated “proliferation of new methods and tools for developing information systems... (could be referred) to as a “methodology jungle,” a seemingly impenetrable maze of competing ideas and notions” (Iivari, Hirschheim, & Klein, 2001). Iivari et. al. go on to discuss the multitude of IA frameworks and how new ones are released often but that for all their information, most simply restate a few basic implementations including the Zachman framework among others. So for all the development that is occurring, one needs to argue the merit of the majority of the effort, and yet all of this should be construed as research within the confines of each implementation. Just because an idea is characterized as a best practice, does not mean that it fits a specific organization, indeed, the idea of a best practice list could be replaced with the idea of “best for purpose” as most “best practices” are modified to fit the needs of the organization applying them and each organization will apply various practices from many sources to build their network.

Information system security research can be classified in four broad categories: checklists, risk analysis, formal methods and soft approaches (Dhillon & Torkzadeh, 2006). Thousands of checklists have been proposed and developed over the years, multiple risk analysis models created and hundreds of formal frameworks and soft approaches to information systems design have been proposed, but yet the notion of information assurance as a science is still young when compared to other computer disciplines. While investigating the usefulness of information security surveys, (Baker & Wallace, 2007) found that much of the previous effort surrounding IA centered on the technological sciences, and further, their survey indicated the lack of concentration on the business sciences that compliment security in other areas. (Hevner et al., 2004) state that “the effective transition of strategy into infrastructure requires extensive design activity on both the organizational and technological sides of a business to create an effective information system”.

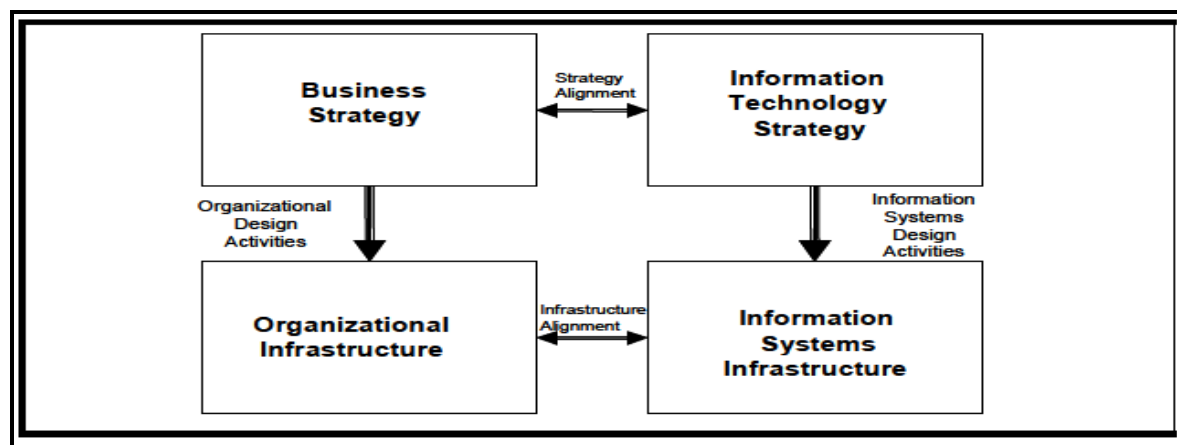


Figure 7. Organizational and design activities showing alignment patterns. (Hevner et al., 2004)

In their work on strategic alignment (Henderson & Venkatraman, 1993) examine the relationships between business and technology development and organizational and IS infrastructure a successful organization will use to leverage technology applications within their organization. Figure 7 explores two predominate areas of alignment in the Business/IT arena.

Business/IT strategy misalignment has been written about to varying degree, and while it is hard to imagine a CEO walking into the board room and discussing the Business/Sales disconnect, or the Business/Finance disconnect, none-the-less the idea has been a popular argument for the miserable shape of IT projects and implementation within business today. Interestingly however, the second area of misalignment, the Organizational/IS Infrastructure disconnect has had very little study. Proponents of technology know that their tools are robust, and thus, assume that everyone will embrace them. Unfortunately this is not the case, and often the technology infrastructure will be adjusted simply because the user base eg. the organizational infrastructure won't accept a system as proposed.

Design science is a way of understanding system development because “management should not conceptualize technology as a tool that can be used to achieve some purposive-rational aim. Instead the constructivist’s (design science researcher) proposal suggests that the managerial use of technology interacts with its use, and forms a part of the environment that shapes its reality”(Zelic & Stahl, N.D.). Design science helps the developers communicate the use and function of a system directly through the development of artifacts that simplify complex transactions in a way the general user can grasp and thus become comfortable. This process of artifact creation offers business the best solution to the organizational/IS infrastructure disconnect.

Conclusion

This chapter presented a literature review detailing the crucial needs that IA can help small business address and some of the benefits that organizations can expect when supplementing their technical security program with the holistic management approach IA offers. Research on risk management lead to an investigation of a system development lifecycle (SDLC)

and the chapter looked at compliance and disaster recovery. Chapter 2 also presented a solid theoretical basis for the methodology used to model information assurance at the subject company, which will be discussed in the following chapter.

Chapter 3 – Methodology

The previous two chapters detailed the importance of Information Assurance (IA) and the benefits of developing a comprehensive process for information system development in the small business arena. The main shortcomings of the information reviewed is that while it is all well known, the volume of work required to properly secure a small business network can be daunting for the typically overwhelmed and understaffed department. This chapter focuses on the processes, tools and artifacts used to analyze the impact of IA on the subject network.

Process

The main goal of this thesis is to answer the question of information technology (IT) professionals struggling to bring security to a small business where the tools and techniques are well known, but little time is given to the governance of these tools in a way that fosters cohesive information system (IS) development.

Design science research was used because it addresses what are considered to be wicked problems (Hevner et al., 2004). That is, those problems characterized by the problems illustrated in Table 4.

Table 4. Character of Information Technology Problems addressed by Design Science.

Unstable requirements and constraints based upon ill-defined environmental contexts
Complex interactions among subcomponents of the problem and its solution
Inherent flexibility to change design processes as well as design artifacts (i.e., malleable processes and artifacts)
A critical dependence upon human cognitive abilities (e.g., creativity) to produce effective solutions
A critical dependence upon human social abilities (e.g., teamwork) to produce effective solutions (Hevner et al., 2004)

Design science is also dominated by artifacts, the creation of which can be expressed as software, formal logic, entity relationship diagrams, network maps and policies; in short, any high level interpretation that enables the end-user to understand the problem and the feasibility of

the approach used to solve it. For the case study, the initial assessment indicated that no formal documentation of any type existed. It was therefore necessary to create a formal approach to how this documentation would be developed. Due to the complex nature of this endeavor, many companies fail to do any formal examinations of their environment. The situation only grows worse over time as users push the systems to their limits; perform their tasks in an insecure manner; and ask for more tools without fully understanding the ability of their current software. As this project evolved, the only logical course was to produce policies, procedures and supporting documents for each step which would guide the project and ultimately create a replicable process for applying information assurance strategy to a small business. Focusing on policy and procedure development as a project in and to itself greatly sped up this tedious process.

Statement of Work

Scope creep, as detrimental as it is to any major undertaking, is particularly pervasive in the IT community. The annals of IT development are filled with stories of implementations or projects going over budget, over time or simply being abandoned due to poor planning. Bringing information assurance strategies to a small business is a major undertaking, especially where none existed before. The participants will uncover major deficiencies in the policies, processes and system configurations that all beg to be addressed immediately. The challenge then is to remain focused on the goals throughout the process. The best way to accomplish this is to write a statement of work (SOW).

Management buy-in is crucial to the success or failure of this type of project and thus the researcher set out to create a statement of work which would define the project in terms that created value to management. Taking the better part of two months to produce, the statement of

work (Appendix A) included an overview of the outcome and defined the timeline and the major deliverables of the project. Focusing on the SOW over the life of the project kept the project on task and clarified what was outside the scope to be addressed at a later date.

Policy and Procedure development

While writing a policy from start to finish can be frustrating, there are many internet sites that provide information and even templates to guide the process. An online search for “information security policy development” yielded over 46,600,000 results in 0.20 seconds; so clearly this is a popular subject. One positive aspect of this research project actually turned out to be the fact that no previous work had been done so consequently there was no reference which meant that process and procedure could be introduced as needed.

From the outset, the SysAdmin, Audit, Network, Security Institute (SANS) information security policies template page available at <http://www.sans.org/security-resources/policies> was a valuable resource. SANS not only provides templates, they encourage their active use stating “there is no cost for using these resources. They were compiled to help the people attending SANS training programs, but security of the Internet depends on vigilance by all participants, so we are making this resource available to the entire community”(SANS Institute, N.D.). SANS feels that information security is so important that their intent is to foster uniform security development by openly offering these resources to policy and decision makers.

At each phase of the project the first question asked was “what are we attempting to accomplish?”

- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel

- Authorize security personnel to monitor, probe and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation

(Canavan, 2006)

Many phases were defined by more than one response, but in every case, a policy, procedure or guideline was established and brought to management for authorization prior to continuing. In some instances, merely approving the policy was sufficient to move on, in others, approval to proceed was given for study purposes, the decision to implement the document would be made, where possible, after the proscribed work was complete; thus establishing a baseline reasoning for the document.

Inventory

One of the important considerations for IT management is to understand what physical and virtual IT assets an organization owns and manages. A good inventory provides information that is useful to daily system management, business office asset tracking, and security incident response. With upper management and department head support, an updated the IT asset inventory policy and procedure was created based on requirements from Theater and Arenas, the managing agency. The disposal policies and procedures are in accordance with the City and County of Denver (CCoD) Technology Department and the CCoD's Environmental Management System (EMS). The CCoD is one of the first municipalities in the country to implement International Standards Organization (ISO) 14001. "From pollution prevention and resource conservation to increased operational efficiency, Denver's EMS has many

environmental and business rewards. An EMS will save Denver residents tax dollars, promote environmental stewardship and improve the city's work" (Denver, 2008). The CCC's efforts in this area represent a major component of the Denver EMS program and a healthy choice for the CCC because the convention industry as a whole creates a large waste stream and any reduction will benefit the operation.

Documentation

Information assurance is design science, that is to say that the information strategies developed to secure an organization rely on the artifacts that design science creates to understand the strategy. For this research effort then it is important that the documentation process, creation of artifacts, is done alongside the strategy development. Too often, management creates a strategy in a "back of the napkin" style, enacting policy and procedure by fiat without committing it to writing. The idea that putting a policy in place and documenting it later, becomes put a policy in place, now put a process in place, put another policy in place and document it all sometime. Small business is challenged to produce more with fewer resources than larger companies and at first, the documentation process will slow a productive process, but if rigorously adhered to, in the long run, documentation will save time.

Instead of viewing documentation as something that slows work, the business should consider documentation part of work. There are a number of time saving benefits to having a well-documented network. Documentation is:

- A troubleshooting tool—when something goes wrong, and it will, documentation serves as a reference that can uncover a cause rapidly. This saves the company time and money.

- A training tool—a new hire can learn more quickly from printed references than from the show as you go approach many small businesses operate from. This saves the company time and money.
- A tool for contractors—Major projects like audits or application development are expensive. If a contract needs to spend time rediscovering details of the network infrastructure, or the processes and procedures governing the organization, they use time that could otherwise be allotted to moving the project forward. This saves the company time and money.

As the research for this project progressed, each and every phase was documented, notes were taken in real time as to what was discovered and as the project moved into each phase, the artifacts, policies, procedures, diagrams and tools were created, written down and presented to management for approval. Each artifact was then placed in a readily accessible place, and used as a guide or reference for subsequent phases of the project. The end results show that this process greatly increased the efficiency and security of the subject network.

Network Management

Though network management software is a given for medium-to-large firms, the average small business can't justify the cost of these expensive programs. After researching the available tools, Spiceworks 4, available at www.spiceworks.com, was the overwhelming choice because it is free network management and discovery software. Aimed at the small business market the software gives resource-scarce firms the capability to install a computerized system to inventory and manage network devices, desktops, servers, and printers. Spiceworks 4 also contains a network mapping utility and a web based help desk and ticketing system built around a queue that allows employees to request assistance. All of these capabilities are essential to insuring that

any policies developed can be effectively implemented, managed and enforced. Once again, policies and procedures needed to be implemented to guide the use of this application, however since the overall outcome to the end user should be a performance gain, these documents required only tactic approval from upper management.

Once Spiceworks was installed on a dedicated workstation it was necessary to configure which subnets to scan and input the administrator account information for the network. The software polls Active Directory, pings the network to locate devices, and gathers information about them via multiple protocols including WMI for Windows PCs, SSH for Mac or Linux systems and SNMP for things like printers, switches, routers, etc.

Risk Analysis

TRA as modified by the Defense Signals Directorate of the Australian Government, approaches analysis by examining threats and risks while looking at the consequences they will bring if they occur. TRA is based on four steps including asset definition, threat assessment, risk analysis, and recommendations. TRA uses a threat rating system such as in table 5 to prioritize a threat.

Table 5: Probability Rating System

Rating	Probability
Negligible	Unlikely to Occur
Very Low	Likely to occur only two or three times every five years
Low	Likely to occur within a year or less
Medium	Likely to Occur every six months or less
High	Likely to occur after a month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to Occur multiple times a day

(Weaver, 2007)

After a threat is prioritized, a second rating system is applied to the consequence of the threat occurring such as illustrated in Table 6.

Table 6: Consequence Rating System

Description	Consequence
Catastrophic	Threatens business continuity and survival
Major	Threatens the continuation of basic functions of the program or project and required senior-level management intervention.
Moderate	Does not threaten business continuity but could result in major review and modification of procedures
Minor	Could threaten the program’s efficiency of effectiveness but can be dealt with internally.
Insignificant	Can be handled in daily operations

(Weaver, 2007)

Assigning both a threat and consequence rating to each risk results in picture of the true risk faced for each occurrence. For instance a fire at the facility would be rated as having a “Catastrophic” impact on the business, but the threat rating is “Unlikely” because the building has modern fire suppression systems. The consequence of data leakage is “Moderate” but the threat rating is “Medium.” IT managers then use the matrices to develop recommendations that control risk by balancing their response and thus focusing their spending and effort on the proper amount of protection without needlessly focusing on the wrong risks.

PCI compliance

During the threat assessment, Merchant-eSolutions, the payment card clearing house for the CCC requested that the organization become PCI-DSS compliant within 90-days of notice. The study organization was identified as a Level 5 Merchant and thus was required to answer Self-Assessment Questionnaire B / Imprint Machines or Stand-alone Dial-out Terminals only, no Electronic Cardholder Data Storage. This created yet another challenge for the project, but it was

a welcome chance to further examine the logical controls and policies of the organization and the timing was prescient given the current activities.

Tool Development

Due to the severe nature of the current economic downturn facing the organization and the City and County of Denver funds for IT auditing firms or specialized PCI compliance software was not available. To minimize the problems of compliance uncovered in Chapter 2 a novel approach was needed. In recognition of the ad hoc style of network development the CCC has experienced and the fact that no formal risk assessment had been conducted to date a modification of the California Office of Information Security and Privacy Protection (COISPP) Information Security Assessment Tool for State Agencies was proposed. The COISPP tool was intended to “assist agencies in determining the degree to which they have implemented an information security program or framework...” (California Office of Information Security and Privacy Protection, 2008). Key to this tool is a scoring system where questions are rated from “not implemented = 0” to “fully implemented = 4”. By applying this scoring system to the 226 questions in the 12 specific requirements of the six categories of PCI the user can quickly establish their organization’s ability to meet compliance and identify the areas of specific concern where the organization should focus its efforts. While the SAQ provided by PCI is limited to yes/no responses, the tool developed based on COISPP efforts is quantitative and thus allows a high degree of initial assessment. The goal, based on the results of the tool survey, was to provide a more nuanced understanding of the security and control deficiencies in the organization’s systems. This understanding focused the organization’s efforts on those areas where compliance was easily addressed and those where the most risk was revealed.

For IT risk assessment, the COISSP effort is easily adapted to the PCI SAQ-D questionnaire. To apply the risk assessment concept the yes/no responses were substituted with scoring fields. The sum of all the fields in each requirement is then divided by the total number of fields revealing the average score. For PCI-DSS compliance, only answers of yes or not applicable (NA) are acceptable. For this assessment, NA was assessed as fully implemented to properly address its irrelevance in the overall analysis. The average score for each requirement is transferred to the Action Plan worksheet. Any average less than 4.0 is judged as an area that will need to be addressed. Lower average scores represent requirements that will require more work to fully implement. The completed spreadsheet is located in Appendix C.

Secure System Development Lifecycle

Most people who work in a technology capacity are familiar with the concept of a system development lifecycle (SDLC); this researcher introduces the concept of a Secure System Development Lifecycle (SSDLC) to inform system administrators, management and contractors on the guidelines necessary to ensure that the organization's systems remain secure as new development occurs.

Rational Unified Process (RUP) with its incremental and rapid development phases was chosen as the starting point for the Colorado Convention Center's SSDLC. Because RUP does not follow the traditional waterfall approach of IS development, the main criticism of RUP is that it relies heavily on artifacts to detail the project. However, because the project relies on design science methodology, this argument lends credibility to RUP in this context because artifacts make it possible for the stakeholders to understand the flow of the project. According to Hirsch, "one key to a successful application of RUP ...is the careful selection of the proper subset of artifacts..." Each implementation is planned according to the level of risk involved, thus the

highest risk IS becomes the framework for all other development. “Effective development teams raise the level of abstraction ... by reusing existing work products, and by focusing on architecture to think through the big issues early in the project.” [Ambler, S.W (2005)]

Essentially Ambler and Hirsch have shown how RUP mimics the ad hoc nature of a small business’ system development, but by using this methodology, structure and therefore security is introduced into the process. By reducing the number of artifacts required for the iteration, the time frame of each life cycle is decreased and the system administrator in such a small business now has a guideline to effectively manage all their development requirements.

In Chapter 2, Figure 2 from NIST detailed an ideal SDLC, the characteristics of each phase and how risk management supported these phases. The target system, and in this researcher’s opinion, most small business systems have reached phase 4, operations or maintenance, but sit at or below phase 1, initiation, in terms of risk management, where risks are identified to support the development of the system.

By introducing RUP the project uses multiple short iterations to increase the level of security rapidly. The focus is not on reengineering the system, but rather through the use of an SSDLC, to reverse engineer risk management so that the system operations and the risk management activities match one another. From this point, the SSDLC is then to be utilized by the system owners to support future development, by moving the organization from ad hoc implementation to managed but rapid development.

Conclusion

This chapter presented the research methodology used to assess the Colorado Convention Center’s level of information assurance. The chapter begins with a justification of the use of design science and how the creation of artifacts impacts the level of understanding for the

participants and an organization's management. The chapter then describes how work would progress with the creation of a Statement of Work intended to maintain the project focus. This was followed by a description of the documentation being done and the creation of policies and procedures to support that work. A detailed discussion of the risk assessment process and the concept of compliance followed and the use of rational unified process (RUP) was discussed as the foundation for the creation of a secure system development lifecycle that the organization could follow for future implementation. Chapter 4 will discuss the application of the concepts in Chapter 3 and provide insight into how quickly an organization can improve their security stance through the implementation of information assurance.

Chapter 4 – Results

The primary objective of this project was to provide small business with a process to follow that would lead to the application of information assurance (IA) principles when evaluating and improving their information security. The previous chapter focused on the methodology used to create a system of evaluating a network, the controls necessary to secure the network and a framework for implementing a secure system development lifecycle into even the smallest of business that will improve security where the technology team is limited in size and expertise.

Inventory and Network Documentation

As noted before, it is difficult to secure an unknown thus a physical examination and inventory of all the associated hardware, servers, security appliances, desktops, peripherals, hubs, switches, and routers was performed. During this preliminary phase, it was noted that a current asset inventory as required by the city was unavailable and that the formal processes recommended by the city were not followed by the Colorado Convention Center (CCC) or its managing department, Theaters and Arenas. At the same time the city lowered the price threshold for technology assets requiring inventory from \$1000 to \$250 which required an invoice search and physical confirmation of all IT assets purchased dating back to January 1, 2004. The first policies developed out of this effort include an IT Asset Inventory policy, and an IT Asset Disposal policy resulting from the stockpile of abandoned gear that needed to be securely removed from the facility. Both policies are located in Appendix E.

These policies were roundly embraced by finance and in one week, the inventory process revealed that the facility had 265 devices and 8 personal devices connected to the network and an

additional 62 workstations that had been taken out of service awaiting disposal. The existing inventory also contained what appeared to be a glaring omission, according to the list, the facility owned 14 laptops, but physical inspection only revealed 12. Fortunately the invoice review revealed that two devices on the existing inventory had actually been issued return merchandise authorizations (RMA)s because they had been traded out after having been found to be defective. The laptop inventory was correct, but due to a poor tracking procedure, difficult to maintain. A Laptop Checkout Policy (Appendix E) was developed to address both the physical and data risk associated with portable devices. The inventory process yielded three quick wins for the project:

1. The discovery of 265 devices connected to a C-Class network explained the IP conflicts and network instability that had been plaguing the network.
2. Personal devices were removed from the system immediately as they were not controlled by the company and the researcher could not ascertain any business related function associated with their use.
3. The proper disposal of 62 workstations immediately decreased the facility's exposure to data loss from theft or improper disposal.

While compiling the physical inventory, it was also noted that there was no cable management; all wiring closets were cluttered and lacked any formal port numbering or wire labeling, and that physical security of the network assets was non-existent. Figure 8 illustrates both lack of physical security and cable management in what then was the main server room; a coat closet, with no lock, adjacent to the reception area of the administrative offices. It was even worse before the cables were bundled to access the back of the server.

Additionally, there were no policies in place regarding how the network should be documented nor were there any wiring diagrams or network maps. These tools are essential to

the baseline security of any network, and critical to the health of a network as wide spread as this facility's.

