2011

# Exploring Identity Management at Community Colleges in Texas with Open Access to College Computer Networks

Michael John Callahan
*Walden University*

# Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Michael Callahan

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Anthony Lolas, Committee Chairperson, Management Faculty
Dr. Nikunja Swain, Committee Member, Management Faculty
Dr. Raghu Korrapati, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2015

Abstract

Exploring Identity Management at Community Colleges

in Texas with Open Access to College Computer Networks

by

Michael Callahan

BS, University of Houston – Downtown, 1989

MBA, Our Lady of the Lake University, 2001

Master's Certificate in ECommerce, Our Lady of the Lake University, 2002

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

October 2015

## Abstract

The study addressed the lack of identity management practices in Texas community colleges to identify guest users who access college computers. Guest user access is required by Texas law and is part of the state's mission to bridge the technology gap; however, improper identification methods leave the college vulnerable to liability issues. The purpose of this study was to eliminate or mitigate liabilities facing colleges by creating and using security policies to identify guest users. This study combined the theoretical concepts of Cameron's internal security management model with the external trust models of the Liberty Alliance and Microsoft's Passport software. The research question revolved around the identity and access management framework used by 13 community colleges in Texas to track guest users and the college's ability to protect the college from illegal acts. Using a grounded theory approach, data were collected by interviewing 13 information technology management professionals at the community colleges regarding their security policies and procedures as well as by campus observations of security practices. The results of constant comparison analysis indicate that no universal theory was being used. Only 3 of the 13 colleges tracked guest user access. Reasons for not tracking guest access included lack of financial and technology resources and process knowledge. Based on these findings, the identity management infrastructure theory was recommended for network access control, self-registration, and identity authentication at these colleges and many other colleges. The implications for social change include raising awareness of the risks most community colleges face from network security breaches, regulatory noncompliance, and lawsuit damages that could result from the lack of an identity management process.

# Exploring the Legal Liabilities Facing Community Colleges in Texas with Open Access to College Computer Networks

by

Michael Callahan

BS, University of Houston – Downtown, 1989

MBA, Our Lady of the Lake University, 2001

Master's Certificate in ECommerce, Our Lady of the Lake University, 2002

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

September 2015

# Dedication

Thanks to my patient wife, the lovely and gracious Julie, for putting up with the 6 year odyssey. I always had her full support no matter how expensive, far away, or time consuming it became. She was my initial editor and greatest supporter.

# Acknowledgments

Three people have been very influential in my life, Gerald and Ruth Monks and Rick Murray. Several times in my life when I did not deserve it, Mr. Monks gave me a job, place to live, and opportunity to learn. Mrs. Monks always had a place for me in her home. For many years I felt like the sixth Monks child. Without the Monks I would not be the man I am today.

Rick Murray was my boss for 2 years at M.D. Anderson Cancer Center. He planted the idea of becoming a doctor in my mind and showed me the benefits of post graduate education. It was through his encouragement I began my post graduate work.

Table of Contents

List of Figures ..... iv

Chapter 1: Introduction to the Study ..... 1

Background of the Study ..... 1

Problem Statement ..... 3

Purpose of the Study ..... 3

Research Questions ..... 6

Theoretical Foundation ..... 7

Nature of the Study ..... 12

Definitions ..... 13

Assumptions ..... 15

Scope and Delimitations ..... 16

Limitations ..... 16

Significance of the Study ..... 17

Significance to Social Change ..... 18

Summary and Transition ..... 20

Chapter 2: Literature Review ..... 21

Conceptual Framework ..... 22

Role Identity Model ..... 36

Summary and Conclusions ..... 72

Chapter 3: Research Method ..... 75

Research Design and Rationale ..... 75

Role of the Researcher ..... 76
Methodology ..... 77
Participant Selection Logic ..... 80
Instrumentation ..... 82
Procedures for Recruitment, Participation, and Data Collection ..... 84
Data Analysis Plan ..... 85
Issues of Trustworthiness ..... 86
Credibility ..... 86
Transferability ..... 87
Dependability ..... 87
Ethical Procedures ..... 88
Summary ..... 88
Chapter 4: Results ..... 90
Research Setting ..... 91
Demographics ..... 93
Data Collection ..... 94
Data Analysis ..... 100
Evidence of Trustworthiness ..... 109
Credibility ..... 109
Transferability ..... 110
Dependability ..... 110
Study Results ..... 111

Summary ..... 112

Chapter 5: Discussion, Conclusions, and Recommendations ..... 115

Interpretation of Findings ..... 117

Limitations of the Study ..... 119

Recommendations ..... 119

Implications ..... 126

Conclusions ..... 127

References ..... 130

List of Figures

Figure 1. IdM authentication.....12

Figure 2. Concept of identity management.....14

Figure 3. The architecture of an isolated identity management system.....28

Figure 4. An example of a federated identity management system architecture.....29

Figure 5. A centralized identity management system architecture.....31

Figure 6. Hierarchy of Published Documentation for Information Security Policy.....61

Figure 7. Information Security Governance Framework.....66

Figure 8. Conceptual Design of Network Security Policy, Procedures, and Practice .....116

# Chapter 1: Introduction to the Study

## Background of the Study

According to Razavi and Iverson (2008), user access to information systems (IS) is managed by direct interaction between the information technology (IT) department and the users. At most community colleges or universities, access is granted traditionally by management to faculty, students, and staff as users of the IT system. All these users go through an application or verification process before access to college resources is granted. Razavi and Iverson stated that this access has grown to include vendors, suppliers, alumni, and guests. The growth in traditional and nontraditional users of community college and university resources has pushed the limit of IT resources in providing services to many academic communities in a secure environment.

As community colleges and universities move away from traditional paper-based business models and move to paperless models, the resources needed to grant and track access have been increasing. This automation of community college and university business processes has increased efficiencies in many areas, but it has made data and resource protection more challenging to IT departments. Tipton and Krause (2012) identified electronic fraud and identity theft as the top risks to community colleges and universities. Identity management (IdM), or the ability to identify users as well as those resources a user can access, has become one of the most important strategic responsibilities of community colleges and universities.

The inability to track guest user activities can leave colleges vulnerable to data breaches, software piracy, financial liability, and institutional embarrassment. This does

not appear to be a new problem in network security. A 2008 Association for Information Communications Technology Professionals in Higher Education (ACUTA) survey revealed a relatively high level of breaches in security systems maintained by college IT professionals. Forty-seven percent of ACUTA survey respondents reported at least one highly significant security breach and 71% reported minor security breaches to their institution security system (Landsman, 2009). None of these security breaches could be traced to the end user. The results of the ACUTA survey mirror the results of an Emory University survey from 2003. The Emory survey showed that nearly 80% of the respondents agreed that network security policies were important; however, only half of the respondents were taking active measures to combat the increases in security breaches (Cox & Kistner, 2003).

These surveys showed that little has changed regarding security breaches in the six years between the Emory and ACUTA surveys. Analysis of the surveys showed that most college IT professionals believe their campus networks are secure; however, they also admit to large numbers of security breaches. College IT professionals ranked high on the survey the need to protect college networks by tracking individuals who access college computer resources.

The IT professionals ranked high the inability to track security breaches on their networks. Consequently, there is a need for further research in the area of granting, identifying, and tracking guest users at community colleges to protect the colleges from potential damages associated with guests using college resources inappropriately. Identity management (IdM) covers nearly all aspects of computer access from virtual and physical

access, to regulating data storage, and to providing protection for individuals under the control of the organization (Jøsang & Pope, 2005). The literature is missing a secure and cost effective methodology to identify users who do not come under the direct control of an organization. More and more emphasis will be placed on college IT professionals to allow access to college resources as colleges move away from paper-based systems to paperless systems. All of this access indicates the need for knowing who is using the college system as a preventative measure to protect against inappropriate use of college assets.

## Problem Statement

The Texas legislature required all community colleges in Texas to grant open access to computer resources to all residents as guest users. This requirement is part of the effort to bridge the digital divide or to bridge the gap initiative (The League for Innovation in the Community College, n.d.). The problem that was explored in this study is the inappropriate use of the computer system and the potential for security breaches at community colleges in Texas that can occur because of the lack of tracking guest users. Initial observation of the methods colleges use to track guest usage are wide-ranging. Standardized methods are needed to eliminate inconsistencies and provide adequate guest tracking methods. Guidance is needed to eliminate inconsistencies in identifying guest users and provide methods that will adequately track the activities of guest users, especially those who intend to use the college system inappropriately.

## Purpose of the Study

The purpose of this qualitative case study is to expand the research on network

security at community colleges in Texas. Much has been written about intrusion detection systems to keep external hackers and intruders out of a college network by using IdM systems to manage access to college resources (Oblinger, 2003). Currently there are no effective guidelines for IT professionals at community colleges in Texas for allowing external guests to have internal access to computer resources in a secure environment. This leaves institutions to develop their own methods for allowing access to computer resources to guests (Oblinger, 2006). Without guidance, colleges could be inviting security breaches into their information technology system without retribution.

Identity management in higher education is not a new phenomenon (Salomon, Cassat, & Thibeau, 2003). Francia and Hutchinson (2014) extended the research into the liability issues associated with guest users. Francia and Hutchinson differentiated the types of users an organization allows access to computer resources. Guests are not under the same controls or scrutiny as college employees and students. Allowing access to computer resources without knowing who is using the resources places a significant potential security liability on community colleges. To allow ease of access to computer resources, many community colleges have adopted generic logins that identify a computer being used, not the user of the computer. Without the ability to track guest access, the college is now open to liability for inappropriate or illegal actions taken by unidentifiable guests. This inability to track guest users leaves the college open to liabilities that may take resources away from the college's primary mission.

Current IdM focuses on allowing access to computer resources to individuals who have gone through a vetting process by the institution. Employees complete an interview

and hiring process through the human resources department (Donnet, Gueye, & Kaafar, 2010). Students are admitted to the college through admissions and registration departments. Vendors are vetted through the procurement department. Access to computer resources is allowed only after the individual has been vetted and the IT department issues user credentials (Donnet, Gueye, & Kaafar, 2010).

Texas community colleges have the additional requirements of allowing access to computer resources to community members or guests who have not gone through any vetting process. According to Nelson, general counsel for the Lonestar Community College district, community colleges in Texas have a mandate to provide open access to computer and Internet resources to the community at large (personal communication, January 22, 2009). This regulation comes from the Texas Department of Information Resources rule 1 TAC 201.13, Information Security Standards. These rules revolve around the funding formula the Texas legislature uses to fund community colleges in Texas. Community colleges in Texas receive approximately 57% of their funding from the State and local property taxes (Dowd & Shieh, 2013). This community funding brings access to the college's resources.

According to Levine and Kater (2012), access to community college resources must be granted; however, that access is not unlimited. Community members or guests do not have access to resources when the college is closed nor can they take the resources off campus. Other security precautions associated with granting access to campus resources should also be followed. Physical security measures such as rooms with locked doors and computers secured with cables are in effect. Virtual security leaves much to be

desired. Employees and students under the direct control of the college are issued user IDs and passwords to access computers and network resources. Identities of both employees and students are verified and signed security policies can be strictly enforced. These policies should also be extended to guests (Levine & Kater, 2012).

Open access to computer resources is part of the mission of Texas community colleges. With the open access requirement to computer resources, community colleges need to be aware of the special security needs to protect the colleges from security breaches by hackers using college computers (Cain, 2003). Anonymity or the lack of tracking is one of the most coveted prizes of the hacker (Backes, Clark, Kate, Simeonovski, & Druschel, 2014). Community colleges are at risk for data breaches and criminal activities when the college does not collect identification from guests and associate that identification with a computer (Cronin, 2010). The purpose of this study is to determine how IdM can be used to protect colleges from security breaches caused by unidentified guest users.

## Research Questions

The central research question of this study is: How do community colleges in the State of Texas implement an IdM system that is capable of identifying guest users and protecting the college from security breaches such as inappropriate information access, hacking into other networks, launching computer viruses or Internet worms, or other white-collar crimes committed by guests using the college's computer network? From this central question, the sub questions to be answered to address the problem are:

RQ1. How do community colleges in the State of Texas implement an Identity

Management (IdM) system that is capable of properly identifying guest users and protecting the college from illegal acts such as inappropriate information access, hacking into other networks, launching computer viruses or Internet worms, or other white-collar crimes committed by guests using the college's computer network? From this central question, the sub questions to be answered to address the problem are:

RQ2. What are the IdM methods used by IT managers at Texas community colleges to identify guests?

RQ3. How affective are the IdM strategies used by IT managers at Texas community colleges in track guest users to improve the security of computer networks?

RQ4. What do IT managers see as the difference between their current IdM practices and their ideal IdM system?

## Theoretical Foundation

This study is based on past identity management research. I combined Cameron's internal security management model of trust, vulnerability, threat, and identity (Cameron, 2005) with both the external trust models of the Liberty Alliance (McEvily & Tortoriello, 2011) and Microsoft's .NET Passport (Alotaibi, Wald, & Gilbert, 2012). All three provide empirical evidence of the importance of a security model, both internal and external to the organization. The design and analysis of a security system are based on security models. These models combine the security policies and procedures needed to enforce identifying those who use the system. These models can be seen as symbolic representations of policies that guide policy makers' requirements into rules that can be

followed and enforced.

Much has been written regarding how organizations should identify users of network resources; however, these guidelines focus on employees, students, and vendors. Nothing is written regarding granting and tracking access to external guest users. Identity management can be assisted by the use of information security governance. Information security governance is a relatively new theoretical construct. Von Solms (2010) described information security governance in terms of waves. Wave 1 is the technological or IT component of information security. Wave 2 is concerned with information security management associated with security. Wave 3 looks at the institutionalization of information security in organizations. Information security governance provides a superb framework in which to introduce IdM. Wave 4 of the framework can guide IdM with regulatory compliance requirements related to the college's own legal and regulatory environments. Identity management can be placed within a governance framework to determine the actual security effectiveness. The management of IdM can now become the focus.

Community colleges in southeast Texas may have already developed IdM policies and procedures that allow guest users to access computer resources (Stasiak & Zielinųki, 2013). These policies and procedures can be compared with information security governance to determine the effectiveness of the college's IdM practices. Current models such as the Bell-LaPadula and Biba models work well for identifying individuals who are vetted by an organization. Both models are wholly lacking for guest access (Stasiak & Zielinųki, 2013). The strategy that will interest community college IT managers is a

specific implementation strategy of IdM (Stasiak & Zielinųki, 2013).

Stasiak and Zielinųki (2013) identified five drivers that influential the success of any identity management system. First is regulatory compliance or following the law. International, federal, state, and many local governments have enacted laws dealing with financial services, healthcare, and homeland security that require minimum standards for secure access control to computer and network infrastructure. Second is operational effectiveness, the time it takes to allow access to resources. Speed and accuracy are the keys to this driver. Improving this balance may require automation. The third driver is business facilitation. This facilitation is the ease of handling the business models used by different areas of the organization. Different areas of an organization may fall under different legal jurisdictions and/or require different levels of authentication and access to resources. An organization must be able to provide processes for these situations. Fourth is cost reduction or simply cost issues. There has been a growth in the number of community colleges in Texas and these colleges have seen an increased enrollment. More and more demands for access to computer resources are placed on organizations every day. Current levels of staffing have difficulty in accommodating the needs of this increasing demand. Organizations must look to cost savings options such as automation and partnerships in order to meet future demand. Fifth, and lastly, is the security risk management of the organization (Stasiak, & Zielinųki, 2013). Many of the laws enacted have compliance requirements to ensure the laws are being followed. This type of audit capability assures compliance with the law and protection for users who access the organization’s resources (Stasiak, & Zielinųki, 2013).

Stasiak and Zielinski's (2013) five drivers are used by the REAL ID Act, .NET Passport, and the Liberty Alliance as part of their best practices guidelines (Alotaibi, et al., 2012). The REAL ID act is a legislative initiative to standardize identification requirements for governmental issued ID cards and driver licenses (Harper, 2012). Texas is one of the states using the REAL ID Act standards for ID cards and driver licenses (Kephart, 2011). The .NET Passport and Liberty Alliance are examples of industry initiatives to allow users to port identification credentials across organizational boundaries in the private sector.

Both Microsoft's .NET frame work and the Liberty Alliance Project have developed various models for IdM within a domain (Kephart, 2011). Although their methods differ, the main goal of both is to provide public and private sector organizations with a standardized method of obtaining and using digital identification issued by a variety of trusted third party identity providers or a centrally verified database. Both stress mutual acceptance of rules, policies, and business processes between organizations, users, and third party identity providers. All these are essential to a cost effective, safe, and secure access to computer systems that connect to network resources and the Internet.

Figure 1 demonstrates the IdM theory behind both the Microsoft's .NET framework and the Liberty Alliance Project. First, organizations need to develop appropriate policies for users to access computer resources. Second, these policies are enforced every time a user logs on to a computer. The third and fourth steps require checking the user's login credentials or issues credentials based upon the organization's policies. User credential can be checked via either internal or external sources. Access to

computer resources and the Internet will be granted once the identity of a user can be confirmed.

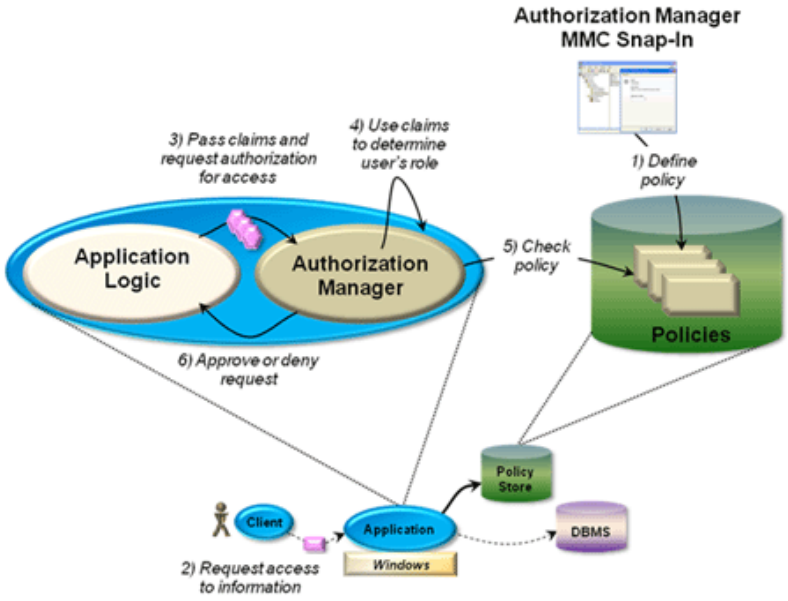


*Figure 1.* IdM authentication (Permission to reproduce image)

The preliminary results of this research indicated that many community colleges in Texas allow open access to anyone who wishes to use college computer resources. A few community colleges asked users to sign a paper log and even fewer asked guest to provide identification before issuing a user ID and password. Most colleges used generic logins that only identifies the computer, not the user. Neither the Texas legislature nor the Texas Higher Education Coordinating Board has issued guidelines to assist colleges in developing their policies and procedures. This leaves colleges to create their own policies based upon IdM solutions provided by the college's software vendors or to look for outside solution such as the Microsoft's .NET framework and the Liberty Alliance Project are the (Alzomai, 2011).

## Nature of the Study

The case study type used in this study is the explanatory study. The explanatory case study should be used when a researcher attempts to identify patterns and relate the variations of those patterns to each other (Yin, 2009). This type of case study answers the how and why questions that would explain an event. I used this type of case study because the focus of this inquirer was on how the IdM policies were created and why they were being (or not being) implemented by community colleges in Texas. Patterns were identified once the case study was completed.

The key concepts of IdM topology and deployment are shown in Figure 2. In this figure an identity uniquely identifies a person, place, or thing. Identity is verified by something that is known, such as a password or PIN; a token, such as an ATM card; a physical attribute, such as a finger print or retinal pattern; or a combination of these items (Vij, Majumdar, Dhar, & Vanecek 2014).

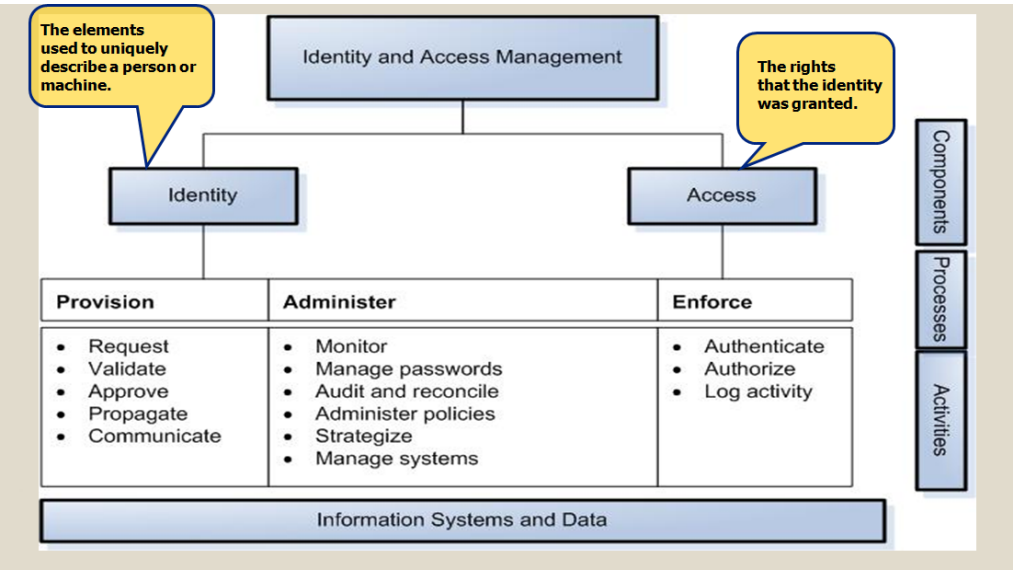


*Figure 2.* Concept of identity management. (Permission to reproduce image)

## Definitions

The following terms will be used in this study. These definitions are to assist noninformation technology professionals to better understand this study.

*Access management*: The ability to control an entity's (usually a person) access to network resources (Vij, et al., 2014).

*Account*: The collection and storage of data about an entity. An account is the basis for access to network resources (Forbes & Davis, 2008).

*Authentication*: The ability to prove one's identity. This works much like providing a driver's license when cashing a check (Ning, Liu, & Wenliang, 2008).

*Authorization*: The list of resources a network user has access to once authenticate to the network (Leggett, 2006).

*Certification authority*: A trusted third party whom an organization accepts identity credentials from. The department of motor vehicles is an example of a trusted third party for identification cards and drivers' licenses (Polk & Hastings, 2006).

*Credentials*: An identifier of a user and proof of the user's identity between network resources and networks (Tsang, Au, Kapadia, & Smith, 2007).

*Digital identity*: A digital token attached to documents, usually e-mails, by a trusted third party as authentication of a user's identity (Ning et al., 2008).

*Directory schema*: All the possible ways in which an entity can be known on a network and how that data can be held in directory structure (Tsang et al., 2007).

*Directory services*: The database where all network resources are identified and make the resources available to authorized users (Wachsmann, 2005).

*EDUCAUSE*: A nonprofit organization that provides IT resources and information to colleges and universities (EDUCAUSE, 2008).

*Enrollment*: Once an entity has an account the entity is registered with permissions to use specific network resources (Ning, et al., 2008).

*Federation*: An organization of a group of organization who agree upon the use of specific policies, procedures, software, and hardware in granting access to network resources. Once an entity is authenticated in one organization, it is authenticated in all organizations in the federation (Bhargav-Spantzel, Squicciarini, & Bertino 2005).

*Integrity*: A security concept that prevents addition, modification, and deletion of data from unauthorized users (Leggett, 2006).

*Microsoft active directory*: A vendor specific directory service that provides standardized software and methods for data storage and retrieval (Microsoft, 2008).

