INFORMATION SECURITY ANALYSIS: A STUDY TO ANALYZE THE EXTENT TO WHICH INFORMATION SECURITY SYSTEMS CAN BE UTILIZED TO PREVENT INTOXICATED INDIVIDUALS FROM DRIVING

By

Joseph D. Pierre

SAMUEL M. NATALE, PhD, Faculty Mentor and Chair

DIANE L. STOTTLEMYER, PhD, Committee Member

EMILE JEAN-BAPTISTE, MD, PhD, Committee Member

William A. Reed, PhD, Acting Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

December 2010

Abstract

Information security systems (ISS) have been designed to protect assets from damages and from unauthorized access internally as well as externally. This research is promising similar protection from ISS methods that could prevent intoxicated individuals under the influence of alcohol from driving. However, previous research has shown significant challenges to the real time estimation of blood alcohol concentration (BAC) levels due to individual variances of body weight and metabolic rate. As a result, BAC validations via ISS have been found difficult to measure. Integrating information security technology into a vehicle to evaluate BAC levels when one inserts the key into the vehicle ignition was found to have the most significant effect in minimizing drunken driving fatalities. ISS methods of determining intoxication based on alcohol consumption to prevent intoxicated individuals from driving have received some attention. Nevertheless, a comprehensive intoxication detector using the current models of ISS has not yet been developed. Such a comprehensive method requires these fundamental questions to be asked: To what extent can ISS be utilized to prevent intoxication related accidents? How can ISS obtain the data to detect the intoxication level of an individual when starting a motor vehicle? What are the significant factors for implementing ISS in motor vehicles to prevent intoxicated individuals from driving? How can ISS make a decision to prevent an intoxicated individual from driving? This study presents several attempts to address these questions through qualitative case study methodology, analyzing the impact of ISS, presenting integrated models of information security context, and offering suggestions for further research.

Dedication

This study is dedicated to my family, friends, and those who have motivated and encouraged me to follow my dream and become who I am today.

Acknowledgments

I would like to express many thanks to my family for their support and tremendous encouragement with this research study. My thanks to my wife, Loudia, who has walked this journey with me and to my children, Loukeisha, Jennica, and Crystal, who have provided me with encouragement and inspiration to complete the dissertation during this challenging moment in our lives.

My special thanks to Dr. Samuel Natale, my mentor throughout the research process, who has provided me with the necessary guidance and encouragement to arrive at this point.

I also want to thank my committee members, Dr. Diane Stottlemyer and Dr. Emile Jean-Baptiste, who have always made time available for dialogue and provided me with insightful comments throughout my dissertation drafts. Your recommendations have made this dissertation a better product. I also want to thank my editor, Arlene, for all the helpful suggestions she provided. I would like to express my gratitude to you all for the suggestions and promptness throughout this dissertation process.

A special thanks to all my participants who shared their experiences with me and made the completion of this dissertation possible. Moreover, many thanks to the doctoral faculty of Capella University for all the help they provided during this journey.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Introduction to the Problem

Over 25 years ago, John Naisbitt predicted a shift to an information based society (1982). Ten years later, the advent of such digital technologies as wireless computing networks, telecommunications, and other innovations contributed to the actualization of this predication (Kantrow, 1980). This research study explores the extent to which information security systems (ISS) can prevent intoxicated individuals from driving. In doing so, it may provide data that helps to determine if ISS can serve to reduce alcohol related motor vehicle accidents (Keen, 1991). This study should also help enhance the understanding of the interrelated issues associated with detection and prevention capabilities of ISS and recognize the static and dynamic capabilities of ISS technology for stopping vehicle engines based on alcohol level measurements of drivers.

According to National Highway Traffic Safety Administration (2006), in 2005 16,885 people in the United States died in automobile accidents while intoxicated. Drugs other than alcohol were involved in about 18% of the motor vehicle crashes. Drugs such as stimulants, depressants, and others, are often used in combination with alcohol (Jones, Shinar, & Walsh, 2003). Given that common biological samples have been utilized to determine whether an individual is intoxicated or not, it is proposed that a variety of concepts incorporate the biological information into a biometric authentication system to identify possible intoxication as one of the information security platforms (Chan, Huff, Barclay, & Copeland, 1997).

As yet, there are no effective information security measures to help prevent the risks of being involved in vehicle crashes caused by driver intoxication. However, this research study aims to develop innovative ISS that detect intoxicated individuals and automatically shut down their vehicles' engines when they attempt to start their vehicles.

Background of the Study

Analyzing existent ISS models, with the goal of minimizing the number of deaths and injuries that result every year from accidents caused by individuals under the influence of alcohol, may lead to a new system for prevention (Choe, 2003). It is not necessary for a major paradigm shift to occur, but new creative theories and methods may accelerate the development of appropriate techniques required for detection and prevention (Kaplan & Norton, 1996). What is needed is an ISS capable of preventing an intoxicated individual from driving and warning the individual of his or her level of intoxication.

Bharadwaj (2000) argued that one can build IT capability by effectively integrating resources to create unique systems. One can build an ISS capable of determining the level of the driver's intoxication when he or she starts a vehicle. Ameri (2004) provided five pillars of information security that deliver practical strategies to secure any organization's resources using terms such as protection, detection, reaction, documentation, and prevention. It is widely accepted that such steps can be used to reduce a company's risk, but it is questionable whether they can serve as the foundation for an ISS that could stop a vehicle engine based on the intoxication level of the driver.

Ye, Newman, and Farley (2005) described different forms of security threats and proposed models and theories to enhance the ability to detect cyber attacks. The proposed models and theories have shown very clearly that "an organization must decide what types of barriers or protection mechanisms are necessary to defend against cyber attacks and where to place such barriers" (Ye et al., 2005, p. 68). They also have shown how system engineering fault modeling and risk assessment theories relate to attack characteristics and developed a system-fault-risk (SFR) framework. Straub and Welke (1998) developed a computer security model (CSM) that offered some strategies for preventing cyber terrorist attacks. The same concepts, with a few modifications, may present a window of opportunity for preventing risks associated with intoxicated drivers.

Given these concepts are driven by due diligence, that would be the best way to reduce operational risks and prevent intoxicated individuals from causing vehicular accidents. However, effective protections to evaluate intoxicated individuals via ISS require network resources and the participation of organized public services to promote public acknowledgement of the critical challenges intoxicated driving presents to the well-being of the society.

SFR could help organizations understand and assess the risks intoxicated individuals present and may assist organizations in formulating decisions about what forms of protection mechanisms are necessary to reduce accidents involving intoxicated drivers. To come to that conclusion, one needs to review the existing literature that addresses the problem. In addition, one needs to consider the three risk phases: pre-risks, risks, and post-risks. This is similar to CSM, which examines deterrent, preventative, and detection techniques (Ye et al., 2005).

Many models and theories exist, but none of them is a magic bullet that can prevent intoxicated individuals from driving. Any proposed models or theories that would enable an organization to determine individuals' risks must offer cause and effect protections throughout the information security network (ISN) and between the segments, and each segment must be understood to minimize security weaknesses (Taylor, 2005).

Statement of the Problem

Given the technology and methods for ISS that exist today, it should be a common purpose for all security controls across the spectrum of information security elements (ISE) to optimize the available resources and knowledge to prevent intoxication related crashes (Backerville, 1994). The National Highway Traffic Safety Administration (2006) reported 16,885 people in the United States died in 2005 in automobile accidents while under the influence of alcohol. This study aims to examine the nature and scope of measures that information security may take to detect and prevent the risks involved in intoxication related accidents with the goal of decreasing the death toll caused by these accidents.

The effects of alcohol consumption are complicated by the fact that body chemistry is shaped by the environment and the individual's state at the time of use. The amount of alcohol in an individual's bloodstream is based on individual biological differences. Another factor that further complicates this issue is the level of an individual's water absorption. Water may dilute alcohol faster in some individuals than in others. All of these elements are concerns in developing a theory or a method to prevent intoxicated individuals from driving.

Developing information security theories that can detect intoxicated individuals may provide opportunities to decrease intoxication related accidents. It also may become a valuable ongoing concept to analyze existing devices, such as LoJack tracking systems and GPS that are used today to unlock vehicles and locate goods, to determine if these devices could be modified or redesigned to prevent individuals from operating motor vehicles while under the influence of alcohol. To develop and implement the required policies and procedures for such a system, one must first have a clear understanding of the standards for evaluating the situation and determining the optimum method of implementation (King, 1978).

Purpose of the Study

The goal of this study was not to develop a new theory. Instead, it was to analyze and evaluate existent ISS mechanisms and techniques to determine the extent that information security could be implemented in preventing intoxicated individuals from driving. The study also sought to provide the basis for developing an integrated ISS for monitoring intoxication, which would prevent the operation of a motor vehicle if the driver were intoxicated. In addition to an alert alarm, the ISS device would indicate whether an individual was in compliance with the ISS protocol for intoxication.

This research study evaluates information system design theories (ISDT) and biometric authentication methods (BAMS) to determine the extent to which ISS can be implemented for preventing intoxicated individuals from driving. It also evaluates the infrastructure of integrated devices of information security theory (IIST) for intoxication monitoring. The proposed structure as shown in Figure 1 is based on Welander's network security design. Welander stated, “A good security design has to offer layers of defense so that when one layer fails another will stand on its own” (2007, p. 40).

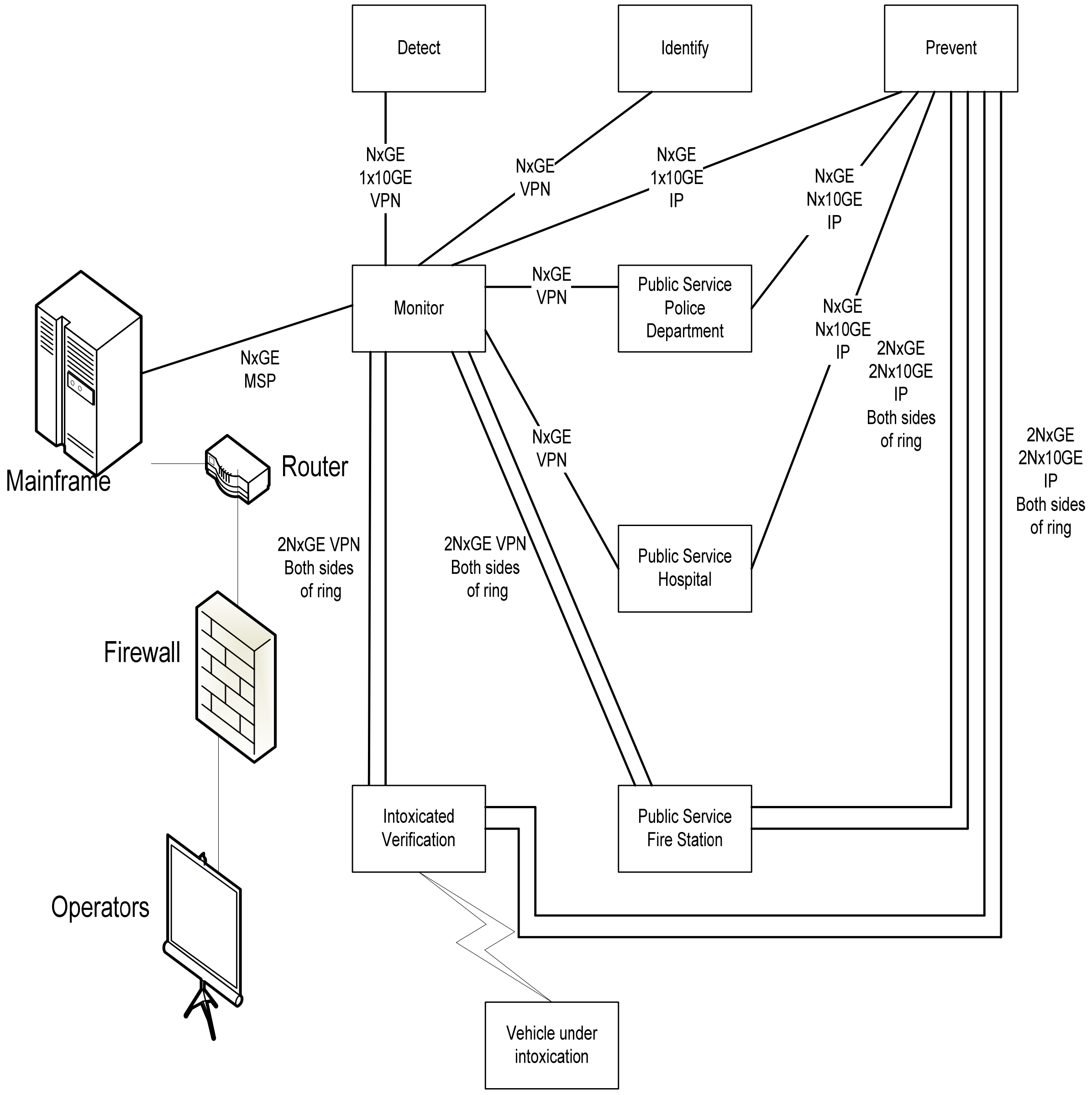


Figure 1. ISS intoxication detection and prevention architecture proposal.