Working with the technology staff and reviewing documents available online, the CCC developed a comprehensive documentation policy. This policy in Appendix E was extremely beneficial; as the physical inventory progressed, the staff also had the understanding of the goals and a process to quickly document and label devices as they performed the inventory.

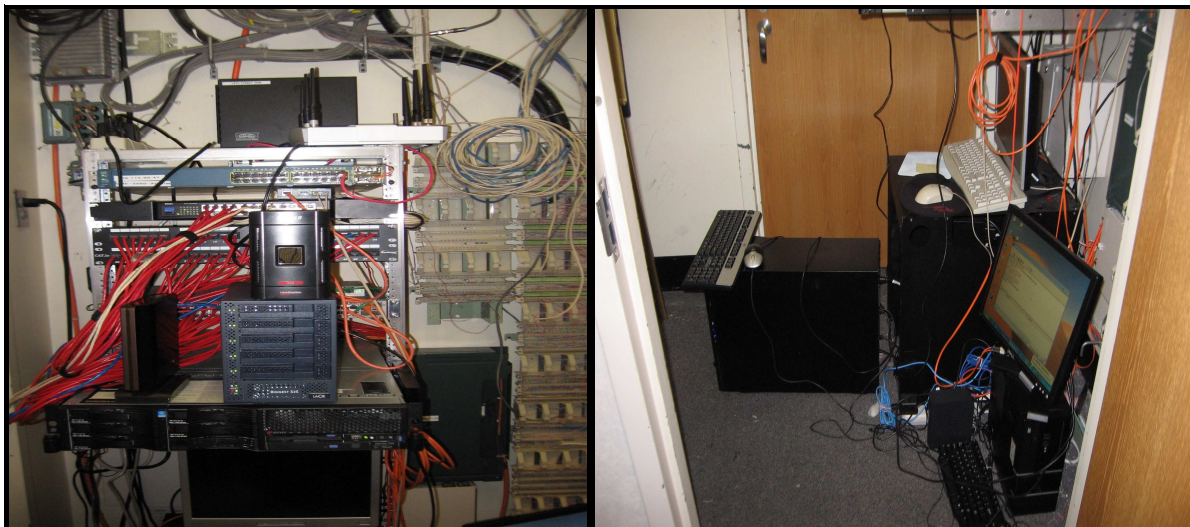


Figure 8. Main server room condition pre-project.

Through this documentation, it was discovered that none of the 26 switches in the system had been reconfigured; all vendor supplied default security settings were still in use. This major security vulnerability had to be addressed immediately and thus another policy was written Appendix E. The standard SANS template for router security is very stringent and some reworking was required as the Scope of Work is to rapidly affect the organization's security stance. In this case the SANS policy can be viewed as the desired ending point; the initial policy was written to address the immediate need to reset the default security policies only, leaving the other recommendations for future development.

The CCC exclusively uses HP Procurve switches on the production network. HP Procurve switches have a reset button that allows anyone with physical access to the device the ability to restore all the settings to the factory default. With this second significant vulnerability related to physical security, a physical access policy was created Appendix E. Implementation of this policy required a complete review of the keying process and resulted in the purchase and installation of new key sets for all 46 locations. In addition, the key process was changed so that only technology staff physically carried keys to these areas; all other support personnel are now required to check out keys from security when they need access to these areas.

Baseline of the Existing Network

In order to evaluate improvements in IA on the target system it was first necessary to measure its current state of security and maturity. Each proposed concept could then be compared to the current configuration, the baseline, to determine which proposals benefited the organization. The initial process of inventory and documentation was necessary to attempt a baseline. The first step was to create a high-level diagram, Figure 9, documenting the logical construction of the network.

With a picture of the logical makeup of the current network, it was quickly apparent that rapid improvements could be made and were necessary. The most glaring issue immediately facing the researcher, as noted in the inventory, was that the single subnet was a C Class block of 255 ip addresses while the organization employed 265 devices. Clearly new subnets were in order.

Another alarming finding was that the organization did not have any management applications or management console to monitor network activity. The existing domain controller was running Websense, an enterprise level web filter, but no reports were being generated and all

logging was shut off within the server so no activity or health data was being collected. Additionally, within Active Directory, there were a number of active accounts belonging to individuals who no longer worked for the company and it was clear that no user audits had been performed.

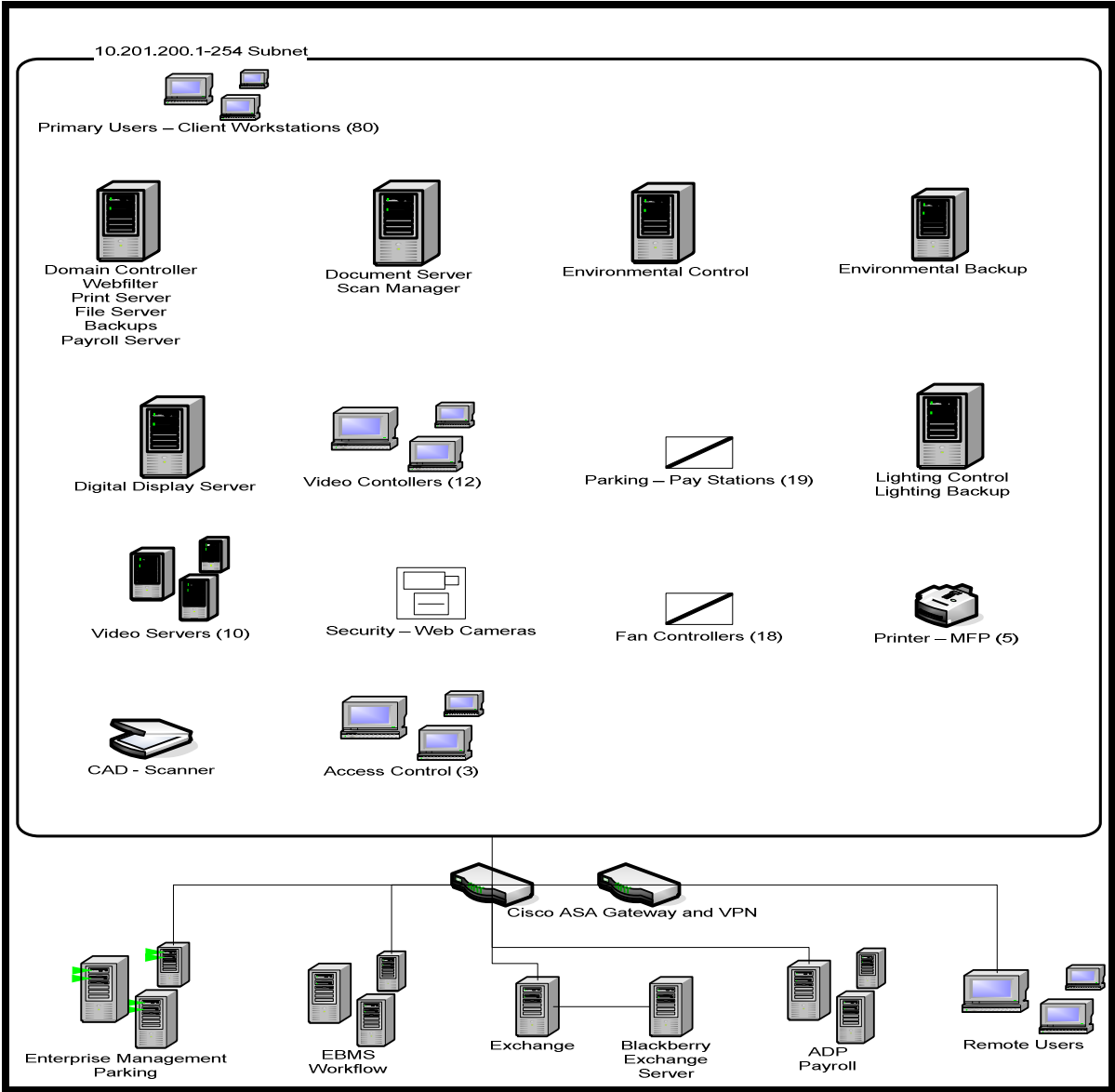


Figure 9. Original logical architecture

Focus then shifted to the desktops within the organization which did not appear too concerning. All the desktops were running Symantec Endpoint and most were set to notify users

when automatic updates were available from Microsoft. Further investigation however revealed that many users were ignoring notices to install updates and had disabled functionality within Endpoint so that Live Update was not running and scanning was stopped. Obviously these were major security vulnerabilities and this finding alone highlighted the aim of the study. The tools were marginally in place, but worse, the organization did not have an acceptable use policy or any security policies dictating user expectations. In light of this, even where the technology department had attempted to protect the organization, users had simply disabled the efforts. Whether these actions were out of ignorance or on purpose, the technology department would never improve the situation without management's backing of policy development. To immediately address this situation, an acceptable use policy and virus protection guidelines were crafted Appendix E.

The most obvious desktop improvement would be to centrally control the Anti-Virus application through a managed console. The Symantec license was out of date and Kaspersky Anti-Virus 6.0 was chosen as a replacement. Cost is always a consideration and a desktop license for Kaspersky was 50% cheaper than a similar Symantec license and Kaspersky packages a server application and a management console with their enterprise edition at no additional charge. Further investigation revealed that Kaspersky has become a well rounded and functional package, and the company is very aggressive in their research and update methodology. To prepare for the installation, the technology department had to go through the entire user base and manually remove all Symantec programs and registry entries. This process was accomplished during an overnight maintenance window when all outside connections to the Internet were disabled. Configuration of the administration console took the better part of two hours, but was straight forward. For system installation, the administration console installs a network client and

the application on each computer. This process began at 10:00pm and by 2:30am working in batches, the client and application had been deployed to all 87 computers and reports began coming in. At 2:30am, the administrative console was used to instruct the client machines to simultaneously perform a deep scan of all processes, files, registries and directories. The results were not good, but not surprising. Of the 87 computers placed under console control the average device had 20 identifiable viruses, trojans or other malware each. Installation of software and control of the network via a management console had never been attempted at the facility and the ease of installation and management proved a motivating factor in upper managements' decision to move. While the general manager supported the effort, a number of the other senior staff questioned the idea of monitoring. The human resources department and the Director of Finance were concerned that the monitoring would give the technology department access to sensitive information, which of course it does. All this concern is warranted, and the researcher felt that, in the best interest of the technology staff, a policy (Appendix E) defining what the monitoring would and would not do, how it would be used and what constituted abuse needed to be understood by all and acknowledged by the technology staff before moving forward.

Spiceworks, the freeware network monitoring suite chosen for the project due to the attractive price, intuitive design for users familiar with current browsers and because the application has a built-in help desk ticketing system that would allow the facility's users to submit help requests. A policy for the use of the help desk was written (Appendix E) and distributed to all users. Enforcement in this particular case is straight forward, regardless of how the request is presented to the technology staff initially; each member would redirect it to the ticket system. Over time users accepted this process because they were given access to check the status of their issue, provided regular updates, and understood that the timeline for remediation

was being followed by the technology staff. The technology department gained a new level of trust from the employees and the overall IT situation began to improve as the technology staff now felt like an empowered part of the overall organization where they had felt isolated and even distrusted in the past.

Spiceworks claims that for best performance their application should be used on networks of 500 or fewer devices, so at 265 devices, the network fit within the parameters. After installation the initial scan was complete in approximately 40 minutes discovering nearly all devices ranging from PCs to SNMP enabled temperature controls. Unfortunately there were a few devices that Spiceworks failed to properly identify, and a smaller number that it simply did not see. By adjusting the logon information and adding an additional scan with different network credentials all the devices were found however some of them still would not fully update their software inventory or configuration levels. This issue was a small inconvenience compared to the wealth of information uncovered.

Once the scanning was complete, the Spiceworks dashboard provided an overview of the network where we found many concerning issues. The inventory page displays devices organized by category and let the researcher obtain a summary of overall configuration info for individual devices, software installations and patch levels. The most concerning discovery was that 23 of the 86 Microsoft XP desktops installed throughout the facility lacked service pack 3 (SP3) and were running Internet Explorer 6.0 (I.E.6) or lower. Microsoft developed SP3 to address major security flaws known to exist in its operating system, and has ended support for anything below Internet 8.0 due to known vulnerabilities in their older browsers. As mentioned in Chapter 2, the majority of exploits come from patches that have been identified for a long period of time. In this case, the organization was exposed to flaws that had been around for

years, but users had ignored recommendations aimed at remediating these issues. Having finally compiled all the baseline artifacts for the network ranging from basic policy and procedure to logical diagrams and network maps, and with the installation of two monitoring tools, the project moved into the threat analysis phase.

Threat Analysis

The CCC's mission is to support adult continuing education through the hosting of meetings, seminars and tradeshow. While not primarily an information technology intensive business, the CCC relies on the IT infrastructure for communications, security and life safety in operation of hosted events. As mentioned in Chapter 3, Threat and Risk Analysis (TRA) based on the Australian Government's interpretations was selected for this phase of the project.

Asset Definition

Step 1 of TRA, asset definition, was greatly enhanced by the initial inventory discovery, but now focus turned to physical assets like air conditioners, wiring closet hardware and other non-IT assets that none-the-less impact the operation. As of February 14, 2010, the Colorado Convention Center (CCC) local area network consisted of 75 windows computers connected to 6 servers, with both copper and fiber optic cable running through 46 wiring closets. 112 users have been granted access to CCC's network resources. This framework serves as the foundation for the CCC's electronic communications and increasingly is becoming an essential component of the operation of the facility. To date, no wireless capability has been included in the network and no users are granted access to services like email from non-company devices or mobile phones. The assets listed in Table 7 became the focus of the initial assessment.

Table 7. Asset Definition List

Asset	Role
IBM X345 Server	Domain controller, File server, Print Server and Web Filter
HP Proliant 5G	Document Management Server
75 HP Desktops varying from New to 5 years old	Primary work tools for information workers
Infrastructure cabling Cat3, Cat5, Cat6 and both Single and Dual mode fiber	Signal propagation throughout the facility
20 HP Procurve Switches	Production network aggregation (layer 3)
8 SMC 1 Gig managed switches	Security system LAN (layer 2)
46 Wiring closets	Signal distribution to all areas of the facility
PBX	Currently housing HP 5G only
Administration Coat Closet	Currently houses the main server and backup
Lacie Biggest S2S (sata drive)	Back up storage
Kaspersky Workstation and Server AV	Anti-virus
MS XP, 2003 and 2003 enterprise	Operating Systems
Alchemy	Document Management Software
Global Scan	MFP Scanning Software
5 Ricoh Multi-function Print devices	Distributed printer scanners for all document production.
Microsoft Office 2007 / Adobe 9 Pro	Standard productivity suites installed on all desktops
Stultz 1 ton internal cooling unit	HVAC unit in PBX
Excel Energy	Utility Provider for the CCC

Threat Assessment

This was the first assessment ever done on the organization's network infrastructure so focus was placed on the obvious essentials. Step 2, the threat assessment was accomplished by examining all the assets identified in Step 1 for both physical and logical vulnerability. A path for future improvements will be discussed later in this chapter with the introduction of the secure system development lifecycle (SSDLC).

Hardware and Infrastructure

The CCC utilizes an IBM X345, named IBMSVR01, running MS Server 2003 and MS SQL 2005 for primary data storage and print server access. IBMSVR01 consists of five installed

250G hard drives and one external LACIE hard drive to store all data and services for the 112 end users in the facility. This server also operates as the domain controller and gateway for CCCDOMAIN supporting the single local area network (LAN) in the facility. In addition the server hosts the application manager and database repository for the organization's web filter.

IBMSVR01 is crucial because all financial data including budgets, profit and loss statements and balance sheets, all policies, procedures and guidelines, all human resource information and all electronic communications rely on the availability of this one machine. It is fair to say that the amassed organizational knowledge of the business is centralized in this one area and a loss of this knowledge would put the organization's long-term business health at risk. Not accounting for purchase price, the data server is the single most valuable asset that the CCC must seek to protect.

This analysis identified a number of vulnerabilities related to IBMSVR01. First, the server is located in a closet converted to a communications closet in the administrative offices of the facility. While the area is under video surveillance, the closet is accessed by many different entities and no locking mechanism is present which leaves the server vulnerable to damage, theft or direct compromise. Second, IBMSVR01 has been in operation for over three years and is beginning to display signs of instability; power supply 2 recently failed and the decision to repair or replace the server has not been finalized. Third, and by far more troubling, the backup device, the Lacie Biggest S2S is located alongside IBMSVR01. Not only are back up jobs failing regularly, leaving the organization exposed to a data loss, the presence of the backup device in the same location as the server it protects, leave the organization dangerously exposed to breach, theft, or destruction. In short, the organization is not prepared for any type of major incident related to its main server.

As mentioned earlier in this chapter, the organization's vulnerability extends to its desktop assets. In most instances, patch management has been left to the individual custodian of the device. No process has ever been introduced to enforce patching levels and no scans have been done to determine the patch levels of individual machines. In addition, prior to the introduction of Kaspersky, the end user had the ability to disable the anti-virus scans and updates. While this management is now performed by the technology department, it is recommended that security policy changes be made to the local computers through group policy so that users can't delete the program outright.

Public assembly facilities are built to be flexible and accommodating to rapid reconfiguration based on the needs of the events occupying their space. This flexibility means that the data infrastructure and the closets protecting them are in a constant state of flux. Wiring closets supporting data distribution are located throughout the building often in out of the way places over 1000 feet from the Main distribution Frame (MDF). The cable running to these closets does not always run in the provided cable trays and all of the cable is exposed. It is concerning that work performed at any distance from the closets could adversely affect connections and that without redundancy, an unintended Denial of Service (DOS) to portions or all of the facility is likely.

Another infrastructure concern lies in the fact that all permanent facility wiring is easily identified, having been run in red jacketed plenum cable. The hallways and corridors that this cable runs in can be accessed by anyone entering the facility and these areas are all but impossible to secure. It would not be difficult for an attacker to enter one of these corridors and with basic data cable knowledge, splice into one of these lines. The amount of storage that occurs in the corridors and the high level of transient traffic seen here create an opportune hiding

location; even if an attacker were detected, by simply explaining that they were “checking the lines” could gain most employees’ trust.

The facility expanded rapidly in the early part of the decade and many areas of the building contain inexpensive non-managed hubs manufactured by Linksys or SMC connected to wall ports for the purpose of increasing the number of data connections in specific rooms. There is no management of these devices and it is difficult to tell how many there are, where they are located and for what purpose they exist. Though the majority of the network is served static IP addresses through IBMSVR01, there is a pool of thirty DHCP capable addresses provided directly by the Cisco ASA. Because there are unmanaged hubs located throughout the facility there is the potential for an attacker to simply walk in, connect to a wall port, obtain an IP address and begin to attack the network from within the domain.

Logical Controls

Little is done by executive management to establish who is responsible for the overall approach to security and internal control. Logical access control is a vital part of an organization’s overall security approach and the conclusion of the audit is that the CCC’s logical access controls do not adequately protect the system from unauthorized use, disclosure, modification, damage, or loss.

To determine whether access privileges for former staff and re-classified employees were properly handled, a list all staffing changes from October 1, 2008 to October 1, 2009 was compared to current access privileges. Five individuals with active accounts were no longer employed by CCC. No written policies and procedures are in place to inform the technology department of terminations and there are no procedures to establish an audit trail when activating and deactivating user accounts. Contrary to PCI-DSS requirement 8, *Assign a unique ID to each*

person with computer access, there were generic department accounts in lieu of individual employee accounts which were used by several individuals throughout the day.

CCC does not use any type of formal process to grant access to the LAN, email server or corporate database. With no formal process, CCC cannot readily verify or confirm levels of access privileges granted. Two reassigned employee's accounts were still valid within critical systems including ones that gave access to financial and human resource related information even though their new roles did not require this.

Many of the security features within Windows Server 2003 (Win2003) are not being utilized. Specifically, when a user ID is established, Microsoft 2003 allows the system administrator the option of specifying a start and end date for an ID and qualifications for users renewing their passwords. Group policy in Win2003 can be configured to force the renewal passwords but CCC does not employ this feature. Further, there are no restrictions on user passwords including no provision for character length or prohibition on the use of words and names. In addition, the operating environment has no established time-out or credential refreshment settings. In two spot checks, one performed at lunch time and one after hours, employees had left their workstations and server sessions and any application they had been using were still accessible.

CCC lacks processes and resources to provide employees with security awareness training, and that the systems administrator was not given access to training related to her responsibilities. Further the CCC has not established adequate controls to ensure all employees understand their responsibilities; there is no formal Acceptable Use Policy (AUP) and no requirement to sign or otherwise indicate understanding of what does or does not constitute an acceptable use of the CCC systems.

Risk Assessment

This analysis utilized a light form of Threat and Risk Assessment (TRA); the list of probabilities was reduced to five factors where the example from (Weaver, 2007) included seven, to the analyze the CCC information systems. Even prior to the formal assessment, it was apparent that the network was vulnerable to software failure due to the anti-virus situation and the lack of a formal patch management plan.

The results of the initial assessment were categorized into a matrix comprised of eleven areas of concern and 35 individual threats. A brainstorming session was then convened for the purpose of assigning a probability and a consequence rating to the identified threats. In this session attended by the technology staff, members of upper management and the security manager, a rating scale and a simple mathematical formula:

$r = p \times c$

where r = risk, p = probability and c = consequence listed in table 8 was introduced to help the team assign the relative risk of each threat on the matrix. The complete matrix is reproduced in Appendix B.

Table 8. Probability X Consequence = Risk; used to prioritize the threat assessment matrix.