*Novell eDirectory*: Another vendor specific directory service. This object oriented structure organizations all network objects in a tree structure. The objects or assets can be organized as people, department, roles, groups, and equipment (Novell, 2008).

*Person registry*: A meta directory that allows users to login to all network resources. This directory contains not only the personal identifier, but also history of all user attributes (Tipton & Krause, 2012).

*Provisioning*: The process used to acquiring, maintaining, and deleting digital identities across a network. Provisioning identifies resources on a network and will track user ID and password requirements such as length, characters, and expiration dates. There are two types of provisioning, identity and user. Identity provision deals with

entities accessing resources and user provisioning deals with services and privileges to data and resources (Vij, Majumdar, Dhar, & Vanecek, 2014).

*Role-based access control (RBAC*): Security privileges assigned to each user based upon their role in an organization (Lyons-Burke, 2007).

*System-development process (SDP)*: The method used to create and implementing an information system (IT). When used correctly it will create repeatable methods to develop an IT and provide methods to measure improvement between systems (Bentley et al., 2004).

*Web-based access management (WAM*): A single sign on for web based resources. Used largely with intranet portals to provide authentication and authorization via a web front end interface (Nikols & Gebel, 2006).

*Worm*: A self-replicating computer program sent across the Internet to infect computers. Worms are designed to exploit security holes in computers connected to the Internet. The worm will install itself on the computer, copy itself, and send the copy to the next computer on the Internet (Sudduth, 2001).

## Assumptions

Community colleges in Texas are required to have their facilities open to the general public; however, that does not mean that the doors should be unlocked at all times. The grounds and facilities of the college must meet minimum security standards to protect and safeguard the college's property and resources. This same level of security should be present also for computer and network usage. Without specific directions on how to manage guest access to network resources, colleges will need to find their own

IdM solutions. The assumption that serve as the foundation for this research is that community colleges in Texas have some policies and procedures in place to identify guest users, these policies and procedures are sufficient to track guest user access, and these policies and procedures are put into practice by those who work in the computer labs.

## Scope and Delimitations

The scope of the study was focused on the policies, procedures, and practices of IT professionals at community colleges in Texas in order to identify guest users on the college's computer system. Examining the IdM methodology used by college IT professionals to identify guest users can be used to determine how secure the college's network is from unauthorized usage and how well the college is protected from liability issues arising from such unauthorized usage.

## Limitations

Computer and network security is a broad and expanding topic. This study was limited to the security issues facing community colleges in the State of Texas because of their open access requirement. Much will be written regarding court cases, laws, and standards regarding security. Several sections will expand into general areas of computer security such as firewalls, proxy servers, traffic monitoring, encryption, privacy, copyright protection, and data theft. These sections are intended to make the reader more familiar with the complex and growing area of computer security and the issues facing computer professionals. Although these sections will appear in this study, they will be limited to only basic information or directly linked to IdM issues facing community

colleges in Texas.

## Significance of the Study

### Significance to Practice

The problem is significant to IT professionals and college administrators who want to balance the open nature of a community college with the rigors of also providing a secure network environment that will protect the college from liability for unauthorized usage.

This study was intended to provide IT professionals at community colleges across the state of Texas a benchmark for allowing guests access to computer resources and methods to implement IdM practices on to a population that has not previously been placed under traditional IdM practices at community colleges.

### Significance to Theory

This study fills a gap in the IdM literature regarding non-traditional users of community college computer resources, or guest users. Because of the open nature of community colleges in Texas, proper IdM is vital to protect the college from liability brought on by guest users who use the college's computer systems for unauthorized usage such as launching DoS attacks, black hat hacking, or launching viruses. Proper IdM implementation will also reduce anonymous computer usage. The ability to identify computer users preforming unauthorized or criminal acts on the college's computers will mitigate the college's liability for such attacks.

Awareness of proper IdM can lead to support from senior management for proper budgeting and resource allocation to help protect the college's computer infrastructure.

The theoretical construct was completed by interviewing IT professionals at 13 community colleges in Texas and verified by visits to open computer labs at each college. The results of this study will provide IT professionals at community colleges with the necessary tools for developing policies and procedures to identify guest users and train computer lab employees how to implement practices to protect the college from liability.

**Significance to Social Change**

Allowing access to computer resources at community colleges helps to narrow the digital divide. The term *digital divide* is used to describe the gap between those with access to and those without access to technology or the Internet. Johnson, et al. (2013) used the research by Millron and Miles to define the problem. The authors stated that members of society who do not have access to technology are at a greater disadvantage of becoming disenfranchised spectators in the new digital economy. Without access to the technology, these members of society have difficulty in developing the skills needed to function in the digital age.

This problem has been taken up by many organizations. One of the notable organizations is the League for Innovation in the Community College (the League). The League has undertaken a substantial project to bridge the digital divide by using community colleges across the nation to provide access to technology and technology skills to the digitally disadvantaged (The League for Innovation in the Community College, n.d.). The League has setup resources to encourage community colleges to take aggressive actions within the community to find ways to reach the diverse populations associated with a community college. The Bridging the Digital Divide Project provides

resourses for community college educators to collaborate with community leaders and corporations to work together to bridge the digital divide.

Many of the community colleges in Texas have taken up the League's challenge of bridging the digital divide. In 2006, Lonestar Community College System instituted a plan to address the issue, called the Workforce Development Environmental Scanning and Strategic Planning. Section, or trend statement, five recognizes the growing dichotomy between the lack of access to technology in many minority and low-income populations and the necessity for technology skills in the workforce. This trend statement lists 14 specific areas of concentration that the college will provide in all workforce programs across the district to narrow the gap in the digital divide (Lonestar College, 2007, p. 5). In 2003, Wimbish, president of Cedar Valley College (one of community colleges in the Dallas County Community College District), began working with local government to procure a $500,000 grant for the college to incorporate methods to narrow the digital divide for the citizens of Lancaster Texas (Dallas Community College District, 2003). Alamo Community College in San Antonio completed a district-wide survey on bridging the digital divide. This 59 page document assessed the success of Alamo Community College's initiative in providing student access to technology and the Internet at school and in their home. This document also provided recommendations for improving Alamo's outreach for narrowing the digital divide for citizens of San Antonio (Alamo Community College, 2008).

These are a few of the initiatives under way at Texas community colleges to narrow the gap in the digital divide. One of the common themes running through all these

projects is the need to allow access to expensive college resources. This access does not come without costs and risks. Community colleges are spending hundreds of thousands of dollars in taxpayers' money to allow access to and training on modern technology. This investment must be protected both physically and virtually (Song & Ma, 2012). Students, employees, and guests are allowed access to the college's computer and network resources; however, these resources are located in rooms with doors that lock. Most of these computers are locked down to a table via cables. Virtual access must be protected. Computer users cannot have access to any resources or data held by the college without proper credentials, such as self identification and verification of identification. One of the key components to narrowing the digital divide is a proper identity management system (Wiburg, Tellez, Altamirano, & Parra, 2015).

## Summary and Transition

The growth in traditional and nontraditional users of community college and university resources has pushed the limit of IT resources in providing services to many academic communities in a secure environment. The problem that was explored in this study is the inappropriate use of the computer system and the potential for security breaches at community colleges in Texas that can occur because of the lack of tracking guest users. The purpose of this study was to eliminate or mitigate liabilities facing colleges by creating and using security policies to identify guest users. This study combines the theoretical concepts of Cameron's internal security management model with the external trust models of the Liberty Alliance and Microsoft's Passport.

# Chapter 2: Literature Review

In this chapter, I will present a review of relevant literature on the topic of network security with a focus on the policies and procedures at community colleges with an emphasis on IdM models. Wolcott (2007) stated the purpose of the literature review chapter is to link the literature to research and methods that complement and enhance the findings of new research. Leedy and Ormrod (2004) further advised researchers of the importance in aligning current research with previous works related to the study. This gives the researcher a historical perspective of the research topic. Since the historical perspective is important to this study, the primary timeframe for this literature review will be mainly from 2000 to 2009. Literature from an earlier time will be introduced in this research only as a historical reference to show that security problems have been with the industry for some time. Current literature during the last five years will be highlighted primarily as extensions of the trends from previous literature.

The works that I reviewed were mainly related to IdM, but were not limited to this topic. Topics contained in this chapter include research on IdM solutions, the capabilities of IdM architectures, the challenges associated with IdM implementation, IdM features and paradigms, the role of IdM solutions, the growing legal importance of IdM solutions in organizations, mobile IdM systems, information security governance, and the use of client-based and server-based IdM applications. Databases searched for this study include, but are not limited to ACM digital library, Computers and Applied Sciences Complete database, IEEE Xplore digital library, Google scholar, Gartner group, and Educause. Each database was searched using terms such as *identity management*,

*community colleges, network security, community college budgets,* and *bridging the digital divide.* Articles selected for use in this study contained information about how community colleges use security systems to monitor computer usage, identity management procedures, internal and external identity best-of-practices, and community college methods for narrowing the digital divide. This chapter concludes with a discussion of how important IdM solutions have become to colleges and universities.

## Conceptual Framework

### The Basic Elements of an IdM System

The first step in IdM is to establish your identity. In an IdM system, an individual is issued a digital identity once an individual's identity is verified to a central authority. Donnet, Gueye, and Kaafar (2010) listed digital identifiers as unique tokens that are assigned to individuals once an account is setup. These tokens are traditionally issued in the form of a password, ID card, and/or biometrics (finger print, retinal scan, voice recognition, etc.). Any of the above or a combination of the above can then be used with a user ID to allow access to network resources.

The second step in IdM is proving your identity or authentication. The process of authentication begins when an individual logs into a networked computer (Vij, Majumdar, Dhar, & Vanecek, 2014). Authentication is based on matching multiple identifiers provided by a user. The process most networked computer users will recognize is the two-factor authentication, a user ID and password. Authentication is only granted when both are presented correctly to a network directory service. Another example is an ATM card and PIN number. Cash will not be dispensed from the ATM unless both are

present (Jaferian, Hawkey, Sotirakopoulos, Velez-Rojas, & Beznosov, 2014).

The third step is Authorization. In this step a user is given access to network resources. Once a user is authenticated to the network, the user now has access to network resources based upon his or her group, role, or function membership (Whitman & Mattord, 2013). For example, a faculty member once authenticated should have access to the department's printers, network drives, course information, and information about students in his or her class. However, this access is not unlimited. The faculty member's access to student information should include only information relevant to the course. The access also is limited to view only. The faculty member should not be able to change or modify student data. Authorization is initially set up via IT's access control rules. These access control rules will determine if an authenticated user has access to specific network resources (Kulkarni & Tripathi, 2011).

The fourth step is to identify what the user can do with the resources he as access to. This step is known as Entitlement. When a network user logs into a networked computer and is authenticated, the entitlement IdM service examines the first piece of user data (usually the login name) to determine the permissions sets available to the user to access online network resources (Vij et al., 2014). The permissions sets are based upon security policies developed by the IT department and will vary from organization to organization (Bertino, Bhatti, & Ghafoor, 2010).

The fifth step is to make sure all data has integrity. Only those with the proper entitlement to the data should be able to modify the data. Once a network user has been granted authorization to network resources, it does not mean the user has full control over

those resources. Resource control or integrity is the process of protecting data and other network resources from accidental or intentional modification, additions, or deletion. Integrity rules are developed by data creators or managers in conjunction with an organization's IT security policies (Camp & DeBlois, 2013). Decker and Martinenghi (2011) further identified integrity, along with confidentiality and availability, as a fundamental building block of a secure IdM system.

The sixth step is to verify a user's credentials to access to network resources. Ardagna, De Capitani, di Vimercati, Foresti, Paraboschi, and Samarati, (2010) stated that credentials are based upon a token that identifies a user to an information system. Ardagna et al. identified tokens as a unique identifier possessed only by an authentic user. These tokens include, but are not limited to, passwords, ID card, and/or biometrics (finger print, retinal scan, voice recognition, etc.). Any of the above, or a combination, is then used with a user ID to allow access to network resources (Camp & DeBlois, 2013).

All of the above starts with user enrollment into the colleges IdM database. The first time a person interacts with an IdM system, the entity must go through enrollment (Vij et al., 2014). The enrollment process gathers data about the entity such as a person's name. This data collection establishes initial access and authorization to a network. Enrollment occurs when a person is hired as an employee, accepted as a student, or chosen as a vendor or supplier (Camp & DeBlois, 2013). All these examples begin with a vetting process. This vetting process is missing when granting access to guests for network access.

Lastly, is the ability of one organization's ability to accept the IdM credentials of

another organizations. When multiple organizations accept each other's credential they create a federation. A federation begins with an agreement between organizations upon standards and technology that will be used by all organizations in the federation (Jiang, Duan, Lin, Qin, & Zhang, 2011). This allows one organization to join with other organizations (a federation) to allow all users access to the organization's resources. A federation identity is much like a passport. As long as one member of the federation accepts the identity credential, the credentials are accepted by all. Current examples of this are Microsoft's .NET Passport and the Liberty Alliance federation (Bertino, & Takahashi, 2011).

**IdM in Use at Colleges and Universities**

IdM solutions at colleges and universities have traditionally been a joint venture between human resources, the registrar's office, and the IT department. Neuenschwander and Gebel (2008) wrote about two universities that implemented their own in-house solutions. The University of Texas at Austin developed their own home grown IdM solution that integrated their human resource system with student records. This point to point feed was only effective with university data and depended wholly on data collected by the university. User information could not be verified against outside sources nor could the data be shared across multiple domains.

The IdM solution installed at California State University (CSU) used a university wide directory system based on applications that store, sort, modify, and organize user data and system resources. CSU uses Microsoft Active Directory and Novell's eDirectory to provide authentication and authorization to computer resources at the university

(Tipton & Krause, 2012). There are limitations to using a large scale directory system, such as data accuracy and access management. This limitation to a university wide directory system hindered the development of a holistic IdM solution at CSU. Roman, Najera, and Lopez, (2011) stated a holistic approach to IdM is important to the creation of a security framework across the university. This ensures user identification and access controls are appropriate to gain access to the system.

**Cyber Incursions at Colleges and Universities**

Cyber incursions using college computer resources have been used to change student grades, modify transcripts, and alter records. Other cyber incursions have caused theft of intellectual property and financial fraud (Murphy, 2014). According to a survey of more than 500 colleges and universities by The Chronicle of Higher Education and the Gartner Group hackers have accessed alumni, student, and financial information of nearly 41% of the institutions (Stamper, 2012). For example, at UCLA 800,000 records of faculty, staff, employees, students, and alumni were hacked into during December of 2006 (Gilbraith, 2012). Gilbraith also found problems at the City University of New York, Ohio University, the University of Texas, and Tufts University where hackers used cyber-incursions techniques to access personal information.

These incursions into confidential data at colleges and universities cause privacy and security advocate organizations to question the integrity of IT systems and demand more thorough protections. As more and more institutional records are being kept electronically, these demands will increase (Sen, 2010). This survey also showed the transformation from traditional paper records to digital records created security

challenges to both identity protection and information privacy. These challenges emphasize the need for proper IdM systems.

**IdM Architecture at Colleges and Universities**

The ability to recognize individuals who are authorized to access resources and information on a network is the basic principle of all IdM architectures (Tipton, 2012). In the past, individual colleges and universities have used a multitude of IdM solutions. C Colleges and universities used isolated, federated, and central designs to develop network security even at the department level. Jensen (2011) identified isolated IdM systems as the most common IdM architecture. Isolated IdM systems function as both a credential provider and identifier for system users. This type of isolated IdM system has both positive and negative associations. Historically, isolated IdM systems are simple to implement, but difficult to administer. Ranga and Flowerday (2010) noted the barriers of an isolated IdM are the multitude of identifiers and credentials a user must remember and IT personnel must administer.

Figure 3 displays an example of the drawbacks of an isolated IdM architecture. The most obvious drawbacks to an isolated IdM architecture are multi-passwords and multi-user names, different levels of password strength, and different reset methods. The likelihood of forgetting one or more user names or passwords increases with each application and may limit the use of all applications a user will use (Jensen, 2011).

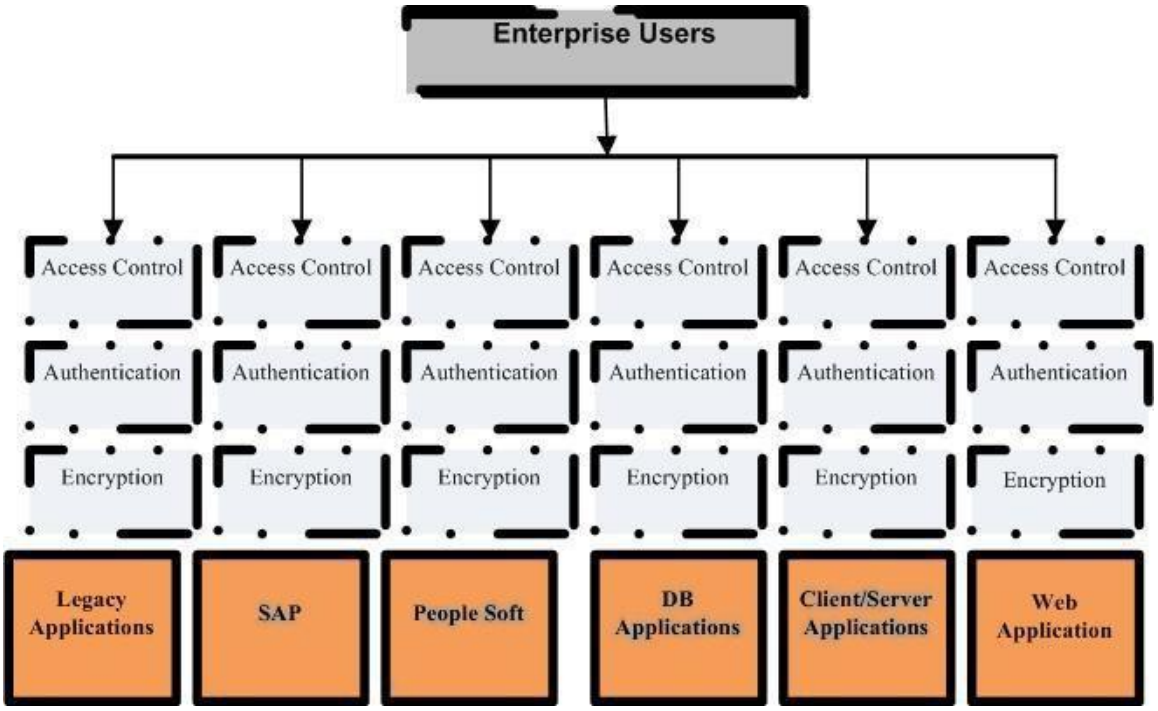


*Figure 3.* The architecture of an isolated identity management system. (Permission to reproduce image)

In response to the growth of isolated systems and its inefficient use of user names and passwords, an internal federated IdM architecture was developed. An internal federated IdM system shares components of credential and identifiers providers within all applications in a domain (Jensen, 2012). This allows IT managers to recognize a unified user name and password combination and share the combination across platforms. As long as one federated application recognizes a user name and password combination, all federated applications become available (Landua & Moore, 2012). Figure 4 shows this relationship between federated applications.

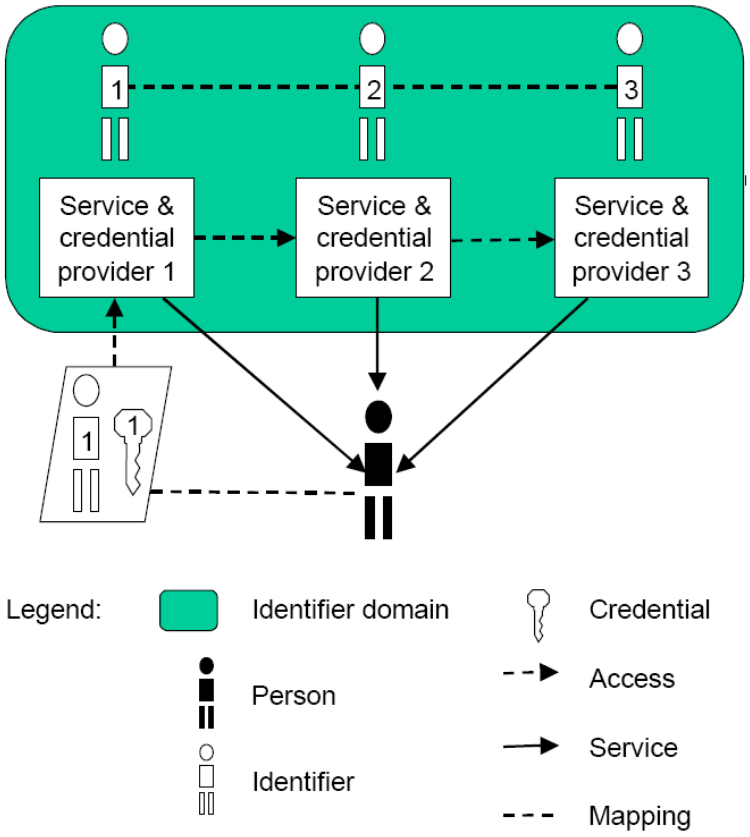


*Figure 4.* An example of a federated identity management system architecture. (Permission to reproduce image)

Federated IdM architectures are being used today in college and university environments. The University of Wisconsin-Madison deployed an internal federated IdM architecture by segregating the organization by business areas such as financial aid, IT, counseling, and human resources. Each business area establishes and maintains its domain's authentication, but participates in the campus wide federated architecture. This allows for university wide resource access while maintaining local control (Stunden, 2006).

The internal federated IdM architecture is much more efficient and effective for users than the isolated IdM architecture; however, there are still some problems. Cao and

Yang (2010) identified the largest problems as mapping. Mapping in a federated architecture requires matching multiple identifiers before the system can identify two or more identities as belonging to one user. Cao and Yang called this synchronization. Another problem occurs with confidentiality. Users should be assured that their information is exchanged and recorded only with their permission.

Lastly is the centralized IdM architecture itself. The centralized IdM architecture has a single identifier and a single credentials provider. The single credential provider is a central repository for all users, groups, and service credentials. Figure 5 shows this configuration. All access is centrally administered which means that all local control is ceded to the IT department. Also, the entire system in a centralized IdM architecture is vulnerable to attack if only one user name and password is discovered by a non-authorized user (Baldoni, 2012). This is a major concern for management in protecting their systems from malicious use.

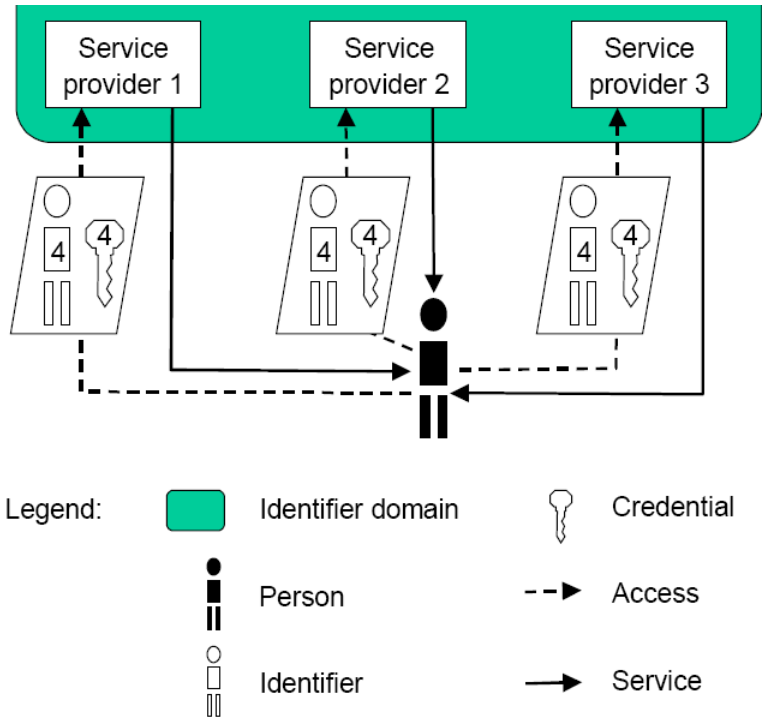


*Figure 5.* A centralized identity management system architecture. (Permission to reproduce image)

Federated centralized IdM architecture has been implemented at CSU-Long Beach (Crase, Malon, Manoharan, & May, 2006). CSU established both the infrastructure and policies of a federated IdM architecture that allowed all areas of the university to participate fully and created an environment that protected stored data including individual user names and passwords and data stored on university servers (Crase et al., 2006). The biggest drawback is all business units have to develop adequate policies and procedures for accessing their applications and data. These standards need to meet minimal security standards and allow access across platforms to users requiring access from another unit (Jensen, 2011).