Rationale

ISS is widely applied in all aspects of human life to safeguard confidential data about an individual's life. However, there is little literature regarding its application to prevent intoxicated individuals from driving. The rationale for this research is to further explore the use of information security concepts and theories to examine how these concepts and theories might detect and prevent intoxicated individuals from starting motor vehicles (Feeny & Willcocks, 1998). Researchers have not yet developed reliable detectors that indicate the level of an individual's intoxication to prevent vehicular accidents. According to the World Health Organization (2007), more than 570,000 people die each year because of injuries incurred while intoxicated. The use of information security to determine the level of an individual's intoxication could be a very important step toward reducing intoxication related accidents.

Thompson (2007) suggested that a rational norm that emphasizes core technology value typically starts from environmental influences and further develops into a framework of the descriptive phenomena. Under this condition, one must attempt to take the logical steps needed to obtain every possible object of knowledge to establish a conceptual framework. The framework of this study merges direct knowledge of the natural limits to determine the input and output structure of ISS intoxication monitoring, and it may help in designing a system that addresses contingencies to support the incoming critical information from ISS prevention (Thompson, 2007).

Arbnor and Bjerke (1997) stated that future characteristic influences, by their historical description, provide a clear understanding and consequently support the handling of unexpected changes. In calling on ISS to prevent intoxicated individuals from driving, this research study faces the double hurdle of quality and practical relevance (Pettigrew, Woodman, & Cameron, 2001). There are many challenges to developing the scientific knowledge and policymaking that enable integration of detection, identification, prevention, and monitoring technology while ensuring information security.

Research Questions

The main purpose of this study is to analyze prior information security methods and theories to determine the extent to which information security can detect and prevent individuals who are under the influence of alcohol from driving. This study has used case study design to investigate ISS and address the primary question: To what extent can ISS be utilized to prevent individuals under the influence of alcohol from driving? To address and answer this question the following research subquestions must be addressed to obtain appropriate perspective on the existing ISS analysis.

1. How do ISS obtain the data to detect the intoxication level of individuals while they are starting a motor vehicle?
2. How do ISS make a decision to prevent intoxicated individuals from driving?
3. What are the significant factors in implementing ISS in motor vehicles to prevent intoxicated individuals from driving?

Significance of the Study

According to prior research, individuals who are intoxicated as a result of drinking alcohol experience a loss of the mental faculties needed to operate a motor vehicle. Intoxication can change the driver’s level of skill and cause him or her to injure others. If ISS can be used to identify and prevent intoxicated individuals from operating motor vehicles, it may make a significant contribution to saving human lives.

Preventing intoxication to reduce intoxication related accidents via ISS is another challenging issue. It requires regular updates from monitoring systems as soon as vulnerability is discovered. It is clear that preventive approaches alone are not sufficient to stop an intoxicated individual from driving.

This study examines the definition of information security as well as the methods to determine the prevention of intoxicated driving. Most significantly, this research study is seeking to examine if ISS can be used to recognize an intoxicated individual and formulate a decision as to whether or not to allow a person to drive a motor vehicle (Jones et al., 2003).

The National Survey on Drug Use and Health (Substance Abuse and Mental Health Services Administration, 2007) estimates that 22.3 million people over the age of 12 are classified with substance abuse or dependence disorders, which represents approximately 9% of the population in the United States. A majority of the 22.3 million (69.5%) abused alcohol; 16.5% abused illicit drugs; 14.3% abused both alcohol and drugs.

According to one recent nationwide estimate (Harvard Medical School, 2008), roughly 18% of Americans will have an alcohol or drug use disorder in their lifetimes. Drug and alcohol abuse can result in car accidents and subsequent hospitalizations. There were 108 million recorded emergency room visits in the United States in 2005; almost 1.5 million were associated with drug use or misuse (Harvard Medical School, 2008).

Many of the drug and alcohol related visits to the emergency room involve motor vehicle accidents.

Motor vehicles are the most common form of transportation, and some motor vehicle companies, such as GM and Toyota, are developing fail-safe systems for cars that detect intoxicated drivers and automatically shut down vehicles if sensors pick up signs of excessive alcohol consumption. Again, this study may reveal prevention methods that can reduce intoxication related accidents.

According to the National Highway Traffic Safety Administration (2007), alcohol related motor vehicle crashes injure someone every 2 minutes and kill someone every 31 minutes. Drugs other than alcohol, such as marijuana and cocaine, are involved in about 18% of all motor vehicle driver deaths, but it is worth noting that people generally use these drugs in combination with alcohol. This study understands the harmful effects of alcohol and drugs are not limited to injuries related to motor vehicle accidents. It is understood that long-term use of these substances can lead to serious health consequences, such as alcohol related liver disease, which alone kills nearly 13,000 people each year (Harvard Medical School, 2008). Drugs such as amphetamines and cocaine attack the heart instead of the liver, sometimes causing strokes or heart attacks. Although this research study recognizes other drugs related to intoxication, it focuses on alcohol related intoxication.

There are detector devices to identity vehicle locations, and there are devices for preventing individuals from operating vehicles when ISS identifiers indicate the individuals are intoxicated. There is not enough data to support recommending approaches for information security to reveal intoxication levels before an accident occurs, but the ability of ISS to recognize biological changes when one is under the influence of alcohol may be a key element to preventing intoxicated individuals from driving.

Definition of Terms

ISS collect activities that relate to the protection of information against the risk of loss or damage as cause and effect are shown in Figure 2. The term information security is related to the terms computer security, information assurance, and communication infrastructure and shares the common goal of protecting information from risks. Preventing risks requires analysis of the following issues:

Availability. Ensuring information is available as needed and the system is functioning correctly (Merali & McKiernan, 1993).

Confidentiality. Preventing information from being accessed by unauthorized users (Welander, 2007).

*Detecting threats. R*ecognizing events that can cause deliberate or accidental misuse, loss, or damage. Reducing exposure to security risks requires ongoing assessment of the network security system (Keller, Powell, Horstmann, Predmore, & Crawford, 2005).

Identifying. Pointing out all possible risks before they occur (Scott & Davis, 2007).

Integrity. Ensuring data cannot be altered without authorization (King & Teo, 1999; LeCompte, 1992).

Monitoring. Using controls to protect information and communication channels (Wen, Schwieger, & Gershuny, 2007).

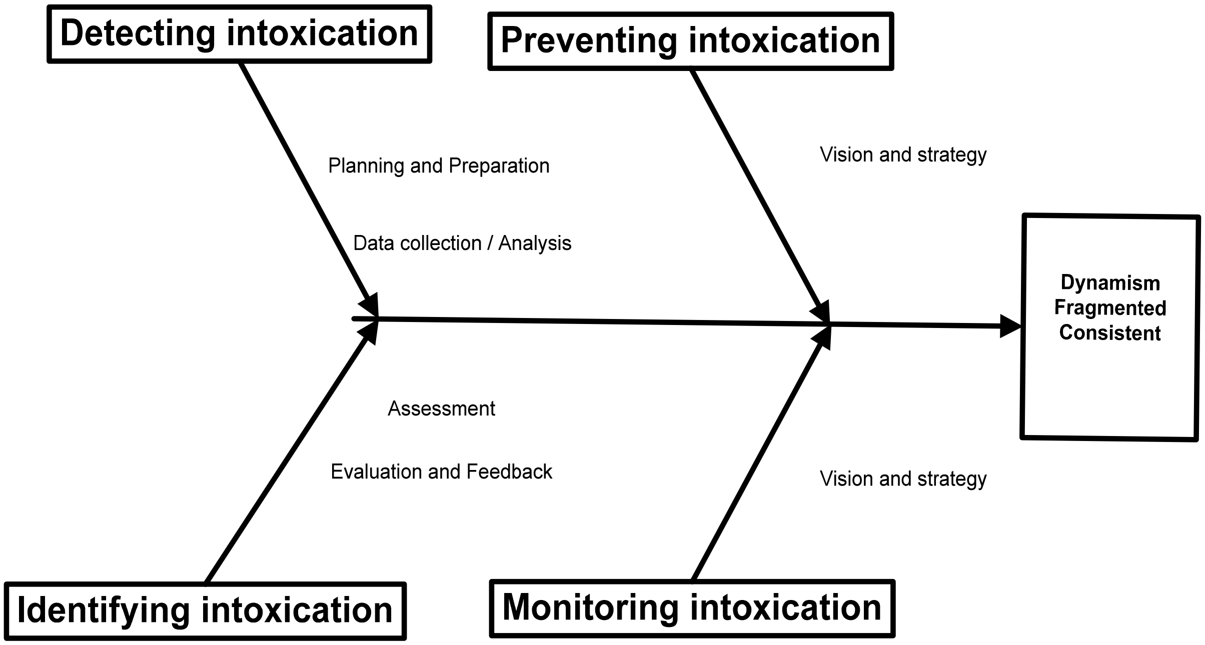


Figure 2. Cause and effect of detection, prevention, identification, and monitoring model.

Assumptions and Limitations

Detecting intoxication to reduce intoxication related accidents via information security is challenging because of the dynamic environment of physiological patterns and psychophysical activities. Trochim (2006) stated that many qualitative researchers operate under different ontological assumptions about the world, and the best way to understand any phenomenon is to view it in its context. On the other hand, Creswell stated, “The logic of mixing is that neither quantitative nor qualitative methods are sufficient in themselves to capture the trends and details of the situation” (2003, p. 179).

The challenge is to focus on examining the issues related to the methodology constructively within the research context.

Denzin and Lincoln (1994) defined qualitative research as multiple methods that focus on interpretation through a naturalistic approach to the subject matter, meaning that qualitative researchers need to study subjects in their natural settings and attempt to make sense from the phenomena interpretations. That is why this research study focuses very heavily on literature that provides the fundamental concepts of information related to the research topic.

Creswell (2003) concluded that experimental research looks at the world through the lenses of the positivists, who tend to hold an ontological view of reality as relatively fixed or stable, independent or outside of the observer, and measurable. Thus, they tend to adopt a quantitative approach. Because of the nature of this research, assumptions of prior researchers on information security theories limited the scope of this study to select one single theory from information security methods (Denzin, 1978). In any case, this researcher acknowledges the benefits of a qualitative approach and the possibility of the discovery of unanticipated phenomenon (Maxwell, 1997).