Probability		Consequence	
Negligible	1	Insignificant	1
Very Low	2	Minor	2
Low	3	Moderate	3
Medium	4	Major	4
High	5	Catastrophic	5

Table 9 takes the weighted average of each threat category recognized and based on these quantifiable observations, a report was prepared detailing the challenges that lay ahead of the

organization measured against the policies that would be required to support proper security for information systems operations.

Table 9. Critical Threat Matrix weighted for prioritization

Threat Scenario	Risk
3. Technical Software Failures or Errors	20
1. Deliberate Software Attack	15
4. Technical Hardware Failures or Errors	13
10. Deliberate Acts of Information Extortion	12
6. Deliberate Acts of Trespass	11
9. Compromises of Intellectual Property	11
2. Acts of Human Error or Failure	9
7. Deliberate Theft	8
5. Quality of Service Deviations from Service Providers	5
8. Forces of Nature	4
11. Deliberate Acts of Sabotage or Vandalism	4

Recommendations

The CCC technology department has conducted an internal system-wide study of network security concentrating on hardware vulnerabilities, logical control issues and policy development. Presently employees store policies, procedures, maps, diagrams and other operations related information on the local area data server. Set up information is transmitted electronically; even the process of ordering utilities by exhibitors for various events is handled by this network. Research in Chapter 2 demonstrates the severe consequences of a breach or data loss incident and serves as a warning to the CCC that improvements are warranted.

Considering the vulnerabilities, focus was placed on the threats facing the assets. Many of these threats are amplified by the vulnerabilities exposed in the asset definition phase. The complete matrix, Appendix B, identifies eleven threat categories and thirty five individual threat vectors that could potentially place the organization at risk. All thirty five vectors have been categorized with a probability and a consequence rating to place them in perspective relative to

the resources that should be expended on remediating them. Although certain access security controls over the CCC's automated systems were found to be in place, logical access security controls need to be strengthened to prevent unauthorized system access and to provide for corrective action if violations are detected. In addition, the organization needs to

The assessment to this point has revealed the likely occurrence of a catastrophic system failure in the near future. With the assessments complete recommendations are based on analysis of resistance, recognition and recovery. The goal of this analysis is to protect against a likely catastrophic service failure and due to the limited time involved in the guiding Scope of Work, only nine of the eleven threat categories will be covered.

Threat Scenario: Technical Software Failures or Errors

Resistance Strategy: Current – none

Recommended – Install Zenith Backup, virtual machine, off-site storage.

Recognition Strategy: Current – none

Recommended – Create the proper written backup and disaster recovery policies

Recovery Strategy: Current – none

Recommended – Setup planning and testing of disaster recovery to include 3 years support of a 250/500GB off-site storage application.

Threat Scenario: Deliberate software attack

Resistance Strategy: Current – none

Recommended – Purchase and install a patch management tool (WinINSTALL by Scalable).

Implement a written patch management procedure to increase administrator interaction with the target network.

Recognition Strategy: Current – none

Recommended –

1. Implement a vulnerability scan using the patch management software that reports changes to the system administrator on a daily basis.
2. Implement a virus scan using the Kaspersky Anti-Virus (AV) console that reports current AV events to the system administrator on a daily basis.

Recovery Strategy: Current – none

Recommended – Create a proper incident management procedure including a step by step troubleshooting and system recovery guide that includes a process for documentation and reporting to upper management upon remediation.

Threat Scenario: Technical Hardware Failures or Errors

Resistance Strategy: Current – none

Recommended –

1. Purchase a new server and install as the new domain controller removing all web filtering and print services from the unit.
2. Create a redundant signal path to the server.
3. Rebuild IBMSVR01 as a management server. Place the web filter and a monitoring and inventory application (Spiceworks) on this unit
4. Deploy the Kaspersky AV management console to the Alchemy server which is currently underutilized.

Recognition Strategy: Current – none

Recommended – Relocate the main machine to the PBX where it can be monitored by a technician.

Recovery Strategy: Current – none

Recommended – Create a proper incident management procedure including a step by step troubleshooting and system recovery guide to include auto redirect to the mirrored server in case of a main server failure. Include a process for documentation and reporting to upper management upon remediation.

Threat Scenario: Deliberate Acts of Information Extortion

Resistance Strategy: Current – none

Recommended – Review and implement all PCI recommendations for credit card security. Focus on a secure system development life cycle to make these changes part of the ongoing security operations; resist the tendency to create a security silo. Appendix D

Recognition Strategy: Current – none

Recommended –

1. See Threat Scenario deliberate software attack
2. Implement a policy of strong log management and regularly review Spiceworks, WinInstall and the Cisco ASA logs for evidence of intrusion.
3. Isolate the Parking pay stations on a separate VLAN to logically restrict access from the main network and limit the subnet to specific ports at that ASA.
4. Isolate the temperature control and display devices on their own subnets and limit the subnet to specific ports at that ASA.
5. Isolate the Security Camera LAN by removing all connections to the main subnet; remove all outside access to this network.

Recovery Strategy: Current – none

Recommended – See *Deliberate Software Attack*

Threat Scenario: Deliberate Acts of Trespass

Resistance Strategy: Current – none

Recommended –

1. Relocate the main machine to the PBX where it can be secured.
2. Lock down all production switches so no open ports are allowed.
3. Re-issue keys for all wiring closets to Technology. All other departments must check out a key which is kept and logged at security base.

Recognition Strategy: Current – none

Recommended – Implement a procedure to regularly examine all cable paths looking for non-CCC networking equipment or unauthorized wire installations.

Recovery Strategy: Current – none

Recommended – Setup planning and testing of disaster recovery by identifying backup service access points for temporary service should main services be stolen or disabled.

Threat Scenario: Compromises of Intellectual Property

Resistance Strategy: Current – none

Recommended –

1. See *Deliberate Acts of Information Extortion*
2. Review and recommend security changes to the document management database.

Recognition Strategy: Current – none

Recommended – See *Deliberate Acts of Information Extortion*

Recovery Strategy: Current – none

Recommended – See *Deliberate Software Attack*

Threat Scenario: Acts of Human Error or failure

Resistance Strategy: Current – none

Recommended – Document all cable installations and create specific as-built wiring maps to be made available to contracts as necessary.

Recognition Strategy: Current – none

Recommended – Add the Systems Administrator to all pre-planning meeting for all maintenance and construction projects. Review the areas affected and highlight all mission critical infrastructure to the project leaders prior to commencing any work.

Recovery Strategy: Current – none

Recommended – Setup planning and testing of disaster recovery by identifying backup service access points for temporary service should main services be disabled.

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls relating to the Colorado Convention Center's (CCC) information systems (IS). General overview procedures included interviews of department management and key personnel; evaluation of policies and procedures and an assessment of the information systems environment. Throughout the assessment it was apparent that CCC had not implemented processes to reasonably provide logical access control to ensure system data integrity. These failings impact the following threat scenarios:

Deliberate Software Attack

Deliberate Acts of Information Extortion

Deliberate Acts of Trespass

Compromises of Intellectual Property

For this reason the additional recommendations should be immediately implemented in the organization's logical structure and/or the human resources manual.

- Remove terminated user and department accounts.
- Develop a policy to notify the technology department of terminations and leaves of absences for any staff member with a computer account. The termination notification should be maintained in the human resources employee files and the technology manager will retain a copy for audit purposes
- Based upon CCC executive management's assessment of risk and established compliance requirements, CCC management should set a timetable for periodic review of user IDs to the list of authorized users. It is recommended that this occur at least semi-annually or as changes occur.
- CCC should begin utilizing all the security functions of Windows 2003. In order to do so, CCC should:
 - Establish and issue a Network Access form. Forms should be duplicate type pre-numbered; one copy maintained by Human Resources and one copy maintained by technology.
 - Create a unique user ID number incorporated into the user profile that can be cross-referenced by HR/Technology for future reconciliation.
- Re-issue user account names and passwords and set conditions that require at minimum:
 - That all users' logon privileges include renewal dates, minimum character lengths, and limited reuse abilities.

- That a condition exists so that all sever sessions log off after 10 minutes as required by the independent audit firm.
- CCC should immediately implement an Acceptable Use Policy. With input from the corporate policy makers, local human resources, legal counsel, technology and finance. The policy should:
 - Require the department head and user's signature along with the date they signed.
 - Be supplied to and signed by all new hires prior to network credentials being distributed.
 - Be reviewed as least annually to address changes in technology and the local operating environment, and whenever a new service is added to the network.
- Specifically, policies need to be written to ensure that user IDs and passwords will be active for only authorized personnel and that access privileges be deactivated in a timely manner for users no longer needing or authorization. Without proper system access restrictions, persons can gain unauthorized access to system data, and/or programs, thereby placing the CCC at risk of unauthorized use, which could lead to modifications to, and deletions or disclosure of critical or confidential data.

While these recommendations do not cover all threats, they do represent the ones of critical need. Once the system is properly configured and a high level of availability is reached, the other risks will be evaluated and the same process of recommendations based on analysis of

resistance, recognition and recovery will be applied. This process will be strengthened by introducing a Secure System Development Lifecycle.

Secure System Development Lifecycle

The primary goal of this research project has been to promote controlled system development. Small business in particular has been subject to a Wild West style of network creation whereby the business owners or system users clamor for the newest technology and then turn to their understaffed and overworked information technology (IT) team to “just get it done.” The IT team is left with the task of bringing new technology to the business and security is overlooked so the project can be delivered on time and under budget.

The application of a Secure System Development lifecycle (SSDLC) based on the rational unified process (RUP) accomplishes two goals; first, it engages management in the process, and second, it provides a clear framework for the IT team to work from. The use of RUP is not intended to create additional work, on the contrary like documentation; the use of RUP should be considered part of the work of developing the organization’s systems. As mentioned in the previous chapters, most small business networks have been designed, built, operated, and then secured only after a major incident has occurred. The focus to this point has been to match the research organization’s risk management activities with its current operational capabilities. The introduction of the SSDLC and the related policies and procedures, Appendix E, are aimed at maintaining risk management support for future initiatives.

The artifacts, Appendix B, created throughout this project lend themselves well to future development. To highlight this, as the project winds down, CCC has begun investigating a new digital document management system. The first question asked by the director of finance did not involve cost, rather, her concern was focused on how the existing system would be taken off line,

how effectively the existing data could be transferred into the new system and what exactly would be done to ensure that the existing data was properly secured and destroyed when the existing hardware was disposed of. In the NIST SDLC model, these risk management activities are strongly associated with Phase 5, Disposal. Clearly the organization is not disposing of all its systems and therefore, disposal factors favorably into the final phase of a RUP cycle, Transition. The project has been successful because management is now focused on information assurance and their decisions related to the handling of information assets. The general manager still doesn't need to understand the technical details, but by acknowledging that a transition is coming, he has increase the organizations level of information assurance.

Putting It All Together

Too often, the system administrator for a small business is overwhelmed when facing the possibility of implementing security let alone discussing information assurance within their organization. Chapter 4 provides an insight into how the methodology detailed in Chapter 3 was applied to the Colorado Convention Center (CCC)'s information systems to bring information assurance to the company. A review of the existing policies leads to the creation of policy and procedure aimed at guiding all subsequent efforts. The system administrator commits to creating these documents to enhance all future work. The next step is to understand what needs to be secured with a detailed inventory. This process should be documented because the information obtained will aid in every subsequent step. Once complete, the administrator should install tools that interact with the network. Inexpensive and even free, these tools are essential in understanding what is happening to the network.

Next the administrator should undertake a simple threat analysis. While many complex frameworks exist, with the input of key staff, this process can move quickly. The idea is not to

detail everything, but look for those areas of most critical vulnerability and remediate them. The administrator will be surprised to find that many of the tools are already in place. Security is simply a matter of crafting the correct policy and procedure to guide their use. With this in mind, the threat analysis then sheds light on where limited resources will make the most impact. The CCC for instance was critically exposed to data loss however the solution was readily available and at only \$5000.00 for three years, affordable and invaluable.

Finally, having brought the organization's risk management activities in line with the operational capabilities of the network, the administrator can institute a secure system development lifecycle that will continually address the organizations information operations in light of risk management activities. At the CCC, this included the creation of a set of guiding information assurance documents. The group brought together to brainstorm threat assessment became the Technology Review Board. Unconsciously, the CCC accepted the idea of information assurance, the technology staff now has management's support and access to a cross functional team tasked with looking at technology as a part of the organization, not just a tool used by the organization.

Chapter 5 – Project Conclusions

The objective of this thesis was to provide small business technology staff with a process to improve their level of information assurance. The resultant process was created to foster an organizational approach to system development that includes management by highlighting the operational nature of information in the corporate environment. The process provides decision-makers with the insight to aid in making the difficult and complex decisions regarding the balance between information assurance, operational availability and cost.

Summary of the Previous Chapters

The first chapter of this thesis discussed the current state of information systems in use in the corporate environment and the inherent risks associated with it. The ease of use and convenience of the Internet has led business to open their information systems to the Internet to take advantage of improved revenue options, data evaluation to aid decision makers and disseminate information to their employees, stakeholders and customers. However the internet was not originally designed with corporate or civilian use in mind. Security concerns began almost from the beginning. Today the corporate world relies heavily on interconnected information for their day-to-day operations and therefore needs to insure that the information contained on their networks is secure. IA is critical to the safety and well being of corporate structure as even one attack on a corporate network whether for mischievous end, corporate espionage or criminal intent, can destroy a company quickly leaving a trail of financial destruction

A literature review detailing IA and the tenants therein was presented in Chapter 2. Initially, a discussion of the Department of Defense DoD was presented to illustrate the importance IA plays in mission preparedness for the defense of the United States. A corollary

was drawn between the ways IA is used to prepare and defend the US from enemy attack to the need for IA in the corporate environment to protect the organization from the devastating consequences of a successful information system breach. Literature was then introduced that showed a strong relationship between high levels of corporate governance and increased return on investment and profitability. While business understands the need for strong information assurance strategies, particularly smaller organizations are paralyzed when faced with the myriad of changes and recommendations that surround these initiatives. Further research in Chapter 2 focused on the concrete evidence available leading to the conclusion that while developing a strong IA strategy is resource intensive, the inevitability of a major information related incident and its repercussions are far more expensive and can even prove fatal to the organization.

Working off of past research about information system design, the various available frameworks and tools, and management decision making, the conclusion is that breaking the impasse regarding improvement should be structured much like a business consultant would approach major process reorganization with a Statement of Work including a scope, deliverables, expectations and timelines. Chapter 3 then set down the methodology for creating the various artifacts, policies and architecture necessary to increase the subject organization's systems. Following closely the statement of work, the project sought to bring an information assurance strategy to the target organization. The results of this study, including findings, a discussion of the appropriate artifacts created and an analysis of the effects on the organization are presented in Chapter 4.

Appendix A is a statement of work created to guide the project. Appendix B samples the various artifacts created to examine the network and guide the organization. Appendix C includes an excel tool and a discussion of the organization's PCI compliance level. Appendix D

is a project timeline that demonstrates that this type of project is possible in other small businesses. Appendix E is the complete set of policies and procedures written to bring information assurance to the subject organization.

Project Objectives

As stated, the goal of this thesis was to provide small business with a systematic approach to applying information assurance strategies to networks where the technical tools were known and utilized, but no prior emphasis had been placed on the policies and procedures necessary to guide system development in a secure fashion. While most of the information presented is known to business leaders, the mere fact that small business lacks a dedicated information technology staff and often does not have the necessary resources to engage in strategy development leaves small business acutely exposed to security incidents. The case study was undertaken with the intention that it could be tailored to a variety of organizations. System administrators can view the results and gain an understanding that this type of effort is not impossible and that any effort undertaken will quickly increase the overall security stance of an organization and lead to a systematic approach for future development that ends the “patch to maintain functionality” mindset. While the project met the objectives, adequately addressing upper management concerns while improving the organization’s security, the project also highlighted the overwhelming amount of work implementing an information assurance strategy represents when applied to systems formally managed in an ad-hoc fashion. “Putting it all together”, Chapter 4, acknowledges that there are no quick fixes, but that doesn’t mean that introducing IA is impossible or not worth doing. A system administrator who begins down this path is already doing more than most small businesses and by doing so they are already introducing IA to their organization.

Future Research

Emerging vulnerabilities and rapid information technology development will keep pushing IA efforts as long as individuals' possess the desire to exploit a company for reasons of personal satisfaction, financial gain, business competition or international intelligence purposes. Therefore, the need for rapid IA strategy development and deployment will continue to evolve. While this study did not introduce revolutionary ideas, it is designed to highlight the fact that IA does have positive implications far beyond security that businesses should consider when facing an impasse related to how they should proceed.

One interesting theme repeated throughout both the research and implementation phase of this study was one of mismanagement or better, lack of understanding how to manage projects and people. While not unique to IT, it is of interest that many of the ideas and processes necessary to bring forth a well designed information assurance strategy require high levels of understanding. In fact, the premise of this study was that technologists know how the technology works, but they lack the business tools to effectively utilize them. Business leaders could be said to have the opposite problem, they understand the strategy at a high level but lack an understanding of how the tools work. Therefore while the idea of a business/IT misalignment is perhaps overused, it is not without merit. The use of design science is crucial to bridging this gap. Often the high level concepts of security and assurance were easier to picture than describe and management buy-in was more sincere when they could see the problem in question. While Rational Unified Process (RUP) details the types of artifacts that are useful to developers, more research is needed on what artifacts the developers can use to convey their efforts to management

Second, and related to the first, problems often arose when implementing the various pieces related entirely too how an individual learns and assimilates knowledge. Time after time the employees assisting in these efforts performed at less than the expected level of engagement either through misunderstanding, or misdirection. Again, this issue is not exclusive to IT; however it definitely impacts how the organization should present information assurance concepts to the staff. Though a system administrator can call together a training session and describe why security is important, each participant will take away portions of the information based on their initial level of understanding or involvement. The staff can be instructed that they shouldn't open email from unknown entities, but how well this advice is followed is based entirely their level of understanding or support of IT. Again, these are often high level concepts that require a designed approach. For individuals who don't routinely think of technology as more than a tool for accessing the internet or performing a particular job function on one particular application, artifacts that detail how and why something occurs may have more impact than any written policy or proctored class.

Conclusion

Small business is slowly awaking to the need for information assurance strategies to protect their information assets and improve their overall return on IT investment; yet they struggle to implement even rudimentary strategy in the face of all the other demands placed on their infinite resources. Overall small business, at best, is managing security in an inconsistent and superficial manner, applying tools, emphasizing technical control rather than taking a strategic approach that emphasizes the overall health of the organization. The work presented here provides organizations with an example of how to quickly move towards a strategic approach; in the end however, small business, as the many headline grabbing stories of exploit

continue to highlight, may not truly grasp the need for comprehensive information assurance strategies until after the trend towards increasing legislation has ensnared even the smallest organization.

References

- Ambler, S. W. (2005). *A manager's introduction to the rational unified process (RUP)*. Retrieved February 27, 2008, from <http://www.ambysoft.com/unifiedprocess/rupIntroduction.html>
- Andrew, C. (2005). The five ps of patch management: is there a simple way for business to develop and deploy an advanced security patch management strategy? *Computers and Security*, 24(no. 5), 362-363.
- Baker, W., H., Hylender, C. D., & Valentine, J. A. (2008). *2008 Data Breach Investigations Report*: Verizon Business Risk Team.
- Baker, W., H., & Wallace, L. (2007). Is Information Security Under Control?: Investigating Quality in Information Security Management, 5, 36-44.
- Beckhard, R., & Pritchard, W. (1992). *Changing the essence: the art of creating and leading fundamental change in organisations*. San Francisco: Jossey-Bass.
- Boehm, B. (2002). Get Ready for Agile Methods, with Care. *Computer*, 35(1), 64-69.
- Brown, R. H., & Browning, J. A. (2003). *SMBs: the biggest little outsourcing market in the world*: Gartner, Inc.
- Browning, J. A., & Pescatore, J. (2003). *Simple and affordable steps can improve SMB security postures*. Retrieved November 11, 2010, from <http://www.zdnet.com/news/simple-and-affordable-steps-can-improve-smb-security-postures/297961>
- California Office of Information Security and Privacy Protection. (2008). Information Security Assesment Tool for State Agencies.
- Canavan, S. (2006). *Information security policy - a development guide for large and small companies*. Retrieved July 1, 2009, from www.sans.org/.../policyissues/information-security-policy-development-guide -large-small-companies_1331

CDW. (2007). *Reality Check - A smart business-continuity strategy can offer maximum results at minimum cost*. Retrieved November 1, 2010, from

<http://webobjects.cdw.com/webobjects/media/pdf/solutions/business-continuity-operations/reality-check-business-continuity.pdf>

Cerny, J. (2009). *10 Questions on practical transformation: an interview with cook county's CIO*. Retrieved December 12, 2009, from

<http://blogs.techrepublic.com.com/10things/?p=1173>

Committee on National Security Systems. (2006). *NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY*. Retrieved December 31, 2010, from

http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf

Denver, C. a. C. o. (2008). *The city of denver is ISO 14001 certified*. Retrieved November 20, 2010, from

<http://www.denvergov.org/EnvironmentalManagementSystem/tabid/427949/Default.aspx>

Desmond, P. (2007). *Good policy makes for good security*. Retrieved October 31, 2008, from

<http://www.networkworld.com/news/2007/091007-your-take-inergy-automotive.html>

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *information systems Journal*, 16, 293-314.

Heiser, J. (2005). The perils of security patch management. *Network Security*, 2003(no. 7), 9-12.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Syst. J.*, 32(1), 4-16.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105.