Although there are problems with all the IdM solutions, there are three common

elements to all IdM solutions (Tipton & Krause, 2012). The authors described these three common elements to all IdM architectures as network security, computer/host security, and college wide services. All three of the common elements are important to a secure college network. Tipton and Krause (2012) emphasized the importance of performing a risk analysis on network security and developing proper security policies and procedures to minimize those risks. The authors identified additional risks associated with colleges as opposed to industry as the need for portability over many campuses and allowing access to those who are not formally recognized by the college. College students, professors, and administrators need to access campus resources from multiple locations. The State of Texas requires community colleges to open their facilities and resources to non-collage users or guests. This is a major challenge for management as the need for portability and openness leaves college networks vulnerable to cyber incursions, especially from guest users.

Roman, et al. (2011) listed several benefits of college wide IdM systems. First, an IdM system helps manage user accounts and passwords. Second, directories limit the need for excess user names and passwords. Third, directories create a single authentication source for users to use across any application or service on the network. Fourth, directories reduce the amount of user names and passwords that must be remembered by the users. Lastly, account management is made much easier. Only one account needs to be changed when a user leaves the college or changes status.

**Challenges in IdM Implementation at Colleges and Universities**

Evans et al. (2004) wrote that implementing an IdM system is a delicate balancing

act between too little or too much access. One of the main purposes of IT at a college or university is to facilitate the free flow of information. Erecting high barriers to information will discourage use of these resources. Setting standards too low will leave the college systems open to abuse. Both of these scenarios run counter to the missions of colleges and universities.

Finding this balance is further complicated by the unique services offered at community colleges and the individuals who use those services. Unlike industry where all employees go through a screening process prior to hire, a community college also has the additional population of students, alumni, and the general population who go through little to no screening prior to needing access to the college's resources (Thain, 2005). Even with granting access by a stable to a semi-stable population or faculty and students, there are additional stresses that must be addressed when a semester begins and ends. Access to resources and data will need to change as students graduate, move to new classrooms, and transfer between campuses. Faculty access also needs to be changed each semester as classes are taught in different classrooms, with different students, and faculty move between campuses. These predictable cyclical changes require a holistic approach to IdM (Beckett, 2006).

IdM requirements are further complicated by the legal environments (Warne & Chun, 2009). In 1974, the U.S. congress passed the Family Education Rights and Privacy Act (FERPA). This act generally protects student personal information and prohibits disclosure without the consent of the parents or guardians of the students (if a minor) or adult students who are pursuing degrees in colleges or universities. Student information

includes financial aid information and grades. The law also grants students the right to access, review, and make corrections to their records. While violations might not result in privacy rights litigation, the U.S. Secretary of Education established the Family Policy Compliance Office tasked to investigate violations. Federal funding to the colleges can be revoked if colleges are found liable, (Francia & Hutchinson, 2014).

There is also the Copyright Act of 1982 which clearly established that computer programs could be copyrighted. This confers upon the copyright holder the right to reproduce the copyrighted work, to prepare derivative works based on it, and to distribute copies of it to the public by sale or transfer of ownership such as leasing or lending. Moreover, it prohibits unauthorized copying and distribution of copies (Johnson, 2000).

Generally, copyright laws help to motivate the creator to continue creating works without fear of losing the proprietary value of their works when distributed publicly. These laws protect the creator's work from "mutilation and deformation" (Hunter, 2005, p. 1). The copyright laws grant intellectual property rights to creators when they register their works formally with their home country's intellectual property rights regulators. The law grants exclusive rights to the artists or creators extending from fifty to seventy years after the death of the artist. The law stipulates that the copyright owner can allow or disallow others from "1) reproducing; 2) distributing; 3) renting; 4) recording; 5) performing in public; 6) broadcasting; 7) translating; and 8) adapting the work or copies of the work" (Hunter, 2005, p. 1).

There are some underlying problems of copyright law when applied to computer applications. Copyright law only covers the source program and object program; it does

not grant the right to control the algorithm. Copyright law "does not extend protection for an original work of authorship to any ideas, procedures, process, and system, method of operation, concept, principle, or discovery" (Johnson, 2000). Thus, when anyone can grasp the underlying concepts and conduct reverse engineering, the original author cannot claim ownership from which the new application was based.

In the United States Copyright Act, Section 106, limits the rights of the Internet users to access, store, and distribute digital materials like "images, sounds, words or data" (Hunter, 2005, p. 1). The Court finds that a violation of intellectual property rights begin when the data or materials are stored temporarily in the computer's RAM. Internet users knowingly or unknowingly violate the copyright act whenever they store or capture data from the web. The Court also found that ISPs are also culpable when their customers use their platform to transmit, disseminate, or access information from the web. The law states "copyright infringement is a form of strict liability" (Hunter, 2005, p. 1). According to Hunter (2005), an individual does not need knowledge and intent to violate a copyright. Thus, enforcement of a copyright law may attach liability to an ISP.

The Health Insurance Portability and Accountability Act of 1996 or HIPAA plays a role in information security if the college collects or keeps medical data on employees or students. This act affects information security in three ways. First, it requires organizations to develop and use information security policies and procedures to protect and maintain health care information. Second, it requires a periodic comprehensive assessment of the policies and procedures set up by the organization to regulate their information security system. Third, it provides guidelines for electronic signatures, user

authentication, and non-repudiation (denial of authenticity). HIPPA does not provide specific procedures for the use or implementation of security technologies for each of the security requirements. It only states that security must be implemented to ensure the privacy of the health records and information.

Colleges and universities are unique in their requirements of having intellectual and academic freedom coexisting alongside user confidentiality and privacy requirements (Oblinger, 2003). IdM solutions must also be able to scale to multiple types of users, both affiliated and non-affiliated, who use network resources. An effective IdM solution for colleges and universities also must take into account legislation such as FERPA, HIPPA, and copyright laws to control access to network resources and safeguard data.

## Role Identity Model

According to Lancianese (2005), the role identity model is another governing principle behind IdM. Role identity modeling enables an individual's identity according to the role the individual serves in the organization. In this situation, the organizational framework of the institution plays a major role. At a community college role categories can include faculty, staff, administrators, students, vendors, or guests. Each of these categories can be subdivided into subgroups. The personal profile allows group members to be modified to meet the specific need of the individual user.

Periodically, the access requirements of these roles will require modification or change. Each semester the access needs for faculty and degree seeking students add additional stresses that must be addressed when a semester begins and ends. Access to resources and data will need to change as students graduate, move to new classrooms,

and transfer between campuses. Faculty access also will need to be changed each semester as classes are taught in different classrooms, with different students, and faculty move between campuses. These predictable cyclical changes require a holistic approach to IdM (Beckett, 2006).

**The IdM Paradigm**

The IdM paradigm is defined by three functions: the pure identity paradigm, the user access or logon, and the secure paradigm (Lips, Taylor, & Organ, 2006). The pure identity paradigm does not depend on roles or user classifications. The pure identity model uses biometrics such as finger prints, voice recognition, or retinal scan. This has become more popular today because more and more devices are being manufactured with biometric reading devices as a standard. Lips et al. pointed out that although the information is classified, the U.S. government is the largest user of pure identification.

IdM solutions are used by colleges and universities to integrate their processes, policies, procedures, and technologies to facilitate and control access to critical systems and resources. IdM not only allows access, but also protects stored information from unauthorized access (Lips et al., 2006). An IdM solution consists of administration over user authentication, access rights and restrictions, account profiles, passwords, and other identification attributes. Lips et al. also stated that an IdM system once installed will facilitate new convergence of systems and resources when they are added, updated, or changed. A true IdM system should integrate all network and data resources. This list contains, but is not limited to devices, network equipment, portals, content, applications, and products as well as the user's credentials, address books, preferences, entitlements,

and telephone numbers (Tipton & Krause, 2012). The service paradigm is used at colleges and universities with convergence technology to upgrade, modify, and change network data via online services. Services include updates to devices, network equipment, portals, content, application, products, credentialing, preferences, entitlements, and even phone numbers (Lips et al., 2006).

**IdM Implementation Challenges**

There are several challenges to implementing an IdM system. Baldoni (2012) stated that the largest challenge to an IdM solution is convincing stakeholders of the needs and benefits of an integrated IdM system. The other challenges include developing proper business procedures, upgrade and maintenance, and the lack of support from community college leadership. It is interesting to note that these challenges are some of the same challenges of change management (Fisher-Hubner, 2008). Successful change management includes understanding and acceptance by organization members, proper planning, buy in by top management, and proper training and motivation of those affected by the change. All these are critical to successful change management. Lips et al. (2006) also listed a lack of proper testing and inadequate focus on long term IT infrastructure planning as additional challenges.

Johnson (2000) stated that community colleges and universities across the country face increased competition for students. Since 1960, the number of community colleges in Texas has quadrupled (Hudson, 2008). Along with this increase in competition comes increased scrutiny by State and Federal governments regarding data security and privacy. This scrutiny has forced community colleges and universities to enact IdM policies and

procedures to avoid fines, penalties, and further regulations. Johnson noted that many community colleges and universities have found answers to IdM requirements in service-oriented architecture (SOA) or a combination of SOA with organizational needs. Since SOA is platform independent it can be used by different departments to meet multiple needs. Departments are now free to develop solutions independent of the IT department and stay within compliance. Departments do not have to wait on IT to respond to changing markets (Johnson, 2006).

Johnson (2006) further stated use of SOA by community colleges and universities has enabled fast response in the IT environment while requiring fewer IT resources. Information technology departments also use SOA in the integration of resources. This allows for better data consistency and ensures compliance with regulations such as FERPA. Johnson noted there are pros and cons to SOA. The largest benefit is speed and agility when integrating heterogeneous platforms. The largest drawback is that it leaves data vulnerable to security breaches during the process. Potential data breaches can occur even when the IT system's architecture is closed or proprietary. At risk are the web applications and internal business functions used by students, faculty, vendors, and suppliers.

Johnson (2006) further pointed out that breaches to online systems such as marketing services, online access to grades, personal data, registration services, medical information, financial aid information, and admissions records, may occur. These risks can be reduced with a proper IdM solution. A properly implemented IdM solution increases institutional effectiveness and efficiency; increases compliance to regulatory

requirements; facilitates improved security for authorization to data, services, and resources; reduces fraud, and improves reaction time to system changes (Mesmer, 2009). Lips et al. (2006) also pointed out that IdM solutions have a high rate of return on investment. The authors stated that organizations just utilizing auto-provisioning an organization with 10,000 employees can see annual savings of over a million dollars. Savings can also be recognized by a decrease in personnel, system downtime, and data breaches. Other potential savings occurred in the reduction of potential litigation. The author based these savings on a calculation that assumed an average reduction of 47% in management of user access and help desk inquiries.

Lips et al. (2006) also noted IdM problems stem from the traditional IT architecture which began by managing small groups of non-related users. As the groups grew and resources need to be shared, both inside and outside of the organization, traditional IT management broke down. A good example of this is multi-user names and passwords a student or faculty member needed to remember in order to access multiple system resources. One user name and password combination was needed to login to a college's network, another user name and password was needed to login to an e-mail account, and then another user name and password combination was needed to access student records, and so on. Each user name and password combination had its own set of minimum acceptable rules for creation and expiration. Rarely were the two systems' rules the same. A forgotten user name and password required the services of the IT department's help desk to verify user credentials and issue a new user name and password. This use of IT resources has a very low rate of return. Lips et al. (2006) stated

the reason for this inefficiency is due to "treating IdM as a separate and distinct solution often inserted into applications as needed post deployment" (p. 212).

Lips et al. (2006) further observed that the primary IdM problem at community colleges and universities is the manner in which access is granted to applications. Systems that worked independently on a small scale were expected to work interdependently on a large scale. This was rarely, if ever, the case. Management of password growth and integration became unmanageable because each application had its own policies and procedures for user name and password. This independence worked well on the small scale; however, with growth, integration, auditing, and compliance issues made this independence unacceptable. Lips et al. (2006) concluded that the current independent IdM systems used by many applications must be replaced by enterprise wide systems that are stronger, more adaptable, and consistent with cross-platform IdM solutions. Continuous improvement to integrated IdM solutions will require buy-in from the community college's top management. It will also require additional human and financial resources. Larger colleges have more of each and can set benchmark standards for smaller colleges. Once larger colleges have integrated solutions in place, smaller colleges can implement integrated IdM solutions that will fit the college's needs.

Lederer, Hong, Dey, and Landay (2004) also wrote extensively about the problems with early IdM solutions. The authors concluded that the difficulty in creating a proper IdM solution was in its meaning. There are multiple interpretations of the word privacy. This ambiguity led to multiple solutions across multiple platforms and applications. Lederer et al. further stated that research in the technical and design issues

of IdM must be addressed. The authors' concerns were groupware privacy practices, access to multimedia environments, e-mail, file sharing systems, and virtual private networks. Their research led to findings that independent IdM systems are problematic to users and IT managers due to improper or antiquated designs. These system designers can avoid these IdM problems or pitfalls and create meaningful IdM solutions based on modern IdM conventions. The authors recognized five pitfalls in many older IdM solutions:

1. *Obscuring potential information flow* – Systems should make clear who and when data might be conveyed to a third party. This can be done in clear security policies.
2. *Obscuring actual information flow* - Systems should make clear when data are actually conveyed to a third party. This can be done with pop-up messaging boxes when data are transferred to a third party.
3. *Emphasizing configuration over action* – Systems should use simple configuration when creating and maintaining privacy. Users should be educated about data sharing and be able to interact with the system.
4. *Lacking course-grained control as related to action* – Systems should give users an obvious method to opt out or limit data as it is being transferred.
5. *Inhibiting establishing practice as related to action* - Systems should not have different practices for data transfer in similar situations.

Identity management systems have two major problems that should be resolved regarding privacy and cold start issues. These issues are not new (Koch & Moslein,

2005). Pentafronimos, Karantjias, and Polemi (2011) continued this research. Privacy is a control issue and can be reduced or eliminated by placing controls on identification information in the hands of the user. Cold start issues can be solved by allowing users to re-use identification information held on servers instead of re-entering all data. This is only possible if users understand and separate the utilizations of identity data and storage of the identity data.

Pentafronimos et al. stated that separating identity usage from identity storage makes it possible to re-use identity data. User data can be stored and accessed in a single location. The authors pointed out that this is not unique to IdM. People give out, limit, and change identification data all the time in real life. Casual acquaintances do not have the same amount of personal data as a closely held friend. Some people even change the identity data they share. Some people will use a nickname in one social setting or with one group, but use their given name in others. By using this as a launching point for IdM systems, users can create different identities for the different roles associated with their personal data and decide which data will be transferred in those different situations. This type of IdM would empower users to maintain their own identity information and control how that information is being distributed.

**IdM Applications**

Donnet, Gueye, and Kaafar (2010) stated that most IdM researchers focused their efforts on user profiling and IdM application and solutions. User profiling involves source coordination of data on a network. Each node on a network sends and receives data. Nodes receiving data should be able to determine if the source node is a legitimate

node or a mischievous node. IdM application and solutions assist network administrators in collecting, analyzing, and disseminating user identification across a network. These applications and solutions are established into two categories: client-based profiles management and server-based IdM solutions.

*Infomediaries:* According to Pentafronimos et al. infomediaries can be stored locally (client-side) and data can be distributed as needed. This solution will keep data near the user and increases trust by allowing the user to control and monitor the usage of their identity data. These infomediaries are small applets located on the client computer that allow users to manage their data and create auto fill-ins for Web forms. The main drawback of this solution is an infomediary is not portability. Also, current configuration of infomediaries is too complex for an average computer user to use on a daily basis.

*Single Sign-On and Server-Based User Profile Databases*: Server-based solutions solve the problem of portability; however, they add complexity. Multiple servers are required in a trusted environment. A single sign on (SSO) allows applications stored on multiple servers in multiple locations access sufficient identification information about a user even if the user does not initially login to the application. Pentafronimos et al. stated many software vendors use SSO for intranet and extranet applications. This service is made possible through the X.500 directory services standard or through the light weight access protocols (LDAP). These solutions are casually proprietary, requiring uniform software and hardware. Global solutions available via the Internet require trusted third-parties such as Microsoft's Passport or Liberty Alliance.

Pentafronimos et al. listed the core of an SSO solution as a centralized user profile

directory accessible via a Web interface. An SSO is certified by accessing a profile stored on a centralized data server and is accessed when a user logs into an application. The two most popular SSO solutions are Microsoft's Passport and the Liberty Alliance Project. The authors stated that both of these SSO solutions are widely used by consumers, but stress the two are not the only solutions.

*Microsoft Passport*: Pentafronimos et al. described Microsoft's Passport as a suite of services that authenticate users across a number of applications. The Passport SSO service solves the authentication problem for users by allowing them to create a single set of credentials that will enable users to sign into any cite that supports a Passport service. As a part of the SSO service, users can store commonly used information in a Passport profile and transmit it to the participating cites they visit. This reduces the barriers to acquiring users because new users are not required to retype information when they register at a new cite. It also enables the sites visited to customize and enhance their experience without having to prompt the user for information. In essence, this centralized user identity management system provides a competitive advantage for Microsoft and gives free access for all Microsoft customers.

Pentafronimos et al. stated the biggest drawback to Microsoft's Passport is the requirement of users to agree to share identity information in order to participate in the Passport services. Once a person signs up with Passport they no longer are in control of their data or how it is used. This lack of control has led to security issues and privacy concerns. Problems occurred with eavesdropping during redirects and the ability to steal authentication tokens have been major issues with Passport.

*Liberty Alliance*: Pentafronimos et al. stated the Liberty Alliance Project is an alliance of more than 150 companies, including nonprofit and government organizations around the globe. Interestingly enough, the alliance does not include Microsoft. The consortium is working on an open standard for federated network identity that supports all current and emerging network devices. Federated identity is supposed to offer businesses, governments, employees, and consumers a more convenient and secure way to control identity information in today's digital economy. The authors stated the goal of the Liberty Alliance is not to create an electronic environment where identity data can be shared among members, but to confirm or deny the credentials of personal information when used to log into a member's application or service.

Members of the Liberty alliance are able to share access to, or gain interoperability among, disparate IdM protocols. This shared access is commonly known as a circle of trust. Members must have a well-defined agreement between the service providers, notify users when their data is being accessed, and have user consent when collecting information to participate in the circle of trust (Pentafronimos et al., 2011).

*Web Service Federation*: Pentafronimos et al. noted that missing from the Liberty Alliance are two big players in the computer industry: Microsoft and IBM. These two companies have formed the Web Services Federation. This uniform approach to Web services environment focused on a security based architecture. This service provides protocols for attaching identification and security cookies to data transferred throughout the Internet. Web Services Federation extends the trust standards throughout all federation members and services through a SSO.

*Profile Information Exchange:* This commercial service synchronizes user profile data that can be exchanged through an electronic business card setup by the user. Members enter their data into a replicable database which makes a subset of all data viewable to other members (Pentafronimos et al., 2011). Profile Information exchange is an IdM solution that uses a decentralized, distributed approach to data storage (Bhargay-Sparntzel et al., 2005). This model uses a distributed protocol for information sharing. Distributed protocols increase security and avoid many of the security issues of a centralized database. Users are responsible for entering and updating their own information. As long as the data is part of the federation, all information is presumed accurate. User data, or attributes, can now be used in a SSO identification model. User attributes are protected from identity theft by combining the user's data with ordinary data.

**Integrated Support**

An IdM solution is not a small project and it is always part of a larger system. Dixon (2005) emphasized as the size of a project increases so does its complexity. Systematic approaches must be used to limit resources needed to complete the project. To develop an IdM system, an organization needs six key components: allocate costs, develop schedules, identify available resources, ensure product quality, evaluate functionality, and maintain optimal performance. Dixon (2005) also identified three additional areas needed for extensive management and support: human resources, resource management, and budget management. All resources are limited including human resources. Quality human resource management, actual resource management,

and budget management ensure that all resources used on the project are used correctly and efficiently.

Both technology and human resources are needed to maintain a secure network. Understanding the balance has been an issue in the IT department for decades. According to Barati et al. (2013), many organization managers believe an IdM system can do all the thinking and analysis needed to protect a computer network. The authors saw this as a natural response to the lack of skilled security professionals and the high cost of training IT professionals in security management. Automated IdM systems are adequate for vetted system users such as employees, students, and vendors. Those outside of the vetting process, such as guests, can only be given authorization to use system resources from trained analysts. Successful IdM solutions need both technical and human resources solutions. Both of these requirements need to fit within budgetary constraints of the organization.

**Mobile IdM Systems**

Access to the Internet on college campuses is becoming more and more wireless. Wireless IdM solutions brings with it new and unique IdM requirements. Mobile IdM systems communicate using role-based access control (RBAC) as well as providing identification information. RBAC protocols will work on almost all mobile devices from smart phones to laptops (Blakely, 2009). Most community colleges in Texas limit wireless access only by range. Identity is rarely an issue when accessing a wireless access point. The major benefit of an RBAC is in providing identification to system users requesting access to resources. These benefits do come with extra costs and additional

infrastructure (Chen, Lin, & Hou, 2011).

The main benefit to the audit trail of users' activities was to protect against law suits at community colleges. Other benefits are account creation and deletion, the ability to break down barriers between data silos, and better management of user data. Limitations were usually associated with institutional applications. Identity management loses scalability when applications were setup as standalone applications which cannot participate in an IdM solution. The solution will come over time as many of the standalone applications are abandoned, updated, or merged into suites that allow SSO (Sen, 2010). Until that time, many IdM solutions will remain complex and expensive to implement. Along with these limitations was a lack of granulation and an all-or-nothing approach to SSO access. Fine grain access controls that allow full or partial access need role definitions as part of the IdM solution. This type of fine grain access currently was only accessible outside of an IdM solution.

Another obstacle to a true IdM solution was mapping to existing identification data. Users of one IdM solution may not have their data in a location or format accessible to the new IdM solution. This problem became more complex as the organization grew and the number of additional IdM solutions go online (Camenisch et al., 2011).

Barrère, Hurel, Badonnel, and Festor (2013) estimated the high cost to integrating mobile IdM solutions. The authors estimated from $20 to $30 per user for a mobile IdM solution and an additional $40 to $180 for integration. These costs are high, but more and more colleges and universities are moving to mobile IdM solutions. Along with the improved security and privacy, an IdM solution also provides tracking and auditing

functions required in FERPA, HIPPA, and SOX (Camenisch et al., 2011). In these situations legal compliance is driving IdM solutions, not ROI or innovation. Once a regulation requirement has been placed into law, college presidents, CIOs, and trustees cannot avoid adhering to compliance issues.

Wilson and Tharakan (2008) and Camenisch et al. (2011) agreed that the future of IdM will include mobile components and be adaptable to rapid change in requirements and technology. Community college CIOs will need to keep pace with this rapid change and allocate technical, labor, and financial resources to meet the challenges to their institutions.