Malterud (2001) believed qualitative research methods are founded on an understanding of the systematic reflective process for developing knowledge that can be somehow contested and shared, implying transferability beyond the study setting. “The findings from a qualitative study are not thought of as facts that are applicable to the population at large, but rather as descriptions, notions, or theories applicable within a specified setting” (Malterud, 2001, p. 70).

Theoretical/Conceptual Framework

The conceptual framework of this research study expresses the vision and strategy that unites the efforts of ISS to prevent intoxicated individuals from driving. The nature of the vision is based on sound knowledge, theories, and research (Porter, 1996). With no doubt, it is informed by historical and contemporary theory and research. This study seeks to best reflect the collective thinking to achieve the objective of this research topic.

The framework looks to generate data from case theory studies that have been proposed in a general form and to explore different process events in different study environments. One of the goals of this research is to exam the linkages of the variables within the context of ISS that have been successfully implemented to detect and to prevent events prior to their occurrence. Figure 3 provides a focus to guide the research design and development of questions (Huberman & Miles, 1994).

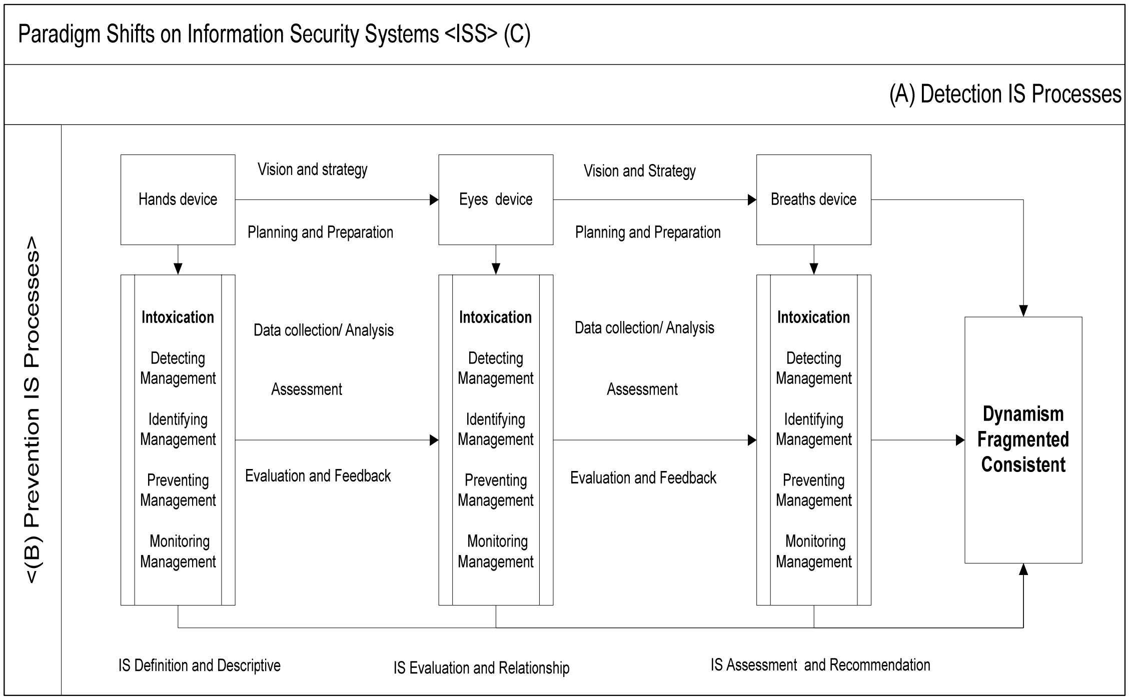


Figure 3. Conceptual framework: ISS method for detecting and preventing intoxicated individuals from driving.

Organization of the Remainder of the Study

Research studies have been analyzed for data findings and identification of the applications studied. Quotations are cited to support each influential concept integrated from the set of interviews for each of the ISS segments. For each article, the ISS concepts are then grouped into categories, and categorical findings are summarized under a consistent context factors system.

This research analyzes 14 research articles on ISS and 7 research studies on intoxication from organizations such as the National Clearinghouse for Alcohol Abuse and Drug Information (2007), National Institute on Alcohol Abuse and Alcoholism (2007), National Institute on Drug Abuse (2006), Substance Abuse and Mental Health Services Administration (2007), National Highway Traffic Safety Administration (2006), and Harvard Medical School on Special Health Report on Alcohol Use and Abuse (2008). The following are the articles analyzed in this research:

1. Ameri (2004) provided five pillars of information security that deliver practical strategies to secure an organization's resources, using terms such as protection, detection, reaction, documentation, and prevention.

2. Barton, Byciuk, Harris, Schumack, and Webster (2005) identified the 10 key sections of ISO 17799 that serve as the foundation for general practices of information security for any company.

3. Bharadwaj (2000) argued that one can build IT capability by effectively integrating resources with other resources to create unique advantages for obtaining intangible resources.

4. Bielski (2007) examined theories to ensure continuity of critical operations and managing risks associated with outsourcing data security.

5. Hoffman, Jenkins, and Blum (2006) developed security trust model related metrics for distributed computer based systems that are useful to face technology changes.

6. Itakura and Tsujii (2005) provided concepts and information for consideration in using biometric methods to address security issues.

7. Oh and Pinsonneault (2007) used conceptual resource centered, contingency based, analytical linear and nonlinear approaches to assess the strategic value of information technology to motivate higher quality process development.

8. Siponen (2006) explored information security standards focusing on the existence of a process rather than the content.

9. Stevens (2008) outlined the Federal Information Security and Data Breach Notification Laws in the *CRS Report* for Congress.

10. Straub and Welke (1998) provided a computer security model (CSM) that illustrates some of the theories used to prevent cyber terrorist attacks. The same concepts, with a few modifications, may provide an opportunity for preventing risks associated with intoxicated driving.

11. Swanson, Bartol, Sabato, and Graffo (2003) provided independent components for results oriented metrics analysis, quantifiable performance metrics, practical security policies, and procedures to support decision

making.

12. Tan, Poslan, and Titkov (2006) presented a semantic approach to harmonizing security models for open services.

13. Wilson (1998) evaluated security metrics using qualitative and quantitative activities to measure the level of information-security awareness competences.

14. Ye, Newman, and Farley (2005) described different forms of security threats and proposed models and theories to enhance detection of cyber attacks.

One of the objectives of this study is to determine the extent to which ISS theories and methods can be used to prevent intoxication related automobile accidents. Since the case study theory process is both iterative and cumulative, the concepts and categories identified early in the research were used in the later analysis.

An analysis of prior case studies, ISS process theories, and the literature on this topic may serve to develop a common operating platform to detect intoxication in any form. Data is to be collected from four ISS segments (detecting, identifying, preventing, and monitoring) in three concepts (detecting intoxication, identifying intoxication, and preventing intoxication related accidents). This research includes semi-structured retrospective interviews with alcohol drinkers and non-alcohol drinkers, as well an overview, as shown in Table 1, of common intoxication detector devices and intoxicating substances.

Table 1.

ISS, Intoxication Devices, and Common Intoxicants

ISS	Intoxication Device	Common Substances Abused

Detector	TruTouch Detector	Alcohol
Identifier	Electrochemical Sensor	Marijuana
Preventer	Breath Analyzers	Cocaine
Monitor	Ignition Interlock	Pain relievers

In this study, the interpretation of the phenomenon focuses on the prior research articles and the data accumulated and analyzed from the interviews with the participants. Losing this focus would diminish the researcher’s interpretation of the data and core meanings of the research topic. This study employs continuous interaction in the research activities using the causal network theoretical model of Miles and Huberman (1994), which attempts to isolate the researcher’s own biases. This approach provides guidelines and processes for data reduction, which represents greater opportunity for developing a verification strategy.

The theoretical perspectives of this research study can be seen in the examination of the four development issues (detecting, identifying, preventing, and monitoring), which are shown in Figure 4. Structural theories, often called stage theories, are based on the belief that later stages are qualitatively different from previous stages. Considering worldviews as different stages results in the development of a dynamic structure (Kuhn, 1996). The conceptual independent variables for this research study are ISS content; the conceptual dependent variables for this research are intoxication under the influence of alcoholism.

The results may change some of the functions of ISS for intoxication prevention in response to the research topic analysis. As Baets (1992) stated, the precise characteristics of the ultimate state are always unclear toward technology development, which may provide opportunities for gaining advantage through superior foresight.

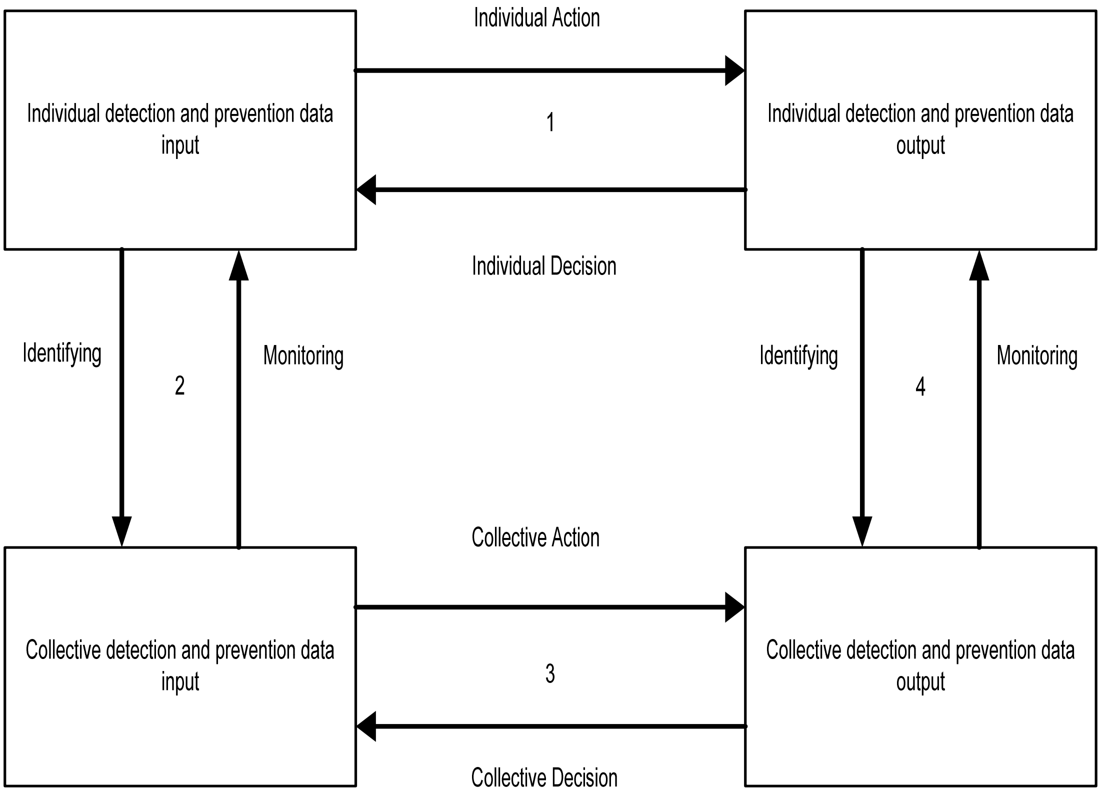

Individual Action
Individual detection and prevention data input
1
Individual detection and prevention data output
Individual Decision
Identifying
2
Monitoring
Identifying
4
Monitoring
Collective Action
Collective detection and prevention data input
3
Collective detection and prevention data output
Collective Decision

Figure 4. Theoretical model of intoxicants data collection.

The study aims to analyze the extent to which ISS can be utilized to prevent individuals from driving while under the influence of alcohol based on their intoxication level. It is important for this research to illustrate the causal network model for data reduction to generate meaning and verify the conclusions of this study. That is why this study uses some of the most common data collection methods: analyzing prior research articles related to ISS and alcoholism behaviors and interviews with alcohol drinkers and non-alcohol drinkers.