- Hirsch, M. (2002). Making RUP agile, *OOPSLA 2002 Practitioners Reports*. Seattle, Washington: ACM.
- Iivari, J., Hirschheim, R., & Klein, H. K. (2001). A dynamic framework for classifying information systems development methodologies and approaches. *Journal of Management Information Systems*, 17(3), 179-218.
- IT Governance Institute. (2007). Cobit 4.1.
- Joint Chiefs of Staff. (1998). Joint Publication 3-13, Joint doctrine for Information Operations. In Department of Defense (Ed.). Washington: Pentagon.
- Kennedy, S. (2009). *HSBC Fined \$5.2 Million over lost data*. Retrieved October 20, 2010, from <http://www.marketwatch.com/story/hsbc-fined-52-million-over-lost-data?siteid=rss&rss=1>
- Longstaff, T. A., Ellis, J. T., Herman, S. V., Lipson, H. F., McMilliam, R. D., Pesante, L. H., et al. (1997). *Security of the internet*. Retrieved September 21, 2010, from http://www.cert.org/encyc_article/tocencyc.html
- Mercuri, R. T. (2002). Computer Security: Quality Rather than Quantity. *Communications of the ACM*, 45(10), 4.
- Miller, D. I. (2006, January 10). *Protect your business from computer intrusion*. Retrieved October 31, 2008, from http://www.cnet.com/4520-10192_1-6411728-2.html?tag=rb
- PCI Standards Council, L. (2008). *About the PCI Data Security Standard (PCI DSS)*. Retrieved June 7, 2009, from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Ponemon, L. (2009). *Fourth Annual US Cost of Data Breach Study*. Traverse City: Ponemon Institue, LLC.

- Price-Waterhouse-Coopers. (2008). *The heart of the matter, is your company experiencing compliance fatigue?* Retrieved April 2, 2009, from http://www.pwc.com/ca/eng/insol/publications/frcwf_0309.pdf
- Reyes, C. (2005). *What makes a good security policy and why is one necessary?* Retrieved October 31, 2008, from http://www.giac.org/certified_professionals/practicals/gsec/1691.php
- Ross, J., & Weill, P. (2004). IT governance: how top performers manage IT decision rights for superior results. *Harvard Business Review*.
- Salkever, A. (2000). *Who Pays When a Business Is Hacked?* . Retrieved September 21, 2010, from <http://www.businessweek.com/bwdaily/dnflash/may2000/nf00523d.htm>
- SANS Institute. (2009). *twenty critical controls for effective cyber defense: consensus audit*. Retrieved November 11, 2010, from <http://www.sans.org/critical-security-controls/>
- SANS Institute. (N.D.). *Information Security Policy Templates*. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>
- Seifert, J. W. (2002). The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned. *Government Information Quarterly*, 19, 225-242.
- Smith, G. (2009). Stay on top of a company's IT security needs. *Denver Business Journal*, pp. A-22.
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). *NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems*. Gaithersburg, MD: National Institute of Standards and Technology.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management.

Computers & Security, 23(5), 371-376.

Weaver, R. (2007). *Guide to network defense and countermeasures* (second ed.): Thompson

Learning, Inc.

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Syst. J.*, 26(3),

276-292.

Zelic, B., & Stahl, B. C. (N.D.). *The Influence of Realist Ontology on Technological Projects:*

The Case of Irish Voting. Retrieved August 9, 2010, from

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.106.4376>

Appendix A. Statement of Work

CCC Statement of Work (SOW)

Information Assurance and Network Management

STATEMENT OF WORK

As of 9/14/2009

1. Background

On January 1, 2009, Sam Fleming, Senior Facility Services Manager for the Colorado Convention Center (CCC), assumed the role of Systems Administrator as a result of a change in contractual obligation between Smart City Networks and the CCC.

This change included the assumption of managerial oversight for the technology department comprised of, at the time, one telephone technician and the responsibilities for managing the day-to-day operations of the CCC facility network backbone and all information technology (IT) assets.

Having managed the network for the past 9 months, the following observations have been made:

- 1) Lack of network continuity
- 2) Lack of network documentation
- 3) Lack of network policy and procedures
- 4) Little to no knowledge of the inner workings
- 5) No application documentation
- 6) No tracking of software license compliance
- 7) Slow and unreliable network segments
- 8) Slow desktop performance, possibly due to network

- 9) No consistency on desktop deployment
- 10) The need for subnets and VLAN configuration
- 11) PCI compliance concerns

The organic nature of system development and the lack of dedicated security staff along with the increasing prevalence of information attacks have left the CCC exposed to security vulnerabilities. While the CCC has many of the technical tools necessary to secure the network, it has failed to systematically develop organizational policies, controls and processes necessary to fully evaluate and optimize information security efforts, maintaining operational functionality while balancing implementation with the associated costs.

2. Objectives

The Senior Facility Services Manager must introduce information assurance into the organization in a way that quickly improves the security position of the organization while optimizing operational capability mindful of costs and introducing a process to guide further development and security improvement.

3. Scope

This SOW applies to all policies and procedures pertaining to all departments of the CCC that address the CCC information resources including networks, desktops, associated hardware and peripherals that cause traffic to traverse the facility network backbone from the Network Access Point (NAP) to the end-user machine.

Task Area 1. IT Asset Inventory

Task Area 2. IT Information Governance

Task Area 3. IT Infrastructure Architecture

Task Area 4. IT Operations and Maintenance

Task Area 5. IT Future Planning

4. Specific Tasks

4.1 Task 1 – IT asset inventory

4.1.1 - Subtask 1 – Conduct a physical verification of all CCC IT assets

- All assets must be identified by model, serial number and location and where applicable identify or install the appropriate City and County of Denver (CCoD) tracking number.
- For assets not currently identified on the City of Denver asset list, fill out and submit the appropriate Asset Inventory Form for proper identification and labeling.

4.1.2 - Subtask 2 – Install appropriate applications to allow for real time identification and asset tracking, to accommodate quarterly asset reviews by the CCC Finance department and yearly by the CCoD, based on asset connectivity and/or track current custodial privileges for assets not immediately connected to the CCC facility network backbone.

4.1.3 - Subtask 3 – Create and implement strong IT asset inventory and surplus policies by January 29, 2010.

4.2 Task 2 – IT information governance

4.2.1 - Subtask 1 – Create a risk assessment strategy, complete a baseline risk assessment and recommendations cognizant of current assets, budgetary constraints and policy inefficiency. This high level priority must be complete by November 27, 2009

4.2.2 - Subtask 2 – Create a managing policy to govern all IT related operations at the CCC by March 26, 2010.

4.2.3 - Subtask 3 – Create a format and process for strong policy creation and a process of adoption for new policy consistent with best practices of Information Assurance that allow for quantifiable results while not hampering operational quality, mindful of CCC and CCoD budget initiatives.

4.2.4 - Subtask 4 – Craft and institute a complete set of polices addressing PCI compliance requirements by June 15, 2010.

4.2.5 - Subtask 5 – Deliver to the, General Manager, a complete governance plan consisting of well documented policy, procedure and guidelines by December 31, 2010.

4.3 Task 3 – IT Infrastructure Architecture

4.3.1 - Subtask 1 – Create policy to govern all network related documentation by May 31, 2010.

- All facility network backbone connections must be documented.
- The configurations for all network gear including, but not limited to switches, routers and firewall must be documented in written form and stored in a minimum of 2 dissimilar locations to aid disaster recovery.
- All physical connections must be recorded and labeled; each wiring closet should be documented and accompanying maps provided in written form at the connection point to aid in troubleshooting.

4.3.2 - Subtask 2 – Create a network map as a visual representation of the network to aid in security and troubleshooting efforts.

4.3.3 - Subtask 3 – Audit all network gear and document and disable all unused or abandoned ports to enhance network security.

4.3.4 - Subtask 4 – Configure and install four separate subnets and a physical LAN for the following:

- Administrative Network
- Engineering (Temperature Control)
- Parking
- Digital Displays.
- Security (Cameras and Access control at Layer 2)

4.4 Task 4 – IT Operations and Maintenance

4.4.1 - Subtask 1 – Research and install a backup and recovery device that aids the technology department with routine document recovery requests, ensures data permanency and prepares the CCC for disaster recovery. Ideally this device will accommodate offsite storage for our three main production servers and will utilize strong encryption for all transited data. This priority task must be accomplished by January 31, 2010.

4.4.2 - Subtask 2 – Research and install network monitoring and help desk software to aid the technology department by notification of events in real time and allowing end-users to submit help requests in a systematic process by February 28, 2010.

4.4.3 - Subtask 3 – Craft and institute polices governing the proper use of monitoring tools at the CCC and create a procedure for end-user participation in a help desk system.

4.4.4 - Subtask 4 – Create policies and tools for effective and enforceable network monitoring whereby the department directors make the decisions as to the appropriate level of use or abuse of the systems with input from the Senior Facility Services Manger.

4.4.5 - Subtask 5 – Research and install network patch management software to aid the technology department by regularly scanning for vulnerabilities, updating end-user desktops with the proper patches in a time sensitive fashion and allowing for the rapid deployment of future desktops through appropriate image inventories.

4.5 Task 5 – IT Future Planning

4.5.1 - Subtask 1 – Prepare and present a secure system development lifecycle (SSDLC) to the general manager and upper management that creates a system for ongoing cooperation and systemic thinking when approaching system development while ensuring the highest level of security to operational capability possible.

4.5.2 - Subtask 2 – SSDLC will include timelines for current policy and process review.

4.5.3 - Subtask 3 – SSDLC will include timelines for Risk Assessments.

4.5.4 - Subtask 3 – SSDLC will include timelines for documentation review.

5. Period of Performance

Performance of this project will commence 5 days after authorization (or September 18, 2009) whichever is earlier. Start and completion expectation are set forth below.

Start/Completion

5.1 Task 1 – IT asset inventory

5.1.1 - Subtask 1 – September 18, 2009/October 3, 2009

5.1.2 - Subtask 2 – September 18, 2009/February 26, 2010

5.1.3 - Subtask 3 – December 7, 2009/January 29, 2010.

5.2 Task 2 – IT information governance

5.2.1 - Subtask 1 –September 18, 2009/November 27, 2009

5.2.2 - Subtask 2 –January 18, 2010/March 26, 2010.

5.2.3 - Subtask 3 – September 18, 2009/December 31,2010

5.2.4 - Subtask 4 – September 18, 2010/June 15, 2010.

5.2.5 - Subtask 5 – September 18, 2009/December 31, 2010.

5.3 Task 3 – IT Infrastructure Architecture

5.3.1 - Subtask 1 – April 5, 2010/May 31, 2010.

5.3.2 - Subtask 2 – September 18, 2009/December 30, 2009

5.3.3 - Subtask 3 – May 31, 2010/June 3, 2010

5.3.4 - Subtask 4 – June 1, 2010/December 31, 2010

5.4 Task 4 – IT Operations and Maintenance

5.4.1 - Subtask 1 –September 18, 2009/January 31, 2010.

5.4.2 - Subtask 2 –September 18, 2009/February 26, 2010.

5.4.3 - Subtask 3 – September 18, 2009/February 26, 2010

5.4.4 - Subtask 4 –March 1, 2010/December 31, 2010

5.4.5 - Subtask 5 –January 4, 2010/March 26, 2010

5.5 Task 5 – IT Future Planning

5.5.1 – All Subtasks – September 18,2009/December 31, 2010

6. Inspection and Acceptance Criteria

The Senior Facility Services Manager will report the results of the technical and procedural impact and make recommendations as to what portions to keep augment or abandon. The general manager of the CCC will have final authority over the business relevance of these deliverables and final decision authority to implement policy and procedures that impact departments outside of technology. This decision process will involve the various department directors, human resources and legal counsel where required.

Appendix B. Sample Artifacts

Appendix B showcases some of the artifacts used to document the target system. Each of these artifacts is combined with others in binders that present an audit of the procedural and operational capabilities of the target system.

Threat Assessment Matrix

Scenario	Threat	Probability		Consequence		Risk
1. Deliberate Software Attack						15
TS1.1	OS system compromise	Medium	4	Moderate	3	12
TS1.2	Application Level Compromise	Medium	4	Minor	2	8
TS1.3	Vulnerable to direct network attack	High	5	Major	4	20
TS1.4	Malware ie. Virus, trojan, keystroke logger infection	Medium	4	Moderate	3	12
TS1.5	Using SA for all database application accounts	High	5	Major	4	20
TS1.6	Telnet services Running	High	5	Major	4	20
2. Acts of Human Error or Failure						9
TS2.1	Physical or logical upstream issue creates DOS	High	5	Minor	2	10
TS2.2	Damage/destruction to server	Medium	4	Moderate	3	12
TS2.3	Improper change management	High	5	Insignificant	1	5
3. Technical Software Failures or Errors						20
TS3.1	Non-current Data Restoration	High	5	Moderate	3	15
TS3.2	Restoration failure	High	5	Catastrophic	5	25
4. Technical Hardware Failures or Errors						13
TS4.1	Power Supply Failure	High	5	Minor	2	10
TS4.2	Drive Failure	High	5	Catastrophic	5	25
TS4.3	NIC failure	Medium	4	Moderate	3	12
TS4.4	Switch failure	Low	3	Moderate	3	9
TS4.5	Server Room HVAC failure	Low	3	Moderate	3	9
5. Quality of Service Deviations from Service Providers						5
TS5.1	Loss of Internet Connectivity for an extended period	Low	3	Minor	2	6
TS5.2	Loss of Power for an extended period	Low	3	Insignificant	1	3
6. Deliberate Acts of Trespass						11
TS6.1	Direct compromise	Medium	4	Moderate	3	12
TS6.2	Compromise through unused accounts	Low	3	Moderate	3	9
TS6.3	Compromise through unknown accounts	Very Low	2	Moderate	3	6
TS6.4	Compromise through Administrator Account	Medium	4	Major	4	16
TS6.5	Attack from the Internet	Medium	4	Minor	3	12
7. Deliberate Theft						8

TS7.1	Theft	Very Low	2	Catastrophic	5	10
TS7.2	Data Loss through employees	Low	3	Minor	2	6
8. Forces of Nature						4
TS8.1	Earthquake	Negligible	1	Catastrophic	5	5
TS8.2	Fire	Negligible	1	Major	4	4
TS8.3	Flood	Negligible	1	Major	4	4
9. Compromises of Intellectual Property						11
TS9.1	Reveal financial information	Medium	4	Major	4	16
TS9.2	No recovery from Breach	Very Low	2	Moderate	3	6
10. Deliberate Acts of Information Extortion						12
TS10.1	Credit Card Personal Account Number (PAN) breach	Low	3	Major	4	12
TS10.2	Reveal Personally identifiable Information (ID Theft)	Medium	4	Moderate	3	12
11. Deliberate Acts of Sabotage or Vandalisim						4
TS11.1	Disgruntled employee Sabotage Physical	Negligible	1	Major	4	4
TS11.2	Disgruntled employee Sabotage Logical	Negligible	1	Moderate	3	3

Sample Switch Configuration

Table 10. Switch Configuration

10.201.200.208 – E2 – Parking	J9279A Configuration Editor;	Created on release #Y.11.01
hostname "Parking"	snmp-server contact "sfleming@somewhere.com"	snmp-server location "E2"
interface 2	disable	exit
interface 4	disable	exit
interface 6	disable	exit
interface 7	disable	exit
interface 8	disable	exit
interface 9	disable	exit
interface 10	disable	exit
interface 11	disable	exit
interface 12	disable	exit
interface 13	disable	exit
interface 14	disable	exit
interface 15	disable	exit
interface 16	disable	exit
interface 17	disable	exit
interface 18	disable	exit
interface 19	disable	exit
interface 20	disable	exit
interface 21	disable	exit
interface 22	disable	exit
interface 23	disable	exit
ip default-gateway 10.201.200.1	snmp-server community "public" Unrestricted	vlan 1
name "DEFAULT_VLAN"	no ip address	no untagged 1-24
exit	vlan 601	name "Admin"
untagged 1-24	ip address 10.201.200.208 255.255.255.0	exit
fault-finder bad-driver sensitivity high	fault-finder bad-transceiver sensitivity high	fault-finder bad-cable sensitivity high
fault-finder too-long-cable sensitivity high	fault-finder over-bandwidth sensitivity high	fault-finder broadcast-storm sensitivity high
fault-finder loss-of-link sensitivity high	fault-finder duplex-mismatch-HDx sensitivity high	fault-finder duplex-mismatch-FDx sensitivity high
primary-vlan 601	password manager	password operator

This is a representative standard of the switch configuration confirming that all unused ports are disabled, only the appropriate VLANs are present on the switch and the vendor supplied defaults have been changed.

Current CCC Architecture

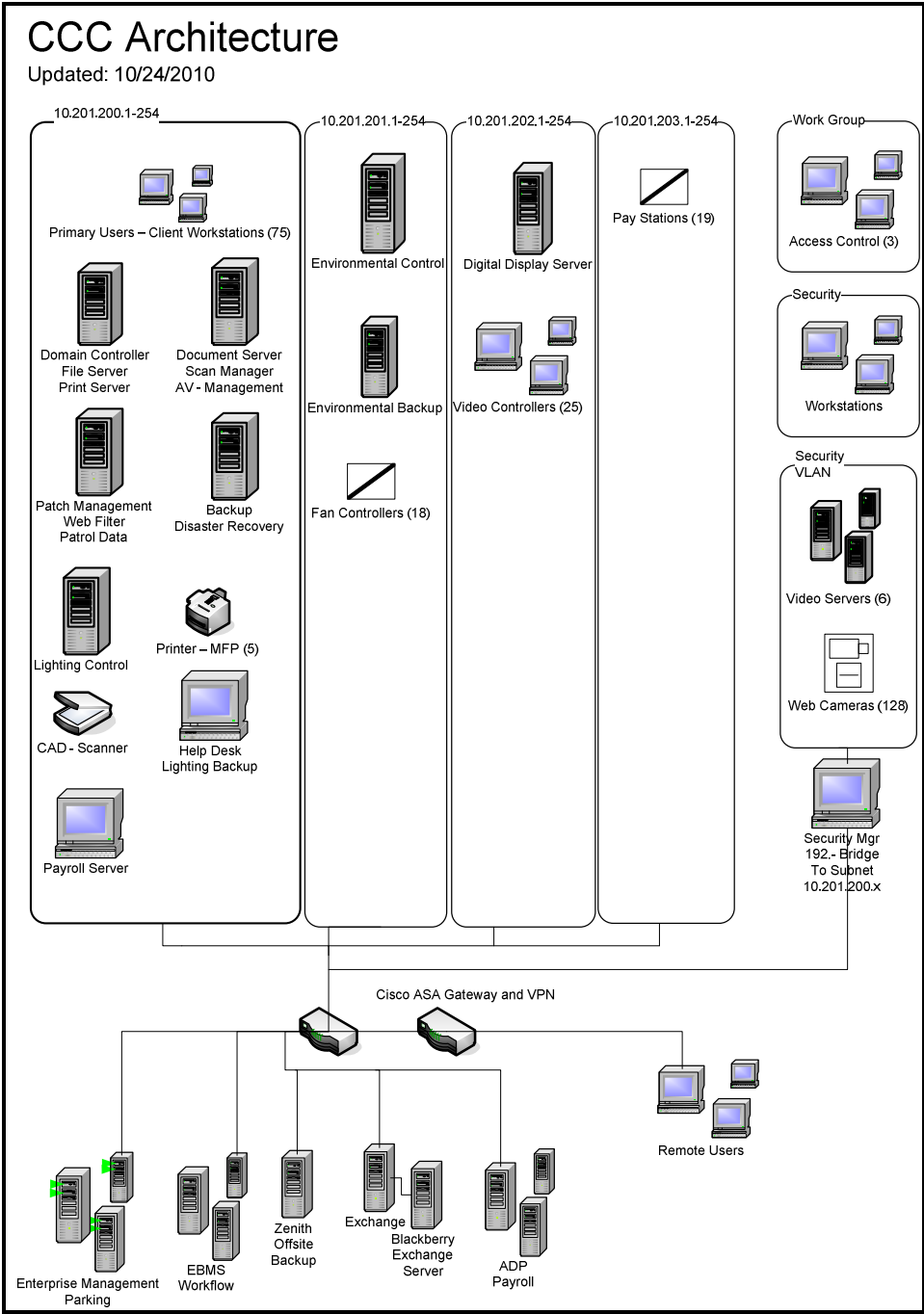


Figure 10. Post project logical architecture

Physical Network Map

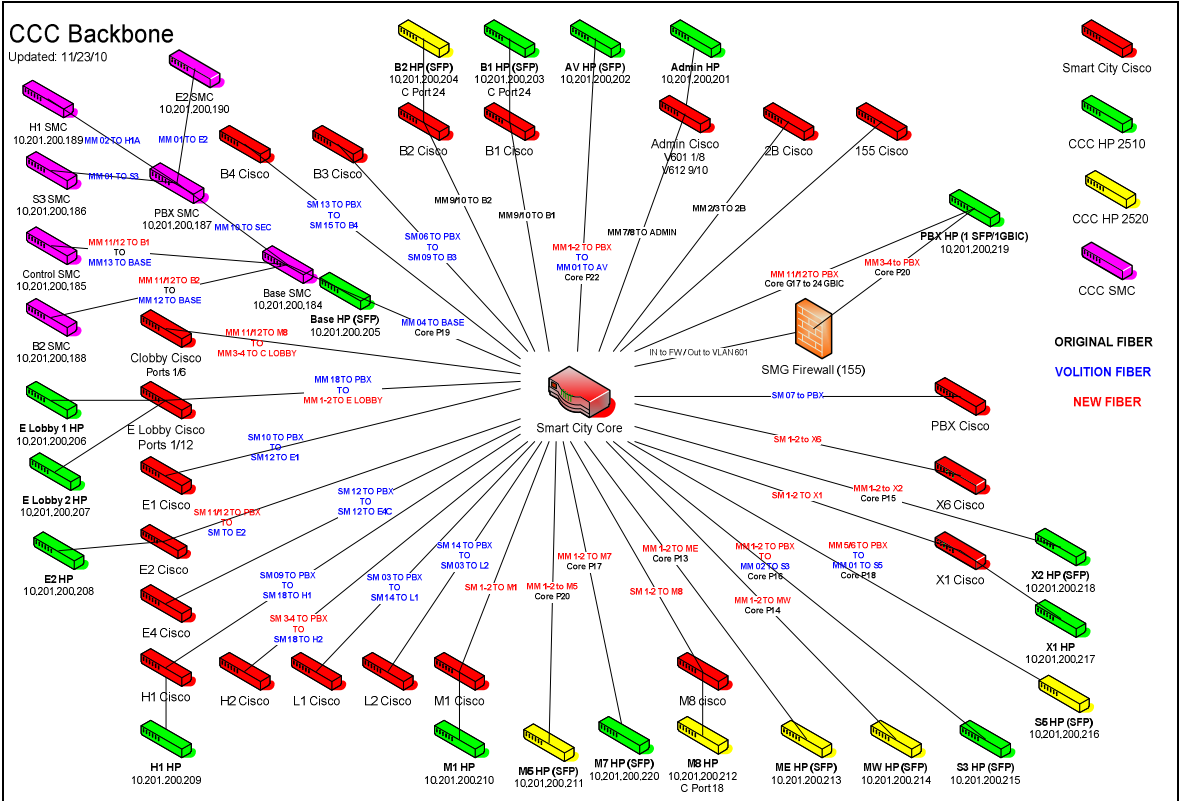


Figure 11. Current Network Topology showing the relationship between the ISP network and CCC supplied equipment crucial for understanding network bottlenecks.