**Recent Contributors**

IdM solutions for corporations and governments have been the focus of much research over the past several years. However, solutions for community colleges and universities are few and far between. Tipton and Krause (2012) studied IdM solutions currently being used by community colleges and universities. Their work focused on how the IdM solution was designed, developed, implemented, and updated. Luallen and Labruyere (2013) also studied IdM solutions at community colleges and universities and found them outdated, inefficient, and actually posed a threat to IT infrastructures.

Reviewing current IdM literature from 2005 to 2014 reflects a change from earlier IdM research. Early IdM research focused on a one size fits all approach. As of 2014, research pointed out the challenges community colleges and universities face because of the wide breath of services provided and the needs of the diverse population served. Scott and Johnson (2011) identified students, faculty, staff, alumni, and applicants as unique

and consistent users of resources of community colleges and universities. Scott and Johnson's research additionally identified guests, vendors, and mobile users as partial users of unique systems. Each of these has unique needs.

The goal of this research was to advance the practice, knowledge, and understanding of IdM in the IT field in overcoming current problems. Protecting data, applications, and hardware, as well as providing an audit trail became mandatory in many cases. Reaching this goal will advance access to community college resources to a wider community with less risk. This goal can be reached as long as access is secure, safe, and auditable resulting in increasing access to community college resources far beyond current traditional community college needs (Luallen & Labruyere, 2013).

**Anonymity and Crime**

In 1988, Morris, a graduate student at Cornell University, drove across Cambridge Massachusetts to the Massachusetts Institute of Technology (MIT) to launch what would become the first Internet worm. Within days, nearly a quarter of the computers on the Internet no longer worked. Morris was only found because he turned himself into authorities. He did not expect this type of large scale damage to the computers (Sudduth, 2001). When asked why he launched the worm from MIT instead of Cornell, Morris stated that he wanted to disguise the fact that he was the author (Newman, 1991). Since that time, there have been many such individuals who derive a strange satisfaction from anonymously causing disruption and damage to computer systems.

Broadhurst, Grabosky, Alazab, and Chon (2014) identified anonymity as a key component in criminal activities. They differentiated true anonymity from pseudo-

anonymity. True anonymity occurs when it is impossible to identify a person. Examples of true anonymity range from unsigned letters to criminals using masks. Pseudo-anonymity occurs when it is difficult to ascertain identity. Examples include reporter's sources, membership lists, whistle blowers, and witnesses to crimes. Criminal activities fall primarily into the true anonymity category (Broadhurst et al., 2014).

Anonymity is not unique to the Internet; however, the Internet offers unique opportunities. Kang, Brown, and Kiesler (2013) wrote extensively about anonymity and the Internet. The authors noted that the identity of Internet users is not directly tracked in many systems. Messages on the Internet are tracked through IP addresses. These IP addresses are issued to identify equipment on the Internet, not to identify individuals. Even individuals who purchase IP addresses through their Internet service provider (ISP) can hide their identity by sending messages through anonymous servers. The Internet does not check personal identification. Even third party service providers, such as hotmail, allow pseudonyms. The authors agreed there is a place for anonymity on the Internet; however, this anonymity should only extend to users on the Internet who use their own equipment. Information sent through the Internet can only be tracked back to the sending computer, not to an individual without proper identity management (Kang et al., 2013).

Many IdM researchers agreed with this assessment. Evans et al. (2004) wrote that implementing an IdM system is a delicate balancing act between too little or too much access. One of the main purposes of IT at a college or university is to facilitate the free flow of information. Erecting high barriers to information will discourage the use of

network resources. Setting standards too low will leave the college's systems open to abuse. Both of these scenarios run counter to the missions of colleges and universities.

Finding this balance was further complicated by the unique services offered at community colleges and the personnel who use those services. Unlike industry, where employees go through a screening process prior to hire, a community college also has the additional population of students, alumni, and the general population who go through little to no screening before accessing the college's resources (Scott & Johnson, 2011). Even with granting access to a stable or semi-stable population of faculty and degree seeking students, there are additional stresses that must be addressed such as when a semester begins and ends. Access to resources and data needed to be changed as student's graduate, move to new classrooms, or transfer between campuses. Faculty access also need to change each semester as classes are taught in different classrooms, with different students, and faculty move between campuses. These predictable cyclical changes require a holistic approach to IdM (Beckett, 2006).

**Liability Issues in Internet Usage**

Whitman, Townsend, and Hendrickson (1999) asked two very interesting questions; What if an organization does not support or even encourage strong ethical conduct on the part of its users? What if an organization does not behave ethically? The authors postulated that there can be liability even if there is no criminal conduct. Liability, or an entity's obligation to do something, can be applied to personal conduct even when no law or contract has been breached. The authors defined liability as a wrongful act which includes the obligation to make payment or restitution compensation

for the wrongful act.

Liability can be placed on an organization if an employee commits an illegal or unethical act that causes harm. This is true even if the employee is acting with or without authorization. This liability can increase if the organization does not have policies and procedures in place (Youngdale, 2009). These policies and procedures are called due care (Gallegos, 2002). Due care not only means that the organization has policies and procedures in place, but that these policies and procedures have also been communicated to employees. This ensures that every employee knows what behavior is acceptable. Due care also includes the consequences for unacceptable behavior. Gallegos (2002) indicated that true due care occurs when an organization makes constant efforts to inform and educate their employees about the policies and procedures. Because of the Internet, it is possible that a person could be wronged by an organization from anywhere in the world. Due care has become very important to the protection of organizations.

**Information Security Policy for an Organization**

All organizations, especially large organizations, need to have policies, procedures, and practices for their employees to follow. These activities came from industry best practices, governmental regulation, and customer requirements. Development and implementation of community college information security policies are defined in this section. Organizational information security policy literature is examined to discover institutional security policies and how structural and functional features are developed to secure an organization.

There are different approaches in developing policies which strive to solve broad

political, social, and organizational problems to serve the public good or advance organizational goals. Even with the different approaches, most strive to increase efficiencies and effectiveness of the organization (Colebach, 1998). Organizational policies are an attempt to standardize business practices, both internal and external, that act as guidelines to describe how an organization's personnel should behave in a given situation. These policies should support the organization's strategic goals and objectives by maximizing the organization's efficiencies and strengthen the effectiveness of the organization's resources (Browne, 1997).

An organization's information security policies are developed around functional areas. Organizational information security policies begin with a statement of the organization's beliefs, goals, and objectives developed at the top level of management (Peltier, 2013). These policies should also describe how the objectives of protecting the organization's assets will be obtained. Lastly, these policies should address how the organizational resources will be used and protected.

Creating policies to protect an organization is not a new issue. Administrators have created organizational policy for many years. Moore (1994) described three levels at which organizational policies should be addressed: industrial, organizational, and societal. Each level has its own construction and elements. Moore gave five elements that should be present at the organizational level for constructing information policies:

1. *Information technology:* Addresses the information systems development to handle current and new technology integration into the organization.
2. *Information markets*: Addresses how the organization will handle access to

information external to the organization.

3. *Information engineering*: Addresses the design of the information systems.
4. *Human resources*: Addresses the skill levels needed by personnel using the organization's information system.
5. *Legislation and regulation*: Addresses the issues associated with organizational compliance to the legal and regulation environment.

These organizational security elements should then be used as directions for guiding and developing the technical security policies for implementation. Baskerville and Peltier (2013) identified two categories related to organizational security policies. The technical or computer security category is the first. This category dealt with securing the information architecture, access control to the organization's computer system, and other security mechanisms needed to keep the organization's computer system from harm. Most of this category is technology driven. The category defined how new technology, both hardware and software, should be integrated into the organization. Security management was the second category and deals with social issues concerning an organization's security. This category focuses on an organization's security governance, access and/or restrictions for users, and system design. An organization's information security policy is the foundation document for information security managers. These policies must support the mission, vision, and objectives of the organization as well as guiding the behavior of the institution's personnel regarding information security (Hone & Eloff, 2002).

One of the primary purposes of organizational security policies is to make sure

that user rights, privileges, responsibilities, and duties are within the organization's control (Hong et al., 2006). In this sense, organizational security policy creates the proper user guidelines that describe the proper environment and behavior for accessing an organization's information system. According to NEC Unified Solutions (2002), compliance was another function of an organizational security policy. NEC defined compliance as an organization's security policy that focuses on meeting external regulation placed on the organization by legislative bodies.

Information security policies should also describe and develop the groundwork for all activities surrounding security programs of the organizations (Walton, 2002; Hone & Eloff, 2002). Additionally, information security policies should also function as to what Fitzgerald (1995) called the basic fundamental building blocks of development for information security. These policies should contain descriptions of all the supported programs of an organization's information security infrastructure.

The concept of organizational governance is a mature discipline. Methodology for creating organizational policies has been around for many decades. Karin (1983) described a four step process for developing organizational policies:

1. *Identify the issues*: In this step an organization defines the information security problems that need to be address.
2. *Formulate an information policy*: In this step an organization creates the policy statements that directs the behavior of the organization's information system and how the organization will support these systems and services.
3. *Define the information policy area*: In this step an organization identifies how

it will facilitate the decision making processes in the policy of information security.

4. *Establish information policy measures*: In this step an organization creates the security policy metrics in which to measure information security policy effectiveness.

Another view of organizational security policy came from Karyda, Kiountouzis, and Kokolakis (2005). The authors believed organizational security policies should be developed in three steps:

1. *Formulation*: In this step, organizations decide the policy issues, develop policy standards, create policy statements around the standard, and create security performance measures.
2. *Implementation*: In this step, organizations take the security policy, created above, and translate them into procedures or best practices to guide the organization when the security policies are implemented.
3. *Adoption*: In this step, organizations formally adopt the policies and they become part of the normal operational practices of the organization.

A fourth step was also identified by Garigue and Stefaniu, (2003) and expanded by Wiant (2005). These authors added a review step to Karyda, Kiountouzis, and Kokolakis' list. In this step, organizations periodically examine their policies and assess their effectiveness.

Creating information security policies has also been taken up by Doherty and Fulford (2006). These authors describe eleven critical elements an organization must identify when developing their information security policies. These authors took a more

technical approach by adding specific topics to address when creating information security policies:

1. *Personal usage of information systems*: This element describes the rights and responsibilities of a user when accessing organizational information systems.
2. *Disclosure of information*: This element describes the organization's security policies individuals need to follow in order to access and disclose private data held by the organization.
3. *Physical security of resources*: This element describes how the organization needs to protect the physical assets of the organization from theft or damages along with how the organization will protect their information system's infrastructure.
4. *Violation and breaches of security*: This element describes how the organization will recover lost data due to a security breach or disaster and how the organization will document their lost data.
5. *Prevention of viruses and worms*: This element describes how the organization will protect against incursions from hackers, viruses, and worms. The policies should also address how the organizational users will handle e-mail attachments and information sharing software.
6. *User access management*: This element describes the requirements needed for users, both internal and external, to access information resources.
7. *Mobile computing*: This element describes the use of mobile devices such as laptops, tablet PCs, and hand held devices and how these resources will be

protected.

8. *Internet access*: This element describes the acceptable Internet access with respect to non-business related browsing.
9. *Software development and maintenance*: This element describes the guidelines needed for software to meet for effective security controls across the information system.
10. *Encryption*: This element describes the methodology to be used to encrypt information passing between user computers and organizational servers.
11. *Contingency/continuity planning*: This element describes how the organization will recover from security breaches and disasters.

Using an organizational approach for security policy development in higher education has two noted champions, Bruhn and Petersen (2003). The authors identified a void in policy development at universities and colleges when writing security policies for their institutions and they argued that top management should embed the informational security policies into their strategic governance structures. The security policies of colleges and universities should clearly define the institution's purpose and scope for securing institutions resources. Security actors also need to be defined. The authors defined security actors as anyone with duties or responsibilities for the security of institution's resources, equipment, or data. Each type of actor should have their own unique needs and requirements. These requirements need to be recognized and addressed by the college's top management.

The institution's security policies should identify and describe the processes,

procedures, guidelines, best practices, and standards used by the institution regarding security. Organizational documents that describe security policies need to state clearly the acceptable behavior of users, both internal and external, when using organizational resources. The primary resource for the institution should be the organization's security policy (Figure 6).

| Information Security Policies |
| --- |
| Additional Organization Policies |
| Information Security Standards |
| Guidelines and Working Papers |

*Figure 6.* Hierarchy of published documentation for information security policy.

From an organizational approach, the college's information security policy is a document that describes the security hierarchal structure. The organization's information security policy should document the objectives and goals of the college. Figure 6 shows the security policy hierarchy for an organization. Bruhn and Petersen (2003) called this the organization's pinnacle document of the organization regarding security strategies. Purser (2004) went further and identified four functions that all security statements must include. First, the organization's information security policy should provide guidance to the organization on all security matters. Second, the organization's information security policy should form the basis for the security control framework of the organization. Third, the organization's information security policy should define the security roles and responsibilities within the organization. Lastly, the organization's information security

policy should articulate the organization's position on issues within the documents. Purser (2004) believed that following these four steps the organization would make its information security policy the essential component that will drive an organization's security standards.

Setting standards in an organization is not a new development. Weiner (1966) linked standards of the organization with IT and technology advances in research and development. Organizational standards could be created for many reasons from regulatory compliance to creating a competitive advantage for products and services (Kleblawi & Sullivan, 2007). Peltier (2013) went deeper with security standards as he believed that security standards play a vital role in guiding, monitoring, and supporting the information system of an organization. Security standards should also establish consistent, objective, and reliable security metrics to measure the effectiveness of security in an organization (Hajdarevic & Allen, 2013).

Bennett and Schuster (2008) went even further and stated the combination of an organization's security policy and security standards will establish the framework for information security programs in the institution. Thus, the establishment of security standards in an organization would create a baseline for security standards and form channels of communication to implement security best practices to support information security programs.

Many IT and security professional organizations have created generic security standards. Though the entire list of standards is beyond the scope of this study, three important security standards are worth mentioning. First is the Control Objectives for

Business Information Technology (COBIT) targeted an organization's business processes relating to security governance (von Solms, 2005a). Second is the National Institute of Standards and Technology (NIST), an agency of the Commerce Department, created several information security standards. The main security standard is SP800-100 (NIST Special Publication, 800-100, 2006). This standard provides guidelines for chief information officers (CIO) and other information security managers of federal departments regarding their responsibilities for creating, managing, enforcing, and evaluating the security infrastructure of an organization.

Third is the International Organization of Standards ISO 17799. This international standards organization divides security management into five categories; strategy, technology, organization, people, and environment (Saleh, Alrabiah, & Bakry, 2005). These five categories can be broken into ten separate security processes that support the development and maintenance of an organization's information security compliance. Any size organization can implement ISO 17799 and there is a certification process (Saint Germain, 2005). In 2005, the standard was expanded to information security management structure and controls identification and renamed ISO 27001. The new standard focused more on Deming's plan, do, check, and act cycle that make measuring key performance indicators easier and more systematic (Humphreys, 2007; Boehmer, 2008).

**Information Security Governance in Higher Education**

In this section, the conceptual framework of information security governance was defined from an organizational perspective. The section concludes with an overview of information security literature that focused on colleges and universities.

Von Solms (2010) described the theoretical construct of information security governance as a series of waves. The first wave consisted of the IT component associated with information security or the technology framework. Second was the organization's security structure or information security management. The third wave was concerned with how the organization institutionalizes information security. The author also stressed that information security governance does not exist in a vacuum. The information security governance framework existed within the regulatory environment of the institution. The authors agreed with Lindup (1996) that legal requirements were the first place security professionals should look when developing information security policies.

Information security governance was the first step to information security management which leads to information security operations. This relationship needs to be more than just policy and procedures that reflect best practices. The relationship needs to be incorporated into the strategic planning of the institution along with the decision making process when it comes to protecting the information assets of the institution (Brotby, 2007). Strategic security planning requires the support of the institution's top management (Pirani & Spicer, 2006). This is where creating an effective information security framework becomes a bigger challenge. Top administrators at academic institutions too often see security as an aside to the academic mission of the institution (Clark & Sitko, 2008).

Moulton and Coles (2003) defined information security as "the establishment and maintenance of a controlled environment to manage the risks relating to confidentiality, integrity, and availability of information" (p. 581). Organizational use of best practices

for information security governance framework should not be limited to just user access. An organization's information security governance framework needs to cover all aspects of information security. Von Solms (2005a) explained that information security governance as top management's commitment to leadership, structure, awareness to policies, procedures, and practices involving IT technology. The author also stressed the use of enforcement mechanisms to ensure the confidentiality, integrity, and availability of the organization's IT and information assets.

Regulatory compliance issues concerning information security management revolve around both internal and external drivers. Information security framework must ensure the information system processes of an organization comply with all governmental legislative and regulative requirements. This due diligence requirement was not new to organizations (Lindup, 1996). Part of an organization's reasonability was to keep security practices aligned with governmental requirements (von Solms, 2006). From the standpoint of governmental compliance, the information security governance framework had the duty of managing organizational information risk with the governmental regulatory environment (Posthumus & von Solms, 2004)

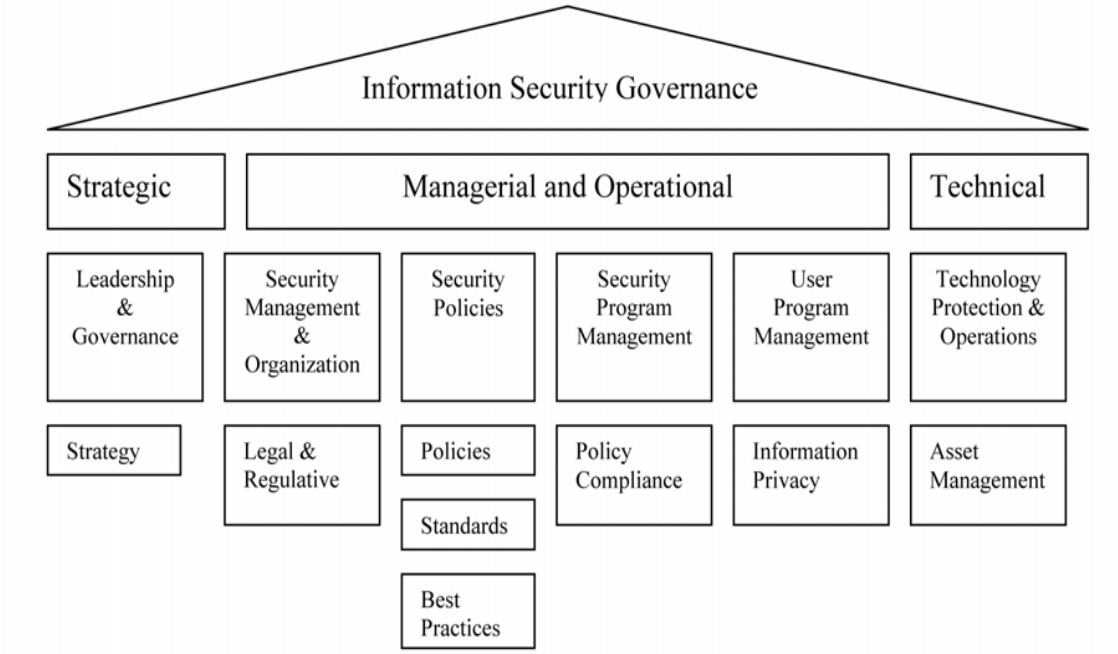


*Figure 7.* Information Security Governance Framework. (Permission to reproduce image)

Information security governance can be viewed as a house (Da Viega & Eloff, 2007). The above diagram (Figure 7) shows information security governance as the roof that covers strategic, managerial, operational, and technological functions of an organization. The strategic level was concerned with leadership and support of information security. Activities such as overall security planning for the organization were completed at this level. The managerial level was concerned with policy development and compliance, program development, standards, best practices, and privacy issues with information security. Lastly, the technical level was concerned with asset management and information integrity issues.

Strategic planning and decision making were activities of information security governance (Garigue & Stefania, 2003). Both also played a significant role in regulative compliance for the organization. Another view of information security governance came

from de Oliveira et al. (2006). The authors argued that the primary responsibility of information security governance was to coordinate people, technology, and processes associated with the security of the organization. The main responsibility of information security governance is to create and support all information security activities of the organization. It should also clearly define the structure, roles, and responsibilities of all entities within the organization. Rosenblatt (2008) added that the responsibility of creating information security programs, such as risk assessment, compliance, asset monitoring and protection, security awareness, and educational programs, were also part of this process.

Information security governance does not exist in a static environment. Information security was originally one of the responsibilities of the IT department. Security awareness and importance have seen an increase in significance in the past decade. Many organizations now have chief information security officers (CISO) whose primary responsibility is the information security of the organization. Some of the traditional security responsibilities of the CISO are policy development, education, awareness, investigation, and disaster recovery. Many CISOs also have taken on the responsibility of vendor relations (Whitten, 2008). The prototypical CISO has deep IT technical skills, strong communication skills, and leadership skills.

Information security in academia has not been studied deeply and even fewer studies have looked at the security governance structure at colleges or universities. In one of the better studies, even though it is ten year old, Burd (2004) found that academic institutions were beginning to develop information security baselines. The study found

that the major information security challenge to an institution was a lack of security standards in higher education. The study found corporate information security models were not well suited for the academic environment. New information security models were needed to match the more open academic environment. The report also showed that top academic administrators were starting to view the subject of information security as an institutional issue, not just an IT department issue.

Pirani and Spicer (2006) completed another case study of the information security programs at four universities. The case study examined the successful characteristics of a university's information program. The study found that the top management of the institutions considered information security as an institutional issue. All the institutions had instituted formal security programs. Also, all four institutions had fully funded and staffed the IT security programs.

Both studies found another similarity with the institutions. All the top administrators at the universities believed institutions of higher education were at a higher risk of security breaches because of the nature of the educational industry. The studies mentioned academic freedom, changing or multiple roles of users, open access requirements, and multi-location access as challenges to information security at their institutions. These issues seemed to be unique to higher education.

The organization that was at the forefront of information security is EDUCAUSE. Kam, Katerattanakul, Gogolin, and Hong (2013) used two of EDUCAUSE's studies from 2003 and 2006 to see if colleges with information security compliance have increased over the years. The authors work focused on information security at colleges and

universities. These multiple method study examined the progression of information security in higher education over four years. The study found that information security management and leadership had shifted from an IT concern to an institutional and system concern. The study showed a shift from IT centric to an organizational/holistic approach to handling information security management at the institutions. The study found that all institutions had developed formal policies for information security structure. All institutions had implemented organizational or system wide security programs that focused on consistent standardized policies, procedures, and practiced. These information security procedures went so far as to describe individual training programs and develop centralized purchasing processes for IT employees.

**Changing a Law in Texas**

There were several solutions that have been suggested to solve the access problem. One solution was to change the law that grants guest access to community college resources. According to Amy Price, legislative director for State Senator Dan Patrick, there were several ways to change a law in Texas. The two most common methods were petition and request.

The petition method was the most formal. An individual or group can start a petition drive on any issue by gathering signatures. The petition would then be submitted to the legislature once the number of signatures needed for the petition had been reached and verified. The number of signatures will vary depending on the subject matter and on the area that the law will effect. This calculation is defined in Texas statute section 227.0024. For example, it could take as few as 50 signatures to change a city or local

ordnance and as many as 500,000 signatures to change a state law (Texas Legislative Council, n.d.).

The second, and less formal, method was to find a legislator who is interested in changing or adding a law. Ms. Price stated there are many legislators who were elected on the promise to make specific changes. These legislators could be eager to help a citizen change a law. Both methods would get the issue into the legislative system; however, there is no guarantee the bill would be presented to the legislature, or passed by the legislature, or signed into law. According to the Texas State Legislature site, there were over 4453 bills proposed in the 2011 legislative session (Stiles and Swicegood, n.d.). Just over 700 were passed by both chambers and only 673 were signed into law (Texas Legistature, 2011).