The causal network theoretical model seeks alternative explanations in the early stages to help simplify assumptions, to understand the leading causes, and to identify variations in prior research results (Shanley, 1987). Given that the clustering tactic typically relies on aggregation and comparison of "what things are like each other/unlike each other" (Miles & Huberman, 1994, p. 436), it is more beneficial to leave contrasts and comparisons for the summary and conclusion stages of this research.

CHAPTER 2. LITERATURE REVIEW

There is a large amount of literature on ISS that can be evaluated in the effort to develop a dedicated concept or theory that can prevent intoxicated individuals from driving before accidents occurred. This research study relies on literature with a strong foundation on examining the extent to which information security can implement and prevent intoxicated individuals from driving. Barton, Byciuk, Harris, Schumack, and Webster (2005) noted the 10 prime sections from ISO 17799 as the general practice foundation for any organization to protect human beings from accidents related to intoxication in any form.

Using terms, such as security policy, system access control, computer/operation management, system development and upkeep, physical and environmental security, compliance, personnel security, security organization, asset classification and control, and business continuity management, seems to be the best practice to identify threats, but none of these concepts can determine the threat level of intoxication (King & Zmud, 1981). While previous attempts have been made to provide devices and methods for personal identification, intoxication detection, and over medication detection, no one has developed an integrated ISS which includes all three of these functions.

Bielski's (2007) theories are based on the potential impact of situations to ensure continuity of critical operations and are related to managing risks associated with outsourcing of data security. These theories may apply to notifying intoxicated individuals while protecting their privacy. The Gramm-Leach-Bliley Act privacy policies to safeguard the security and confidentiality of information and protect individuals from any anticipated threats (Stevens, 2008). Hong, Chi, Chao, and Tang (2003) stated, "Information is a vital asset and needs to be appropriately protected" (p. 245). One must have the backup resources necessary to respond to disruptions.

Oh and Pinsonneault (2007) used two conceptual resource centered and contingency based approaches and two analytical linear and nonlinear approaches to assess the strategic value of information technology to motivate higher quality process development. The fact that one may have in place a security process or security activity prescribed by the information security standards does not imply the ultimate goal has been attained (Mehta & Hirschheim, 2004). Without process activities that lead toward the goal, there would not be any success in goal achievement (Siponen, 2006). Analyzing quality is always an essential ingredient of a successful strategy, but every party involved must participate (Thompson, 2007). Engaging individuals who drink alcohol in the process of creating an ISS device to prevent intoxicated individuals from driving may be the best source for generating ideas and may lead to operating excellence.

Hoffman, Jenkins, and Blum (2006) developed security trust model related metrics for distributed computer based systems that are useful to face technology changes. They also provided a clear explanation of how there may be protocols or standards for driving in certain areas to prevent collisions, but that these protocols or standards do not make collisions impossible. Prior security models lack a holistic solution, which presents a major obstacle in the development of open systems critical applications. These models help refine common security strategies that maximize effectiveness while minimizing risk factors (Tan et al., 2006).

The value of assets expressed in terms of cost are clear; however, processes for securing assets require critical safeguards, which include the concepts of backup creation and disaster recovery plan testing of continuing operations while the system is impacted (Hong et al., 2003). As the safeguard is intended to protect the assets and availability of the ISS system, the procedures and techniques used to prevent the occurrence of security incidents have to be measured and controlled to respond and to recover from security incidents (Bielski, 2007). It is the responsibility of those individuals who are authorized within the organization to allocate resources and to perform due diligence of risk assessment to make these decisions (Tan et al., 2006).

Unfortunately, an individual's definition of what is right and wrong changes depending on the nature of the situation (Mehta & Hirschheim, 2004). Ensuring that no single individual can compromise the applications of the security system, firewall procedures are used to enforce security policy and to protect the data against unauthorized users (King & Zmud, 1981). In the ISS world, confidentiality requires data to be protected against nonauthorized users, integrity requires data not to be changed without authorization, and availability requires access for authorized users must be assured (Ye et al., 2005).

Individuals who utilize ISS knowledge to compromise network security are traditionally called hackers. Their activities generally cause disruption and loss of ISS data, which could be costly to recovery. That is why the concept of individual responsibility and accountability drive security procedures, such as identifiers, trend of trails, and access protocol/policies (Stevens, 2008). Training is necessary to enforce accountability, to determine what functions an individual is authorized to perform, and to provide the descriptions of one's responsibility.

Security incidents are preventable when individuals implement activities that provide awareness of the asset values and the nature of the threats and vulnerabilities associated with selves-compliance and selves-objective to protect the assets (Wilson, 1998). Therefore, compliance is necessary and comes with the laws that have been enacted to regulate and establish policy structure to prevent privacy violations and potential risk of lawsuits (Stevens, 2008).

Given the rate of technology changes, the need to understand the characteristics of dynamic technologies and regulations is one approach to minimizing threats and addressing vulnerabilities of an information security network (Tan et al., 2006). Threats and vulnerabilities are always present; therefore, quality control should always be present in a security network environment to ensure consistency and integrity of the ISS (Oh & Pinsonneault, 2007). It is understandable that this research analyzed prior methods of ISS to determine the extent to which its concepts may prevent individuals under influence of alcohol from driving. That is why the characteristics of change on technologies have to be understood as a risk management process (Hoffman et al., 2006). In this way one may provide unique identifiers to eliminate vulnerabilities to potential threats while implementing good quality control to prevent incidents, not just for protecting assets, but for protecting lives as well (Tan et al., 2006).

Wilson (1998) evaluated security metrics using qualitative and quantitative activities to measure the level of information security awareness competences. Wilson's model concluded any concept of metrics should have an affect on its performance. Swanson et al. (2003) provided independent components for results oriented metrics analysis, quantifiable performance metrics, practical security policies, and procedures that are supportive for decision making, which does not mean more criteria cannot be added. These metrics may help in understanding the extent to which information security can be implemented for preventing intoxicated individuals from driving. However, they cannot reveal the level of an individual's intoxication to prevent the individual from driving.

Itakura and Tsujii (2005) conducted a study using a biometric system for solving security problems. Their study was based on a multifactor biometric authentication methods system, which included fingerprints, iris, face, voiceprint, signature, and DNA. Biometric characteristics are divided into two categories that deal with physiological and behavioral differences. The determination of whether an individual is intoxicated may use biometric analysis of skin pores, iris, and voiceprint because of the physiological and behavioral aspects of speech production. Indeed, the complexity of this method might be so complex that the devices and the details of how these processes work to prevent intoxicated individuals from driving may be challenging to understand. Currently information technology security has not limited its requirements to accommodate future technology and risk management decisions. The following is a list of current ISS requirements.

- Protect assets (hardware, applications, and data).
- Safeguard assets (backup media).
- Controls to detect, prevent, and recover from incidents.
- Manage risk through authorized system operations.
- Protocols that control and evaluate individuals' behavior toward ethicality.
- Separation of duties through firewalls to minimize potential incidents and threats.

- Privacy through confidentiality, integrity, and availability.
- Eliminate intruder threats to any system.
- Responsibility and accountability for one's own actions.
- Incident prevention through compliance and awareness.
- Establish control and security objectives based on laws and regulations.
- Training related to responsibilities through model of frameworks.
- Limit access to data and set objectives based on a need to know basis.
- Asset protection responsibility and accountability.
- Establish policies and procedures for tasks accomplishment.
- Ensure the integrity of the processes through quality control and quality assurance.
- Balance potential risk impact safeguards through risk management and cost analysis.
- Evaluate return on investment against security safeguards.
- Prepare for unexpected threats (they occur when least expected).
- Facilitate access control through unique identifiers.
- Detect vulnerabilities to determine weaknesses through which threats may impact the system.
- Primary issues with security system based in fraud and abuses.
- Evaluate critical factors to maintain effective security environment actions or non-actions.
- Establish security layers to minimize any type of incident or threat for the good of the people.

Summary

A review of the literature indicates that identifying the unique pattern of an individual's biological elements is the best approach for determining whether an individual is intoxicated and should not be allowed to operate a motor vehicle. ISS monitoring systems have the potential to detect an individual's intoxication level based on biological factors and then to communicate this information via ISS transmitters as shown in Table 2. Despite the strengths of biometric systems, they also have their shortcomings in regard to false acceptance rate (FAR) and false rejection rate (FRR) (Itakura & Tsujii, 2005). For example, an individual's eyes may indicate the individual is intoxicated, but the tear film might send the wrong information based on the surface of the eyes. In addition, certain physical and performance characteristics could indicate different states of intoxication when used in different situations and in different environments (Barton et al., 2005).

The literature reviewed for this research indicates that biometrics is the system that relies most heavily on physiological and characteristic behaviors to obtain intoxication information. The physiological concepts of biometric measurements are based on the biological characteristics of an individual, which include fingerprint verification, iris verification, hand patterns, odor detection, DNA pattern analysis, and sweat pore analysis. These biometric elements may add value to the detection of intoxicated individuals, but its method for retrieving data relies on the majority coding technique, which uses the results of the multiple applications of the biometric system for the initial detection and identification of a individual (Biometric, 2004).

Table 2.

Features of ISS Biological Information (Itakura & Tsujii, 2005)

Biological Information	Detecting	Identifying Matching Accuracy FAR FRR	Data Size and Template	Feature and Issues	Preventing Risk	Monitoring Risk
Hand pores	Sensors	Different algorithms	Based on features and relational data	Intoxication verification due to dried skin or sweat pores, high precision	Risk level of intoxication	Managing risk to save
Iris	Camera	Difference in Iris patterns	Based on features and relational data	Intoxication verification due to tear eyes captures, stress and high precision	Risk level of intoxication	Managing risk to save

Voiceprint	Microphone	Difference in vocal sounds	Based on features and relational data	Voice change in puberty or due to intoxicate/air odors, stress	Risk level of intoxication	Managing risk to save
DNA	DNA Analyzer	Differences in short tandem repeats	Based on features and relational data	High precision, uniqueness, high stability with time, privacy concerns	Risk level of intoxication	Managing risk to save

CHAPTER 3. METHODOLOGY

Traditionally, case study research is an approach used to study subjects in social science and management. Also, qualitative case studies have been used as a teaching method for professional development. In recent years, case studies have received increased attention as a valid approach because of their holistic emphasis. A qualitative case study seeks to obtain in-depth understanding of any given situation's meaning (Merriam, 1998) and needs to be based on a diverse array of data collection materials (Yin, 2003).

As Stake (1995) stated, "A case study might be either intrinsic or instrumental, but its defining feature is that the researcher examines several cases" (p. 116). Case studies can be extremely varied and the approaches taken to the analysis of the data can be equally diverse. "Every book, every magazine article, represents at least one person who is equivalent to the anthropologist's informant's or the sociologist's interviewee" (Merriam, 1998, p. 88). For a qualitative case study to obtain an in-depth understanding of a topic, it needs to be based on a diverse array of data collection materials (Yin, 2003). One may say case studies can be extremely varied in the approaches taken to the analysis of the data that are generated.

The selected participants in this study have experience in the subject matter related to the research topic, which helped to develop the theory that explained the extent to which information security can be used to prevent intoxicated individuals from driving or provide frameworks for further research (Straus & Corbin, 1990). According to Miles and Huberman (1994), "A case study could be approached as an exercise in the generation of grounded theory; or it could be thoroughly ethnographic, with the major concern being to gain an understanding of the culture of whatever constitutes the case" (p. 156). A case study can utilize knowledge derived from prior cases as well, and it really depends on what the researcher is seeking to discovery (Merriam, 1998). As mentioned by Merriam (1998), "There is no standard format for reporting case study research" (p. 118). In any event, a researcher who uses a case study method, still needs to present a holistic description and analysis of any given phenomenon.