Sample New Employee Access Memo**SMG – CCC Facility Services**

Memo

To: John Doe
From: Sam Fleming, Senior Facility Services Manager
CC: Debbie Welsh, Director of Event Management
Date: 11/29/10
Re: Welcome to the Colorado Convention Center

DESKTOP

Your computer has been added to the company's data server. You now have access to the corporate drive and your department's shared drive. To log onto your computer follow instruction below.

LOGON

User Name: John.Doe
PSW: «PASSWORD» 0 is a zero not capital O
Computer: CCCdomain

PASSWORD

When you log onto your computer for the first time you will be prompted to change your password.

Your password must meet the following requirements:

The password must be at least seven (7) characters long.

The password must contain characters from at least three of the following four categories:

- English uppercase characters (A - Z)
- English lowercase characters (a - z)
- Base 10 digits (0 - 9)
- Non-alphanumeric (For example: !, \$, #, or %)

The password may not contain three or more characters from your account name.

Passwords change every 90 days and can't be reused for one year.

OUTLOOK

Your name has been added to the company's email server. You now have access to outlook. To log onto your outlook account follow instruction below. To get to your email click on the Outlook icon.

User Name: somewheremsg\jdoe

PSW: jdoe5\$%

REMOTE

You have access to your email from offsite computers. To access your email remotely follow instructions below.

Open Browser Link: <https://outlook.somewhere.com/xyz>

User Name: jdoe

PSW: jdoe5\$%

Please do not share your passwords with anyone.

Please call Jane Doe at 555-444-5555 if you have any problems logging on.

Group Policy Screenshots

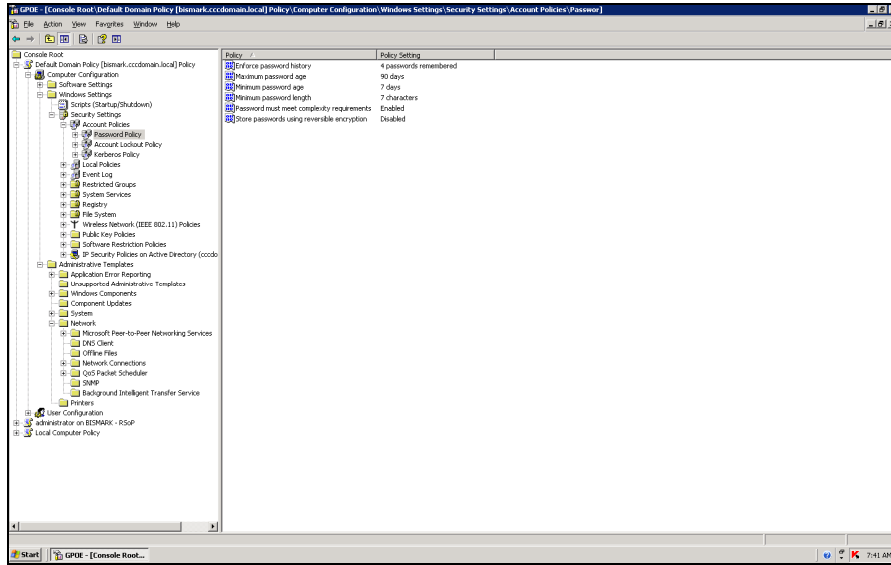


Figure 12. Group Policy settings enforcing password strength and 90 day reset.

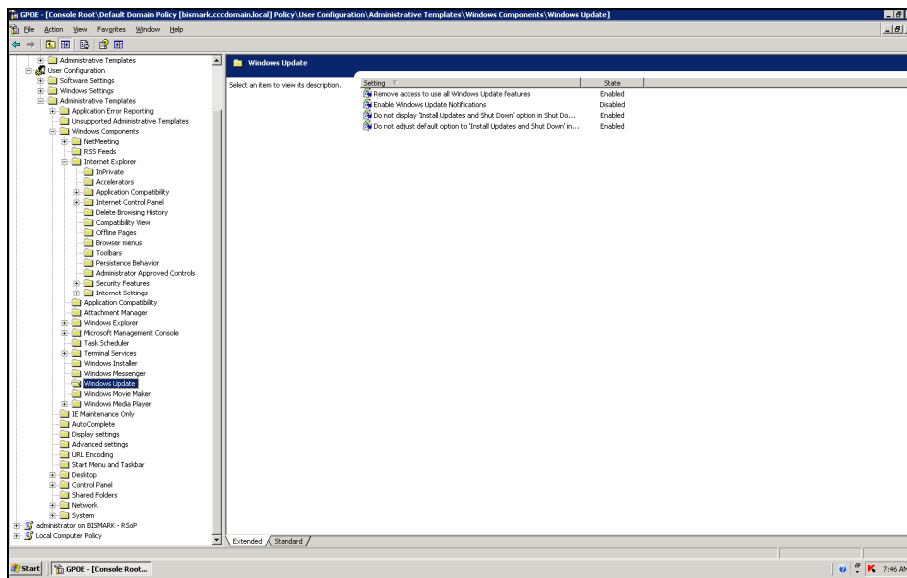


Figure 13. Windows update disabled by Group Policy allows WinINSTALL to manage.

Logical Computer Audit

Active Directory		WinINSTALL		Kaspersky	
Name	Type	Name	Agent	Name	Version
ALCHEMY	Computer	ALCHEMY	Agent Running	ALCHEMY	8.0.2090
		bismark	Agent Running	BISMARCK	8.0.2090
BS1	Computer	BS1	Agent Running	BS1	8.0.2090
BS2	Computer	BS2	Agent Running	BS2	8.0.2090
B55	Computer	B55	Agent Running	B55	8.0.2090
CCC88	Computer	CCC88	Agent Running	CCC88	8.0.2090
ELEC1	Computer	ELEC1	Agent Running	ELEC1	8.0.2090
ELEC2	Computer	ELEC2	Agent Running	ELEC2	8.0.2090
EM1	Computer	EM1	Agent Running	EM1	8.0.2090
EM10	Computer	EM10	Agent Running	EM10	8.0.2090
EM11	Computer	EM11	Getting status...	EM11	8.0.2090
EM12	Computer	EM12	Agent Running	EM12	8.0.2090
EM25	Computer	EM25	Agent Running	EM25	8.0.2090
EM4	Computer	EM4	Agent Running	EM4	8.0.2090
EM5	Computer	EM5	Agent Running	EM5	8.0.2090
EM6	Computer	EM6	Agent Running	EM6	8.0.2090
EM7	Computer	EM7	Agent Running	EM7	8.0.2090
EM8	Computer	EM8	Agent Running	EM8	8.0.2090
EM9	Computer	EM9	Agent Running	EM9	8.0.2090
ENDURANCE	Computer	Endurance	Agent Running	ENDURANCE	8.0.2090
ENG1	Computer	ENG1	Agent Running	ENG1	8.0.2090
ENG2	Computer	ENG2	Agent Running	ENG2	8.0.2090
ENG3	Computer	ENG3	Agent Running	ENG3	8.0.2090
ES2	Computer	ES2	Getting status...	ES2	8.0.2090
ES3	Computer	ES3	Agent Running	ES3	8.0.2090
ES4	Computer	ES4	Getting status...	ES4	8.0.2090
ES5	Computer	ES5	Agent Running	ES5	8.0.2090
ES6	Computer	ES6	Agent Running	ES6	8.0.2090
ETIME-SVR	Computer	ETIME-SVR	Agent Running	ETIME-SVR	8.0.2090
EXEC4	Computer	EXEC4	Agent Running	EXEC4	8.0.2090
EXECUTIVE1	Computer	EXECUTIVE1	Agent Running	EXECUTIVE1	8.0.2090
EXECUTIVE2	Computer	EXECUTIVE2	Agent Running	EXECUTIVE2	8.0.2090
EXECUTIVE3	Computer	EXECUTIVE3	Agent Running	EXECUTIVE3	8.0.2090
EXECUTIVE5	Computer	EXECUTIVE5	Agent Running	EXECUTIVE5	8.0.2090
FINANCE1	Computer	Finance1	Agent Running	FINANCE1	8.0.2090
FINANCE2	Computer	FINANCE2	Agent Running	FINANCE2	8.0.2090
FINANCE4	Computer	FINANCE4	Agent Running	FINANCE4	8.0.2090
FINANCE5	Computer	FINANCE5	Agent Running	FINANCE5	8.0.2090
FINANCE6	Computer	FINANCE6	Agent Running	FINANCE6	8.0.2090
GROUNDS1	Computer	GROUNDS1	Agent Running	GROUNDS1	8.0.2090
GS2	Computer	GS2	Agent Running	GS2	8.0.2090
GS4	Computer	GS4	Agent Running	GS4	8.0.2090
HK1	Computer	HK1	Agent Unavailable	HK1	8.0.2090
HK2	Computer	hk2	Getting status...	HK2	8.0.2090
HK3	Computer	HK3	Agent Running	HK3	8.0.2090
HK4	Computer	HK4	Agent Running	HK4	8.0.2090
HR1	Computer	HR1	Agent Running	HR1	8.0.2090
HR2	Computer	HR2	Agent Running	HR2	8.0.2090
HR3	Computer	HR3	Agent Running	HR3	8.0.2090
LUTRON-27086	Computer	LUTRON-27086	Agent Running	LUTRON-27086	8.0.2090
LUTRON-27086-B	Computer	LUTRON-27086-B	Agent Running	LUTRON-27086-B	8.0.2090
LUTRONSHOP	Computer	LUTRONSHOP	Agent Running	LUTRONSHOP	8.0.2090
LUTTRON	Computer	LUTTRON	Agent Running	LUTTRON	8.0.2090
MADDOX	Computer	MADDOX	Agent Running	MADDOX	8.0.2090
OPS1	Computer	OPS1	Agent Running	OPS1	8.0.2090
OPS2	Computer	OPS2	Agent Running	OPS2	8.0.2090
OPS3	Computer	OPS3	Agent Running	OPS3	8.0.2090
PK1	Computer	PK1	Agent Running	PK1	8.0.2090
PK2	Computer	PK2	Getting status...	PK2	8.0.2090
SALES02	Computer	SALES02	Agent Running	SALES02	8.0.2090
SALES1	Computer	SALES1	Agent Running	SALES1	8.0.2090
SALES2	Computer	SALES2	Agent Running	SALES2	8.0.2090
SALES4	Computer	SALES4	Agent Running	SALES4	8.0.2090
SALES5	Computer	SALES5	Agent Running	SALES5	8.0.2090
SALES6	Computer	SALES6	Agent Running	SALES6	8.0.2090
SALES7	Computer	SALES7	Agent Running	SALES7	8.0.2090
SEC1	Computer	SEC1	Agent Running	SEC1	8.0.2090
SEC2	Computer	SEC2	Agent Running	SEC2	8.0.2090
SEC4	Computer	SEC4	Agent Running	SEC4	8.0.2090
TECHNOLOGY1	Computer	TECHNOLOGY1	Agent Running	TECHNOLOGY1	8.0.2090
TECHNOLOGY3	Computer	TECHNOLOGY3	Agent Running	TECHNOLOGY3	8.0.2090
THING3	Computer	THING3	Agent Running	THING3	8.0.2090
THING4	Computer	THING4	Getting status...	THING4	8.0.2090
THING6	Computer	THING6	Getting status...	THING6	8.0.2090
THING7	Computer	THING7	Agent Running	THING7	8.0.2090
TITANIC	Computer				
TS1	Computer	TS1	Agent Running	TS1	8.0.2090
TS2	Computer	TS2	Agent Running	TS2	8.0.2090

Figure 14. Manual audit of Active Directory, WinINSTALL and Kaspersky

Figure 14 confirms that all machines are accounted for in all systems. The DC is not accounted for in AD and the Zenith BDR is not managed in Kaspersky or WinINSTALL. This confirms all machines are managed properly.

Appendix C. PCI Assessment Tool

In response to this alarming increase in the theft of payment card information from individual merchants and processors, the major credit card companies including Visa, Master Card, and American Express, collaborated on the development of the Payment Card Industry Data Security Standard (PCI-DSS). The Colorado Convention Center (CCC) accepts debit and credit card payments to process service orders requests both online and via printed sheets. Merchant-eSolutions, the payment card clearing house for the CCC has requested that the organization become PCI-DSS compliant by July 1, 2011.

In general, merchants are required to comply with PCI-DSS regardless of their transaction volume. Each Level has its own Self-Assessment Questionnaire (SAQ) designated as SAQ A through D; CCC has been identified as a Level 2 merchant and thus is required to answer SAQ-B or Imprint Machines or Stand-alone Dial-out Terminals Only, no Electronic Cardholder Data.

CCC uses Ungerboeck Systems International (USI)'s Event Business Management Systems (EBMS) as the main Enterprise Resource Planning software. Contained within this application is a service work order processing component that allows the Exhibitor Services staff to process orders and accept payment via credit card. By hosting the application on USI's servers, the burden of logical control shifts to the vendor. As an application service provider (ASP), USI is responsible for certifying to PCI that their systems and software are PCI compliant. CCC in contracting USI required that they show proof of certification and abide by the CCC ASP Security Standards document contained in Appendix E.

In recognition of the ad hoc style of network development CCC has experienced and the fact that no formal risk assessment has ever been conducted on CCC IT assets, a modification of

the California Office of Information Security and Privacy Protection (COISPP) Information Security Assessment Tool for State Agencies was proposed.

Key to this tool is a scoring system where questions are rated from “not implemented = 0” to “fully implemented = 4”. By applying this scoring system to the 226 questions in the 12 specific requirements of the six categories of PCI the user can quickly establish their organization’s ability to meet compliance and identify the areas of specific concern where the organization should focus its efforts. While the SAQ provided by PCI is limited to yes/no responses, the tool developed based on COISPP efforts is quantitative and thus allows a high degree of initial assessment. The goal, based on the results of the tool survey, is to provide a more nuanced understanding of the security and control deficiencies in the organization’s systems. All questions of the full assessment were considered, however policy and procedures were adjusted only for those required of CCC under questionnaire B.

Based on this analysis, the following Policies and Procedures, Appendix E, were accepted by CCC:

1. Requirement 4.1 – Crafted a Data Sensitivity Policy
2. Requirement 7.1 and 9.6-9.10.1 – Reviewed and corrected deficiencies in the logical controls of EBMS so that only Finance and Exhibitor Services could access Credit Card information. Confirmed that all Credit Card information is classified as confidential automatically upon entry by field within EBMS.
3. Requirement 12 – Crafted the following policies:
 - a. ISPP-02 requires that all security information be reviewed at least annually.
 - b. ISU-01 defines the proper use of CCC applications generically and addresses misuse and abuse.

- c. ISPP-04 defines incident handling and response
- d. ISU-01 establishes yearly reviews of security policies for all staff
- e. ITN-01 establishes the technology department's responsibilities to document all ASPs and to monitor their compliance regularly.

Table 11. PCI compliance tool

Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to completion = 3; Fully Implemented = 4

Requirement	Description	Score	Action Plan	Remediation Date
1	Install and maintain a firewall configuration to protect data	3.17		
2	Do not use vendor-supplied defaults for system passwords and other security parameters	4.00		
3	Protect stored cardholder data	3.40		
4	Encrypt transmission of cardholder data across open, public networks	4.00		
5	Use and regularly update anti-virus software or programs	4.00		
6	Develop and maintain secure systems and applications	4.00		
7	Restrict access to cardholder data by business need-to-know	3.67		
8	Assign a unique ID to each person with computer access	3.15		
9	Restrict physical access to cardholder data	3.62		
10	Track and monitor all access to network resources and cardholder data	3.10		
11	Regularly test security systems and processes	1.56		
12	Maintain a policy that addresses information security for employees and contractors	1.52		

Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to completion = 3; Fully Implemented = 4 **SCORE**

Build and Maintain a Secure Network

Requirement 1	Description	SCORE
1.1	Install and maintain a firewall configuration to protect data Do established firewall and router configuration standards include the following?	
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall and router configurations?	2
1.1.2	Current network diagrams with all connections to cardholder data, including any wireless networks?	4

1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	4
1.1.4	Description of groups, roles, and responsibilities for logical management of network components?	3
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure?	2
1.1.6	Requirement to review firewall and router rule sets at least every six months?	0
1.2	Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder data environment as follows:	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?	4
1.2.2	Secure and synchronize router configuration files?	4
1.2.3	Include installation of perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from wireless environment into the cardholder data environment?	4
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder environment?	
1.3.1	Is a DMZ implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder environment?	4
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	4
1.3.3	Are direct routes prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	4
1.3.4	Are internal addresses prohibited from passing from the Internet into the DMZ?	4
1.3.5	Is outbound traffic restricted from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ?	4
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?	0
1.3.7	Is the database placed in an internal network zone, segregated from the DMZ?	4
1.3.8	Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space?	4
1.4	Has personal firewall software been installed on any mobile and/or employee-owned computers with direct connectivity to the Internet which are used to access the organization's network?	2

TOTAL SCORE FOR REQUIREMENT 1	3.17
--------------------------------------	-------------

Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1	Are vendor-supplied defaults always changed before installing a system on the network?	4
2.1.1	a) Are defaults for wireless environments connected to the cardholder data environment or transmitting cardholder data changed before installing a wireless system?	4
	B) Are wireless device security settings enabled for strong encryption technology for authentication and transmissions?	4
2.2	a) Have configuration standards been developed for all system components?	4
	b) Do these standards address all known security vulnerabilities and are they consistent with industry-accepted system hardening standards?	4
	c) Do controls ensure the following?	
2.2.1	Is only one primary function implemented per server?	4
2.2.2	Are all unnecessary and insecure services and protocols disabled?	4
2.2.3	Are system security parameters configured to prevent misuse?	4
2.2.4	Has all unnecessary functionality been removed?	4
2.3	Is all non-console administrative access encrypted?	4
2.4	If you are a shared hosting provider, are your systems configured to protect each entity's hosted environment and cardholder data?	4
TOTAL SCORE FOR REQUIREMENT 2		4

Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to completion = 3; Fully Implemented = 4 **SCORE**

Protect Cardholder Data		
Requirement 3	Protect stored cardholder data	
3.1	a) Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and/or regulatory purposes?	4
	b) is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?	3
3.2	<i>Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)?</i>	
3.2.1	Do not store the full contents of any track from the magnetic stripe. This data is alternatively called full track, track 1, track 2 and magnetic-stripe data?	4
3.2.2	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	4
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	4
3.3	Is the PAN masked when displayed?	0

3.4	Is PAN at a minimum, rendered unreadable anywhere it is stored by any of the following approaches? - One-way hashes based on strong cryptography - Truncation - Index Tokens and pads - Strong cryptography with associated key management processes and procedures	4
3.4.1	If disk encryption is used: a) Is logical access managed independently of native operating system access control mechanisms? b) Are decryption keys independent of user accounts?	4
3.5	Are cryptographic keys used for encryption of cardholder data protected against both disclosure and misuse?	4
3.5.1	Is access to cryptographic keys restricted to the fewest number of custodians necessary?	4
3.5.2	Are cryptographic keys stored securely, and in the fewest possible locations and forms?	4
3.6	a) Are all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, fully documented and implemented? b) Do they include the following?	4
3.6.1	Generation of Strong cryptographic keys	4
3.6.2	Secure cryptographic key distribution	4
3.6.3	Secure cryptographic key storage	4
3.6.4	Periodic changing of cryptographic keys: - As deemed necessary and recommended by the associated application. - At least annually.	0
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	1
3.6.6	Split knowledge and establishment of dual control of cryptographic keys.	4
3.6.7	Prevention of unauthorized substitution of cryptographic keys	4
3.6.8	Requirement for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	0

TOTAL SCORE FOR REQUIREMENT 3		3.4
--------------------------------------	--	------------

Requirement 4	Encrypt transmission of cardholder data across open, public networks	
4.1	Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?	4
4.1.1	Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	4
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies?	4

TOTAL SCORE FOR REQUIREMENT 4		4
--------------------------------------	--	----------

Scoring: Not Implemented = 0; Planning Stages = 1;
 Partially Implemented = 2; Close to completion = 3;
 Fully Implemented = 4