Many of these bills failed because passing a law may not be a singular matter. Many of the bills did not pass in previous legislative sessions because the bill did not pass through the Texas Legislative Council. The Texas Legislative Council checks the bill for related issues already enacted. One of the hurdles of changing the law for open access at community colleges is that it would require changes to the funding formula definition for community colleges. The funding formula allows community colleges to collect taxes from the local tax base for such issues as providing access to the local populace. Also, the charter of all community colleges in the state would need to be changed (Texas Legislative Council, n.d.). These hurdles make changing the law to restrict guest access to community college resources very difficult.

**Automation in Identity Management**

A second solution was to automate the process of gathering guest ID information and granting access to computer resources. From a technological standpoint, IT automation capabilities could be handled through an existing API such as Active Directory. Information technology departments can leverage this existing technology to automate college IdM systems (Ward, 2013). An automated IdM access system should offer a familiar and intuitive interface, such as an ATM or kiosk, for users requesting access and the flexibility to collect user information from multiple sources (Buchan, 2013). This would allow ease of use for both those granting access to computer resources and those seeking access to computer resources. ATMs have been in wide use in the United States since the late 1970s. Using an ATM card and keying in a PIN number is common place in the banking industry. According to Lenpenzo (2012), there were nearly 2 billion ATM transactions in 2012. This was more than half of all banking transactions that year. Kiosks for purchasing movie tickets or checking in at airline counters have also become common place (Kiosk Market Place, 2011).

The Identity Security Project from the State of Iowa consists of a clearinghouse where various identity documents are linked together (Combs, 2002). These include birth certificates, Social Security number, driver's license, marriage license, and death certificates. This system allows multiple agencies to perform cross linked identity verification and provide better tracking for identity theft. The concepts of primary identification (PID) and secondary identification (SID) were used in this case. The birth certificate was the PID. This was the document that all other SIDs were associated. Only

SIDs that linked directly to a PID would be issued. At the same time, the birth certificate was electronically associated with all other SIDs issued in the future (State of Iowa, 2004).

Under this system, a more strict security check could be established when an ID was presented and a concurrent check was run against the department of transportation's (DOT) database. Attempting to submit a second birth certificate would not be allowed since the PID was already on file. This identity management system incorporated an individual's picture ID, such as a driver's license, with documentation and processes to prevent identity theft and fraud.

As a state agency, Texas community colleges can access the Texas DOT database. A college can use a kiosk connected to the Texas DOT database to verify identification and link that identification to the college's active services directory to issue a user ID and password. The college now has a valid identification linked to a user ID and can track guest access in the same manner as employees, faculty, and students (Texas Department of Transportation, 2009).

## Summary and Conclusions

Identity management is a combination of policies, risk management controls, software, and hardware technologies. On the policy side, an organization must establish a system that enhances privacy, anonymity, emergency response, law enforcement, and cost saving. Once IdM policies are developed, technologies and architectures should be chosen that support the execution of the policies. It is important for security professionals to find creative ways to build an IdM system that provides liberties, privacy, and other

key policy imperatives.

The identity management infrastructure model (IDIM), a sample identity management system, was presented in this section. While no exact implementation followed the IDIM, I found similar functionalities and components in all IdM solutions. A good IdM solution should always provide universal identity data access, workflow, delegated administration, detail auditing and logging, and modeling of the organization. Depending on the deployment, the IdM solution should also provide access control, provisioning, public key infrastructure (PKI) functions, networking, and Web services management. Identity management in the area of security has been gathering great momentum for further research.

The information security governance framework was discussed. This section contained information regarding the different approaches for creating information security governance framework and how the discipline had matured from an IT department concern to becoming part of the organization's mission guided by top management. The section concluded with a discussion on how information security governance framework was addressed in higher education and unique challenges facing colleges and universities when implementing security policies.

Lastly, methods for solving this problem were presented. The two methods for changing the law requiring open access at Texas community colleges require passage in the Texas legislature. This process is long with many hurdles. Passing all the hurdles does not guarantee the bill will become a law. Automation technology for accessing guest identity information through the Texas DOT was also presented. This will simplify the

process for both those granting access to computer resources and those seeking access to computer resources.

# Chapter 3: Research Method

A discussion of the tradition of inquiry using the qualitative case study methodology, the research sample and population to be used, the method of data collection and procedures, data management procedures, method of data analysis, and the issues of ethical considerations are presented in this chapter. Research of existing literature indicated that there are laws and legal precedent that can hold community colleges liable for the misusage of their open computer labs (Galuszka, 2004). Professional organizations also have guidelines for the protection of data (Wang & McClung, 2011). Both the guidelines and laws emphasized the development of policies and procedures for protecting data from external and internal abuse.

Much has been written regarding how organizations should identify users of network resources; however, these guidelines focus on employees, students, and vendors. I could find nothing written regarding allowing access to guests, those who were not registered in some manner with the college. Current methods used by community colleges in Texas to identify users of their network resources are the focus of this chapter.

## Research Design and Rationale

Thirteen community colleges in Texas provided the basis for this study. This section began with identifying the study questions that guided the research. Next the participants are identified and data collection defined. Lastly, the criteria for interpreting the results are explained. The research questions are:

RQ1. How do community colleges in the State of Texas implement an Identity Management (IdM) system that is capable of properly identifying guest users and

protecting the college from illegal acts such as inappropriate information access, hacking into other networks, launching computer viruses or Internet worms, or other white-collar crimes committed by guests using the college's computer network? From this central question, the sub questions to be answered to address the problem are:

RQ2. What are the IdM methods used by IT managers at Texas community colleges to identify guests?

RQ3. How affective are the IdM strategies used by IT managers at Texas community colleges in track guest users to improve the security of computer networks?

RQ4. What do IT managers see as the difference between their current IdM practices and their ideal IdM system?

## Role of the Researcher

Since I was the main collector of data for this research, I conducted the entire research from the stages of data collection, data analysis, to report writing. I traveled to the 13 community college listed to collect relevant data on the security of their open computer labs. I found all the participants to interview for the research and sought the necessary permission to conduct interviews and collect documents. I used e-mail and the telephone to contact all participants. I personally conducted and transcribed all interviews. These interview notes were used to aid the analysis of this report.

According to Goulding (2002), a qualitative researcher must be a skillful interviewer in order to obtain relevant data required for the study. I was able to conduct this research based upon my work experience with over 20 years in the information

technology field. The experience was both in industry and academia. I worked in the IT department or related departments for two major hospitals in the Houston medical center for 10 years. My positions included IT focal, database manager, and consultant in the human resources department administering the applicant tracking submissions applications. For the last 15 years, I have held the position of professor of computer science for North Harris College. For the first 6 years, I was the assistant chair of the department and the lead instructor for the Net+ courses (Operating Systems, Introduction to Hardware, and Fundamentals of Networking). For the past 8 years, I have been the lead instructor for the largest class the department offers, Introduction to Computers. During the last 8 years, I have also worked for Our Lady of the Lake University - Houston as the IT manager and adjunct faculty teaching IT courses in both the graduate and undergraduate programs.

## Methodology

The qualitative case study methodology was used as the primary method of inquiry. This inquiry was an in-depth multi-case study of the policies, procedures, and practices of 13 community colleges in Texas. The goal of this multi-case study was to develop guidelines for IT professionals who may use IdM practices for identifying guests using a college's network.

Yin (2009) defined a case study as an empirical analysis used to investigate a contemporary event(s) when the delineation between the occurrences and context is not readily apparent. Yin's case study definition works well for this research. I did not know the current state of IdM policies, procedures, and practices at community colleges in

Texas. Yin stated that case studies are the research method of choice when asking how or why questions regarding an event. Again, the multi-case study method works well for this research. Before starting this research, I did not know how IdM policies were created or why there was a gap in the IdM literature. Yin (2009) also wrote about factors that favor choosing the case study method. These factors included focusing on contemporary events and issues that arise when the researcher's control over the event(s) is limited and when the researcher wants to describe, understand, and explain an event. Identity management is a contemporary issue arising from the expansion of computer networks beginning in the late 1990s. Although I had no control over the creation or implementation of the IdM policies, I wanted to understand the process of creation and implementation of these policies (Halperin & Backhouse, 2007).

Yin (2009) listed the three types of case study as exploratory, descriptive, and explanatory. Exploratory studies are used when a researcher can construct the research frame work, but has not defined the research question or the hypotheses. In this case, the research sets the question or hypotheses. Exploratory studies are also used when existing literature and research are limited. This type of study was not used because I already have research questions and a hypothesis.

Yin (2009) described the descriptive case study starting with a descriptive theory that would cover both the depth and scope of the case study. In this situation, related patterns were only relevant if the patterns were defined before the research begins. Any pattern will be purely incidental as a result of the research. I did not use this type of case study because I believe there were patterns; however, I could not know the patterns until I

researched the 13 different and distinct community colleges' IdM methods.

The case study type used in this study is the explanatory study. The explanatory case study should be used when a researcher attempts to identify patterns and relate the variations of those patterns to each other (Yin, 2009). This type of case study answers the how and why questions that would explain an event. I used this type of case study because the focus of this inquirer was on how the IdM policies were created and why they were being (or not being) implemented by community colleges in Texas. Patterns were identified once the case study was completed.

Yin (2009) also noted that the case study method is very useful in communicating research information to non-specialists, those who were not in the field of study. He stated that the case study, specifically the explanatory case studies, can convey information to individuals outside of or new to an industry. This benefit assisted my goal of linking policy and procedures to the practices used by employees. Yin's insights worked well for this study. Top-level management often look to mid-level content experts to create the policies first drafts in order to form user level policies (Jones & George, 2012). For example, community college CIOs would look to IT professions to develop the first drafts of computer related policies. These policies will then need to be explained to executive committees and college leadership who are non-IT professionals. Once these policies receive top-level management approval, the policies will need to be explained to computer lab employees for implementation.

Yin (2009) gave a frame work for designing a case study. He identified five components a researcher should use when building a case study. They were (a)

identifying the study questions, (b) setting the study propositions, (c) developing the units of analysis, (d) linking the data to propositions, and (e) setting the criteria for interpreting the results. The first three components lay the foundation to the case study and the last two components provide analysis of the data collected.

In the first step, identifying the study questions, the researcher should develop the how and why questions that allow a researcher to achieve his or her goal. Second, a researcher should develop the study's propositions. This is derived from the how and why questions and is the researcher's tool that will focus the study (Yin, 2009). Third, is the development of the units for analysis. Here, a researcher defines what will be analyzed. The last two components are the data analysis framework of the case study, linking data to the propositions and selecting criteria for interpreting the findings. I followed this frame work.

**Participant Selection Logic**

The community colleges that were studied for this research were located in south east, north east, and central Texas. Thirteen of the 55 community colleges in Texas have been purposely selected as participants for the research. These 13 colleges fit into the Katsinas, Lacey, and Hardy classification (2006). This classification system is used by the federal and state governments to categorize community colleges for funding. The colleges were divided throughout the categories and they could be reached using limited resources. These 13 colleges also made up the vast majority of campuses and satellite campuses of the 55 community colleges in Texas. Between the 13 colleges, there were 45 independent campuses and 40 satellite campuses. The IdM policies of these 13 colleges

made up nearly 36% of all the campuses and 59% of all the satellites of the community colleges in Texas (Texas Association of Community Colleges, 2010).

The Katsinas, Lacey, and Hardy classification breaks community colleges into three categories: rural, suburban, and urban (Hardy & Katsinas, 2006). Katsinas et al. used the federal government's Primary Metropolitan Statistical Areas (PMSA) and Metropolitan Statistical Areas (MSA) to place community colleges into the three categories. Colleges located in a city that were included in a PMSA or MSA were considered urban. Colleges located in a city that were not included in a PMSA or MSA, but within the PMSA or MSA area were considered suburban. College located in a city not included in a PMSA or MSA and were not within a PMSA or MSA area were considered rural (Hardy & Katsinas, 2006).

Travel was required to complete this research. To maximize my limited resources, the colleges investigated spanned across Texas from Dallas in the north, to San Antonio in the west, to Beaumont in the east, and Galveston in the south. The number of colleges studied by category were five urban, four suburban and four rural.

**Linking the data to propositions**

The main proposition of this research was that community colleges in Texas had policies and procedures in place to identify guest users on their network; however, these policies and procedures may not be followed by employees. Either the procedures may be too complex for the employees to understand, whether there was training offered to the employees regarding the procedures, or whether there were consequences for not following the procedures. An alternative proposition is that colleges did not have policies

and procedures in

**Instrumentation**

The method for collecting data for this study came from interviews, archived data, and direct observations. The first phase of the research started with contacting the 13 CIOs of the colleges to understand the college's policies and procedures for allowing guests onto the college's network. I ask the 13 CIOs if he or she would be willing to participate in this research. CIOs who did not wish to participate were not contacted in the future. Each CIO who wished to participate received a packet containing an introductory letter explaining the study, a consent form, and a list of five questions for response. The follow is a list of the interview questions:

1. The State of Texas has a mandate that all community colleges in the state provide open access to its computer resources to guest users who are not associated with the college. These guests are non-students, non-employees, non-vendors, and non-suppliers.

   What are the college's policies for guest usage?

2. With the college's policies for guest usage in mind, let's look at how these policies are put into practice.

   How are the policies put into practice by workers at the college?

   How are guests identified before they use the college's computer?

   What are the current practices of the college to collect identity data of the guest users?

   Are these policies in electronic or hard copy for guests to review?

3. Policies and procedures are only effective if they are put into practice.

   What training is given to employees who are responsible for collecting information on guest users? How is that training delivered?

   What are the practices used by the college to enforce these policies?

4. How would I go about using a computer at the college?

   Where is the open computer lab on your campus?

   Is prior notification required?

   Is so, how and whom do I need to notify?

   Does the notification need to be done before visiting the campus or while on campus?

These questions were pretested with two academic IT professionals before the interviews were conducted and were modified based on the feedback received. None of the feedback was used in this study. The IT professionals asked to review the questions were not used in the study's interview pool.

The interviews were recorded accept when the interviewee objected. An archive data search was conducted after the interviews were completed. This archive data search investigated the published policies and procedures records of the colleges such as policy manuals, and handbooks. Archive data were then compared with the answers to the interview questions for alignment.

Lastly, I visited each college's open lab to observe the practices used by the colleges in complying with the policies and procedures identified in the interviews. Data were collected regarding the methods used by lab workers to collect computer user

identification and the methods used to link the user identification to the time of day and the computer used. Lab computer usage was then investigated. I analyzed login procedures, Internet availability, download capability, and access to network resources such as network drives, network printers, the computers console, and access to the computer's IP address. Question four from the interview questionnaire guided me on how to gain access to the college's open computer lab.

The data collected were then used to compare how top management creates policies and procedures and how these policies and procedures were put into practice by management, lab employees, and student workers. This comparison was the final step in determining the colleges' compliance with IdM. Compliance was defined by how closely the IdM practices aligned with the college's IdM policies and procedures.

Additional material and resources needed to complete this research were many and varied. Published works such as textbooks, scholarly journals, and web resources were utilized for the research sections of this work. The computers, software, and facilities of the community colleges' were also used.

**Procedures for Recruitment, Participation, and Data Collection**

For this research, the community colleges were the main unit of analysis. Sub units included managers, employees, policies, procedures, and practices. Managers defined in this study were anyone in the paid employment of the college who oversaw IT personal or IT functions. Policies were the plans of action that guide the decision making process of an organization to achieve an outcome. Procedures were the specific series of actions, based on policies, taken in order to obtain a result. Practices were the method

used by employees of an organization to implement the organization's policies and procedures. All these were analyzed in this study.

**Data Analysis Plan**

The data analyzed in this section comes solely from the data collected in the interviews and college visits. Each interview question was treated as a separate entity in order to analyze the data collected more efficiently and systematically. All interview results were recorded as percentages of the total responses. Questions not answered were counted as a non-response. All percentages were rounded to the nearest whole number using standard rounding methodology.

Data analysis follows the description of the answers to the interview questions. The data analysis also includes any discrepancies in the responses between IT professionals working at the same college. For example, an anomaly exists when the CIO of a college district stated that all major network implementation decisions of college policies are handled at the system level. In contrast, the local IT director stated that the implementation decisions of college policy are handled at the college level. The in-depth analysis of the interview results appears in Chapter 5 of this study.

All the colleges in this study were represented either by interviews, college visit, or both. Thirteen IT professionals responded to interview requests. These colleges were distributed using the Katsinas, Lacey, and Hardy community college classifications as follows; five urban, four suburban, and four rural.

The Katsinas, Lacey, and Hardy classifications used the federal government's Primary Metropolitan Statistical Areas (PMSA) and Metropolitan Statistical Areas

(MSA) to place community colleges into these three categories. Colleges located in a city included in a PMSA or MSA were considered urban. Colleges located in a city but not included in a PMSA or MSA, but within the PMSA or MSA area of influence were considered suburban. Colleges located in a city not included in a PMSA or MSA and not within a PMSA or MSA area of influence were considered rural (Hardy & Katsinas, 2006).

The college visits involved locating and gaining access to the open computer labs at each college visited. I gained access to one of the college's computers during each visit. The purpose of the college visits was to determine how well the college's IdM policies and procedures were put into practice. The three colleges not represented in the interviews were visited. All calculations regarding college visits were based on the full 13 colleges in the study.

## Issues of Trustworthiness

### Credibility

Credibility was built into this study using triple verifications. This began with interviews with top college CIOs regarding policies the college uses for allowing guests access to computer resources. These interviews were followed up by interviews with college IT managers who create procedures to allow guest access to their college computer resources. Lastly, each college in the study was visited to observe the practices used by computer lab employees to allow guest access to college computers. The purpose of the college visit was to check how well the policies created by IT CIOs and procedures developed by IT managers were put into practice.

**Transferability**

Transferability for this study will be difficult because of the transient nature of IT professionals and the awareness of the guest access issues. The positions of CIO and IT manager will exist at all college in the study as long as there are IT issues at the colleges. However, the college IT professionals may not remain the same. College IT professionals may retire, move, be reassigned, or depart for other organizations. The campus visits can also be replicated; however, awareness of the guest access issue may be more prominent once this study is released.

**Dependability**

Golafshani (2003) struck a comparison between quantitative and qualitative research. He stated that the quantitative researcher sees reliability as whether the results can be replicable. With regards to validity, this is also dependent on whether the researchers actually measure what they intended to measure. With qualitative research the question of replicability may not be possible because the researcher was looking at a one-time phenomenon. Golafshani (2003) cited the studies of Glesne and Peshkin (1992), Winter (2000), and Hoepf (1997) on reliability and validity in qualitative research as precision, credibility, and transferability.

I used several methods to ensure reliability and validity in this study. First, there was a variety of literature from multiple sources cited in this work. Second, a narrative was generated of each for the 13 encounters describing the phenomenon (being a guest on the college's computer network). This narrative followed the guidelines established by Yin's (2009) research for maintaining a chain of evidence of all records and field notes.

Third, a college-by-college comparison was conducted after each college visit to determine patterns with the visits (Yin, 2009).

**Ethical Procedures**

Merriam (2002) stressed the importance of conducting qualitative research in an ethical manner. Merriam believed that willing participants who choose to be part of a study are invaluable. Their contribution to a research study may enable the generation of new knowledge. It is the ethical responsibility of the researchers to ensure that their studies would not jeopardize the participants in any way, shape, or form. For this study, I asked for consent and approval from the participants by providing them with a description of the goals and methods of the study and I assured them of their anonymity. I also gave each interviewee an opportunity to ask any questions they had before they decided to participate. Participants were given the option to answer as many or as few of the questions as they wish and they could end the interview at any time.

I also needed to be respectful and sensitive toward the participants. In order to do so, I spent time at the beginning of the interview explaining the goals of the study, as well as that the information collected will remain confidential, and how the data would be used and safeguarded. A pseudonym was created to protect the privacy of each participant. All participants received a copy of this research as a token of appreciation.

## Summary

The methodology that was used during the course of this research was discussed in this chapter. The chapter started with a discussion of the case study methodology and the use of a multi-case study. Next, the instrument of measurement for this research (the

IAM) model was described. Third, IT departments at community colleges were identified as the primary audience for this research. Fourth, the primary methodology and procedures for collecting field data were discussed followed by a discussion on how the data from the field research would be presented along with the outcomes of the research. Lastly, the issues of reliability and validity for this research were discussed along with my credentials.

# Chapter 4: Results

Identifying guest users on an open community college computer system is an intricate and complex social construct. Texas state law requires community colleges to give guests access to computer resources. This regulation comes from the Texas department of information resources rule 1 TAC 201.13, information security standards. This state law also requires guest users to be identified before using computer resources. The main difficulty in analyzing and defining this social construct is the experiences of those studied may be very different.

The experience may occur in different locations, with different people, or with different levels of knowledge. The experience may be different even in the same environment depending on the time of occurrence or the device used. Qualitative data were gathered regarding the identity collection of guest users and the management methods used to collect pertinent information. The data were collected via interviews, campus observations, and policy searches. The focus of the analysis and interpretation of the data collected was not only on how identity information was obtained, but also on how closely the practice of collecting identity information matched the policies and procedures set by the IT professionals.

Gathering the qualitative data was time-consuming, but not difficult. As in many qualitative studies, the difficulty was in finding meaningful categories and relationships within the data collected. The primary focus of my research problem was to determine how closely the identity management policies, procedures, and practices align at each college. With that the findings are compiled into three logical categories: interviews with

college CIOs, interviews with other college managers knowledgeable regarding IT, and visits to the college campuses.

The qualitative data collection was oriented in three areas. First was with the IdM policies, procedures, and practices of the college. Second was in determining how well these policies, procedures, and practices aligned. Third was in determining how well these IdM approaches protected the college from liability from inappropriate or illegal acts. Miles, Huberman, and Saldaña (2013) stated that qualitative research should come from two distinct approaches, paradigmatic and syntagmatic. In the paradigmatic approach, the data is variable-oriented, and in the syntagmatic approach, the data is process oriented.

Since IdM at community colleges is hierarchical in nature, there is a natural and direct interaction between policymakers and the implementation of those policies. Qualitative patterns should exist in these relationships. In this study, these relationships were analyzed to determine how members at each level view their roles in the process and how each level is synchronized within the overall IdM process.

## Research Setting

Originally, 24 IT professionals were identified as potential interviewees for this study. Two CIOs and one IT manager accepted the invitation. One IT manager declined the invitation. Additional e-mails and telephone calls were needed to convince the rest of the potential interviewees to participate in this study.

The follow-up e-mails and phone calls revealed an additional CIO and four IT managers from the original list willing to participate in the study. The interviews began at

this time. An additional 10 IT professionals were identified during the initial interviews as possible additional participants. E-mails were sent to the additional IT managers between December 17, 2013 and January 6, 2014. In total, 34 IT professionals were identified as potential participants. Eleven of the potential participants declined participation in the study and 10 did not reply to e-mail and phone invitations. The final sample population for the interviews was 13 (38%) IT professionals.

The 13 participants held the following positions:

CIO – 3

IT Director – 5

IT Manager – 1

Vice Chancellor, Network Services – 1

Dean – 1

Network Engineer – 2

The initial position classifications for the interviews were college CIOs and IT managers. Several of the above positions did not fit neatly into the initial classifications for this study. Definitions for title classification had to be expanded in order to fit all the actual job titles into the existing categories of this study. For the purposes of this study, all those interviewees who were the head of the IT department for the college were classified as CIOs. Anyone interviewed who reported to someone else in the IT department and made procedural decisions for the college's open computer lab were classified as IT managers. The two network engineers were categorized as IT managers. Both network engineers were in charge of the IT department of their colleges' satellite

campuses and answered to a campus or district IT CIO. There was an anomaly with the title of IT Director.

At three of the colleges, the IT directors were classified as IT managers, and at two of the colleges, they were classified as CIOs. The IT directors at three of the suburban colleges reported to district CIOs. The IT directors at two of the rural colleges were the head of the colleges' IT departments. There was seven interviewees classified as CIO and six interviewees classified as IT managers. Regardless of how the different colleges classified their positions, all these IT professionals had managerial responsibilities. The college interviews resulted with eight colleges with one IT professional interviewed, one college with three IT professionals interviewed, one colleges with two IT professionals interviewed, and three colleges with no IT professionals interviewed.