Lincoln and Guba (1985) also described the need for explications of the problem, a thorough description of the concept setting, a description of the transaction processes observed in the context, and the outcomes of the inquiry. One might state, a case study can be written in several different ways given the flexibility of its design and its analysis processes. The problem is that with this type of flexible structure, it may be difficult to establish whether important data have been omitted. This study has chosen to utilize case study analysis to obtain more detailed procedures to help develop categories of information security and to address a discursive set of theoretical propositions (Stauss & Corbin, 1990).

This research uses open code processes to initialize the set of categories and to centralize phenomenon of interest: detection product network, identification process network, and prevention process management for each systems concept. The objective behind coding in this research is to identify the patterns or themes of the data prior to fieldwork and to link the relationships of four ISS perspectives: detecting, identifying, preventing, and monitoring (Miles & Huberman, 1994).

Research Design

Case study is a qualitative research design in which the inquirer generates a general explanation of a process, action, or interaction shaped by the views of a single or large number of participants (Creswell, 2007). This research utilizes prior research on ISS to develop the qualitative descriptive methods for the case study analysis and interviews. It uses flexible data collection techniques, such as semistructured interviews, to help in determining or identifying opportunities for data collection techniques based on what the interviewees view as important concepts in the phenomenon under study. The semistructured nature of the interviews also helps the researcher to pursue additional information from the interviewees to explore the ISS concepts interviewees consider to be the most important and why.

Strauss and Corbin (1990) have provided the following guidelines for data collection:

1. Gather data from multiple points of view to improve objectivity in the data collection process.

2. Check conclusions with respondents to ensure accuracy of the conclusions drawn from the data.

3. Guide questions to provide an open structure for the data collection that allows the participants to suggest new directions for the study.

4. Use theoretical sampling in areas where little is known to improve the theoretical return from the research.

Earlier studies and literature on the topic have been used to suggest areas for theoretical sampling and to guide the researcher into theoretically interesting areas (Creswell, 2007). Miles and Huberman (1994) stated,

> As a study proceeds, there is greater need to formalize and systematize the researcher's thinking into a coherent set of explanations. One way to do this is to generate propositions, or connected sets of statements, reflecting the findings and conclusions of the study (p. 201).

At present, there are no research studies that can provide a strong theoretical base on which to build the current research study on preventing intoxication related accidents via ISS. Instead, the existent studies identified strategies and concepts that are likely to influence decisions about the use of diverse approaches.

Sample

This research study has gathered the perceptions of participants as to the strengths of ISS to prevent intoxicated individuals from causing vehicular accidents (Creswell, 2007; Miles & Huberman, 1994). The research has been supported through an examination of related research. To obtain various perspectives and validate the information, two distinct research studies have been conducted.

Twenty participants have been voluntarily selected through a local Alcoholics Anonymous (AA) intergroup meeting to participate in the interview component of this research study. There are no fees or dues involved in AA intergroup membership; it is supported through contributions from AA groups, and visitors are always welcome. As Creswell (2007) stated, "For a phenomenological study, the process of collecting information involves primarily in-depth interviews with as many as 10 individuals" (p. 131). This research involves twice Creswell's recommended number of individuals. The researcher conducted interviews with 10 male and 10 female participants between the ages of 30 and 50 who reside in two counties in South Florida and have experience with intoxication related accidents, but have not been convicted of DUI. The interviews were conducted in order to find the important points that describe the meaning of the phenomenon, which might be relevant and consistent with the research study regardless of gender differences and experiences (Yin, 2003).

Participants have been invited to participate in this research during an intergroup AA meeting. They have been presented with a letter describing the nature and purpose of the research study (Appendix A), a preliminary questionnaire (Appendix B), a consent form for participation (Appendix C), and a self-addressed stamped envelope to return the completed preliminary questionnaire and consent form to the researcher.

The preliminary questionnaire enabled the researcher to identify and eliminate participants from the study who have been convicted of DUI. The preliminary questionnaire also provides the researcher with the telephone or email contact information for the participant, the age and sex of the participant, and whether they have experience with intoxication related accidents. Once the researcher acquired an adequate pool of participants and received the informed consent forms, the researcher contacted the participants via telephone or email to schedule the interviews. Two mock interviews were conducted with colleagues to field test the questions (Appendix D) for face validity, to determine the timing for the interviews, and to test the adequacy of data recording equipment.

Interviews with study participants were conducted at a public library in close proximity to the participants' homes or work sites. Interviews were scheduled with the intent of giving flexibility and convenience to the participants. Interviews were audiotaped and the responses were transcribed and condensed onto an Excel spreadsheet to analyze consistencies, common themes, and variations in responses.

The purpose and goal of recruiting participants from the AA intergroup meeting was to obtain input on some of the most important aspects of planning an ISS to prevent intoxicated individuals from driving. Participants were selected based on their age, sex, and experience with intoxication related accidents. The interview survey was retrospective and served to gather information from the participants' past experiences with intoxication related automobile accidents. As participants answered questions independently from each other, the data developed new concepts that could actually be utilized in this research study or implemented in future research studies.

It was essential for the participants' viewpoints to be heard in this study in order to measure the priorities and views of the public and to aid in discovering techniques to prevent intoxication related accidents via ISS. Research on ISS and its application for driving while under the influence of alcohol face the double hurdle of quality and practical relevance (Pettigrew et al., 2001). Pattern recognition achieved by combining special signal processing methods with statistical decision theory (Itakura & Tsujii, 2005) led to a statistical test of independence based on similarity of metrics computed from codes of ISS data formats (skin, eyes, breath, air, sweat) to measure blood alcohol concentration (BAC). The United States legally mandates intoxication at a BAC level of .05-.08+ (Harvard Medical School, 2008). This measure is used to confirm or disconfirm intoxication of an individual (Harvard Medical School, 2008). It is also used to generate an objective confidence level for ISS prevention decisions.

With that in mind, the analysis and coding have been conducted using prior research articles related to the topic along with the data collected from the participant interviews. Obtaining various perspectives and validating the information requires two distinct methodologies: interviews with 20 participants and analysis of 14 previous research studies related to ISS and intoxication factors. With this type of focus, constructive ideas and processes might be generated on how ISS can be implemented to prevent an individual who is intoxicated from driving. As qualitative studies are about words and their relationships, the challenge here is to synthesize the meaning of data from the large volume of information on ISS garnered from articles on the topic and documentation provided by the device manufacturers.

Setting

The data analysis plan uses Creswell's (2007) protocol and Moustakas' (1994) five phases. The study has ensured identification of pre-existing biases, pre-judgments, and assumptions about the phenomenon challenges, described the phenomenon, and placed them in context (Tesch, 1991). The study focuses on collecting data from literature and interviews, coding the processes, and transcribing them into a document. The setting also includes an initial framework with the coding process and document notes, the coding start list (Table 3), and the list of ISS in Figure 5 data collection management systems (Cook & Campbell, 1979).

Literature shows that there are strengths and weaknesses in the use of various interview styles. Open-ended, focused, and normal question interviews are generally used as a technique to elicit facts from the interviewees. With open-ended interviews, one will elicit facts as well as opinions from the interviewees. The focused interview is a short version of the open-ended interview, but it requires the interviewer to stay focused on the questions developed from the protocol in the case study. Formal interviews are by nature surveys and use both the sampling procedures and a survey for data collection.

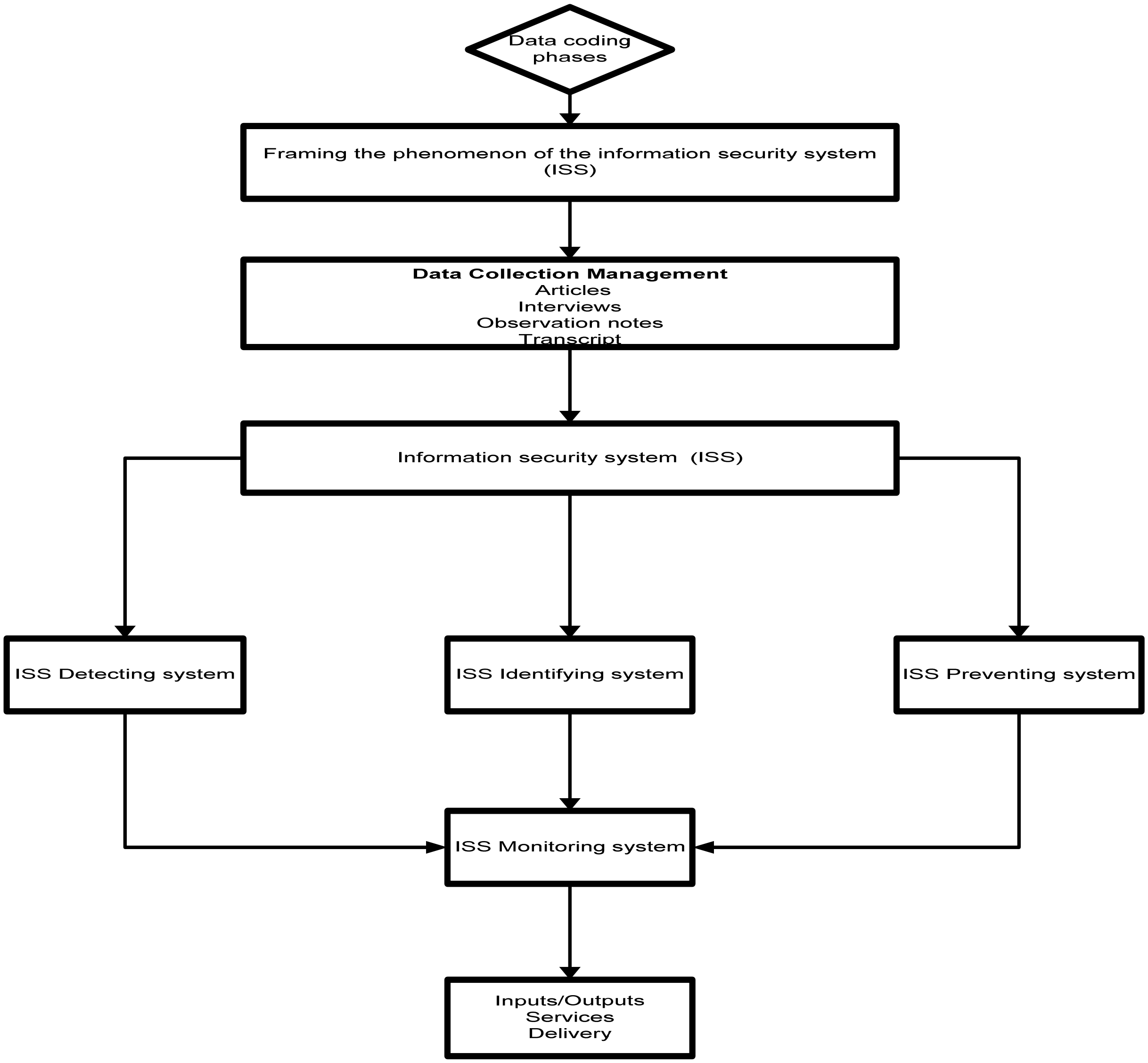


Figure 5. Data collection management model.

This research addresses the factors that influence the selection of ISS strategies for support, synthesis, and replacement of ISS application systems in detection hardware. According to Miles and Huberman (1994), one method of creating codes often preferred is to create a start list through prior provisional fieldwork, which comes from the conceptual framework, research questions, hypotheses, problem areas, and key variables that the researcher brings to the study. Table 3 illustrates the coding start list.

Table 3.