SCORE

Maintain a Vulnerability Management Program			
Requirement 5		Use and regularly update anti-virus software or programs	
5.1		Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?	4
	5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?	4
5.2		Are all anti-virus mechanisms current, actively running and capable of generating audits?	4
		TOTAL SCORE FOR REQUIREMENT 5	4
Requirement 6		Develop and maintain secure systems and applications	
6.1		a) Do all system components and software have the latest vendor-supplied security patches installed?	4
		b) Are critical security patches installed within one month of release?	4
6.2		a) Is there a process to identify newly discovered security vulnerabilities?	4
		b) Are configuration standards updated as required by PCI-DSS requirement 2.2 to address new vulnerability issues?	4
6.3		a) Are software applications developed in accordance with PCI-DSS and based on industry best practices, and do they incorporate information security throughout the software development lifecycle?	4
		b) Do controls ensure the following?	
	6.3.1	Testing of all security patches and system software configuration changes before deployment, including but not limited to the following:	4
	6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	4
	6.3.1.2	Validation of proper error handling	4
	6.3.1.3	Validation of secure cryptographic storage	4
	6.3.1.4	Validation of secure communications	4
	6.3.1.5	Validation of proper role-based access control	4
	6.3.2	Separate development/test and production environments?	4
	6.3.3	Separation of duties between development/test and production environments?	4
	6.3.4	Production Data (Live PANs) are not used for testing or development?	4

6.3.5	Removal of test data and accounts before production systems become active?	4
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers?	4
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability?	4
6.4	(a) Are change control procedures followed for all changes to system components?	4
	(b) Do procedures ensure the following?	4
6.4.1	Documentation of impact?	4
6.4.2	Management sign-off by appropriate parties?	4
6.4.3	Testing of operational functionality?	4
6.4.4	Back-out procedures?	4
6.5	a) Are all web applications (internal and external, and including web administrative access to application) developed based on secure coding guidelines such as Open Web Application Security Project Guide?	4
	b) Is prevention of common coding vulnerabilities covered in software development processes, including the following?	
6.5.1	Cross-side scripting (XSS)?	4
6.5.2	Injection flaws, particularly SQL injection? Also consider LDAP and Xpath injection flaws as well as other injection flaws.	4
6.5.3	Malicious file execution?	4
6.5.4	Insecure direct object references?	4
6.5.5	Cross-site request forgery (CSRF)?	4
6.5.6	Information leakage and improper error handling?	4
6.5.7	Broken authentication and session management?	4
6.5.8	Insecure cryptographic storage?	4
6.5.9	Insecure communications?	4
6.5.10	Failure to restrict URL access?	4
6.6	For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods? * Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or * Installing a web-application layer firewall in front of public-facing web applications.	4

	TOTAL SCORE FOR REQUIREMENT 6		4.00
--	--------------------------------------	--	-------------

Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to completion = 3; Fully Implemented = 4

**Implement
Strong**



Access Control Measures Requirement 7		Restrict access to cardholder data by business need-to-know	
	7.1	a) Is access to system components and cardholder data limited to only those individuals whose jobs require such access?	4
	7.1.1	b) Do access limitations include the following Restriction of access rights to privileged user IDs least privileges necessary to perform job responsibilities?	4
	7.1.2	Assignment of privileges based on individual personnel's job classification and function?	4
	7.1.3	Requirement for an authorization form signed by management that specifies required privileges?	1
	7.1.4	Implementation of an automated access control system?	4
	7.2	a) Is an access control system in place for the systems with multiple users to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed?	4
		b) does this access control system include the following:	
	7.2.1	Coverage of all system components?	4
	7.2.2	Assignment of privileges to individuals based on job classification and function?	4
	7.2.3	Default "deny all" setting?	4

TOTAL SCORE FOR REQUIREMENT 7			3.67
--------------------------------------	--	--	-------------

Requirement 8		Assign a unique ID to each person with computer access	
	8.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	4
	8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? ?? Password or pass phrase ?? Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	4

8.3	Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	4
8.4	Are all passwords rendered unreadable during transmission and storage on all system components using strong cryptography (Defined in PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms)?	4
8.5	Are proper user authentication and password management controls in place for non-consumer users and administrators on all system components, as follows?	4
8.5.1	Are addition, deletion, and modification of user IDs, credentials, and other identifier objects controlled?	4
8.5.2	Is user identity verified before performing password resets?	4
8.5.3	Are first-time passwords set to a unique value for each user and must each user change their password immediately after the first use?	4
8.5.4	Is access for any terminated users immediately revoked?	4
8.5.5	Are inactive user accounts removed or disabled at least every 90 days?	4
8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?	4
8.5.7	Are password procedures and policies communicated to all users who have access to cardholder data?	4
8.5.8	Are group, shared, or generic accounts and passwords prohibited?	4
8.5.9	Must user passwords be changed at least every 90 days?	1
8.5.10	Is a minimum password length of at least seven characters required?	1
8.5.11	Must passwords contain both numeric and alphabetic characters?	4
8.5.12	Must an individual submit a new password that is different from any of the last four passwords he or she has used?	1
8.5.13	Are repeated access attempts limited by locking out the user ID after no more than six attempts?	1

8.5.14	Is the lockout duration set to a minimum of 30 minutes or until administrator enables the user ID?	1
8.5.15	If a session has been idle for more than 15 minutes, must the user re-enter the password to re-activate the terminal?	2
8.5.16	Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)	4

	TOTAL SCORE FOR REQUIREMENT 8	3.15
--	--------------------------------------	-------------

Requirement 9	Restrict physical access to cardholder data	
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	4
9.1.1	(a) Do video cameras or other access-control mechanisms monitor individual physical access to sensitive areas? Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder Data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.	4
	(b) Is data collected from video cameras reviewed and correlated with other entries?	4
	[c] Is data from video cameras stored for at least three months, unless otherwise restricted by law?	4
9.1.2	Is physical access to publicly accessible network jacks restricted?	4
9.1.3	Is physical access to wireless access points, gateways, and handheld devices restricted?	4
9.2	Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible? For purposes of this requirement, an "employee" refers to full-time and part-time employees, temporary employees and personnel, And contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	4
9.3	Are all visitors handled as follows:	
9.3.1	Authorized before entering areas where cardholder data is processed or maintained?	4

9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as no employees?	4
9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration?	4
9.4	[a] Is a visitor log in use to maintain a physical audit trail of visitor activity?	4
	[b] Are the visitor's name, the firm represented, and the employee authorizing physical access documented on the log?	4
	[c] Is visitor log retained for a minimum of three months, unless otherwise restricted by law?	4
9.5	(a) Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?	4
	(b) Is this location's security reviewed at least annually?	4
9.6	Are all paper and electronic media that contain cardholder data physically secure?	4
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	4
	(b) Do controls include the following:	
9.7.1	Is the media classified so it can be identified as confidential?	4
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately tracked?	1
9.8	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is Distributed to individuals)?	1
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?	4
9.9.1	(a) Are inventory logs of all media properly maintained?	2
	(b) Are media inventories conducted at least annually?	2
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:	4
9.10.1	Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	4
9.10.2	Is electronic media with cardholder data rendered unrecoverable so that cardholder data cannot be Reconstructed?	4

TOTAL SCORE FOR REQUIREMENT 9 3.62

Scoring: Not Implemented = 0; Planning Stages = 1;
 Partially Implemented = 2; Close to completion = 3;
 Fully Implemented = 4

SCORE

Regularly monitor and Test Networks

Requirement 10

	Track and monitor all access to network resources and cardholder data	
10.1	Is a process in place to link all access to system components (especially access done with administrative privileges such as root) to each individual user?	4
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:	
10.2.1	All individual user accesses to cardholder data?	4
10.2.2	All actions taken by any individual with root or administrative privileges?	4
10.2.3	Access to all audit trails?	4
10.2.4	Invalid logical access attempts?	3
10.2.5	Use of identification and authentication mechanisms?	3
10.2.6	Initialization of the audit logs?	2
10.2.7	Creation and deletion of system-level object?	2
10.3	Are the following audit trail entries recorded for all system components for each event:	
10.3.1	User identification?	1
10.3.2	Type of event?	1
10.3.3	Date and time?	1
10.3.4	Success or failure indication?	1
10.3.5	Origination of event?	1
10.3.6	Identity or name of affected data, system component, or resource?	1
10.4	Are all critical system clocks and times synchronized?	4
10.5	(a) Are audit trails secured so they cannot be altered?	4
	(b) Do controls ensure the following?	
10.5.1	Is viewing of audit trails limited to those with a job-related need?	4
10.5.2	Are audit trail files protected from unauthorized Modifications?	4
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	4
10.5.4	Are logs for external-facing technologies written onto a log server on the internal LAN?	4

10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	1
10.6	Are logs for all system components reviewed at least daily? Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	1
10.7	Is audit trail history retained for at least one year, with a minimum of three months' history immediately available for analysis (for examples, online, archived, or restorable from backup)?	4

	TOTAL SCORE FOR REQUIREMENT 10	3.10
--	---------------------------------------	-------------

Requirement 11	Regularly test security systems and processes	
11.1	Is the presence of wireless access points tested for by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use?	4
11.2	Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)? Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal Staff.	3
11.3	(a) Is external and internal penetration testing performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a Web server added to the environment)?	1
11.3.1	(b) Do these penetration tests include the following: Network-layer penetration tests?	

	11.3.2	Application-layer penetration tests?	1
11.4	(a)	Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises?	1
	(b)	Are all intrusion-detection and prevention engines kept up-to date?	1
11.5	(a)	Is file-integrity monitoring software deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and	1
	(b)	Is the software configured to perform critical file comparisons at least weekly?	1
		Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).	

TOTAL SCORE FOR REQUIREMENT 11	1.56
---------------------------------------	-------------

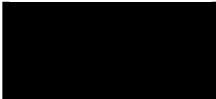

Scoring: Not Implemented = 0; Planning Stages = 1;
 Partially Implemented = 2; Close to completion = 3;
 Fully Implemented = 4

SCORE

Maintain an Information Security Policy Requirement 12

		Maintain a policy that addresses information security for employees and contractors	
12.1		Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:	
	12.1.1	Addresses all PCI DSS requirements?	
	12.1.2	Includes an annual process to identify threats and vulnerabilities, and which results in a formal risk Assessment?	
	12.1.3	Includes a review at least once a year and updates when the environment changes?	1
12.2		Are daily operational security procedures developed that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)?	1

12.3	(a) Are usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all employees and contractors?	2
	(b) Do these usage policies require the following?	
12.3.1	Explicit management approval?	2
12.3.2	Authentication for use of the technology?	2
12.3.3	A list of all such devices and personnel with access?	3
12.3.4	Labeling of devices with owner, contact information, and purpose?	2
12.3.5	Acceptable uses of the technologies?	3
12.3.6	Acceptable network locations for the technologies?	1
12.3.7	List of company-approved products?	1
12.3.8	Automatic disconnect of sessions for remote-access Technologies after a specific period of inactivity?	4
12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use?	4
12.3.10	When accessing cardholder data via remote-access Technologies, does the policy specify the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media?	2
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?	1
12.5	Are the following information security management responsibilities assigned to an individual or team?	
12.5.1	Establishing, documenting, and distributing security policies and procedures?	1
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	0
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	0
12.5.4	Administering user accounts, including additions, deletions, and modifications?	4
12.5.5	Monitoring and controlling all access to data?	3
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?	2
12.6.1	Are employees educated upon hire and at least annually?	0
12.6.2	Are employees required to acknowledge at least annually that they have read and understood the company's security policy and procedures?	0

12.7	Are potential employees (see definition of “employee” at 9.2 above) screened prior to hire to minimize the risk of attacks from internal sources? For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	3
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?	4
12.8.1	A list of service providers is maintained.	4
12.8.2	A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	3
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.	4
12.8.4	A program is maintained to monitor service providers’ PCI DSS compliance status.	2
12.9	Has an incident response plan been implemented to include the following in preparation to respond immediately to a system breach?	
12.9.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	0
	(b) Does the plan address, at a minimum:	
	?? Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum	0
	?? Specific incident response procedures	0
	?? Business recovery and continuity procedures	0
	?? Data back-up processes	0
	?? Analysis of legal requirements for reporting compromises	0
	?? Coverage and responses of all critical system components	0
	?? Reference or inclusion of incident response procedures from the payment brands	0
12.9.2	Is the plan tested at least annually?	0
12.9.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	4
12.9.4	Is appropriate training provided to staff with security breach response responsibilities?	0
12.9.5	Are alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems included?	0

12.9.6 Is process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments? 0

			TOTAL SCORE FOR REQUIREMENT 12	1.52
--	--	--	---------------------------------------	-------------

Appendix D. Project timeline

To fully understand the challenges a small organization faces, the following project timeline is presented.

November 2009

- Network Analysis begins and the threat matrix is established.

December 2009

- Network Analysis complete and high level recommendations presented

January 2010

- Purchase of Zenith BDR, Kaspersky AV
- Realization that main server is extremely compromised

February 2010

- Begin upgrade with installation of BDR and Kaspersky AV on secondary server. True scope of deferred maintenance evolves and a new server is requisitioned to become new DC.
- Install Spiceworks network management tools and help desk, begin tracking incidents.
- First full-scale Kaspersky scan takes three days and results in major system reconfigurations. Know Trojans discovered on a majority of machines.
- Develop AV Policy
- Develop support policy and procedures.

March 2010

- Develop User review
- Develop Acceptable use policy

- Develop Websense policy

March 10, 2010

- While attempting first full system state backup, the existing DC experiences a full crash, Spiceworks and Websense data lost. Data recovery is spotty and the Symantec recovery agent has not kept track of system drivers etc. AD is impossible to recover and must be rebuilt from scratch.
- Users associate service issues with server issues. Plan for orderly migration is disrupted and all users need to be migrated in a marathon four day period.

April 2010

- Continue attempts to consolidate the needs of the users with proper access control, Network layout upgrade in full swing.
- Discover a payroll program that is not supported by the new hardware and not documented. Move payroll program to standalone machine.
- Discover that Kaspersky is creating access issues based on ownership permissions requiring all data to be assigned new ownership.

May 2010

- Begin exploring Group policy and data structure long days keeping existing data in production.
- Develop Password Policy
- Switches all identified and ports on existing VLAN.
- Network cable identification begins.
- All infrastructure is documented.

May 1-2, 2010

- Install new DC. Realize that all existing workstations SID are corrupt and must be rebuilt to join to new DC, as a result DC must be taken down and rebuilt.
- Password policy put in place and enforced logically by group policy.
- All users given new strength enhanced credentials and required to change passwords every 90 days.

June 2010

- Reconfigured server receives WinInstall and Spiceworks , however Websense cannot be added due to unknown issues.
- First major vulnerability scan uncovers 3700 vulnerabilities on the 81 machines. 45% of desktops lack winXP SP3 and critical patches dating to 2003 missing on most machines. First round of updating takes two days, 22 machines fail requiring each to be investigated individually. Process uncovers major differences in configuration between machines and user related failures because each user is administrator of their own machine.

July 2010

- Successfully transition EBMS database to USI, however some reports don't convert. Two weeks of remediation required, no testing time was allowed due to corporate decision of a hard turn down.
- New VLANs created and ASA upgraded. Admin subnet has security to enter all subnets; additional subnets have no permission on any other subnet.
- Lose remote access due to stronger ASA configuration. Remote users previously configured with Public IPs at ASA with no encryption. Now require Cisco 5.0 remote client and full VPN

- Successfully move parking and video displays onto their respective subnets without a major hitch.
- Parking Passes PCI compliance.
- Determine that Video displays need AV installed. Security Cameras to follow in October and Temperature control in December.

August 2010

- Discover that WinInstall was preconfigured to install with SQL 2005 Light. Install licensed version of SQL 2005 to operate interoperate with Websense.
- Conflict between ODBC's causes server crash. Maintenance server taken offline and rebuilt.
- Loss of all Wininstall data and Spiceworks data.
- Move Spiceworks to standalone machine to safeguard this application in the future.
- Hardware Audit by the City of Denver
- Develop IT asset inventory and disposal policy

September 2010

- Apply Websense policy as redefined by GM.
- Second round of major patches brings all machines current but requires multiple restarts and causes system disruptions minimized only by a three-day weekend.
- Major virus scan uncovers additional spamware clients requiring three desktops to be taken offline and rebuilt. Cause traced to infected removable data storage.

September 28, 2010

- Finalize GPO but go too far and lock administrator out of DC and MMCs.
- Utilize BDR to restore GPO on server

- Confusion caused by these over restrictive changes prompts the GM to request a proper change management policy with notification and reporting requirements.

October 2010

- Spiceworks beginning to show effectiveness. Ticketing system becoming accepted reducing response time and creating a feeling of good will. Error reporting uncovering configuration errors that reduce system latency. Network mapping showing major improvement, rouge machines identified and open ports disabled.
- WinInstall used to test and patch all vulnerabilities.
- Software inventory proceeding. Identifying many unnecessary items, outdated, unneeded and non-approved.
- Video Camera Architecture finally fully understood and video system brought to functioning.
- Patrol system added to management server based on utilization and software policy.

November 2010

- Scope of work signed off and all new policies sent to corporate for legal review. Anticipate acceptance by January 30, 2011.
- Begin investigating a new digital document management system using RUP. Time to implementation measured in just weeks due to the amount of prior work. Security is baked into the development rather than added later.

December 2010


- Engineering completes the transition of all controls to the new subnet. The admin subnet is now free of miscellaneous equipment and the technology department begins to MAC lock the system.

- Wininstall is working well, all devices are identified, events are being recorded and remediated which increases network efficiency and work ticket system has brought order to the once hectic technology department
- Kaspersky and WinInstall continue to have minor performance issues. Most are traced back to overly restrictive group policy. Changes are documented and monitored for impact and rolled back if necessary.

January 2011

- Full scale disaster recovery drill planned for February 1, 2011. Incremental tests have shown positive results, the data is safe and the server state is backing up nightly. The test, known to the Senior Facility Services Manager and upper management only, will allow the remaining technology team to experience a disaster in real time. This event will take place after hours, but the team is in expecting to work on side projects.
- The test will simulate a full data loss and the team will along with the Zenith BDR hardware will be evaluated for effectiveness.
- Revisions to policies presented in appendix E have been requested by corporate. These are to be delivered for final review by March 1, 2011.

Appendix E. Policies and Procedures

	
Policies and Procedures	
Department: Executive	Issued By:
Topic: Information Governance Policy	Procedure Number: ISPP-1
Effective Date: Pending	Status: DRAFT 12/1/10

Scope

This policy applies to the high-level governance (as detailed in the four bullet points of the policy statement) of all SMG / Colorado Convention Center (CCC) information, regardless of the location or format of the information. It also applies to all individuals encountering CCC information, regardless of the user’s role or affiliation. It does not extend to the special governance requirements that may be necessary for certain information types such as research information, intellectual property, health information, etc. It also does not apply to personal data that may reside on CCC information technology resources as a consequence of incidental personal use of those resources.

Reason for Policy

Information represents a valuable asset that is critical to the operation of the CCC. The value of information as an institutional resource is increased through its widespread and appropriate use, and its value is diminished through misuse, misinterpretation, or unnecessary restrictions on its access. In addition, various legal, regulatory, and contractual terms require the CCC to document and employ reasonable safeguards to protect information. Therefore principles of information assurance (IA) must be articulated and applied uniformly to maintain and increase the value and

to promote the confidentiality, availability, and integrity of the information while promoting its widespread and appropriate use.

The over-arching goals of the SMG / Colorado Convention Center's Information Security and Privacy Program and associated policies and standards are to maintain CCC's viability, both reputational and operational, as a premier public assembly facility destination; supporting its mission of education (teaching and learning), research, and engagement (outreach and service); and to guide the conduct of CCC business.

Policy Statement

Employees and associated vendors of the CCC are to be able to efficiently and effectively execute and enhance their duties through facilitated access and informed use of information, in accordance with applicable laws and regulations, CCC policies, and aspects of prudent stewardship.

The Technology Review Board (TRB), appointed by the General Manager of the Colorado Convention Center, has overall responsibility for coordinating high-level policies, standards, guidelines, and procedures needed to facilitate use of CCC information. Activities of the TRB include, but are not limited to:

- Establishing and maintaining roles and responsibilities for individuals and groups who are charged with various aspects of managing information throughout its entire life cycle.
- Creating and maintaining a program for the classification of information in order to facilitate access, and to establish appropriate confidentiality, integrity, availability, use control, and accountability expectations for information commensurate with each classification level.

- Articulating and maintaining coordinated information management standards in order to promote widespread, appropriate, efficient, and effective use of information.
- Developing and maintaining priorities and strategies to educate users of information on their responsibility to adhere to established policies, standards, guidelines and procedures, and supporting documents.

Procedures

The General Manager has assigned oversight of the TRB to the Assistant General Manager who, in consultation with the General Manager (as needed) and with other stakeholders, will strive for appropriate and broad representation on the committee and account for the changing needs of the facility.

In addition to setting high-level guidance related to the use and management of CCC information, the TRB will collaborate and coordinate with other CCC departments that have more granular responsibility for certain information types (e.g., financial information, digital copy rights property, health information, etc.) in order to identify common standards for all types of information.

The TRB will also follow the policy development process of the CCC Information Policy Office in the development of policy. Other documentation such as standards and guidelines will be available for stakeholder review, comment, and feedback for at least 30 days prior to adoption.

Questions and exception requests can be made to the TRB, and appeals can be directed to the General Manager or Human Resources Manager.

Technology Review Board Membership

- Assistant General Manager
- Director of Finance
- Director of Event Management

- Director of Operations
- Director of Sales
- Senior Facility Services Manager
- Human Resources Manager
- Accounting Manager
- Security Manager

Sanctions

CCC will handle reports of misuse and abuse of information and information technology


resources in accordance with existing policies and procedures issued by appropriate departments.

Failure to comply with CCC information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access,); the individual's employment up to and including immediate termination of employment in accordance with applicable CCC disciplinary policy and/or civil or criminal prosecution. See policy ISPP-02, Misuse and Abuse of Information Technology Resources, for more detail.