## Demographics

For this research, the community colleges were the main unit of analysis. Sub units included CIOs, managers, employees, policies, procedures, and practices. CIOs were defined as a person who has overall responsibility for the college's information system. Managers defined in this study were anyone in the paid employment of the college who oversaw IT personal or IT functions of a college campus or satellite campus and answered to the college's CIO. Employees were defined as those Policies were the plans of action that guide the decision making process of an organization to achieve an outcome. Procedures were the specific series of actions, based on policies, taken in order to obtain a result. Practices were the method used by employees of an organization to

implement the organization's policies and procedures. All these were analyzed in this study.

## Data Collection

All the individuals interviewed in this study were IT professional managers at community colleges in Texas. All the IT professionals held managerial positions in the college's IT departments and have knowledge of the security policies used for guest access. I e-mailed an invitation to the 24 original participants identified as IT CIO and IT managers at each 2-year college in the study between October 1, 2013 and October 3, 2013. These individuals were identified via their colleges' websites.

During the next few weeks, additional participants were suggested by the original participants. The new participants were identified and contacted in the same manner as the original participants. Consequently, I e-mailed additional invitations to those who met the study's criteria between December 17, 2013 and January 6, 2014. Several e-mails were sent to all identified potential participants during the dates listed. A copy of the consent form and a copy of the interview questions were attached to all e-mails.

A total of 34 community college IT professionals were identified and invited to participate in this study. Of the 34 IT professionals invited, 13 (38%) agreed to be interviewed for this study. These 13 IT professionals represented 10 colleges in the study. Three colleges were not represented in the interview process. The college interviews resulted with eight colleges with one IT professional interviewed, one college with three IT professionals interviewed, one colleges with two IT professionals interviewed, and three colleges with no IT professionals interviewed. These IT professionals either denied

my request to be interviewed or never replied to the invitations to be interviewed. Even though the IT professionals from these colleges were not interviewed, the colleges were visited to observe IdM practices in the open computer labs. The college IT professionals represented the first part of the study. The second half of the study required visits to the computer labs of the college in the study.

I identified 13 community colleges in Texas to visit. The colleges selected were divided between the three Katsinas, Lacey, and Hardy classification. This system has been used to identify community college by the federal and state governments for more than a decade. The primary purpose of this traditional classification was to create an empirically supported, valid tool for researchers to use when studying 2-year colleges (Hardy, 2006). Five colleges were classified as urban, four were classified as suburban, and four were classified rural. All 13 colleges were visited during the fall of 2013. The purpose of the college visit was to check how well the policies created by IT CIOs and procedures developed by IT managers were put into practice. Nine of the colleges had multiple independent campuses and multiple satellite campuses. Two of the colleges had one campus and a satellite campus. One college had only one main campus.

**Data Collection from College Visits**

The purpose of the college visit was to check how well the policies created by IT CIOs and procedures developed by IT managers were put into practice. All 13 colleges were visited during the fall of 2013. Most of the answers to the interview questions between a college's CIO and IT manager agreed; however, there was one noted exception. The CIO of one college system stated all network security policies originated

at the system level. One of the IT managers in that system stated the network security policies were all local decisions, with each campus having different policies, procedures, and practices.

The IT professionals at three colleges did not participate in the interview portion of this study; however, the college's open computer labs were visited to determine IdM practices used. Determining how closely the IdM policies, procedures, and practices aligned could not be determined; however, the actual IdM practices used at the colleges could be observed. The following data were collected at the college visits.

**Sign-in required.** Of the 13 campuses visited only five required some sign-in to access one of the college's computers. Eight of the campuses did not require any sign-in.

**ID checked.** Only three (23%) of the 13 campuses visited required guest users to provide some identification. Ten (77%) of the campuses did not require any proof of identification. Of the three campuses, two campuses tied the state-issued ID to actual login credentials. The staff at these two colleges held the ID for the duration of the guest's stay. Both of the campuses linked the ID to the user ID and password issued to the guest. One college required a library card to access a computer instead of a state-issued ID. Applications for a library card were available at the college's library if a guest did not have a library card. A state-issued ID was required to apply for a library card.

**User ID and Password issued.** This mirrored the ID check section. Only three of the colleges required a guest to acquire a user ID and password. Two of the college linked the user ID and password directly to the guest's driver's license. Both colleges recorded the driver's license information and kept the card while the guest used the

computer. One (7%) college used a county library card as identification. The username and password were the name and number on the library card. Eleven (79%) of the campuses visited had generic credentials and did not require the quest to provide identification. These generic credentials were already entered into the computers. All the guest had to do was sit down at the computer to use the college's resources. An employee at one of these colleges knew guests were allowed, but did not know the procedures to log the guest into the library computer. Eventually she provided her own credentials to allow the guest access to the college's computer.

**Staff available at the college.** Staff availability at the college library or open computer lab were minimal, usually one or two employees on duty at the time the guest arrived. Five (35%) of the campuses had one employee and five (35%) had two employees. Three (21%) of the colleges had three employees and one (7%) had no employee at all on duty. It is interesting to note that the two colleges with the most employees on duty were the colleges with the strictest, most labor intensive identification policies.

**IP address acquired.** The computer's IP address is the key to identifying a device connected to the Internet (Rock, 2007). With a computer's IP address, any beginning hacker can take control of the computer, make it a zombie, or clone the computer. Cloning a computer makes the computer appear as a legitimate computer in order to circumvent network security systems. Of the 13 colleges visited, nine (69%) allowed access to the computer's IP address. Four (31%) of the colleges locked down their computers, so IP addresses were not accessible by a computer user.

**Computer in an open lab or library.** All the colleges visited had both a library and at least one open computer lab. I went to the college's information booth and asked where to go for computer access. The employees at seven (50%) of colleges directed me to an open computer lab. Employees at five (35%) of the colleges directed me to the college's library. The information receptionist at one (8%) of college did not know where to direct me. The computer labs at both of these colleges were designated for students only and required a student ID to enter the computer lab. Guest access to the colleges' computer were in the campus libraries. It is interesting to note that one of the colleges where a guest must use a library computer did not have a practice in place to identify or login a guest user. The librarian on duty used her user ID and password to allow me to use a computer.

**Computers restricted for guest usage.** At three (23%) of the 13 colleges computers were allocated for only guest usage. One of the colleges offered guest users a bank of two computers available on a first come, first served basis. The computers were kept in a separate part of the library. These two computers were far from the top of the line. The reserved computers at the other two colleges were not segregated. These computers were part of the college computer lab and could be used by a student if guests were not using the computers. The identity practices at two of these three colleges were the strictest. The policies at both of these colleges require guests to present a state-issued ID, the ID was held during the time the guest was on the computer and the guest information from the ID was recorded on a log by the attendant. The attendant then issued a temporary user ID and password to the guest. The guest was then escorted to a

computer. The guest's ID was returned after the guest logged off of the computer. Once the guest ID was returned, the user ID and password were deactivated.

**Download available.** All but one of the computers tested allowed downloads. The researcher accessed the Internet and downloaded an image from a trusted cite and the Power Point viewer from the Microsoft cite. Nine of the 13 computers allowed installation of the Power Point viewer. The same nine computers also allowed the downloaded image to be placed on the desktop as a background image. Both of these types of downloads are potential security concerns. The ability to change system settings and installing applications outside of the local configuration are methods hackers can use to disrupt normal computer usage, glean information from other users, or gain access to other computers.

**Access to a printer.** Access to a printer was available at all 13 campuses. Three of the campuses requested payment for printer services; however, only one kept the printer behind a desk. The librarian on duty collected payment of ten cents per page. Printing fees were collected at the other two colleges only when the employee on duty was near the printer.

**Access to network drives.** Access to network directories was not allowed at any of the campuses. Other than access to a network printer, access to other network resources was not available.

**Ability to change computer configuration.** All but one of the computers tested allowed for some type of configuration change. On all computers, I attempted to open the control panel to change the background settings of the computer. Nine of the 13 allowed

full access to the control panel. On these computers, I was able to place a picture downloaded from the Internet as the desktop image. Four of the 13 computers restricted access to the control panel. The ability to change system configuration from the control panel and install downloaded files are methods hackers use to disrupt normal computer usage, glean information from other users, or gain access to other computers. All these were potential security concerns.

**Ability to access the command prompts.** I was able to access the command prompt from nine of the 13 computers tested. The command prompt provides direct access to the computer's operating system, system controls, and the root directory. Access such as this can give hackers control of the computer and access to all system resources.

## Data Analysis

Thirteen individuals representing ten of the 13 colleges agreed to be interviewed. The IT professionals at three of the colleges either declined to be interviewed or did not reply to any of the invitations to participate in the study. E-mail invitations were sent to all 34 potential participants of the study detailing the topic of the study and asking them to participate in the study. Attached to each e-mail were the IRB and interview questions. By the end of invitation period, 13 of the 34 identified potential participants agreed to be interviewed, seven classified as CIOs and six classified as IT managers. In total, there was a 38% participation rate.

### Interview Question Analysis

#### Interview Question 1: What are the college's policies for guest usage?

All 13 participants said their college had policies regarding guest access to their network computers. Eleven of the participants indicated that their colleges had guidelines available on the college's website. The other two used the policies of the county library system, also found on the college's websites. Although the guest usage policies were found on all the colleges' websites, I would not have been able to find the policies without the exact document titles. Since these policies are important to potential guest users, as well as college management, they should be easily accessed from the college websites.

Much of the difficulties in finding the colleges' written policies revolved around terminology. Prior to the interviews and college visits, I looked for guest usage policies on the colleges' websites. Using the search term guest users on the college's websites did not return any findings. The interviewees did not use the term guest users. Ten (77%) of the interviewees used the term public access instead of guest access. The remaining three (23%) of interviewees used the term open access instead of guest access. The colleges' policies found on the Internet mirrored the different terminology. All three of these terms, guest users, public access, and open access have the same meaning, making the search more difficult without knowing the label that reflected the intended meaning.

The responses from the interviewees ranged across a broad spectrum of security levels. The most common policy nomenclature that was mentioned regarding guest user access is summarized below:

1. Open access to the college's computer system requiring no user ID or password to be issued to guest users

2. Sign-in sheets at the entrance of the computer lab with no user ID and password to be issued to guest users
3. Sign-in sheets at the entrance of the computer lab and a user ID and password to be issued to guest users
4. Sign-in sheets at the entrance of the computer lab, requiring a State-issued ID to be presented, and a user ID and password to be issued to guest users
5. Sign-in sheets at the entrance of the computer lab, no user ID and password to be issued to guest users, guests assigned a particular computer
6. Library cards required to use the college's computers

**Interview Question 2: With the college's policies for guest usage in mind, let's look at how these policies are put into practice.**

**How are the policies put into practice by workers at the college?**

Four (31%) of the 13 actual participants stated that all computer policies came from the IT department to the employees of the computer labs. Two (15%) stated the policies came from the college's board of directors/trustees to the IT department and then relayed to the employees of the computer labs. Seven (54%) stated the IT department made recommendations to the board of directors/trustees. The IT department informed the employees of the computer labs once the board approved the policies.

Although the classification methodology used in this study relied on the Katsinas, Lacey, and Hardy (2006) community colleges classification system, it is important to note how each of the three categories, rural, suburban, and urban, were represented. There were 13 colleges in total for this study; four rural, four suburban, and five urban

colleges. A total of four colleges fell into the rural classification. Two of these colleges had only one campus and no satellite campuses. One of the rural colleges had one main college and a satellite campus and one college had two main colleges and a satellite campus. All four of the suburban colleges had at least one main college with multiple satellite campuses. All five of the urban colleges had multiple independent campuses with satellite campuses. Three of the suburban colleges exercised district control over campus computer access and two colleges exercised local control. Two of the urban colleges exercised district control over campus computer access and two exercised local control over campus computer access. All four rural colleges exercised local control over campus computer access.

**How are guests identified before they use the college's computer?**

All the interviewees stated that guest users did not need prior notification to use the college's labs or library computers. All the interviewees stated that their campuses were open to the public for a range of purposes including the use of their computer labs and libraries. It is interesting to note that nine of the interviewees stated there were no guest identification requirements to use the college's computers; however, at five of the colleges guests were required to show identification at the open computer lab before using a college computer. Practices used computer lab employees did not match the procedures setup by college IT managers.

**What are the current practices of the college to collect identity data of the guest users?**

Five (38%) of the interviewees stated their college had policies in place to require

guests to show a government issued identification before using a college computer. The remaining eight (62%) stated the policies at their colleges did not require proof of identification. Five (38%) required guests to fill out a sign-in log. Only two interviewees stated their college's policy required guests to show a Texas driver's license or Texas issued ID before granting access to a computer and kept the ID while the guest used the computer. Another interviewee stated that the policy at their college required guests to show a county issued library card. The college's board of trustees partnered with the local county library system to provide library services to the college and community at large. The college library was built, equipped, and supplied by the college as part of the college's initial footprint. The library was staffed, maintained, and resupplied by the county library system.

**Are these policies in electronic or hard copy for guests to review?**

All the interviewees stated the college policies for allowing guests were available in electronic format on the college's website. This also included the colleges using the county library system to manage computer resources.

All 13 participants said their college had policies regarding guest access to their network computers. Eleven (85%) of the participants indicated that their colleges had guidelines available on the college's website. The other two used the policies of the county library system. Although I was able to find the guest usage policies on all the colleges' websites, they were very difficult to find in several cases. I would not have been able to find the policies without the exact document titles. If I had such difficulty, perhaps guest users have similar difficulty.

**Interview Question 3: Policies and procedures are only effective if they are put into practice.**

**What training was given to employees who are responsible for collecting information on guest users? How was that training delivered?**

Training was important to most of the interviewees. Eleven (85%) of the interviewees stated that the computer lab employees received some training regarding allowing access to the college's computers. The divergence came in knowing which department was responsible for the training and the depth of the training. The IT department was responsible for the training at only one (8%) of the colleges. The college's open computer lab management was responsible at two (15%) colleges. At eight (62%) of the colleges, the library staff was responsible for the training. Two (15%) of the interviewees could not identify the department responsible for the training.

**What are the practices used by the college to enforce these policies?**

The departments responsible for enforcing the security policies mirrored the departments responsible for training. Eleven (85%) of the interviewees stated enforcement of the security policies of the college was an important issue. The IT department was responsible for enforcing the security policies in only one (8%) of the colleges. The open computer lab management was responsible in two (15%) colleges. At eight (62%) of the colleges the library staff was responsible for enforcing the security policies. Two (15%) of the interviewees could not identify the department responsible for enforcing security methods.

**Interview Question 4: How would I go about using a computer at the college?**

Nine (69%) of the interviewees knew how a guest would be guided to a computer lab. Four (31%) stated that all employees on campus knew how to conduct the guest to the proper location. Three (23%) stated librarians or library workers were the only ones who knew how to guide guests to a computer. As long as a guest found the library, they could find help. Two (15%) of the interviewees stated that only open computer lab employees or IT employees would be able to guide the guest to the open computer lab or library. Four (31%) of the interviewees did not know how a guest would find the computer lab or library on their campus.

**Where is the open computer lab on your campus?**

All the interviewees knew the location of the open computer labs on their campus. Eight (62%) of the interviewees stated that all guests would be directed to the campus library. Two (15%) of the interviewees stated guests would be directed to an open computer lab on campus. Three (23%) identified some place other than an open lab or library. These other locations for computer usage by guests included specially designated areas on campus, specific computers in the library, or a particular open computer lab.

**Was prior notification required?**

According to all the interviewees, prior notification was not required to use any of the colleges' computers. All the interviewees stated their campuses were open to the public for all purposes including the use of computer labs and libraries. Five (38%) colleges require guests to identify themselves at the open computer lab before using a campus computer. Eight (62%) of the interviewees stated there was no guest identification requirement to use the college's computers.

**If so, how and who do I need to notify?**

All the interviewees stated there was no prior notification required to use any of the colleges' computers.

**Does the notification need to be done before visiting the campus or while on campus?**

Again, all the interviewees stated there was no prior notification required to use any of the colleges' computers.

**Interview Question 5: How would you describe the ideal IdM system for collecting guest ID information to provide guest's access to your college's computers?**

The ideal Identity management (IdM) system described by all the interviewees fell into four categories: biometrics, partnerships, showing ID, or not concerned. Two (15%) of the interviewees stated they would like to have biometrics introduced across their campuses. Both interviewees liked the fingerprint scan and thought that the biometric methods was the simplest and most secure method of obtaining guest identification. Six (46%) of the interviewees looked for partnerships with trusted third parties such as the Texas Department of Public Safety, the county/local library systems, or third party federated alliances. Three (23%) of the interviewees were satisfied with obtaining state-issued identification cards. Two (15%) of the respondents were not concerned with improving their IdM system.

All the interviewees had other IdM concerns outside of those associated with guest access to college computer access. Five (38%) of the interviewees were more concerned with a relatively new phenomenon on college campuses, the notion of bringing

your own device (BYOD) to the campus. Individuals who bring their own electronic devices to campus expect the devices to work seamlessly with the college's network. However, because the college did not issue these devices, the devices may not have software or hardware compliant with the college's Wi-Fi system. Examples of these devices were personal laptops, tablet PCs, iPads, smart phones, and e-text readers such as Amazon's Kindle Fire, Barnes and Noble's Nook, and Sony's eReader. Due to the unique configuration of these devices, BYOD also requires multiple Wi-Fi connections. For example, one person could be using a college computer to complete a term paper while listening to iHeart radio on their smartphone, checking a Facebook post on a tablet computer, and referencing an e-text on their eReader. That one person used four Internet connections. Multiple devices used by one person add additional stress to the campus Wi-Fi network which was another cause of concern among the interviewees. The issue of BYOD to campus is an important issue; however, it is outside the scope of this study. Consequences, costs, and value to colleges of BYOD would be a good topic for future studies.

The remaining eight (62%) of the interviewees identified IdM on the campus Wi-Fi system as a primary security concern. Common to all eight of these interviewees was a concern with access to the college's network through guest Wi-Fi access. Students, faculty, staff, and administrators have user IDs and passwords to access the college's Wi-Fi Internet access. All other users simply use the guest access. The guest access does not require a user ID or password. Anyone with a wireless network card on a computing device can gain access to the Internet at the college. Eight IT professionals saw this type

of guest access as the primary IdM concern for their departments.

### College Visit Analysis

Community colleges are not all equal. The Katsinas et al. (2006) study classified community colleges using data from the National Center for Education Statistics' Integrated Postsecondary Educational Data System (IPEDS) and Higher Education General Information Surveys (HEGIS) into three categories: urban, suburban, and rural. This classification method puts community colleges into like categories for funding, size, and population. For example, local funding capabilities and population needs of an urban community college differ from those of a suburban community college, and both are different from a rural community college.

The 13 colleges chosen for this study were separated into the Katsinas, Lacey, and Hardy classification. All of the colleges visited were located across the southeast, central, and northeast sections of Texas. These categories were developed in order to provide researchers, policymakers, and government officials the ability to understand service areas associated with each community college. The needs and resources of students in an urban environment are different from those of a suburban student, and much different from a rural student. These three categories also identify the tax base available to the community colleges.

## Evidence of Trustworthiness

### Credibility

The intent of this study was to interview top college CIOs regarding how policies for allowing guests access to computer resources. These interviews were followed up by

interviews with college IT managers who create procedures to allow guest access to their college computer resources. Lastly, each college in the study was visited to observe the practices used by computer lab employees to allow guest access to college computers. The purpose of the CIO interviews, IT manager interviews, and the college visit was to check how closely the policies created by IT CIOs and procedures developed by IT managers were put into practice.

**Transferability**

Although this study can be replicated, the outcome may be very different for future researchers. Transferability for this study will be difficult because of the transient nature of IT professionals and the awareness of the guest access issues. Two college CIOs and five IT managers were replaced during the three months between identification and interviews. By the time this study is published all of the IT professionals interviewed my not be in the same positions as they are now. No advanced notification was given to college IT professionals regarding college visits. Awareness of the guest access issue will be more prominent once this study is released.

**Dependability**

Dependability relies on whether a researcher actually measured what was intended to be measure. With qualitative research, the question of replicability may not be possible because the researcher was looking at a one-time phenomenon. Additionally, Golafshani cited the studies of Glesne and Peshkin (1992), Winter (2000), and Hoepf (1997) on reliability and validity in qualitative research as precision, credibility, and transferability.

I used several methods to ensure reliability and validity in this study. First, there was a variety of literature from multiple sources cited in this work. Second, a narrative was generated of each for the 13 encounters describing the phenomenon (being a guest on the college's computer network). This narrative followed the guidelines established by Yin's (2009) research for maintaining a chain of evidence of all records and field notes. Third, a college-by-college comparison was conducted after each college visit to determine patterns with the visits (Yin, 2009).

## Study Results

This study found a link between the policies, procedures, and practices for guest access at community colleges in the study. However, the link was only valid where the policies, procedures, and practices followed strong IdM guidelines. Only three of the colleges in the study had strong IdM guidelines for identifying guest users at their colleges. The policies set by college CIOs matched procedures set by college IT managers. Computer lab employees use strong IdM practice at colleges with strong IdM policies and procedures. At these colleges the computer lab employees collect guest identification, issue unique user IDs and passwords, return the guest's ID after the guest has completed the computer usage, and deactivate the user ID and password. Colleges that have week IdM policies and procedures also have poor IdM practice. The lab employees at these colleges either have generic logins assigned to a computer or use personal user IDs and passwords to allow a guest access to computer resources.

There was two common denominator for all of the study. First, was the locus of control at the college. The IT professionals at colleges with strong central administration

used strong IdM practices. Colleges with weak central administration did not. This was most apparent in of the interviews with two college districts CIOs. Both colleges have similar make up. Both are suburban college districts with multiple independent campuses. One of the colleges had a strong centralized administration located at the college's district office. The campuses, although independent, relied on the district IT office for funding, equipment, policies, and other resources. The other college district had a weak central administration. Funding, equipment, policies and other resources were allocated directly to the independent campus, thus by-passing the central administration.

The second driving factor was funding. Small rural colleges with small budgets also had very weak IdM practices. These colleges simply did not have the funding resources to purchase the additional software needed to track guests or did not have the funding to hire and train employees on proper IdM practices. Nearly all of the rural colleges had only one lab assistant on duty at the time of my visit. The lab assistant also doubled as a tutor for students needing help with class assignments and homework.

## Summary

This chapter contained the results of the field research of this study. The Katsinas, Lacey, and Hardy classification for evaluating community colleges was explained. This classification system categorized community colleges by their service area: urban, suburban, and rural. Next, the interviews with community colleges' CIOs, and IT managers were summarized. Initially, 24 individuals were identified for interview in this study. During the initial set of interviews another 10 individuals were identified as

potential interviewees. Totally, 34 IT professionals were identified for interview. However, only 13 IT professionals from 10 colleges agreed to be interviewed.

Initial contact was made with the potential interviews via e-mail. This e-mail included the Walden consent form, details of the study, and the interview questions. Those interested in participating in the study were asked to reply to the e-mail with I Accept in the body. Thirty-six percent of the identified potential interviewees accepted to participate. The interviewees were chosen for their specific knowledge and understanding of the college's development and implementation of security policies, procedures, and practices. Their response to the interview questions appear in the first half of the chapter.