Coding Start List

ISS Code	Preventer Process	Detector Process	Identifier Process	Monitor Process
ISSD	Detecting initiation intoxication	Vehicle/positioning	Individuals/ intoxicated values	Services/results evaluation
ISSI	Identifying intoxication input via detector	Individuals/ intoxicated values	Vehicle/positioning	Monitoring intoxicated vehicle
ISSP	Preventing ISS operation models	Vehicle/positioning	Individuals/intoxicated values	Identify intoxicated vehicle
ISSM	Monitoring new information security input to save mode	Monitor intoxicated vehicle	Services/results evaluation	Vehicle/positioning

The basic principle behind the matrix illustrated in Table 4 is explanatory, rather than purely descriptive (Miles & Huberman, 1994). The descriptive data focuses on variables in which data have been collected via literature and interviews and seeks to identify patterns that require further study before drawing conclusions.

Table 4.

Data Conceptual Sources

Cite	Research Method	Purpose	ISS Detection/Prevention	Influential Context Factors	Summary Findings
Creswell (2007); Cook and Campbell (1979); Lincoln and Guba (1985); Merriam (1998); Miles and Huberman (1994)	Conceptual	Identifying theory for which ISS can prevent intoxicated individuals from driving. Wolcott (1992) talks about "theory first or theory after approach.	Diverse approach. Assuming detecting intoxicated approach. Developing a model via information security strategies.	The concepts of information security on biometric method prevention techniques (Itakura & Tsujii, 2005). Information security threats as proposed models/theories that enhance ability to detect attack (Ye et al., 2005).	Set of propositions refer to integrating ISS detector networks and expanding ISS prevention services.
Cook and Campbell (1979); Creswell (2007); Lincoln and Guba	Multiple descriptive case studies.	Examine the combining variations of ISS products and applications.	Integrating and differentiating (Linder, 1989). The 10 prime sections from ISO 17799 as general practice foundation of ISS (Barton et al., 2005).	Information security standards focus on the existence of process (Siponen,	Description of ISS lessons learned during intoxication monitoring.

(1985); Merriam (1998); Miles and Huberman (1994).				2006). Semantic approach to information security models for open services (Tan et al., 2006).	The practical information security policies and procedures to support decision making (Swanson et al., 2003).
Creswell (2007); Miles and Huberman (1994).	Interviews with alcohol drinkers/non-alcohol drinkers.	Is there a reduction of the complex operating environment as a result of the activities?	The measurement level of information security awareness competences (Wilson, 1998). Information technology integrating resources with other resources to create unique intangible resources (Bharadwaj, 2000)	The five pillars of information security that deliver practical strategies to secure resources (Ameri, 2004). The best source to create ideas (Thompson, 2007).	Supporting platform detection ISS based architecture. Applications and operational prevention relationship between monitoring multiple activities.
Cook and Campbell (1979); Creswell (2007); Miles and Huberman (1994); Lincoln and Guba (1985); Merriam (1998).	Interviews with alcohol drinkers/non-alcohol drinkers.	Streamlining goods and improving customer services (Arbnor & Bjerke, 1997).	Policies and individuals values. Information security on Breach Notification Law (Stevens, 2008). Approaches to assessing the strategic value of information technology (Oh & Pinsonneault, 2007).	Theories based on potential impact to ensure continuity of critical operations (Bielski, 2007).	Consistent ISS detecting systems and ISS preventing processes (services delivery). Descriptive variables of interest.

The primary methodologies utilized in this research include qualitative descriptive methodologies, case study analysis, and interviews because qualitative research is conducted in natural settings where human behavior and events occur (Creswell, 2007). Using secondary sources for this topic and developing a qualitative data display for describing the phenomenon being studied is part of the conceptual framework, which was determined through the case study process for explaining the phenomenon of this research.

The conceptual linkages between the concept process categories and the category factor strategies capture the suppositions present at the end of each ISS concept analysis. This study provides a theory or steps to determine how ISS can simplify the input of data regarding driver intoxication and can be of use in the preventing intoxicated drivers from operating motor vehicles or in developing a new paradigm based on multiple ISS activities. An integrated information security system for identifying intoxicated individuals in vehicles would have to include devices to monitor intoxication levels and alert the individuals if they exceeded the pre-determined intoxication level. There should also be devices for preventing individuals from operating the vehicle when devices indicate an individual is intoxicated. Currently, ignition interlock systems use breath alcohol detectors to sample the individual's breath alcohol concentration prior to starting vehicles (Couper & Logan, 2004). Whenever, the detectors sense BAC between .05 to .08% grams, the ignition interlock acts as a switch to prevent the motor vehicle from starting.

Instrumentation/Measures

Matrices have been used for data reduction and identification of the dynamics of what questions to be asked and how the questions should be presented. Table 5 is an explanatory matrix which represents processes in the four areas of ISS that can potentially detect and prevent intoxicated individuals from driving.

Table 5.

Explanatory Matrix

Symbolic of ISS Objective Analysis	People and ISS Organizations	Intoxication Detectors	Intoxication Identifier Locations	Intoxication Prevention Methods	Intoxication Monitoring Support
ISS detection definition	Document ISS steps. Identify required data. Establish ISS rule. Pinpoint vehicle areas in question.	Document ISS steps. Identify required data. Establish ISS rule. Pinpoint vehicle areas in question.	Document ISS steps. Identify required data. Establish ISS rule. Pinpoint vehicle areas in question.	ISS input activities management system	The cycle of ISS monitoring input/output workflow systems
ISS identify development	Develop executable ISS design interface. Develop enforcement mechanisms for prevention.	Develop executable ISS design interface. Develop enforcement mechanisms for prevention.	Develop executable ISS design interface. Develop enforcement mechanisms for prevention.	ISS embedded into ISS platform with look back to drive prevention system development.	Logical design for detector products and prevent ISS network deliveries.
ISS prevention executions	Status monitoring activities. ISS monitoring, optimization and evaluation.	Status monitoring activities. ISS monitoring, optimizatio n and evaluation.	Status monitoring activities. ISS monitoring, optimization and evaluation.	Real-time status information security system input.	Streamlined operations to better serve dynamic input and output.

The integration of ISS is to be the common denominator for running the operations network to detect intoxication and prevent intoxicated individuals from driving. This research does not seek to establish a recommendation for standardizing particular system types; rather, it is seeking a basis for categorizing system types for comparison of multiple ISS activities: ISS intoxication detection, ISS intoxication identification, ISS intoxication prevention, and ISS intoxication monitoring (Kantrow, 1980).

Data Collection

The case study method focused on collecting data through the use of 14 research articles, interviews with 20 participants, and product documentation. Merriam (1988) states a case study arrives at a comprehensive understanding within general theoretical statements in social structure and process. Data collection consisted of a semistructured retrospective review of prior research studies, journal articles, product documentation, and interviews with individuals who acknowledged some involvement with intoxication and the operation of motor vehicles.

This research study utilized interviews with individuals who had experiences with alcoholic beverages, which helped to improve the understanding of some of the data collected from earlier research and reports. However, the study uses factor analyses to develop new theories of ISS processes.

Data Analysis

The data analysis and data collection relied on predetermined procedures based on the content of the prior research articles on ISS. The conclusions involved analyzing the 14 articles, interviewing 20 participants, recording the interviews, and reviewing the observation field notes, which included validating and checking for biases of the interviewers and implementing coding for interview data (Creswell, 2007). The case matrix was used to support the coding and transcription of the qualitative interviews. A conceptually oriented display integrates the data and an expanded version of cross-case analysis integrates the findings (Miles & Huberman, 1994).

Validity and Reliability

One of the focuses of this study is to improve objectivity and reduce bias, which brings value and clarification to research on this topic (Arbnor & Bjerke, 1997). As stated by Miles and Huberman (1994), validity is a key issue in determining the legitimacy of any qualitative research study. Miles and Huberman suggest that there are five dimensions of validity in qualitative research that should be used in shaping the design of a qualitative research study. Descriptive validity in this study is concerned with the specific research articles on ISS and reports on intoxication events from well known organizations (Miles & Huberman, 1994).

With descriptive validity, the data analysis is supported by facts rather than speculations and biases. Accomplishing this objective required that the interviews with the participants be documented and audiotaped, as well as coded and clustered for auditing and data validation. “The credibility criteria involve establishing that the results of qualitative research are credible or believable from the perspective of the participant in the research" (Trochim, 2006, p. 1). One of the roles of the conceptual framework in this research is to support the theoretical constructs from interaction of the different components, which is validating the unbiased interpretation of the data.

Ethical Considerations

"Regardless of the approach to qualitative inquiry, a qualitative researcher faces many ethical issues that surface during data collection in the field and in analysis and dissemination of qualitative reports" (Creswell, 2007, p. 141). As this study focuses on case study methodology for data collection, its inquiry relies primarily on prior literature and interviews. That is why one of the research goals is to ensure none of the participants experience harm or adverse consequences from the study activities (Cooper & Schindler, 2006). Seeking to analyze ISS to reveal theories or concepts to prevent individuals under the influence of alcohol from driving can be very challenging, but also very important. This topic is dealing with critical activities and must secure the permission of participants before the interviewing process. As the 20 participants have been recruited from an AA intergroup meeting, they have been considered a vulnerable population. Therefore, this research study applies the concept of subjects' vulnerability under the regulations of the Department of Health and Human Services, Food and Drug Administration, and Health Insurance Portability and Accountability Act, as well as the guidelines of the International Conference of Harmonization and Protected Health Information, which delineates the different levels of vulnerability the IRB considers (CITI, 2009). Given that any risks to subjects are always in relation to anticipated benefits, it is important for one to acknowledge what may or may not be expected in evaluating risks and benefits in which one's research will be conducted.

This research has been applying knowledge gained under the Collaborative Institutional Training Initiative modules Research with Protected Populations-Vulnerable Subjects, Group Harm: Research with Culturally or Medically Vulnerable Groups, and HIPAA and Human Subjects Research (CITI, 2009). These modules provide adequate provision to maintain safety in this research study. Their concepts added to the basic protocol which the IRB phase required and also provided strategies to reduce risks and offer additional safeguards while collecting data for this research.

The data that have been collected from participants need to be highly monitored to control which part of the information may be released to the public. It has been suggested that "researchers with a utilitarian view address the recruitment of respondents via informed consent" (Miles & Huberman, 1994, p. 289).

The researcher informed the selected participants that there would not be any reward for participating in this research study, other than acknowledging that this study is seeking to discover unanticipated phenomenon that may save lives. Participants were fully aware of the benefits and risks of the study activities. This research utilizes the Academy of Management's ethical code that preserves and protects the privacy, dignity, and freedom of participants (IRB). Maintaining confidentiality, such as consent forms, initial contact information, privacy of participants, and anonymity of data, requires only the researcher in this study to have access to the information collected. Securing the data requires the following: backup data from computer to disk, paper data are to be stored in secure safe, and any additional remaining paper data that are not needed are to be shredded.

CHAPTER 4. RESULTS

The primary purpose of the study was to analyze the extent to which ISS can be utilized to prevent individuals under influence of alcohol from driving. Since the case study theory process is both iterative and cumulative, the concepts and categories identified in Chapter 3 have been used to answer the main research question and the sub-questions in Chapter 4. Several common themes were identified through the analysis of the 14 articles and some similarity suggestions from the 20 individuals who were interviewed for this study.

MQ-To what extent can ISS be utilized to prevent individuals under the influence of alcohol from driving?

SQ1-How do ISS obtain the data to detect the intoxication level of an individual when the person is starting a motor vehicle?

SQ2-How do ISS make a decision to prevent an intoxicated individual from driving?

SQ3- What are the significant factors in implementing ISS in motor vehicles to prevent intoxicated individuals from driving?

Analysis

The research conducted through the articles and the individual interviews brought to light the innovative theories and methods that are currently being used in ISS and brought attention to what needs must be addressed for better understanding of the extent to which ISS could prevent individuals who are under the influence of alcohol from driving (Miles & Huberman, 1994). The articles each shared some type of similarity regarding concepts that related to their theories or methods. The analysis gathered from these 14 articles (ART) extrapolated where ISS currently are and provided insight for what may work best in preventing individuals intoxicated through excessive alcohol consumption from driving (Creswell, 2007).