Reference

Indiana University. (2009). Information governance. Retrieved January 22, 2010, from

<http://informationpolicy.iu.edu/policies/ISPP-25>

	
Policies and Procedures	
Department: Human Resources	Issued By:
Topic: Misuse and Abuse of Information Technology Assets	Procedure Number: ISPP-02
Effective Date: Pending	Status: Draft 12/1/10

Scope

This policy applies to all users of SMG / Colorado Convention Center (CCC) information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from within the facility or from a remote connection.

Rationale

Taxpayers, Lessees, exhibitors and attendees providing sources of funding that support information technology resources at the CCC expect that these assets will be used in a lawful manner and in support of the facility's mission of hosting opportunities for teaching, learning, and civic engagement.

Policy Statement

CCC will handle misuse and abuse of information technology resources in accordance with existing policies and procedures issued by appropriate departments. The university may also take legal action against individuals or entities involved in misuse or abuse of CCC information technology resources.

Procedures

Reporting:

Reports of apparent misuse or abuse of CCC information technology resources are to be made to the human resources, the appropriate department director, manager or executive administrator of an employee.

Where violations of law are alleged, the reporting party must also contact Human Resources. Human resources will consult with the Security Manager regarding the involvement of the Denver Police Department.

Suspension or termination of access:

The Senior Facility Services Manager or technology department staff may temporarily suspend or block access to an account when it reasonably appears necessary to do so in order to protect the integrity, security, and functionality of CCC computing resources, or to protect the organization from liability.

Access to CCC technology resources may be removed immediately given a written request from Human resources, the appropriate department director, manager or executive administrator of an employee. Reasons for removal may include, but are not limited to, the following: the individual is terminated for cause and there is concern for safety of systems or data; there is reasonable belief that the individual to whom the account is assigned has perpetrated or is involved in illegal activities or activities that violate CCC policy.

The Senior Facility Services Manager or a member of the Technology staff may disable access unilaterally if processes in an assigned account are causing or reasonably appear likely to cause damage to systems or data or serious service degradation for other users. Except when prohibited by law, inappropriate, or impractical, the technician will notify the involved individual prior to disabling the computer account. Where prior notification is not permitted, appropriate, or practical, the technician will make all efforts to notify the involved individual afterward in a timely manner. Unless other policies are invoked, access will be restored as soon as possible after the removal of the threat.

Technical Investigation:

The CCC Technology Review Board (TRB) will coordinate technical investigation and computer forensics for complaints of misuse or abuse of CCC information technology resources.

Investigations must not commence until Human Resources has been notified and time has been allotted for legal review. All investigations must comply with applicable law, and CCC policies and procedures.

Disciplinary Process:

Reports of misuse or abuse are normally resolved through established CCC disciplinary policies and procedures applicable to the employee. CCC may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. SMG corporate counsel and or the City Attorney of the City and County of Denver, the Denver Police Department and other law enforcement officials as appropriate shall address misuse or abuse of CCC resources by persons not affiliated with the facility.

Definitions**Information technology resources**

includes all CCC-owned computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared single-user or multi-user; they may be stand-alone or networked; and they may be stationary or mobile.

Misuse or abuse

are uses of CCC information technology resources that violate existing laws or CCC policies and


Misuse or abuse also includes the sharing or transferring of an individual's CCC accounts, including network ID, password, or other access codes that allow them to gain access to CCC information technology resources, with one or more other persons.

CCC Policies

Departments may have issued policies and standards governing the appropriate use of information technologies deployed specifically to support their specific activities. The Senior Facility Services Manager may have issued service-level polices and standards governing the appropriate use of specific services and applications. In order to understand and adhere to these requirements, users of these resources are responsible for consulting with the appropriate department or technology staff.

Reference

Indiana University. (2010). Misuse and Abuse of Information Technology Resources. Retrieved July 31, 2010, from <http://informationpolicy.iu.edu/policies/IT02>

 <p>Policies and Procedures</p>	
Department: Technology	Issued By: Sam Fleming
Topic: Application Service Provider Security Standards	Procedure Number: ISPP-03
Effective Date: 7/1/10	Status: Active

Overview

This document defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by The Colorado Convention Center (CCC). As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. CCC will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. CCC approval of any given ASP resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by CCC.

Scope

This document can be provided to ASPs that are either being considered for use by CCC, or have already been selected for use.

Responding to These Standards

The CCC is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Bad: "We have hardened our hosts against attack."

Good: "We have applied all security patches for Windows 2000 as of 8/31/2000 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to The Colorado Convention Center."

Bad: "We use encryption."

Good: "All communications between our site and The Colorado Convention Center will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

Standards**General Security**

1. The CCC reserves the right to periodically audit the application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.
2. The ASP must provide a proposed architecture document that includes a full network diagram of the application environment, illustrating the relationship between the environment and any other relevant networks, with a full data flowchart that details where CCC data resides, the applications that manipulate it, and the security thereof.

3. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

Physical Security

1. The equipment hosting the application for CCC must be located in a physically secure facility, which requires badge access at a minimum.
2. The infrastructure (hosts, network equipment, etc.) hosting CCC application must be located in a locked cage-type environment.
3. CCC shall have final say on who is authorized to enter any locked physical environment, as well as access the CCC application infrastructure.
4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for CCC.
5. CCC finance department requires that the ASP disclose their ASP background check procedures and results prior to CCC granting approval for use of an ASP.

Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means CCC application environment must use separate hosts, and separate infrastructure.
2. How will data go between CCC and the ASP? Keep in mind the following two things:
 - a. If CCC will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the CCC extranet.

- b. If, on the other hand, the data between CCC and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between CCC and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.
2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.
3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?
4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.
5. The ASP must provide information on their password policy for application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
6. CCC cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

Web Security

1. At CCC discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).
2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP (active server page) technology.
3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)
4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.
5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

Cryptography


1. The application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the application infrastructure

must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.
3. Preferred hashing functions are SHA-1 and MD-5.
4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.
5. If the application infrastructure requires PKI, please contact CCC Senior Facility Services Manager for additional guidance.

Reference:

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: SDLC and Change Management Policy	Procedure Number: ITN-5
Effective Date: 10/1/10	Status: Active

PURPOSE:

To promote a controlled environment around change management procedures for the Colorado Convention Center (CCC)’s IT systems and applications. The Change Management Procedures are designed to provide an orderly process in which changes to CCC infrastructure are requested and approved prior to the installation or implementation of the change. This policy should be periodically reviewed and updated, where necessary, to reflect changes in the technology environment.

SCOPE:

The policies and procedures within this document apply to CCC IT Systems and applications. The scope of this document is limited to development and changes to 1) applications 2) database structures and 3) IT infrastructure (including hardware, system software and configurations).

RESPONSIBILITIES:

The Technology department is responsible for executing this SDLC and submitting the resulting artifacts to the Director of Finance. This submission consists of the names and signatures of the participants, and the actual artifacts. (Artifacts are the documents, diagrams, etc., that are created as a result of following the SDLC.)

The technology department and the other involved CCC operational departments must jointly consider this SDLC as an integral part of their overall project plan.

The Director of Finance is responsible for enforcing this Policy.

PROCEDURES:

1. An information system development typically undergoes several lifecycles, corresponding to its creation and subsequent upgrades. Each such development lifecycle constitutes a project. Such projects continue until the underlying technology ages to the point where it is no longer economical to invest in upgrades and the application is considered for either continued as-is operation or retirement. The CCC SDLC defines a standard methodology for the creation and upgrades of software applications. It also addresses routine maintenance that occurs as part of the operational management of an application and retirement.
2. The CCC SDLC is a subset of the IBM Rational Unified Process. This SDLC is structured in two dimensions Phases and Disciplines.
3. This SDLC is sequential with respect to the Phases, while iterative, or incremental, with respect to the Disciplines. More specifically, each Phase ends with a go/no-go decision on whether to proceed to the next Phase. Each Discipline ends with a set of deliverables encapsulating the results of a specific activity, which is incrementally refined over multiple iterations of the Phases. While it may appear that a one-to-one correspondence exists between the elements of the Phases and the elements of the Disciplines, this is absolutely not the case. In reality, designing, coding, and testing continue incrementally across multiple Phases.

A. REQUESTS:

Requests for all system development work, including break/fix, continuous improvements, data scripts, and projects will be documented in Spiceworks. Each ticket will include:

- Initiator's name and contact information;
- Date/Time of notification;
- Description of requested change and/or problem;
- Priority set by the IT Personnel;
- Category of the change and/or problem.

Types of Changes:

- *Custom Development*

Currently, CCC utilizes purchased software for all financial applications and does not customize the application's functionality or database structures internally. In the event that minor customizations (i.e. report development) are required, the process will mirror the vendor upgrade process. All applications are supported by the software vendor.

- *Vendor Upgrades*

The majority of CCC's future recurring application changes will be minor version upgrades to the applications. Version upgrades, issues, and bug fixes are handled directly by the software vendors. CCC does not have access to the source code and therefore does not have the ability to modify these proprietary packages. All issues, bug fixes, and modifications are completed by the software vendors. Version upgrades are included as part of vendor maintenance agreements. The Senior Facility Services Manager and/or the Director of Finance are notified via email when version upgrades are available, and a time is scheduled to migrate to the new versions. Release notes come with each upgrade and/or service pack.

Projects

Projects arise in a number of ways, from a phone call or e-mail, to a formal functional specification. The initiation phase focuses on authorizing the project. It includes understanding of the request, assessing the project category, and communicating an early project scope to CCC's management. This is a starting point for discussions with interested parties. During this phase, the priority of the request is determined relative to other outstanding requests and a go/no-go decision is made.

- *Objectives:*

- Needs identification;
- Senior Management identification;
- Sizing and prioritization of the project;
- Management approval for the project.

- *Major Activities:*

- Request new development;
- Define high-level business requirements;
- Estimate project size for budgetary purpose;
- Prioritize project;
- Communicate results to Senior Management;
- Get approval for the project.

- *Deliverables:*

- Request for development or project charter:

CCC will create a project ticket within Spiceworks to track these requests.

- High-level Business Requirements:

An early view of the project scope.

- High-level Estimate:
An initial estimate that represents a rough order of magnitude sizing of the project.
- Project Categorization:
An initial sizing category based on an estimate of the man-hours and level-of-impact of the project on the organization.
- Project Prioritization:
Prioritize new request relative to other projects and initiatives.
- Approval:
(Go/No-Go decision).

Types of Project category:

- *Large Projects:*
 - Criteria: A project is categorized under *large* if it affects the organization as a whole and requires 100 or greater man-hours to complete.
 - Evaluation Process: A formal evaluation and system selection process will be followed. The Director/Department Manager making the request for the new a development will create a business case, which will include a high-level requirements definition, project overview, proposed resource requirements and estimated cost. A formal risk and impact analysis will also be completed during the project identification process.
 - Approvals: If the Technology Review Board (TRB) determines that the application implementation is feasible, technical specifications will be completed and reviewed by the Director of Finance. Upon approval a business case will be presented to Senior Management for formal approval.

- Evidence: The approval will be maintained with the project documentation within a Spiceworks ticket.
- *Medium Projects:*
 - Criteria: Projects that do not fall under the large or the break/fix category are defined as medium-sized projects. A medium-sized project would require anywhere between eight to 100 man-hours for completion and may not impact the organization to the extent of large projects.
 - Evaluation Process: For medium projects, some tasks and activities become optional in order to balance project deliverables with project scope and risk. The evaluation process may not be very detailed due to the nature of the project.
 - Approvals: Senior Facility Services Manager will evaluate the project and present the case to the director of finance for approval.
 - Evidence: The evidence will be maintained in a Spiceworks help desk ticket.
- *Break/Fix:*
 - Criteria: Break/fix issues require eight or less man hours for completion and do not impact the organization to the extent of large- and medium-sized projects.
 - Evaluation Process: These projects include minor customizations to the application and software patches. The Senior Facility Services Manager or Technology staff will evaluate the problem forward the Help Desk ticket to the appropriate personnel to perform the fix.
 - Approvals: There is minimal approval required for break/fix issues and is obtained from the Senior Facility Services Manager.
 - Evidence: The request is initiated and documented within Spiceworks.
- *Emergency Change:*

- In the event of an emergency, the change control process will follow the same steps; however, it will be prioritized as highest priority and surpass all other requests in the queue. The Technology department will update Spiceworks with a detailed description of the emergency fix. Documentation and management approval will be obtained after the fix takes place and is reflected within the Help Desk ticket.

B. ROUTINE PATCH MANAGEMENT:

- The Senior Facility Services Manager will upgrade or patch by downloading as necessary individual application fixes or installing directly from the WinINSTALL patch management console.
- Once the upgrade(s) are installed on vendor supported application(s), the Senior Facility Services Manager will test the changes.
- Once changes and/or upgrade are complete, e-mail is sent to the Director of Finance, the General Manager and users notifying them that the change is in the production environment. In addition, manual logs/system logs are used to track changes made to the production environment. As an additional compensating control, no modifications to financial systems may be made on any Monday due to the weekly payroll processing, or in the two weeks leading up to or following a quarter or year-end close.


C. TESTING:

- Specific users will be asked to test the upgrade and/or fix by running a series of before-and-after reports to provide reasonable assurance of the data accuracy.
- Once completed, the user will send an e-mail to the Senior Facility Services Manager confirming the success of the upgrade and/or fix.

- For data conversions, testing should involve the evaluation of key test balances as appropriate.

Reference:

Knowledgeleader.com. (n.d.). SDLC and Change Management Policy. Retrieved June 12, 2010, from <http://www.knowledgeleader.com>

	
Policies and Procedures	
Department: Security	Issued By: Mike Chin
Topic: Physical Access Control	Procedure Number: ITA-01
Effective Date: 8/1/10	Status: Active

Purpose

The purpose of this policy is to establish standards for securing the PBX, network closets, and other information systems (IS) facilities within the Colorado Convention Center (CCC).

Effective implementation of this policy will minimize unauthorized access to these locations, and provide more effective auditing of physical access controls.

Scope

The policy applies to all closets and locations containing IS equipment at CCC. This policy is specifically for the PBX located in the 300 Meeting Room Service Corridor and the wiring closets identified on the attached facility maps.

Policy

Ownership and Responsibilities

The technology department is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

Physical Access


- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all restricted locations must be documented and managed.
- All IS locations must be physically protected in proportion to the criticality or importance of their function at the CCC.
- Access to the referenced locations will be granted only to the CCC support personnel, and contractors, whose job responsibilities require access to those locations.
- The process for granting card and/or key access to IS locations must include the approval of the technology department.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to CCC Security. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the technology department.
- Card access records and visitor logs for IS locations must be kept at security base for routine review.

Enforcement

Employees found to have violated this policy may be subject to appropriate disciplinary action.

Reference

<http://www.its.umd.umich.edu/policies-standards/um-dearborn-it-policies-standards/physical-access-policy/>



Policies and Procedures

Department: Finance	Issued By: Cheri Wilbur
Topic: Technology Asset Inventory	Procedure Number: ITI-1
Effective Date: 2/1/2010	Status: Active

Scope

This policy applies to all technology equipment purchased by the Colorado Convention Center (CCC).

Rationale

The taxpayers, lessees and the users of the CCC, understanding that the facility is a publicly funded entity, expect the proper level of fiduciary responsibility from the CCC. Additionally, one of the most important steps in IT management and IT security is understanding what physical and virtual IT assets an organization owns and manages. A good inventory provides information that is useful to daily system management, business office asset tracking, and security incident response.

Policy

A CCC Asset Inventory form must be completed by the department manager and received by Finance for the following:

- All stand alone assets \$500.00 or greater.
- All TV’s, Radio’s, and Computer Equipment \$250.00 or greater.

The CCC Asset Inventory form must be completed with all information requested.

Each department manager and or director is responsible for any items purchased for their department.

Each department manager and or director is responsible to maintain and track the current assets assigned to their Department. Please refer to the attached list of assets for your department. This list will be updated annually during the City's annual inventory review.

Procedures

1. When a Purchase Requisition form for a new IT asset is submitted to Finance, the need for an Asset Inventory Form will be noted and the order will be flagged.
2. When the purchase is received the appropriate manager must fill out the Asset Inventory Form and submit it to Finance.
3. Finance will not release payment on the vendor invoice until this process is complete.


Disciplinary Process

Failure to submit the necessary form will result in non-payment to the vendor until the proper procedures have been followed.

Attachment:

CCC Asset Inventory Form

CCC ASSET INVENTORY FORM	
APPLIES TO ALL STAND ALONE ASSETS \$500 OR GREATER	
DATE:	10.07.2010
FROM:	Apple
PO NUMBER:	NA
DESCRIPTION:	iPad WiFi 64GB
SERIAL NUMBER:	GB0388NFZ3A
MODEL NUMBER:	A1219
MANUFACTURER:	Apple
DATE RECEIVED:	10.07.2010
COST OF ASSET:	\$883.47
INTERNAL LOCATION:	Event Management
Please return form to Laura Tateyama in Finance when completed.	
Form Completed By:	

	
Policies and Procedures	
Department: Finance	Issued By: Cheri Wilbur
Topic: Technology Disposal Policy	Procedure Number: ITI-02
Effective Date: 2/1/2010	Status: Active

Scope

This policy applies to all technology equipment owned by the Colorado Convention Center (CCC).

Rationale

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and mandated by the City of Denver Technology Department in conjunction with the City of Denver’s Environmental Management System. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of CCC data, some of which is considered sensitive. In order to protect our constituent’s data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal. Failure to properly dispose of technology equipment can have several negative ramifications to the company including fines, negative customer perception and costs to notify constituents of data loss or inadvertent disclosure.

Purpose

This policy has been developed to define the requirements for proper disposal of technology equipment at the CCC.

Procedure**Technology Equipment Disposal**

1. A CCC Asset Surplus form must be completed by the department manager and received by Finance for all assets that will be removed from the property of the Colorado Convention Center. A copy of the Asset Surplus form shall accompany the device to the designated disposal collection point.
2. When technology assets have reached the end of their useful life they should be sent to the Box Office B2 for proper disposal.
3. The Technology department will securely erase all storage mediums using DBAN, a freeware utility that completely overwrites storage media in accordance with current industry best practices.
4. All equipment will be marked with yellow tape upon completion of step 2 to identify that it is prepared for removal from the premises.
5. All IT equipment regardless of working condition will be sent to MeTech, the electronics recycler of record for the City and County of Denver. An itemized list of the serial numbers associated with the pickup shall be given to MeTech and a copy sent to Finance upon removal from the facility by MeTech.
6. No equipment shall ever be made available to employees for purchase or otherwise.
7. Prior to scheduling equipment for disposal by MeTech, the Senior Facility Services Manager shall confirm with accounting that the equipment has either been removed from the Information Technology inventory system or that the Asset Surplus Form has been submitted to the city for proper documentation.

Enforcement

The last recorded custodian of an asset will be considered in breach of CCC policies which may result in sanctions up to and including immediate termination of employment in accordance with

applicable CCC disciplinary policy and/or civil or criminal prosecution should an asset be discovered missing or having not been properly disposed of.


CCC may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. SMG corporate counsel and or the City Attorney of the City and County of Denver, the Denver Police Department and other law enforcement officials as appropriate shall address theft of CCC resources by persons not affiliated with the facility.

Reference

SANS Institute. (N.D.). Equipment Disposal Policy Template. Retrieved December 18, 2009, from <http://www.sans.org/security-resources/policies/>

Attachments**CCC Asset Surplus Form**

CCC SURPLUS FORM	
APPLIES TO ALL STAND ALONE ASSETS \$500 OR GREATER	
SURPLUS DATE:	
SURPLUSING DEPARTMENT:	
SURPLUSING AGENCY:	DEPARTMENT OF TECHNOLOGY - MeTech
DESCRIPTION:	
SERIAL NUMBER:	
MODEL NUMBER:	
MANUFACTURER:	
INVENTORY NUMBER:	
LOCATION PLACED FOR SURPLUS PICKUP:	
Please return form to Laura Tateyama in Finance when completed.	
Form Completed By:	

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: Laptop Computer Checkout	Procedure Number: ITI-03
Effective Date: 11/1/2009	Status: Active

Policy:

The Colorado Convention Center has a limited number of laptop computers to offer employees for checkout. Laptops are available for checkout from the Senior Facility Services Manager in B Mezzanine and may be used for travel, work, and research performed by employees for the Colorado Convention Center.

Limits & Availability

- The laptop computers can only be checked out with approval of an employee’s department director.
- The laptops are for use only for Colorado Convention Center purposes and the borrower will be denied future borrowing privileges if the device is used for personal activity.
- Laptops will be available on a first-come, first-serve basis, but can be reserved ahead of time if available.
- Borrowers may not install software on the machines.
- Borrowers may not alter, delete or copy any software loaded on the laptop or otherwise change its existing configuration.

- Printing is not enabled on the laptops but most plug-and-play printers will install automatically.

Procedures:**Checkout Procedure**

- An employee borrowing a laptop should read and agree to abide by the Colorado Convention Center laptop Checkout Policy and the SMG Use of Technology Policy.
- The request for an employee to borrow a laptop should be made by the employee's department director to the Senior Facility Services Manager. There are no exceptions to this policy unless approved by the General Manager or Assistant General Manager.
- A borrower must sign the Laptop Checkout Inventory Tag before he/she can take a laptop away from the Senior Facility Services Manager's office. One copy of the tag will be attached to the case; one copy will remain with the Senior Facility Services Manager.
- At the time of checkout, the laptop will be inspected by the Senior Facility Services Manager to make sure it is intact and functioning properly.
- A borrower will be cautioned to save his/her files in his/her flash or jump drives, floppy disks, CD, or to send them via an email attachment. All files will be erased after the computer is returned.