The next section of the chapter contained the field data from the college visits. I was able to locate the open computer lab and use a computer on all the campuses. I followed all the rules for campus computer usage. Three colleges required users to sign-in before accessing the computer lab. All sign-in sheets were filled out and identifications were shown at all campuses when requested. All instructions from college employees were followed. Some form of ID was required at only three of the computer labs. A driver's license was required at two of the labs. The driver's license was kept until my computer session was complete. A temporary user ID and password were generated by computer lab employees. At one college a county library card was required at one of the open labs. The remaining 10 college open labs required no identification to access computer resources. At one campus the librarian used her own user ID and password to log into the computer I used. This lack of computer security by the majority of colleges demonstrates community colleges in Texas need further security awareness and

additional security tools for IT professionals to prevent inappropriate usage.

# Chapter 5: Discussion, Conclusions, and Recommendations

One of the greatest challenges at all educational institution, including community colleges is network security. Community colleges are looking for ways to increase the protection of its networks and information systems from internal and external threats such as hacking, identity theft, viruses, and data loss and corruption. All of these security concerns can be mitigated by identifying all users of college computer resources. Identifying guest user is the focus of this study. Institutions of higher education are at a greater risk for these outside threats because of the open nature of the institution. Many IT departments are stretched to the limits to meet the equipment and staffing needs of an ever increasing and changing student body. Finding cost effective, labor friendly methods to identify guest users can alleviate budget and labor concerns as well as help protect colleges from liability caused by hackers, disgruntled employees, and dissatisfied students (D'Amico, Katsinas, & Friedel, 2012).

IT professionals interviewed in this study at community colleges in Texas believe all aspects of computer security are important. Alerts and warnings are issued from IT departments every time a new virus, such as Heartbleed, or a new spam social engineering technique appear. This study reflected the views and beliefs of 13 IT professionals at 10 Texas community colleges regarding network security policy, procedures, and practices.

Chapter 3 contained the research methodology and conceptual framework of policy, procedure, and practice of this study. The design of the interview questions asked of the IT professionals in this study remained the same. It was expected that fewer IT

professionals would participate in the study than initially planned. Even after data were collected from interviews and from college visits, the design remained primarily the same. The definition for college CIO and IT manager needed to be redefined and one new category was added to the design plan. The definition of CIO and IT manager needed to be expanded because the position titles used at the different colleges varied widely. I added a new category of outsourcing the college's network security authentication based on the information gathered during the college visits and interviews. The colleges added to the new category outsourced their library's computer management. This outsourcing included identification and authentication of open lab computer users to the college's library system. Figure 7 shows the complete conceptual design for this study.

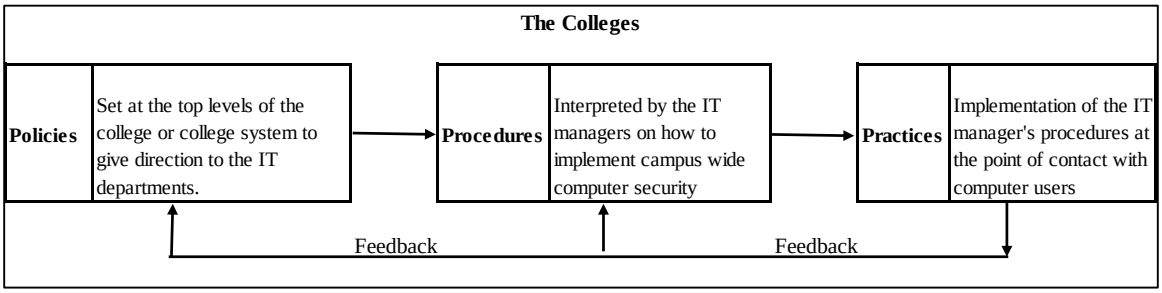


*Figure 8.* Conceptual Design of Network Security Policy, Procedures, and Practice. (Permission to reproduce image)

It is noteworthy that all interviewed were keenly aware of security issues facing their respective colleges and saw the importance of identity management on their campuses. The interviewees also saw the importance of IdM in other areas of network security. The data collected indicated that the college CIOs and IT managers have two great concerns beyond identity management of guest users. The first area of concern was identity management of the college's wireless infrastructure. The second area of concern

was budget constraints. These findings also match research found at other universities (Educause, n.d.). The data collected provided an interesting insight into the security policies, procedures, and practices at these community colleges in Texas. For the most part, these community colleges in Texas appear to have a good balance of security and academic freedom of research for faculty, students, and employees; however, this breaks down when it comes to guest access.

## Interpretation of Findings

Texas law states that all computer users must have a unique identifier before access to computer resources can be accessed (Texas Administrative Code, 2014). This can be avoided if a risk assessment shows no risk. None of the interview participants mentioned completing a risk analysis on computer users. Nine of the 13 colleges visited had generic computer logins assigned to open lab computers. These generic logins only identified the computer being used, not the person using the computer.

There was a contradiction between IT professionals at two different colleges. Both colleges were suburban college systems with multiple campuses. The CIO of one college stated the campuses were all autonomous with little to no intervention by the district office regarding IdM procedures for any user classification. An IT manager at one campus stated the exact opposite. He said the CIO in the system's IT department handled all identity management decisions. At another college, the CIO stated all the identity management decisions are made at the system level. One of the campus IT managers stated the opposite. He stated each campus was responsible for creating and implementing all IdM policies, policies, and procedures. When visiting the campuses, I

found the first anomaly was resolved in favor of the college system's CIO.

Only three colleges, 31%, had robust IdM policies, policies, and procedures in place to identify guest users. Two of the colleges used time consuming methods of gathering a state-issued ID from the user, logging the information, developing a guest account, and issuing the guest user ID and password. The other college outsourced the identification to the local county library system. This system was far less labor intensive; however, it relies on secondary identification without a photo identification for verification. All three of these colleges were considered suburban college systems with multiple campuses. This low percentage of identification verification among the sample indicates that the rest of the colleges may also be at risk for misuse of the college's computer assets by guest users.

I began this study with the assumption that community colleges in Texas have IdM policies, policies, and procedures in place to identify guest users on the college's network. Only three (23%) of the 13 colleges studied had strict policies and procedures in place for identifying guest users. Seven (54%) of the colleges studied did not require guest to identify themselves when using college computers or had only an unverified sign in sheet. This apparent lack of alignment between policies, policies, and procedures was confirmed after interviewing the IT CIOs and managers at the colleges and visiting the colleges' computer labs. Three (23%) of the colleges studied had nonverified sign-in sheets. These sheets only listed names, dates, and times of visits. There were no correlations between the sign-in sheet, who signed in, and which computer was used. There were also no corroboration of identification of those signing in on the sheets and

the signer's actual identification.

Ten (77%) of those interviewed did not see guest login as an issue at the forefront of IT security needs. Initial responses by most of the interviewees revolved around the college's policies used to allow guest users on the college's wireless network. This lack of concern by the IT professionals was unexpected.

## Limitations of the Study

Computer and network security is a broad and expanding topic. This study was limited to the security issues facing community colleges in the State of Texas because of their open access requirement. Much will be written regarding court cases, laws, and standards regarding security. Several sections will expand into general areas of computer security such as firewalls, proxy servers, traffic monitoring, encryption, privacy, copyright protection, and data theft. These sections are intended to make the reader more familiar with the complex and growing area of computer security and the issues facing computer professionals. Although these sections will appear in this study, they will be limited to only basic information or directly linked to IdM issues facing community colleges in Texas.

## Recommendations

Texas law is clear when it comes to securing computer resources at colleges. A user must have a unique user ID and password to access any computer resource (Texas Administrative Code, 2014). Two (15%) used a time consuming ID collection process. One (8%) outsourced guest identification to the county library system. Either method is preferable to no method; however, both have flaws. Collecting an ID to create a user ID

and password profile was time consuming and required two lab workers. One college allowed nonexpiring guest user ID that allowed the guest access to the college's computer resources that never expires. Using a noncollege issued identification, such as a library card, to gain access to college computer resources is less time consuming; however, the college is still at risk.

The Texas legislature also placed an additional mandate on community colleges to allow any member of the community access to the college's computer resources. Three (23%) of the campuses visited showed a good alignment between the state requirement to identify all computer users and the policies, procedures, and practices used at the college. Ten (77%) of the Texas community colleges' IT professionals in this study appeared not see guest user identification as a security concern. A risk analysis should be conducted by the IT professionals at these colleges before deciding to issues generic computer logins instead of issuing guest user login IDs. The Texas legislature meets every two years. Community college IT professionals should conduct a review during this time to ensure security policies, procedures, and practices that allow guest users access to the college's network align with State law.

This study can also be expanded to guest use of the community colleges wireless Internet portal, using strong password policies for guest users, and internal intrusion detection. The findings of this study indicated that 62% of the respondents see wireless access as a major security concern. Guest access to college computer resources via a college's computer or via the college's wireless Internet is closely related. Identification of all users makes internal intrusion detection much easier.

The review and improvements may come with some cost. Budget analysis and modification will be needed to find the funding. Information found in this study can be used as a rationale for the funding changes and help convince community college budget managers of the necessity of the budget increases and network changes. Using existing data found in State DMV databases or using existing federated tools could mitigate costs.

A different strategy for gaining information from the IT professionals could also be implemented. Interviewing the IT professionals was a very labor intensive and time consuming process. Future studies using an online survey would allow for broader distribution. Fine grain questioning can be written using a Likert scale and framing open-ended questions. Follow-up interviews can be held if additional information is needed or issues arise with the survey. There are many online survey cites, such as Survey Monkey, that will allow educators to create and distribute surveys easily and inexpensively.

Awareness of the lack of computer security for guest users is also an excellent opportunity for state legislatures, government agencies, the IT industry, and IT associations to begin creating standardized approaches to network security at community colleges. For example, in response to the REAL ID Act the State of Iowa legislature authorized the Identity Security Project. This project consists of a clearinghouse where various identity documents are linked together (Combs, 2008). These include birth certificate, social security number, driver's license, marriage license, and death certificate. This system allows multiple agencies to perform cross-linked identity verification and provide better tracking of identity theft. The concepts of primary identification (PID) and secondary identification (SID) are used in this case. The birth certificate is the PID.

Primary identification is the document associated with all other SIDs. Only SIDs that can be connected directly to a PID would be issued. At the same time, the birth certificate is electronically associated with all other SIDs issued in the future (State of Iowa, 2008).

Under this system when a guest user presents an ID to a computer lab employee, a concurrent check is run against the department of transportation's (DOT) database. This IdM system incorporates an individual's picture ID with documentation and processes to prevent identity theft and fraud. A guest user's ID would be rejected if a guest user attempted to submit a false ID.

Industry provided solutions for quick and accurate identification of users are also available. Microsoft developed the .NET Passport suite of services for authenticating (sign-in) users across a number of applications (Microsoft, 2003). The Passport single sign-in service solves the user authentication problem across multiple platforms. The .NET Passport allows users to create a single set of credentials that will enable them to sign into any cite that supports a Passport service. As part of a single sign-in service, commonly used information can be stored in a Passport profile and transmitted to the participating cites when visited. Passports reduce the barriers to acquiring user information because new users are not required to retype all their information when registering at a new cite. It also enables the site to customize and enhance the guest user's visit experiences without having to prompt them for user information (Microsoft, 2003).

The nonprofit industry also provided solutions for quick and secure user access across platforms. The .NET framework is not the only passport type IdM solution. Information technology associations, such as the Liberty Alliance Project, include more

than 150 companies and nonprofit and government organizations around the globe. Interestingly enough, the alliance does not include Microsoft. The consortium developed an open standard for federated network identity that supports all current and emerging network devices. Federated identification offers businesses, governments, employees, and consumers a more convenient and secure way to access and control identity information (Liberty Alliance, n.d.).

**Suggestions for Future Research**

Matching community college security policies, procedures, and practices for identifying guest users is a small, but important, part of the security issues facing IT professionals at community colleges. Security issues at community colleges have become varied and wide. Information technology managers are facing new security issues and challenges on an ever increasing rate. The IT managers at the college level are facing these challenges with ever shrinking budgets, personnel, and resources, while also trying to meet the ever increasing demands of network users. Using an inexpensive, labor unintensive, reliable IdM system will make network security much easier for IT professionals to implement.

This study covered the policy, procedures, and practices used by community college in Texas to allow guest users access to the college's network. One of the outcomes of this study highlighted the lack of standardization from the State or educational industry regarding IdM security at Texas community colleges. This wide range in the responses indicated that there are issues that need to be addressed. The first issue revolved around passwords. Only six of the respondents stated the need for all users

to login with a user ID and password. Of that six, only two required strong password creation.

Strong password policies may seem a small issue for a temporary guest password; however, strong password usage has become standardized practices across industries. Identity theft increases the longer a guest account remains open. The college's risk increases with the length of time a guest account stays active. A good example occurred at one of the colleges in this study. The college policy for guest users allowed for unlimited access time. Without strong password policies, there is an increased potential for ID theft. Lack of login security leaves the community college open to hackers, exposing the college to lose of data security, and opening the community college to potential lawsuits. Future research could revolve around the method the college uses to construct a strong password and how long the guest ID remains usable.

The second area that needs additional research was intrusion detection. Many network professionals view intrusion detection as protecting the community college data from outside intrusions. However, inside intrusions by students, employees, vendors, and guest users are just as dangerous. Intrusion detection software that analyzes data usage and access from both inside and outside of the network and shuts off access when inappropriate activity occurs will help protect the community college. More research on the use of intrusion detection software used by community college and industry can verify this concern.

While visiting the community colleges, I noticed a general lack of security awareness in 77% of the community colleges. This lack of security awareness was

present in all the community colleges that did not require a guest user ID and password. Stallings (2008) stated that security awareness needs to be the first step to preventing security breaches. During the community college visits, I did not address training specifically; however, there was one question in the interview questionnaire about training. That question was limited to which department was responsible for training open lab employees. The interview did not address security training content. Future studies regarding the IT professional's views on the importance of security training, the content of the security training, which employees to train, making the training voluntary or mandatory, the type of training (such as face-to-face, online, webinar, etc.) and the methods used to verify the employees' level of knowledge after the training are all suitable areas for emphasis.

Access to the college's wireless service was the biggest area of confusion during the interviews. A full 62% of the interviewees stated that securing the college's wireless services was part of their ideal security system. All the community college visited have Wi-Fi access points (WAPs) across the campus that provide access to the college's wireless network. All the colleges' WAPs provided users with access to the Internet without requiring a user ID and password. Simply opening a browser and clicking on the guest user button while within the college's Wi-Fi network gave the user full access to the Internet. Wireless access on many of the campuses reached far into the college's parking lots. This reach of a WAP allows users to gain access to the community college's network without leaving their cars. Although wireless Internet access was not part of this study, it is an area of concern that needs to be addressed. Similar interviews questions

could be used in a study about community colleges wireless network security policies, procedures, and practices.

Another unexpected theme from the interviews involved IT budgets and funding. Budgets and funding were especially apparent in the small, single campus rural community colleges. In retrospect, this should not have been a surprise. Daniels (2001) wrote at length about the lack of funding for IT departments at community colleges and the steps IT professionals can take to make IT budgets more effective. There are several additional topics about funding that need future consideration. One topic should revolve around the budget allocation the state provided to the IT department and how the funds are distributed. Another topic should involve locally generated income such as technology fees charged by the college to students. A third topic can be added regarding how often these funds are collected, how these funds are allocated, and who pays the fees. Lastly, outside funding resources such as grants and industry funding should be examined. Usage of outside funding resources would give college IT professionals addition funds to upgrade network security or free budgeted funds to upgrade network security.

## Implications

This research study's findings yielded implications for positive social change by increasing the ability for the general public to use computer resources at community colleges, keep the access secure, and protect the community colleges from liability for unauthorized or illegal usage. Other methods include, but were not limited to, improved IdM methods to identify guest users, provided inexpensive and labor un-intensive

information security methods, and provide the ability of college IT professionals to request additional funding to implement this protection.

Until now, tracking guest users at most community colleges in Texas has been a hap-hazard mishmash of either the use of generic access codes for each computer that did not identify guest users, to a very labor intensive screening before issue a temporary user ID and passwords, to accessing an outside database for proof if identity. Each of these methods have their pros and cons. Using generic was simple and labor un-intensive, but offered the least amount of protection. Requiring quest to furnish identification in order to receive a temporary user ID and password was very secure, but labor intensive. Lab assistants were taken away from other duties for a long period of time to process the guest and issues the user ID. Depending on a third party data base to identify guest users was a labor un-intensive method to offer secure user access; however, the third party identification did not come with a photo ID of the user. Again, the security of the network was put at risk.

## Conclusions

The lack of IdM practices at the majority of colleges visited, 77%, was unexpected. This dissertation began with the assumption that all community colleges in the State of Texas have ample policies and procedures in place to identify guest users who wanted to access the college's network. I also assumed these policies and procedures were used to develop security practices at the college's open computer labs. The findings of this study show the opposite. There were no uniform policies, procedures, or practices in place. The colleges that do follow IdM practices use antiquated, labor intensive

practices that could be overwhelmed when the number of guest users increases. Further automation using a centralized identification database is needed.

This research contributed to the understanding and implementation of IdM by expanding the traditional view of network users at community colleges. IdM theory assumes that all network users go through some vetting system to verify exact identity credentials before the user receives access to network resources. This study indicated there is an active group of college computer users who do not receive any vetting at most colleges in the sample population. Calling attention to this group should cause college IdM professionals to broaden their scope of users and begin to implement IdM solutions for all users. Even the colleges where IdM practices were in place had problems. The college employees used antiquated, time consuming methods to identify the guest user. Improvements are needed in both systems.

This study is significant in two areas. First, it keeps an avenue for bridging the digital divide open. Early in the research, it was suggested that the focus should be to find ways to change the law that allowed guest users access to community college computer resources to limit the potential for abuse. This suggestion was abandoned because it meant changing the funding system for community colleges in Texas. Local access to the community college's resources comes with the local tax base. A local tax base keeps the tuition very low. Losing open access would mean losing or significantly modifying the local tax base. This study indicated the need to provide a standardized, inexpensive method of identifying guest users that can be implemented with very little labor or supervision. Implementing such practices should allow the colleges to budget funds more

effectively and be assured that liability for any malicious criminal activity will not be the college's responsibility.

# References

Alamo Community College. (2013). Acceptable technology use policy.

Alamo Community Colleges. (2008, May). Bridging the digital divide. Retrieved from http://www.alamo.edu/uploadedfiles/district/about_us/chancellor/reports_and_documents/digitaldivide.pdf

Alotaibi, S., Wald, M., & Gilbert, L. (2012). Limitations in the current federated access management systems. *International Journal of Innovation, Management and Technology, 20*(38), 28-30. Retrieved from http://eprints.soton.ac.uk/273095/1/IJIMT_Sara%20Alotaibi%20-%20%20Limitations%20In%20The%20Current%20Federated%20Access%20Management%20Systems.pdf

Alvin Community College. (2009). 2008-2009 Student handbook. pp. 34-36

Alzomai, M. (2011). *Identity management: Strengthening one-time password authentication through usability* (Doctoral dissertation, Queensland University of Technology).

Amer, S. H., & Hamilton, J. A. (2008). Understanding security architecture. In SpringSim '08 Proceedings of the *2008 Spring Simulation Multiconference*. (pp. 335-342). San Diego, CA.

Ardagna, C. A., De Capitani di Vimercati, S., Foresti, S., Paraboschi, S., & Samarati, P. (2010, October). *Supporting privacy preferences in credential-based interactions. 9th annual ACM workshop on Privacy in the electronic society* (pp. 83-92). Retrieved from http://spdp.di.unimi.it/papers/wpes2010.pdf

Association of Computing Machinery. (2008). Home Page. Retrieved from www.acm.org

Backes, M., Clark, J., Kate, A., Simeonovski, M., & Druschel, P. (2014). BackRef: Accountability in anonymous communication networks. In *Applied Cryptography and Network Security* (pp. 380-400). Springer International Publishing.

Baldoni, R. (2012). Federated identity management systems in e–government: The case of Italy. *Electronic Government, an International Journal, 9*(1), 64-84. doi:10.1504/EG.2012.044779

Barati, M., Hakimi, Z., & Javadi, A. (2013). A Flow based horizontal scan detection using genetic algorithm approach. *Life Science Journal*, *10*(8), 331-335. Retrieved from https://sites.google.com/site/ahjavadi/cv/engineering-publications

Barker, G. (2000, May). Microsoft may have been target of lovebug. *The Age*.

Barrère, M., Hurel, G., Badonnel, R., & Festor, O. (2013). A probabilistic cost-efficient approach for mobile security assessment. *IFIP/IEEE International Conference on Network and Service Management*, 235-243. Retrieved from http://www.cnsm-conf.org/2013/documents/papers/CNSM/p235-barrere.pdf

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*, 337-346. http://dx.doi.org/10.1108/09576050210447019

Becket, N., & Brookes, M. (2006). Evaluating quality management in university departments. *Quality Assurance in Education, 14*(2), 123-142.

Beckett, D., (2006, May). *Burton Group recommendations report for MnSCUs' identity management architecture final revision V2.2*. Retrieved from

http://www.its.mnscu.edu/projects/current/idm/documents/mnscu-idm-assessment-v2.2.pdf

Bennett, C., & Schuster, S. (2008, May). Establishing an information security program. Seminar, *EDUCAUSE Security Professional Conference*. Arlington, VA.

Bentley, L., Dittman, K., & Whitten, J. (2004). *Systems analysis and design methods* (6th ed.). New York: McGraw-Hill.

Bertino, E., Bhatti, R., & Ghafoor, A. (2010, August). A policy framework for access management in federated information sharing. *IFIP International Federation for Information Processing*. *193*(1). Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-42.pdf

Bertino, E., & Takahashi, K. (2011). *Identity management: Concepts, technologies, and systems.* Norwood, MA: Artech House Publishers.

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2005). Establishing and protecting digital identity in federation systems. *2005 Workshop on Digital Identity Management* (pp. 11-19). Retrieved from http://homes.cerias.purdue.edu/~bhargav/IdM/dim13-bhargav.pdf.

Blinn Community College. (2008, March 18). Your Blinn college guest computer card - bryan campus.

Boehmer, W. (2008). Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001. *The Second International Conference on Emerging Security Information, Systems and Technologies*. doi:10.1109/SECURWARE.2008.7

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups. *Cyber Crime. International Journal of Cyber Criminology, 8*(1), 1-20. Retrieved from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Brotby, K. (2007). Information security governance: who needs it? *Information Systems Control Journal, 2,* 13-14. Retrieved from http://www.isaca.org/Journal/Past-Issues/2007/Volume-2/Pages/Information-Security-Governance-Who-Needs-It-1.aspx

Browne, M. (1997). The field of information policy: Fundamental concepts. *Journal of Information Science*, 23, 261-275. doi:10.1177/016555159702300401

Bruhn, M., & Petersen, R. (2003). Policy development for information security, Computer and Network Security in Higher Education. *EDUCAUSE Leadership Strategies. 8*. (pp. 59- 72) San Francisco: Jossey-Bass.

Buchan, B. (2013, February). *Identity management delegation and automation*. Retrieved from http://www.slideshare.net/billbuchan/identitymanagementdelegationandautomation

Burd, S. (2004). The impact of information security in academic institutions on public safety and security: Assessing the issues and developing solutions for policy and practice. *Information Security in Academic Institutions. U.S. Department of Justice*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/215953.pdf

Cain, M. (2003). Cybertheft, network security, and the library without walls. *The Journal of academic librarianship, 29*(4), 245-248.

Camenisch, J., Fischer-Hübner, S., & Rannenberg, K. (2011). *Privacy and identity management for life*. Zurich, Switzerland: Springer.

Cameron, K. (2005, May). MyInstantID. *The Laws of Identity*. Retrieved from http://myinstantid.com/laws.pdf

Camp, J., & DeBlois, P. (2007). Current issues survey report, 2007. *Educause Quarterly, 30*(2), 12.