The interviews with the 20 individuals were conducted to completely isolate the participants from one another, and the data collected from the participants pertained to what was going on with intoxicants. These data findings consolidated into commonalities on the four main themes of ISS. The four main themes as shown in Figure 5 and Table 6 emerged as ISS detecting system, ISS identifying system, ISS preventing system, and ISS monitoring system.

Table 6.

Articles Analysis ISS relevant items require and findings

ISS Detectors require the	ISS Identifiers require to	ISS Preventers require to	ISS Monitors require to
Technical devices at different stages of the ISS intrusion detection based on definition of a BAC measure.	Examine/identify all of the ISS connection points that address information defensive BAC countermeasure	Implement protection measure state to achieve greater ISS success to prevent accidents related to BAC measurement	Enact and monitor continuing protection within the evolving threats, vulnerabilities, and changes.

Symbolic Articles ISS analysis	ISSD findings from articles	ISSI findings from articles	ISSP findings from articles	ISSM findings from articles
ART1	Incident response	Identify intruder location and vulnerabilities	Strategy awareness schemes	Real time alerting/reporting
ART2	Configuration management	Practical techniques to identify threats	Implementation and Compliance	Self-assessment to cover all activities
ART3	Continuity of operations	Integrating resources	Maintain security objectives	Automated reports
ART4	Access control	Managing risk and securing data	Direct and indirect moves of the target objectives	Synthesis tracking issues and concerns
ART5	Computer-based systems	Develop security trust model	Measurements prevented by security evaluation	Generate the characteristics of the issues
ART6	Biometric cryptosystem	Authentication	Approach to aggregate measurement	Current vulnerabilities
ART7	Resources strategy	Performance and values	Integrated into most effective framework	Mapping metrics
ART8	Processes improvement	Best security practices	Determine the extent of which practices provide values	Identify gas between practices
ART9	Detect an	Control fraud	Resist possible	Assisting with

	attack	and confidentiality	attacks	networks penetrability analysis
ART10	Retention policies	Cyber attacks	Modifications and Upgrades	Share communicating results
ART11	Data recovery	Metrics analysis	Insuring against cyber threats	Monitoring development activities
ART12	Computer network attack	Policy based and access control	Network protocol and infrastructures	Applications competency
ART13	Determination of adequacy	Evaluate metric	Mandate Policies and compliance	Ongoing assessment
ART14	Security mechanism	Attack characteristic	Security breach prevention	Evaluate information

ART1

In the case of the article “The Five Pillars of Information Security,” risk management practices are based on implementing theories that promote protection, detection, reaction, and documentation to precisely know what needs to be protected (Ameri, 2004). However, it is required to have an existing system in place to identify the selected objects that need to be protected before considering the implementation of any methods to prevent a critical issue. In this ISS study, the detection system would have to use an identity intrusion protocol relative to static network elements and dynamic application environments. The prevention system would need to test and readjust as needed to prevent an event from happening based on the selected assets that need to be protected. The five pillars alone cannot not reveal any defect characteristics to stop a motor vehicle from moving, but its theories added a significant input into ISS for planning to identify potential threats in an ISS environment.

The five pillars methods can also be used to establish goals and measure how well ISS achieves the goals of preventing an individual under influence of alcohol from driving. The protection pillar is used to minimize information security risk associated with the actual insecurity itself. Detection is used to determine how strong protective measures are for both internal and external breaches. Reaction deals with the action that is actually taken to address breaches that have occurred. Documentation establishes the trends of vulnerability and could identify the past breaches to prevent the same breaches from happening in the future. Prevention deals with the concept of protecting against risk by learning from past events and applying the knowledge gained to avoid the same problems in the future.

ART2

Barton et al. (2005) identify the 10 key sections of ISO 17799 that serve as the foundation for general practices of information security for any company. The 10 key sections (security policy, system access control, computer/operation management, system development and upkeep, physical and environment security, compliance, personnel security, security organization, asset classification and control, and business continuity management) reveal practical techniques to identify threats. However, the theory of this article cannot determine the threat of intoxication level to prevent an individual from driving.

Nevertheless, these applications provide advantages to the core of ISS and may enable ISS organizations to enhance process efficiencies, workflow management, and communications between its operators and drivers who are under influence of alcohol. The need to develop better methods to intercept behavior via ISS is limited to the characteristics of the technical concepts to support intoxication data in this article. However, its technical models enable prediction of threats and detection of vulnerabilities for overall risk management processes in organizations.

ART3

Bharadwaj (2000) argues that one could build information technology capability by effectively integrating resources with other resources to create unique advantages for obtaining tangible and intangible resources. The analysis in this article shows a control system could come from numerous sources, but using these concepts for controlling individuals under influence of alcohol would be very challenging. Furthermore, it does not provide a protective system that is useful via ISS to predict threats, equipment failures, or natural disasters.

However, the author makes the case for converging services and technologies and the concern regarding incompatibility when integrating new products with legacy products. Integration cannot be asserted to have security functionality without reviewing historical data trends and correlations of vulnerabilities. Bharadwaj's (2000) models identify six dimensions underlying IT capability to share resources in which data and applications can be accessible through communication networks. Within its dimensions, there are IT business partnerships, IT external outsources, IT business strategic, IT process integration, IT management, and IT infrastructure. Its dimensions combined may provide ISS architecture, ISS infrastructure, ISS human resource, and ISS resource relationship (Bharadwaj, 2000). In any case, this article provides information to assist one in understanding how technologies should be used to face future challenges and growth.

ART4

Bielski’s (2007) article provides theories to ensure continuity of critical operations and managing risks associated with ISS. However, its theories have no relationship to preventing accidents related to intoxication levels, although they do have a direct relationship to managing risks that are associated with securing data privacy. Findings in this article indicate that organizations have a low success rate of maintaining privacy while implementing new technologies. When new technologies are introduced, permission for failure and doing things differently from the past are necessary. Ensuring continuity is effective as the information contained provides a level of success during an incident.

This article incorporates recovery strategies based on potential impact to ensure continuity of critical operations. Critical operations include methods designed to recover business functions, systems, and facilities. Business functions have strategies and procedures for recovering business goods and service processes. Systems ensure that there is the information and data needed to execute a current business plan, to identify and document plan deficiencies, and to follow-up. Facilities ensure internal and external resources for resolution and implementation on a timely basis and recovery staff members who are trained and capable of executing the strategies during an incident.

Although this article presents a comprehensive framework for enhancing business continuity, its concepts can also be utilized in ISS for developing an integrated data server platform, protocols, and applications in case of ISS network downtime. The article calls for ISS network availability, referring to the ability of a redundant servers operating environment to provide efficient access to data and applications while minimizing downtime.

ART5

Hoffman et al. (2006) developed a security trust model related to metrics for distributing computer based systems that are useful to face technology changes. The analysis has clearly shown an understanding of how its theories could be useful in certain areas to prevent vehicle collisions, but not specifically collisions that related to intoxication. Given that existent ISS lack holistic solutions to control tangible assets from intruders, developing critical security systems to prevent intoxicants from driving would have to be a breakthrough of the common paradigm of the information security environment.

However, this article has refined common security strategies that maximize effectiveness while minimizing risks that ISS can use to prevent drunken drivers from starting motor vehicles (Tan et al., 2006). Its trust model includes security, usability, privacy, and expectation, which produce infrastructure systems to address authentication between senders and receivers, message integrity, and data confidentiality.

The trust model explores the connection between verification and human trust. It supports a cryptographic mechanism that allows verification to be authenticated with protection of data integrity and confidentiality intact. With its metrics designed to measure trust and distrust, in some aspects the model provides redundant features for enhancing security reliability and availability.

ART6

Itakura and Tsujii (2005) provide concepts and information to be considered regarding biometric methods to address security issues. The analysis derived from the infrastructure guidelines would provide information to better integrate resources in revealing intoxication facts to stop a motor vehicle from moving. It has shown that as devices and data become increasingly interconnected within ISS, it is possible to detect an intoxicated individual, and the risks of unauthorized access become higher.

This article provides information on the biometric method system as an ISS to prevent individuals under influence of alcohol from driving. It is based on a multifactor biometric authentication method using fingerprints, iris, face, voiceprint, signature, and DNA. Biometric characteristics divide into two categories, physiological and behavioral differences, that preclude accuracies between two particular values "false rejection rate" and "false acceptance rate," which alone cannot be used to determine the right judgment of an individual's intoxication level (Itakura & Tsujii, 2005).

Dealing with physiological and behavioral factors, it is difficult to create standards for identical encryption paths due to the dynamic challenges involved in obtaining accurate information and making a method to standardize processes that the biometric security system can constantly update. This article argues that if a person's biometric data is stolen, it might allow someone else to access the information and the damage could be irreversible (Itakura & Tsujii, 2005). Indeed that is a true statement because biometric security solutions are based on matching at the point of transaction, and the information obtained by the scan needs to match with a pre-stored static information created when the user is originally placed in the security system.

The article proposes six technical practices to embed biological information, and its cryptosystem becomes one of the keys of the multifactor biometric security system to meet data requirements. Its concepts rely on how the ISS would obtain the data to detect the intoxication level of an individual when placing a key into the ignition to start a motor vehicle.

The ISS devices would then alert the operators when an individual exceeded .05-.08 grams BAC level and make a decision to implement the prevention process to stop the motor vehicle from moving. Prior research revealed that 96% of fatal crashes involve individuals who had BAC levels of .08+ grams. Nevertheless, unifying each technique collectively would require a standardization procedure that would force exposure of information, which might represent a threat to privacy rights.

As stated in this article (Itakura & Tsujii, 2005), “The fruits of study on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures for the purpose of solving a problem” (p. 91) is accepted for verification of individuals’ characteristics to ensure higher security access. It is also concluded these concepts are not completely concrete approaches; it will require further research.

ART7

Oh and Pinsonneault (2007) primarily aim at the evaluation of alternative conceptual and analytic approaches for assessing the strategic value of information technology. Using a contingency based perspective and a resource centered perspective would definitely provide a good analytic approach for better understanding the strength and weaknesses of ISS. One may argue that the contingency based perspective is a better predictor of organizational performance than the resource centered perspective. A contingency perspective provides the ability to identify resources through multiple dimensions of strategies. It is understood profitability and productivity have not always emerged to positive outcomes in information technologies.

This article's theoretical discussion suggests that it is possible to realize productivity benefits from effective management of IT. Effective IT management requires three different measures of IT value dimensions: productivity, profitability, and consumer surplus. This article's framework focuses on the integration of information security components that serve to discipline processes and workforces, which would re-enforce the quality of services to prevent an intoxicant from driving.

Moreover, its theory provides a clear understanding and measuring environment of relationship changes, values, and performance in ways that best establish strategy for ISS. On the other hand, the resource centered perspective considers strategy that directly influences performance when combined correctly with other strategy resources. However, it would not directly provide decisions that could affect security control. Nonetheless, the two approaches add value to both the concepts and analysis that are relevant to the intervention of ISS.

ART8

Siponen (2006) explores several prior methods for designing information security standards to address the fundamental ISS requirements. Given that process is a series of actions directed toward a specific aim, then the quality of the process would be the set of tasks, knowledge, and techniques required to identify the needs and determine the solutions to problems. Solutions often include systems development, but may also consist of process improvements or changes. It uses design theory to develop a framework that defines six requirements for information security design methods and shows how prior design methods have failed to meet these meta-requirements.