Loan Period & Renewals

- The checkout period for each laptop is up to one week.
- A checked-out laptop can be renewed for another week if no other requests are pending.
- The borrower must return the laptop along with accessories to the Senior Facility Services Manager at the end of each period to renew the checkout.

Check-in Procedure

- When returning, the borrower should allow at least five minutes for the Senior Facility Services Manager to check the equipment.
- Borrowers must return the laptop to Senior Facility Services Manager directly. A laptop should not be left unattended in the manager's office or B Mezzanine.
- The Senior Facility Services Manager will verify that all parts are present and that the computer and all accessories are in good working order.
- The laptop will be booted up and checked for functionality upon return.
- The laptop will then be checked in and the Laptop Checkout Inventory Tag will be removed from the carrying case, signed in and dated.

Liability


- An employee's privilege to check out a laptop may be denied for up-to one year if the employee fails to return loaned equipment by the due time on more than two occasions or leaves before the check-in procedure is complete.
- If a laptop is not returned when promised, after 24 hours the laptop will be considered stolen or lost. Security will be notified and an investigation may be initiated.
- The borrower is responsible for making sure that the laptop is in working order and without physical damage when it is checked out.
- Under no circumstances should a borrower leave the laptop unattended. The Colorado Convention Center will not be responsible for a lost or stolen laptop even when it is used within the facility.
- It is the borrower's full responsibility and fiscal liability for all costs associated with damage to the laptop computer or its associated peripheral equipment during the period it is checked out or its replacement costs should it be lost or stolen.

Troubleshooting Problems & Questions

- If an employee experiences problems with laptop hardware or applications or has questions, they should ask the Senior Facility Services Manager.
- The borrower will be fiscally responsible for any damage to a laptop if he/she tries to troubleshoot problems.

Disclaimer

- The Colorado Convention Center is not responsible for damage to any removable drive (i.e. floppy, CD or flash drive) or loss of data that may occur due to malfunctioning hardware or software.

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: Network Documentation	Procedure Number: ITN-01
Effective Date: 11/1/2009	Status: Active

Overview

This network documentation policy is an internal IT policy and defines the requirements for network documentation. This policy defines the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

Documentation

The network structure and configuration shall be documented and provide the following information:

1. All Cable paths will be documented.
 - a) A record of patch panel, device port, cable color and cable length will be kept in each wiring closet.
 - b) Each cable will be labeled in accordance with its purpose.
 - i. Cables interconnected on the same rack require one label identifying purpose, and both connecting points.
 - ii. Cables interconnected on separate racks require two labels, one at each connector, identifying purpose and both connection points.
2. IP addresses of all devices on the network with static IP addresses.
3. Server documentation on all servers as outlined in the “Server Documentation” document.
4. Network drawings showing:
 - a) The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
 - b) The various security zones on the network and devices that control access between them.
 - c) The locations of every network drop and the associated switch and port on the switch supplying that connection.
 - d) The interrelationship between all network devices showing lines running between the network devices.

- e) All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information.
5. Configuration information on all network devices including:
- a) Switches
 - b) Firewalls
6. Configuration shall include but not be limited to:
- a) IP Address
 - b) Netmask
 - c) Default gateway
 - d) DNS server IP addresses for primary and secondary DNS servers.

Access

The Technology staff exclusively shall have full access to and the ability to read and modify all network Designated operations staff shall have access to read department mission related network documentation but cannot change it.

Change Notification

The Technology staff will notify one another when any network changes are made including.

1. Reboot of a network device including switches, routers, and firewalls.
2. Changes of rules or configuration of a network device including switches, routers, and firewalls.
3. Upgrades to any software on any network device.
4. Addition of any new software on any network device.

Notification shall be through the diary function in Spiceworks and in the event of a Reboot, via email prior to the occurrence with sufficient time for all Technology staff to respond (a minimum of 15 minutes).

Documentation Review

The Senior Facility Services shall ensure that network documentation is kept current by performing a quarterly review of documentation with other team member assistance. The remedy or help desk requests within quarter shall be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings shall be reviewed to determine whether there were any network changes made to support the project.

Storage Locations


Network documentation shall be kept in written form in both the Senior Facility Services Manager's office and the PBX so that if one portion of the facility is destroyed, information from the other location may be used to help reconstruct the IT infrastructure. The PBX copy will be locked within a designated cabinet that only Technology employees may access. Network documentation shall also be stored in electronic form within the secure folder on the Technology Shared Drive. All copies shall be updated quarterly at the time of the documentation review. Any changes made to the electronic version shall be printed and updated in the written copies at this time.

Sanctions and Violations

CCC will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate departments. Failure to comply with CCC information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access,); the individual's employment up to and including immediate termination of employment in accordance with applicable CCC disciplinary policy and/or civil or criminal prosecution.

9.0 Reference

Irfan, Y. (2008). Sample Campus Network Documentation Policy. Retrieved November 20, 2009, from <http://itknowledgeexchange.techtarget.com/network-technologies/sample-campus-network-documentation-policy/>

	
Policies and Procedures	
Department: Human Resources	Issued By:
Topic: Network Management Policy	Procedure Number: ITN-02
Effective Date: Pending	Status: Draft 10/1/10

Scope

This policy applies to all users of the Colorado Convention Center (CCC) information resources over networks that cause traffic to traverse the Facility network backbone. The policy extends from the Network Access Point (NAP) to the end-user machine.

Rationale

The purpose of this document is to outline CCC policy regarding the monitoring, logging and retention of network packets that traverse the facility network backbone.

The goals of this policy are:

1. To maintain the integrity and security of the facility’s network infrastructure and information assets,
2. To collect information to be used in network design, engineering, troubleshooting and usage-based accounting.

This policy acts in conjunction with the Acceptable Use Policy (ITU-01) along with the Network Documentation Policy (ITN-01), and provides additional information with regard to the practice of the monitoring, of CCC network activity.

Policy Statement

1. Monitoring network traffic at the CCC will involve only the collection of packet header information, not the packet data, unless required to check for viruses, to monitor the

- improper release of confidential, employee or client information, or for intruder detection.
2. The Technology Department is the only department and/or staff authorized to routinely monitor traffic on the network backbone.
 - a. The use of sniffers or devices, which operate in promiscuous mode, are to be used only by the authorized Technology staff for diagnostic purposes of network traffic only.
 - b. Employees must not intercept or attempt to intercept or access data communications not intended for that employee, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines, and must respect users' rights to privacy as outlined in ITU-01
 3. Personnel authorized to analyze network backbone flow as set forth in paragraph 2 above, will not disclose any information realized in the process without approval of the Human Resources Manager.

Procedures

1. Directors may request flow information with Human Resources approval. The method to request this information is as follows:
 - a. A memo from the department director must be sent to Human Resources requesting network backbone flow information generated by an employee's machine.
 - b. The Human Resources Manager must determine if the request merits the involvement of the Senior Facility Services Manager (SFSM) and authorize their involvement via email.

- c. The SFSM will analyze the backbone flow information to establish the security risk to the CCC. If there is a risk, the SFSM will proceed to examine the flow of the packets, and will inform the Human Resources Manager as to the legal infractions contained for proper legal course of action. If no security risk is found, but other issues are identified, (e.g., acceptable use as defined in ITU-01 and ITN-03) the SFSM will return the request to the department director to handle directly with Human Resources.
2. Technology department staff will contact the SFSM for resolution of anomalies or other suspicious activity noticed via any network monitoring application.
3. The technology department must be capable of monitoring the facility backbone network 24 hours a day, 7 days a week. All network failures and excessive utilization will be reported to the SFSM for problem resolution or design enhancement. Technology department employees will act as the Point of Contact for facility network backbone traffic problems.
4. This policy does not govern the monitoring of employee electronic transmissions via email or the Internet. These activities are governed by ITU-1, ITU-3 and ITN-1.
5. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they shall be purged.

Disciplinary Process


Breach of CCC policies may result in sanctions up to and including immediate termination of employment in accordance with applicable CCC disciplinary policy. CCC may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. SMG corporate counsel and or the City Attorney of the City and County

of Denver, the Denver Police Department and other law enforcement officials as appropriate shall address infractions identified as originating from persons not affiliated with the facility.

Reference

Office of Information Technology. (2001). Network Monitoring Policy, from

www.it.utah.edu/leadership/policies/NetworkMonitoring.pdf

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: Employee Internet Use Monitoring and Filtering Policy	Procedure Number: ITN-03
Effective Date: 3/1/10	Status: Active

Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the Colorado Convention Center's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

Scope

This policy applies to all the Colorado Convention Center employees, contractors, vendors and agents with a Colorado Convention Center-owned or personally-owned computer or workstation connected to the Colorado Convention Center network. This policy applies to all end user initiated communications between the Colorado Convention Center's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

Policy

Web Site Monitoring

The Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source

IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the Technology Department. Technology Department members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the Technology Department upon written or email request to the Senior Facility Services Manager from a Human Resources Representative.

Internet Use Filtering System

The Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for the Colorado Convention Center's corporate environment.

The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services

- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

Internet Use Filtering Rule Changes

The Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. A Technology Department employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Director. The Director will present all approved exception requests to the Technology Department in writing or by email. The Technology Department will unblock that site or category for that associate only. The Technology Department will track approved exceptions and report on them upon request.

Enforcement

The Senior Facility Services Manager will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

User ID – User Name or other identifier used when an associate logs into the corporate network.

IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.


Peer to Peer File Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking – Sites that provide content about breaking or subverting computer security controls.



Policies and Procedures

Department: Technology	Issued By: Sam Fleming
Topic: Network Router Policy	Procedure Number: ITN-04
Effective Date: 11/20/2009	Status: Active

Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the Colorado Convention Center (CCC).

Scope

All routers and switches connected to CCC production networks are affected.

Policy

Every router must meet the following configuration standards:

1. All vendor supplied security defaults shall be modified with the corporate security credentials prior to being placed on the production network.
2. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
3. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
4. Disallow the following:
 - a. IP directed broadcasts

- b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
 - c. TCP small services
 - d. UDP small services
 - e. All source routing
 - f. All web services running on router
5. Access rules are to be added as business needs arise.
 6. The router must be included in the corporate enterprise management system with a designated point of contact.
 7. All unused ports must be disabled on all production switches.
 8. Written documentation of each device configuration shall be reviewed and updated quarterly. Refer to ITN-1.

Enforcement

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


Definitions

Terms	Definitions
--------------	--------------------

Production Network	The "production network" is the network used in the daily business of the CCC. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the CCC employees or impact their ability to do work.
--------------------	---

Reference

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: Password Policy	Procedure Number: ITN-5
Effective Date: 5/1/2010	Status: Active

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Colorado Convention Center (CCC)'s entire corporate network. As such, all CCC employees (including contractors and vendors with access to CCC systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CCC facility, has access to the CCC network, or stores any non-public CCC information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at CCC. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. All employees must be familiar with how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)

- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "CCC", "Colo", "Denver" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-
=\`{ }[]: ";' < > ? , . /)
- Are at least fifteen alphanumeric characters long and is a passphrase
(Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for CCC accounts as for other non-CCC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share CCC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential CCC information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call the Technology Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every three months (except system-level passwords which must be changed yearly).

If an account or password is suspected to have been compromised, report the incident to the Technology Department.

Password cracking or guessing may be performed on a periodic or random basis by the Technology Department. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Use of Passwords and Passphrases for Remote Access Users


Access to the CCC Networks via remote access is to be controlled using a public/private key system with a strong passphrase contained within the Cisco 5.0 VPN client.

5.0 Enforcement

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

Reference:

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Executive	Issued By:
Topic: Technology Risk Assessment Policy	Procedure Number: ITRA-01
Effective Date: 11/1/2009	Status: Active

Scope

Risk assessments (RA) can be conducted on any portion of the Colorado Convention Center’s information systems (IS) assets or any outside entity that provides IS services and may include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Rationale

To empower the CCC Technology department to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Policy

The execution, development and implementation of remediation programs is the joint responsibility of the CCC technology department and the various departments utilizing the systems being assessed. Users are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Users are further expected to work with the Technology department in the development of a remediation plan.

The current RA process will be enhanced as the process is repeated, moving from the basic procedures outlined below to a more in-depth framework as the CCC invokes a system development lifecycle to approach a more mature and repeatable model.


Procedures**Disciplinary Process****Definitions**

Risk – Factors that could affect confidentiality, availability, and integrity of the organization's information assets and systems. The Organization is responsible for ensuring the integrity, confidentiality, and availability of critical information and assets, while minimizing the impact of security procedures and policies upon business productivity.

System Development Lifecycle -

Reference

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Human Resources	Issued By:
Topic: Acceptable Use Policy	Procedure Number: ITU-01
Effective Date: Pending	Status: DRAFT

Overview

The Colorado Convention Center’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SMG’s established culture of openness, trust and integrity. The Colorado Convention Center is committed to protecting SMG's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

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

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

Purpose

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

Scope

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

Policy**General Use and Ownership**

1. While SMG's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SMG. Because of the need to protect SMG's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SMG.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. The Colorado Convention Center recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see The Colorado Convention Center's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to The Colorado Convention Center's Awareness Initiative.

4. For security and network maintenance purposes, authorized individuals within SMG may monitor equipment, systems and network traffic at any time, per The Colorado Convention Center's Audit Policy.
5. SMG reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with The Colorado Convention Center's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".

6. Postings by employees from a SMG email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SMG, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the SMG Internet/Intranet/Extranet, whether owned by the employee or SMG, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

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

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

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not

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

to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

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

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within SMG's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SMG or connected via SMG's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

 Blogging

1. Blogging by employees, whether using SMG's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of SMG's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate SMG's policy, is not detrimental to SMG's best interests, and does not interfere with an employee's regular work duties. Blogging from SMG's systems is also subject to monitoring.
2. SMG's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of SMG and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by SMG's Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to SMG when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of SMG. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, SMG's trademarks, logos and any other SMG intellectual property may also not be used in connection with any blogging activity.

Enforcement

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


Definitions**Term Definition**

Blogging Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam Unauthorized and/or unsolicited electronic mass mailings.

Reference

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

 <p>Policies and Procedures</p>	
Department: Executive	Issued By:
Topic: Information Sensitivity	Procedure Number: ITU-02
Effective Date: Pending	Status: Draft 12/1/10

1. Rationale and Background

The Colorado Convention Center (CCC) requires controls to manage risks to the confidentiality, integrity and availability of CCC information. This handling standard defines the controls required for highly sensitive information in any form. These required controls represent a minimum standard for protection of highly sensitive CCC information. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data), may also apply.

Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys highly sensitive CCC information is responsible and accountable for complying with this standard.

In addition to compliance with this standard, all computers owned by the CCC and/or connected to a CCC network must comply with the this policy

2. Creation

CCC employees create records as part of the normal course of conducting the business. These records document the decisions and activities of our complex enterprise. It is essential that they be created and maintained appropriately throughout their entire life cycle.

Highly sensitive information contained in CCC records constitutes an area of critical concern because of the severe risk to CCC should records be mishandled or information inappropriately accessed or disclosed. As a consequence, records containing highly sensitive information should exist only in areas where there is a legitimate and justifiable business need, as authorized by the Director of Finance, and maintained under strict controls as outlined in this document.

Departments should work to identify and track all CCC records through their life cycle by way of records retention schedules prepared in collaboration with the director of finance. A first priority in this effort should be the identification of highly sensitive information. Records schedules will document the existence of these materials, the rationale behind keeping them, and help ensure their availability during the period in which they are vital as either active administrative or historical records. Record retention schedules also will work to ensure the timely disposal of non-permanent, inactive records, thereby mitigating the risk of exposure of information when it no longer serves an active administrative or historical function.

3. Access

Highly sensitive information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. In some cases, information is highly sensitive because of its aggregation into a single document, regardless of whether it contains highly sensitive data elements..

Only CCC *employees* who have authorization from the Director of Finance may have access to highly sensitive information. Any other disclosure of highly sensitive information requires the written approval of the director of finance in consultation with the general manager or assistant general manager as necessary.

4. Use, Transmission and Storage

The following controls are **required** when using, transmitting or storing highly sensitive information.

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying or faxing it, ensure that only authorized personnel will be able to see the output.
- Store paper documents in a locked drawer *and* in a locked room, or in another secure location.
- Properly identify such information as highly sensitive to all recipients, by labeling it "Highly Sensitive," providing training to personnel, explicitly mentioning the classification, or similar means.
- Encrypt electronic information using an encryption algorithm approved by the director of finance when:
 - Placing it on removable media;
 - Placing it on a mobile computer (e.g., laptops, PDAs, smart phones); or

- Sending it via e-mail to *non-CCC addresses*.
- Do not send this information via instant message or unsecured file transfer unless it is encrypted.
- Follow an established and documented software development lifecycle when building applications that process highly sensitive information.

5. Transport

The following controls are **required** when transporting highly sensitive information:

- When sending paper copies of highly sensitive information via United States Postal Service, UPS or FedEx, information must remain secure. Consult with the director of finance for specific handling restrictions.
- When carrying highly sensitive information, or devices containing such information, ensure that it is physically secure at all times.
- Do not remove highly sensitive information from an approved secure location without prior approval of the director of finance.

6. Destruction


CCC records should be destroyed only as detailed in the City and County of Denver records retention requirement of the management contract.

- Destroy electronic instances of CCC information using a certified records destruction contractor.. Refer to Asset Disposal Policy ITA-02 for instructions on media destruction.

- Crosscut shred or pulp all highly sensitive information in paper form. This includes all transitory work products (e.g., unused copies, drafts, notes).

7. Reference

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Human Resources	Issued By:
Topic: Email Use Policy	Procedure Number: ITU-03
Effective Date: Pending	Status: Draft 12/1/2010

1.0 Purpose

To prevent tarnishing the public image of the Colorado Convention Center (CCC) when email goes out from CCC the general public will tend to view that message as an official policy statement from CCC.

2.0 Scope

This policy covers appropriate use of any email sent from a CCC email address and applies to all employees, vendors, and agents operating on behalf of the CCC.

3.0 Policy

3.1 Prohibited Use.

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

3.2 Personal Use.

Using a reasonable amount of CCC resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a CCC email account is prohibited. Virus or other malware warnings and mass mailings from CCC shall be approved by the CCC Assistant General Manager before sending. These restrictions also apply to the forwarding of mail received by a CCC employee.

3.3 Monitoring

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

4.0 Enforcement

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


5.0 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.

- Chain email or letter Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
- Sensitive information Information is considered sensitive if it can be damaging to the CCC or its customers' reputation or market standing.
- Virus warning. Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
- Unauthorized Disclosure The intentional or unintentional revealing of restricted information to people, both inside and outside the CCC who do not have a need to know that information.

6.0 Reference

SANS Institute. (N.D.). Information Security Policy Templates. Retrieved October 10, 2009, from <http://www.sans.org/security-resources/policies/>

	
Policies and Procedures	
Department: Technology	Issued By: Sam Fleming
Topic: Guidelines on Anti-Virus Process	Procedure Number: ITU-04
Effective Date: 6/1/2010	Status: Active

Recommended processes to prevent virus problems:

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with The Colorado Convention Center's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan removable media from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Revised 8/25/10



Policies and Procedures

Department: Technology	Issued By: Sam Fleming
Topic: Support Policy and Procedure	Procedure Number: ITU-05
Effective Date: 2/15/10	Status: Active

PURPOSE

The purpose of the technology support policy is to improve quality of services and assure proper support for all SMG - Colorado Convention Center employees and equipment maintenance. Furthermore, this policy serves the purpose of communicating details of the technology and operations support protocols, responsibility and accountability, and work order logistics.

SCOPE

This policy applies to all SMG - Colorado Convention Center employees, and any other personnel granted access to SMG - Colorado Convention Center’s computing resources and telecommunications equipment.

POLICY

HELPDESK SUPPORT PROTOCOL

All SMG - Colorado Convention Center employees have four options to request assistance from Helpdesk (technical support or operations). It is highly recommended that all employees use the web portal <http://maddox/portal> or email help@somewhere.com in order to expedite the work order process. If the Internet connection is down building wide or another emergency (i.e. operations disruption) occurs employees may contact Technology directly via radio.

Option #1: Submit Work Order Online

Employees should request assistance via web portal at <http://maddox/portal>. It is recommended that employees first try the web portal to contact the Helpdesk. Employee’s login is as the email

account. Example email address is sfleming@somewhere.com so the login would be sfleming@somewhere.com.

Option #2: Submit an Email

Employees should request assistance via email at help@somewhere.com when experiencing difficulty with the Internet.

Option #3: Call the Technology at 303-228-8133

The Technology Department will take phone calls and voicemail and place them into the ticketing system for tracking and prioritization.

Option #4: Call the Technology Department via Radio

Use this means of communication ONLY when it is an emergency or you cannot connect to internet or email.

WORK ORDER REQUESTS

All SMG - Colorado Convention Center employees will be assigned a work order number by the help desk staff for tracking purposes.

WORK ORDER PRIORITIES - TECHNOLOGY

Employees may prioritize their personal work orders; however, Helpdesk personnel will re-prioritize the work orders accordingly to serve all users more effectively. The following are the priorities established to serve employees better.

Priority	Qualifying Troubles
Critical	Impacting entire building
High	Impacting Business
Medium	Impacting Individual User
Low	Request for new items

WORK ORDER RESPONSE TIMES: TECHNOLOGY

Priority	Estimated Response Times	Status Update
Critical	1 Hour	Response Time + 1 Business Hours
High	2 Hours	Response Time + 1 Business Hours
Medium	1Day	As needed
Low	5 Days	As needed

WORK ORDER TRACKING

When a technician closes the work order, the employee (work order requestor) will receive an email notification and information regarding the disposition of the problem, request or repair. Again, verbal requests for support will not be honored and the employee will be asked to follow the protocol and use email or the help desk phone line

If you have any questions or concerns in regards to this policy please feel free to contact Sam Fleming – Senior Facility Services Manager – sfleming@somewhere.com