Cao, Y., & Yang, L. (2010, December). A survey of identity management technology. In Information Theory and Information Security (ICITIS), *2010 IEEE International Conference* (pp. 287-293). IEEE. doi:10.1109/ICITIS.2010.5689468

The Carnegie Foundation for the Advancement of Teaching. (2007, June). Basic classification technical details. *Carnegie Foundation for Advanced Teaching*. Retrieved from jma-inc.clubwizard.com/IMupload/CarnegieTechnical.pdf

Chen, K., Lin, C., & Hou, T. (2011, December). The low-cost secure sessions of access control model for distributed applications by public personal smart cards. Parallel and Distributed Systems (ICPADS), *IEEE 17th International Conference* (pp. 894-899). doi:10.1109/ICPADS.2011.136.

Clark, T., & Sitko, T. (2008). Information security governance: Standardizing the practice of information security. *ECAR Research Bulletins, 17*. Washington: Retrieved from: http://connect.educause.edu/Library/Abstract/InformationSecurityGovern/47191

College of the Mainland (COM). (2001, April 2). Information technology resources and systems. Retrieved from College of the Mainland.

Combs, D. (2002, August). *Identity security project.* Retrieved from State of Iowa: http://www.iowa.gov

Constantinescu, R., & Corlan, L. (2009). An adaptive authorization model based on RBAC. Journal of Mobile, *Embedded and Distributed Systems, 1*(2), 119-126.

Cox, J., & Kistner, T. (2003, July). Security lessons. *Network World*, p.35

Crase, D., Malone, M., Manoharan, M., & May, T. (2006). California State University: The identity management collaborative: Remote middleware support. *NMI-EDIT* Retrieved from http://www.nmi-edit.org/case_studies/CalState200602.pdf

Crosbie, M., & Spafford, E. (1995). *Applying genetic programming to intrusion detection*. Retrieved from http://citeseer.ist.psu.edu/crosbie95applying.htm

D'Amico, M., Katsinas, S., & Friedel, J. (2012). The new norm: Community colleges to deal with recessionary fallout. *Community College Journal of Research and Practice, 36*(8), 626-631.

Da Viega, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management, 24*, 361-372. doi:10.1080/10580530701586136

Dallas County Community College District. (2003, February). *New CVC president comes home to Dallas*. Retrieved from http://dcccd.edu/cgi-bin/MsmGo.exe?grab_id=0&page_id=15927&query=%22digital%20divide%22&hiword=DIGIT%20DIGITALLY%20DIGITS%20DIVIDED%20DIVIDES%20D

IVIDING%20digital%20divide%20

Daniels, J. (2001). The weakest link…This is not a game. *SANS Institute InfoSec Reading Room*. Retrieved from http://www.sans.org/reading-room/whitepapers/basics/weakest-linkthis-game-440

de Oliveira, G., da Carmo, L., & de Ameida, A. (2006). Enterprise security governance: a practical guide to implement and control information security governance. *Business driven IT management2006*. BDIM06. The first IEEE/IFIP Conference, p. 71-80. doi:10.1109/BDIM.2006.1649213

Decker, H., & Martinenghi, D. (2011) Inconsistency-tolerant integrity checking, knowledge and data engineering, *IEEE Transactions 23*(2), 218 -234, doi:10.1109/TKDE.2010.87

Department of Justice (n.d.). *The Privacy Act of 1974*. Retrieved from http://www.justice.gov/opcl/privacy-act-1974

Doherty, N., & Fulford, H. (2006, February). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), 55-63.

Donnet, B., Gueye, B., & Kaafar, M. A. (2010). A survey on network coordinates systems, design, and security. *IEEE Communications Surveys & Tutorials, 12*(4), 488-503.

Dowd, A., & Shieh, L. (2013). Community college financing: Equity, efficiency, and accountability. *The NEA Almanac of Higher Education*, 37-65.

Educause. (n.d.). *Effective security practices guide*. Retrived from https://wiki.internet2.edu/confluence/display/2014infosecurityguide/Home

Educause. (2008). *About EDUCAUSE*. Retrived from http://www.educause.edu/about

Evans, E., Kotlas, C., Bailey, D., Crystal, A., & Bruckner, T. (2004). It's eleven o'clock: Do you know where your identity is? 32nd Annual ACM SIGUCCS Conference on User Services (pp. 361-363). Baltimore: ACM Press.

Fischer-Hubner, S. (2008). *The future of identity in the information society*. New York: Springer.

Fitzgerald, K. (2014). Information security baselines. *Information Management & Computer Security, 5*(22), 8-12. doi:10.1108/09685229510088575

Forbes C., & Davis, E. (2008, February). The development of preservice elementary teachers' curricular role identity for science teaching. *Science Education, 92*(5), 909-940. doi:10.1002/sce.20265

Francia, G., & Hutchinson, F. (2014). Regulatory and policy compliance with regard to identity theft prevention, detection, and response. *Crisis Management: Concepts, Methodologies, Tools and Applications,* 280. dio: 10.4018/978-1-4666-4707-7

Gallegos, F. (2002). Due professional care. *ISACA Journal,* 2. Retrieved from http://www.isaca.org/Journal/Past-Issues/2002/Volume-2/Pages/Due-Professional-Care.aspx

Galuszka, P. (2004). The War over Internet Piracy: Fearing Lawsuits, College Officials Crack down on Illegal Downloading of Music and Videos on Campus. *Black Issues in Higher Education, 21*(2), 24.

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security, 12,* 36-40.

doi:10.1201/1079/43855.31.6.20031201/78849.3

Glesne, C., & Peshkin, A. (1992). *Becoming qualitative researchers: An introduction* (p. 6). White Plains, NY: Longman.

Golafshani, N. (2003, December). Understanding reliability and validity in qualitative research. *The Qualitative Report*. Retrieved from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Goulding, C. (2002*). Grounded theory: a practical guide for management, business and market researchers.* London: Sage

Hajdarevic, K., & Allen, P. (2013, May). A new method for the identification of proactive information security management system metrics. Information & Communication Techno*logy Electronics & Microelectronics (MIPRO), 2013 36th International Convention* (pp. 1121-1126). IEEE.

Halperin, R., & Backhouse, J. (2007, December 28). A roadmap for research on identity. *Identity Journal Limited*, p. 17. doi:10.1007/s12394-008-0004-0

Hardy, D., & Katsinas, S. (2006). The Katsinas, Lacey, and Hardy classification system for 2 year Institutions. *Instructional Leadership Abstracts*, 1-16. Retrieved from http://www.accbd.org/articles/index.php/attachments/single/98

Hardy, D., Katsinas, S., & Stephen G. (2006, April-May). Using community college classifications in research. *Community College Journal of Research & Practice*, 339-358.

Harper, J. (2012). *Understanding the realities of REAL ID: A review of efforts to secure drivers' licenses and identification cards.* Retrieved from

http://www.cato.org/publications/congressional-testimony/understanding-realities-real-id-review-efforts-secure-drivers-licenses-identification-cards

Health Insurance Portability and Accountability Act (HIPAA) Advisory. (2013, January). *New rule protects patient privacy, secures health information*. Retrieved from http://www.hhs.gov/news/press/2013pres/01/20130117b.html

Hone, K., & Eloff, J. (2002, October). Information security policy – what do international security standards say? *Computer Security, 21*, 402-409

Hong, K., Chi, Y., Chao, L., & Tang, J. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security, 14*, 104-115.

Hudson, D. (2008). *A Policy Analysis of Community College Funding in Texas*. Austin, TX: University of Texas. Retrieved from http://www.tacc.org/documents/dhudson_dissertation.pdf

Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management system standard*. Boston: Artech House.

Hunter, G. (2005). Status of intellectual property law in the age of the internet. *Law Technology, 38*(1), 1-31.

International Organization of Standardization. (2001). *Information technology – security techniques – code of practice for information security management*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human–Computer*

*Interaction*, *29*(4), 311-350.

Jensen, J. (2012). Federated identity management challenges. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on* (pp. 230-235). IEEE. doi:10.1109/ARES.2012.68

Jensen, J. (2011). Benefits of federated identity management-a survey from an integrated operations viewpoint. Lecture Notes in Computer Science. 6908. 1-12. Berlin Heidelberg: Springer doi:10.1007/978-3-642-23300-5_1

Jiang, J., Duan, H., Lin, T., Qin, F., & Zhang, H. (2011, August). A federated identity management system with centralized trust and unified single sign-on. *Communications and Networking in China (CHINACOM) 2011 6th International ICST Conference* (pp. 785-789). IEEE. doi:10.1109/ChinaCom.2011.6158260

Johnson, B. (2006). Identities management: Challenges in modern security protocol. *Information Systems Journal*, *9*(1). Retrieved from http://www.blackwellpublishing.com/journal.asp?ref=1350-1917&site=1

Johnson, D. (2000). Should computer programs be owned? *Social and Moral Issues in the Computer Age.* Amherst, NY: Prometheus Books.

Johnson, D., & Simpson, C. (2005). Are you the copy cop? Why copyright violations happen in colleges and how to prevent them. *Learning and Leading with Technology*, 14-20.

Johnson, L., Adams-Becker, S., Cummins, M., Estrada, V., Freeman, A., & Ludgate, H. (2013). Technology outlook for community, technical, and junior colleges 2013-2018: *An NMC horizon project sector analysis*. Retrieved from

http://www.nmc.org/pdf/2013-technology-outlook-community-colleges.pdf

Jones, G., & George, H. (2012). *Essentials of contemporary management*. New York: McGraw-Hill/Irwin.

Jøsang, A., & Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference* (p. 77).

Kam, H., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information security policy compliance in higher education: A neo -institutional perspective, *PACIS 2013 Proceeding*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1106&context=pacis2013

Kang, R., Brown, S., & Kiesler, S. (2013, April). Why do people seek anonymity on the internet?: informing policy and design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2657-2666). ACM.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security, 24*, 246-260.

Kephart, J. (2011, January). REAL ID Implementation. *Center for immigration studies*. Retrieved from: http://www.cis.org/sites/cis.org/files/articles/2011/real-id.pdf

Kiosk Market Place. (2011, December). *Study: Kiosk usage on the rise. Kiosk market place.* Retrieved from http://www.kioskmarketplace.com/article/188291/Study-Kiosk-usage-on-the-rise

Kleblawi, F., & Sullivan, D. (2007). The case for flexible NIST security standards. *IEEE Computer Society, 40*(6), 19-26. doi:10.1109/MC.2007.223

Koch, M., & Moslein, M. (2005). Identities management for e-commerce and

collaboration applications. *International Journal of Electronic Commerce, 9*(3), 11-29.

Kulkarni, D., & Tripathi, A. (2011). *Context-aware role-based access control in pervasive computing systems.* Retrieved from http://ajanta.cs.umn.edu/papers/sacmat2008.pdf

Lancianese, D. (2005). A new unified theory of sociobehavioural forces. *European Sociological Review, 24*(4). Retrieved from http:www.oxfordjournals.org/lancianese/article123098756.htm

Landsman, K. (2009, August). College IT leaders confident about network security. *Community College Journal, 8*(1). 8-17

The League for Innovation in the Community College. (2000, February). *Bridging the digital divide project*. Retrieved from http://www.league.org/league/projects/digital_divide.cfm

Lederer, S., Hong, J., Dey, A., & Landay, J. (2005). Personal privacy through understanding and action: Five pitfalls for designers, in designing secure systems that people can use. *Information Systems Journal, 12*(3). Retrieved from http://www.blackwellpublishing.com/journal.asp?ref=1350-1917&site=1

Leedy, P., & Ormrod, J. (2004). *Practical research planning and design* (7th ed.). Columbus, OH: Merrill.

Leggett, T. (2006). Single sign-on and the corporate directory, Part IV. *Linux Journal. 6*(143).

Levine, J., & Kater, S. (2012). Community college mission in historical perspective.

*Understanding community colleges*. New York:Routledge.

Liberty Alliance. (n.d.). Identity governance. Retrieved from http://www.projectliberty.org/liberty/strategic_initiatives/identity_governance

Lindup, K. (1996). The role of information security in corporate governance. *Computers and Security*, *15*, 477-485.

Lips, A., Taylor, J., & Organ, J. (2006). Identity management as public innovation: Looking beyond ID cards and authentication systems. In V. J. J. M. Bekkers, H. P. M. van Duivenboden, & M. Thaens (Eds.), *ICT and public innovation: Assessing the modernization of public administration* (pp. 204-216). Amsterdam: IOS Press.

Lonestar College. (2007). *Lone Star College System workforce development environmental scanning and strategic planning 2006-2007*. Retrieved from http://www.lonestar.edu/documents/instresrcheffect-cs/Summary_of_Trends_with_Implications.pdf

Luallen, M., & Labruyere, J. (2013, January). Developing a critical infrastructure and control systems cybersecurity curriculum. *System Sciences (HICSS), 2013 46th Hawaii International Conference on Cyber Security*. 1782-1791. doi:10.1109/HICSS.2013.176

Lyons-Burke, K. (2007). Federal agency use of public key technology for digital signatures and authentication. *NIST Special Publication 800-25*. Gaithersburg, MD: National Institute of Standards and Technology.

McEvily, B., & Tortoriello, M. (2011). Measuring trust in organizational research:

Review and recommendations. *Journal of Trust Research. 1*(1). 23-63.

Merriam, S. (2001). *Qualitative research and case study applications in education*. San Francisco: Jossey-Bass.

Mesmer, E. (2009, February). Data-breach costs rising, study finds. *Network World*. Retrieved from http://www.networkworld.com/news/2009/020209-data-breach.html

Microsoft. (2003, March). *Microsoft .NET passport review guide*. Retrieved from http://www.microsoft.com/net/services/passport/review_guide.asp

Microsoft. (2008, May). *Directory services.* Retrieved from http://msdn.microsoft.com/en-us/library/ms682458(VS.85).aspx

Microsoft. (2009, January). *MSDN, SQL server development center*. Retrieved from http://msdn.microsoft.com/en-us/library/aa273982(SQL.80).aspx

Miles, M., Huberman, A., & Saldaña, J. (2013). Qualitative data analysis: *A methods sourcebook.* Los Angeles:SAGE

Millron, D., & Miles, C. (2000, November/December). *Education in a digital democracy*. Retrieved from http://net.educause.edu/ir/library/pdf/erm0064.pdf

Moore, N. (1994). Information policy research priorities for Europe. *Policy Studies, 15*(1), 16-25.

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

Murphy, R. (2014, February). *Usability and network security in higher education.* Retrieved from http://www.educause.edu/blogs/vvogel/usability-and-network-

security-higher-education

National Institute of Standards and Technology. (2007, March). *Information security handbook: a guide for managers. NIST SP800-100.* Washington: United States Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

National Institute of Standards and Technology. (2008, March). *Drivers*. Retrieved from http://csrc.nist.gov/drivers/index.html

NEC Unified Solutions, Inc. (2007, March). *Information security: A perspective for higher education.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Neuenschwander, M., & Gebel, G. (2008, April). Vantage poiecure systems that people can use. *Information Systems Journal, 12(*3). Retrieved from http://www.blackwellpublishing.com/journal.asp?ref=1350-1917&site=1

Newman, J. (1991, March). *United States of America, appelle v. Robert Tappan Morris defendant.* Retrieved from http://www.loundy.com/CASES/US_v_Morris2.html

NICC. (n.d.). *National interagency coordination center*. Retrived from www.nifc.gov/nicc/

Nikols, N., & Gebel, G. (2006). Identify lifecycle management. *Burton Group.* Retrieved from http://www.burtongroup.com/research/research_consulting/publicdoc.aspx?cid=165

Ning, P., Liu, A., & Wenliang, D. (2008). Mitigating DoS attacks against broadcast

authentication in wireless sensor networks. *ACM Transactions on Sensor Networks, 4*(1). doi:10.1145/1325651.1325652

Novell. (2008). eDirectory. Retrieved from http://www.novell.com/products/edirectory/

Oblinger, D. (2003). IT Security and academic value. In M. Luker & R. Peterson (eds.), *Computer and Network Security in Higher Education* (pp. 1-14), San FrancusciL Jossey-Bass.

Oblinger, D., & Hawkins, B. (2006). The myth about IT security. *Educause Review, 41*(3), 14-15.

Peltier, T. (2013). *Information security policies, procedures, and standards: Guidelines for effective information security management*. CRS Press.

Penzo, L. (2012, March). *ATM machine statistics*. Retrieved from http://statisticbrain.com/atm-machine-statistics/

Pentafronimos, G., Karantjias, A., & Polemi, N. (2011, June). Open issues on privacy and trust in collaborative environment. *Computers and Communication (ISCC*), 2011 IEEE Symposium (pp. 876-880). IEEE

Pirani, J., & Spicer, D. (2006). *Most improved: how four institutions developed successful it security programs*. ECAR case study 6 (p. 16). Washington: EDUCAUSE Center for Applied Research.

Polk, W., & Hastings, N. (2006). Bridge certification authorities. *Connecting B2B Public Key Infrastructure*. Gaithersburg, MD: National Institute of Standards and Technology.

Posthumus, S., & Von Solms, R. (2004). A framework for the government of information

security. *Computers and Security*, 23, 638-646.

Purser, S. (2004). *A practical guide to managing information security*. Norwood, MA:Artech House.

Ranga, G., & Flowerday, S. (2010). Identification now and in the future: Social grant distribution process in South Africa. *International Federation for Information Processing Digital Library, 232*(1).

Razavi, M., & Iverson, L. (2008). A framework for privacy support in group information management systems. In *Group '07 Doctoral Consortium Papers* (pp. 1-2). New York: ACM Press.

Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer. 44*(9), 51-58.

Rosenblatt, J. (2008). Security metrics: A solution in search of a problem. *Educause Quarterly*, 31(3), 8-11.

Rock, B. (2007, September). Why IP addresses are important for computer networking. Inside Technology 360. Retrieved from http://www.insidetechnology360.com/index.php/why-ip-addresses-are-important-for -computer-networking-33687/

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

Saleh, M., Alrabiah, A., & Bakry, S. (2005). E-Business diffusion requirements: A STOPE view for easing the use of ISO 17799 information security management standard. *Organization*, 6, 16.

Salomon, K., Cassat, P., Thibeau, B., Dow, L., & Albertson, P. (2003). IT security for higher education: a legal perspective. *EDUCAUSE/Internet2 Computer and Network Security Task Force*, 1-19.

Scott, K., & Johnson, M. (2011). Strategic leadership: A model for promoting, sustaining, and advancing institutional significance. *Community College Journal of Research and Practice*, *35*(6), 454-469.

Sen, J. (2010). Internet of things-A standardization perspective. *This article is property of Tata Consultancy Services*.

Song, D., & Ma, F. (2012). Strategy and implementation of campus network security. In *Systems and Informatics (ICSAI), 2012 International Conference on* (pp. 1017-1019). IEEE. doi:10.1109/ICSAI.2012.6223184

Stallings, T. (2008). *Network security in two-year colleges*. ProQuest.

Stamper, L. (2012). Higher education leaders' roles in access security management. *Higher Education*, *1*, 1-2012.

Stasiak, A., & Zieliński, Z. (2013). An approach to automated verification of multi-level security system models. New Results in Dependability and Computer Systems. 375-388. doi:10.1007/978-3-319-00945-2_34

State of Iowa. (2004). IOWA return on investment program. *State of Iowa*. Retrieved from http://stae.ia.us

Stiles, M., & Swicegood, T. (n.d.). 82nd Legislative session bills. The Texas Tribune. Retrieved from http://www.texastribune.org/session/82R/bills/

Stunden, A. (2006). Identity management conference report. In Proceedings of the

Identity Management Conference. 5-32. New York: ACM Press.

Sudduth, A. (2001, July). The what, why, and how of the 1988 Internet worm. Retrieved from http://snowplow.org/tom/worm/worm.html

Texas Administrative Code. (2014, March). *ADMINISTRATION*. Retrieved from http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=25

Texas Association of Community Colleges. (2010, Fall). *Other Texas community college information*. Retrieved from http://www.tacc.org/ccenrollment.htm

Texas Department of Transportation. (2009, February*). Local government project procedures*. Retrieved from http://ftp.dot.state.tx.us/pub/txdot-info/cso/lgpp/data.pdf

Texas Legislature. (2011, September). *New laws effective September 1, 2011*. Retrieved from http://www.lrl.state.tx.us/whatsNew/client/index.cfm/2011/8/22/New-laws-effective-September-1-2011

Thain, D., Tannenbaum, T., & Livny, M. (2005). Distributed computing in practice: The Condor experience. *Concurrency and computation: practice and experience*, *17*(24), 323-356.

Tipton, H., & Krause, M. (2012). *Information security management handbook*. Boca Raton, FL: CRC Press.

Tsang, P., Au, M., Kapadia, A., & Smith, S. (2007). Do background images improve "draw secret" graphical passwords? In Proceedings of the *14th ACM Conference on Computer and Communications Security*. 36-47. New York: ACM Press.

U.S. Congress subcommittee on crime. (2001, May). *Fighting cybercrime hearing before the subcommittee on crime*. Retrieved from http://www.globalsecurity.org/security/library/congress/2001_h/hju72616_0.htm

UT System. (2001, September). *University liability for student infringements*. Retrieved from http://www.utsystem.edu/OGC/IntellectualProperty/napster.htm

Vij, D., Majumdar, I., Dhar, N., & Vanecek, G. (2014, March). Trust blueprints and use cases. ICDS 2014, *The Eighth International Conference on Digital Society*. 93-101.

Von Solms, S. (2006). Information security governance: COBIT or ISO 17799 or both? *Computers and Security, 24*, 99-104. London: Sage.

Von Solms, S. (2010). The 5 waves of information security–from Kristian Beckman to the present. *Security and Privacy–Silver Linings in the Cloud*. 1-8. Berlin Heidelberg:Springer

Wachsmann, A. (2005). Centralized authorization using a directory service, Part II. *Linux Journal, 7*(131), 5. Retrieved from http://www.linuxjournal.com/article/7334

Walton, J. (2002). Developing an enterprise information security policy. *SIGUCCS '02 November 20-23, 2002*. Providence, RI. doi:10.1145/588646.588678

Wang, X., & McClung, S. (2011). Toward a detailed understanding of illegal digital downloading intentions: An extended theory of planned behavior approach. *new media & society, 13*(4), 663-677. doi:10.1177/1461444810378225

Ward, R. (2013, February). What's bigger than identity and access management? IAM IT automation is…. *Avatier Identity Management*. Retrieved from

http://blog.avatier.com/whats-bigger-than-identity-and-access-management-iam-it-automation-is/

Weiner, C. (1966). Science and higher education. *Science and society in the United States*. 163-190.

Wharton Community College. (n.d.). WCJC libraries internet policies and guidelines.

Whitman, M., & Mattord, H. (2003). Principles of information security. Boston MS: Thompson.

Whitman, M., Townsend, A., & Hendrickson, A. (1999). Cross national differences in computer use ethics: A nine country study. *The Journal of International Business Studies*, pp. 673-687.

Whitten, D. (2008). The chief information security officer: an analysis of the skills required for success. *The Journal of Computer Information Systems, 48*, 15-19.

Wiant, T. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, *24*, 448-459.

Wiburg, K., Tellez, K., Altamirano, A., & Parra, J. (2015). Digital democracy: Panelists will share technology-based projects for empowering marginalized populations in K-12 and adult education. Attendees will be invited to discuss uses of technology for addressing a deepening digital divide in the US. In *Society for Information Technology & Teacher Education International Conference* (Vol. 2015, No. 1, pp. 2122-2124).

Wilson, G., & Tharakan, U. (2008). The institute of internal auditors. *The Institute of Internal Auditors*. Retrieved from: http://www.theiia.org/ guidance

Winter, G. (2000). A comparative discussion of the notion of validity in qualitative and quantitative research. *The qualitative report, 4*(3), 4.

Wolcott, H. (2007). *Writing up qualitative research*. London: Sage.

Yin, R. (2009). *Case study research design and methods, fourth edition*. Thousand Oaks, CA: SAGE, Inc.

Youngdale, E. (2009). Reviewing the law reviews. *Defense Counsel Journal, 74*(1).