As a result, its design theory leads to a meta-notion framework that addresses four of the six meta-requirements. Its meta-notion includes capturing available solutions and best practice standards, addressing access controls and data flow, integrating structured methods through the analysis phase, and restricting design methods autonomy. It is known that information security is divided into two parts, design product and design process, which consist of meta-requirements found within the components that would apply to testing hypotheses and design theories. In the case of this study analysis, ISS may use this concept to test the prevention of car crashes related to intoxication. The article introduces six normative theories as kernel theories for information security policies and guidelines that point out the extent ISS can apply in its policies criteria.

Kernel theory is one of the three criteria presented in the article and offers the necessary foundation from which information security can take create concrete guidance for policy processes. Application criterion is to advise on how to handle any given situation that may prevent objectives achievement. Testable hypotheses are to address systematic agendas that guide the improvement of security policies and new approaches to future guidelines.

ART9

Stevens (2008) article outlines the Federal Information Security and Data Breach Notification Laws in the *CRS Report* for Congress, which created several programs to control fraud and abuse of information systems. The laws lay out security safeguards to ensure confidentiality and require entities to notify individuals of security breaches. Its concepts capture the issue of access security control on a theoretical level, on a methodological level, and on a practical level.

The theoretical level develops a terminology to understand the differences between access control practices and the support mechanisms, which are emphasized in the term "computer supported access control" (CSAC). The methodological level is concerned with empirical investigations of access control behavior from a given action perspective, which may differentiate a set of practices with traditional access control practices. The practical level improves the conceptual design of CSAC mechanisms through a matrix of technical mechanisms, which may accept or reject access automatically according to pre-configuration design.

One of the programs from this Act defines control structures that indicate the results of the syntactical analysis of transaction, which helps to check the consistency of the policies and procedures and can be applied to any given ISS. The Notification of Risk to Personal Data Act requires federal agencies to disclose any breach of sensitive information, which relates to ISS because ISS may reveal personal information and disclose critical information while preventing an intoxicated individual under the influence of alcohol from driving (Stevens, 2008).

ART10

Straub and Welke (1998) provide a CSM that illustrates some of the theories designed to prevent cyber-terrorist attacks. This concept could be modified to intercept an intoxicated individual from starting a motor vehicle. However, interception is not prevention when it comes to CSM. It is a concept that could be used as a firewall to prevent an unauthorized user by employing deterrent, preventive, and detective techniques.

The deterrent method is primarily used to help reduce misuse of information systems. Its theory essentially explains the concept of accept and reject when information is misused. The preventive method consists of active measures such as passwords and encryption, which limit access to the system and critical data. The detective method is designed to detect misuses after they occur so that recovery process can start data retrieval. The goal of this article is to provide theories that can be utilized when an incident occurs to control and minimize any damage, restore evidence, promote effective recovery, prevent similar events from happening, and capture external and internal data threats.

In addition, the article highlights the need for an overall security risk planning process with methods that analyze risk, identify threats, prioritize risks, present alternative solutions, and match threats with appropriate solutions. Its concepts seem to be more applicable to preventing cyber-terrorism than preventing individuals under influence of alcohol from driving. It may provide managers with a better understanding of the actions that can be taken to reduce information security risk.

ART11

Swanson et al. (2003) identify elements that must be considered in the definition of effective metrics, which enable tracking the performance of a security program. The metrics provide independent components for developing processes to measure implementation, efficiency, effectiveness, and security controls. The framework facilitates a metrics oriented analysis with quantifiable performance metrics, practical security policies, and procedures to support decision making.

However, the concept of the metrics requires obtaining performance results through measurements that allocate information security resources to monitoring progress and the corrective actions as needed. Moreover, the measurements can reveal areas of concern in the ISS, but are limited in areas concerned with intoxication level of an individual and preventing an individual under influence of alcohol from driving.

This article provides guidance on how an organization may use its metrics to identify the quality and validity of security controls, policies, procedures, and regulations, but not enough of the analysis concerns identifying vulnerabilities, defining threats, and risk analysis processes for preventing security breaches. Often risk analysis needs to prioritize assets, identify threats, and determine the actions needed for protection. It also prioritizes corrective actions based on what the risk analysis reveals and provides a contingency plan with a restriction mechanism to improve an ISS.

ART12

Tan et al. (2006) address the core concerns at each stage of threats assessment and response to the gaps of the process. The main objective of the article is to provide a description of the core concerns of security management as dynamically as possible and in a manner that is as friendly as possible to various standards through a holistic security ontology model that develops open security systems with multiple configuration settings for any given security specification. Its settings use security interoperability as a common security standard to support security discovery and dynamic security reconfiguration within an open service infrastructure.

The article concludes that a common security model could be used to address any security process and allows for keeping prior security specifications from various standards and refining security strategies to support interoperability between heterogeneous systems (Tan et al., 2006). Both taxonomy dictionaries (TD) and extensible markup language (XML) concepts use knowledge based approaches, and policy based and access control solutions to transport information and store data accurately. Interoperability and heterogeneous concepts in this article's analysis have shown how different products or systems could work together to exchange information. The theory of this article provides the ability to identify potential intoxicated drivers via ISS using different methods and devices.

TD described security concepts can be utilized through applications to detect intrusion and build trust based systems. XML approaches focus on protecting the transmission of the data to support confidentiality, integrity, and authentication, which can benefit ISS from policy-based environments in managing changes through consistent profiles related to intoxication BAC levels.

ART13

Wilson (1998) addresses theories that evaluate security metrics using qualitative and quantitative activities to measure the level of information security awareness competences. Evaluation security is a process of collecting data and risk evidence to determine whether the security system safeguards the assets, maintains data integrity, and achieves effective goals and resource efficiency.

The security metrics require measuring the impact and effectiveness of security controls, threats, vulnerabilities, quality, and risks, which is supported in this article to assess threats from different levels within mitigating approaches. Assessing competences has been a major topic in organization theory literature for many years. The analysis in this article shows how one must conduct an empirically tested model for measuring performance across multiple dimensions. Although a metric presents multiple phenomena, it will have to measure via multiple dimensions to evaluate an intoxicated individual.

Metrics that are supporting information security systems have to compare systems with respect to security, privacy, usability, risk measurements, test methodologies, and data to support testing. This article provides sufficient information to assist in determining whether performance levels meet the requirements of a security system. However, metrics alone will not be enough to increase performance of an ISS. Nevertheless, these concepts will be very helpful in finding ways to develop competences among ISS staff to focus more on the solutions, not just the problems.

ART14

Ye et al. (2005) describe different forms of security threats and propose models and theories that enhance detection of cyber attacks to assist an organization in deciding what types of barriers or protection mechanisms are necessary to defend against cyber attacks and where to place such barriers (Ye et al., 2005). Understanding the characteristics of cyber attacks and identifying threats and attack activities can help in choosing effective barriers to prevent them from damaging an organization's network performance.

This article presents a system-fault-risk (SFR) framework for cyber attack classification, which is based on a scientific foundation that combines theories from systems engineering, fault modeling, and risk-assessment. These theories provide a well founded protection against cyber attacks and help in evaluating security resources while establishing a knowledge base to face and prevent critical challenges. SFR helps in assessing the risks of cyber attacks and making decision about the kind of protection mechanisms and techniques needed for minimizing security risks during the pre-attack, attack, and post-attack phases.

With no doubt, these theories will enable any organization to defend its networks against cyber terrorist attacks and defend its ISS from takeover by an unauthorized user or third party. Cyber attackers always seek vulnerability on network system resources. Exhibiting availability of the network, violating the integrity of networks, and aiming for more confidential information will always be their objectives. This article identifies a framework to uncover activities that can improve the accuracy and efficiency of intrusion detection. Although, these theories have been implemented in several aspects of information security, however, they have not been applied to an ISS for the intervention or prevention of moving a motor vehicle. Currently the possibility of preventing an intoxicated individual from driving via ISS requires the interpretation of BAC level data when the intoxicated driver inserts the key into the vehicle ignition, meaning validity data is a matter of referencing characteristics from events, words, and actions of the intoxicated individual (Miles & Huberman, 1994).

However, there is no application found in the articles analysis, as shown Table 7, for a qualitative research to account for meanings to prevent individuals under the influence alcohol from driving (Maxwell,1997), except for the conceptual framework where meanings are questionable. As the study progressed into answering the research questions, the interview questions were more supportive than the articles analysis for accumulating data that could be interpreted and validated. “Qualitative research occurs in natural settings where human behavior and events occur” (Creswell, 2003, p. 119).

Table 7.

Article Condensing List

Article	Keywords	Findings
ART1, **ART2**, ART4, ART7, ART11, ART12	Policies in management, threats, and vulnerabilities	Regulations, provisions, and defending against intruders
ART3, ART5, ART6, ART8, ART11, ART14	System infrastructure and availability	Containing capacity for data collection as needed
ART4, ART5, ART6, ART7, ART10, ART14	Data integrity and identification	Resources for data protection and evaluation instruments.
ART1, ART7, ART8, **ART9,** ART10, ART13	Confidentiality and monitoring	Protection of privacy and monitoring multiple attacks against access points

The conceptual framework in this study supports the theoretical constructs from interaction with participants, which led to different perspectives on detector devices, identifier applications, preventer techniques, and monitoring methods as the ISS intervention is to stop intoxicated individuals from driving. These different components address explicitly the theoretical constructions to help ISS in developing descriptions and interpretations during intoxication events. Data collected from participant interviews as shown in Table 8 has provided discoveries correlation and responses on components for each function of the ISS security layers.

Table 8.

Participant Data Analysis

Interview question	Men Yes	Women Yes	Total % Yes	Total % No
Prefer ISS-detected and auto-notified intoxicants not to drive	8	4	60%	40%
Prefer ISS-detected and prevented intoxicants from driving	2	8	50%	50%
Will such intervention add significant value to you and others?	6	9	75%	25%
Will you purchase a vehicle with such intervention to prevent you from driving while you are under influence of alcohol?	4	7	55%	45%
Will ISS intervention minimize vehicle crashes or death toll related to individuals under influence of alcohol?	7	10	85%	15%
Do you foresee this ISS study creating some type of government control with intervention?	7	8	75%	25%
Mandate ISS intervention to be implemented in individuals' vehicles who have been convicted of DUI.	7	9	80%	20%
Will you pay a 5% to 10% increase in vehicle cost for such feature in a new vehicle?	3	8	55%	45%
Will you pay an 11% to 15% increase in vehicle cost for such a feature in a new vehicle?	2	6	40%	60%
Will you pay a 16% to 20% increase in vehicle cost for such feature on a new vehicle?	1	6	35%	65%
Will you pay a 21% to 25% increase in vehicle cost for such feature on a new vehicle?	0	6	30%	70%
Do you foresee any demand for such technology intervention in vehicles?	8	10	90%	10%

ISS-Detector

Data from participants suggests detecting individuals under influence of alcohol is not an area of concern to participants. It appeared that the most frequent critical issue to the participants was the technologies that would make the decision to prevent them from driving. The data collected showed the highest need was for detecting blood alcohol levels and auto-notifying intoxicated individual. Detecting intoxication, as the data suggest, includes an implementation process that involves securing the incoming data for privacy protection. The data also indicate that the intoxicated individuals should determine their own competency to drive or not, and ISS should store acknowledgement data of the individuals' detection alerts.

The participants' detector preferences suggest a high level of intoxicated drivers may need a responsive ISS that would teach the signs of excessive alcohol consumption and when to not drive. Nevertheless, that must include a support system where intoxicants do not face a constant learning process, which could lead to lack of motivation to stop drinking.

ISS-Identifier

Identifying data gathered from the participants indicate strong support and commitment, if it were possible to get positive identification surrounding the motor vehicle in question and obtain the necessary data from intoxicated individuals. Then, the result would be innovation and successful implementation of new ISS technologies.

Findings indicate that ISS may have a low success rate at implementing its methods. However, its development must provide opportunities for intoxicated individuals to be evaluated for alcohol consumption.

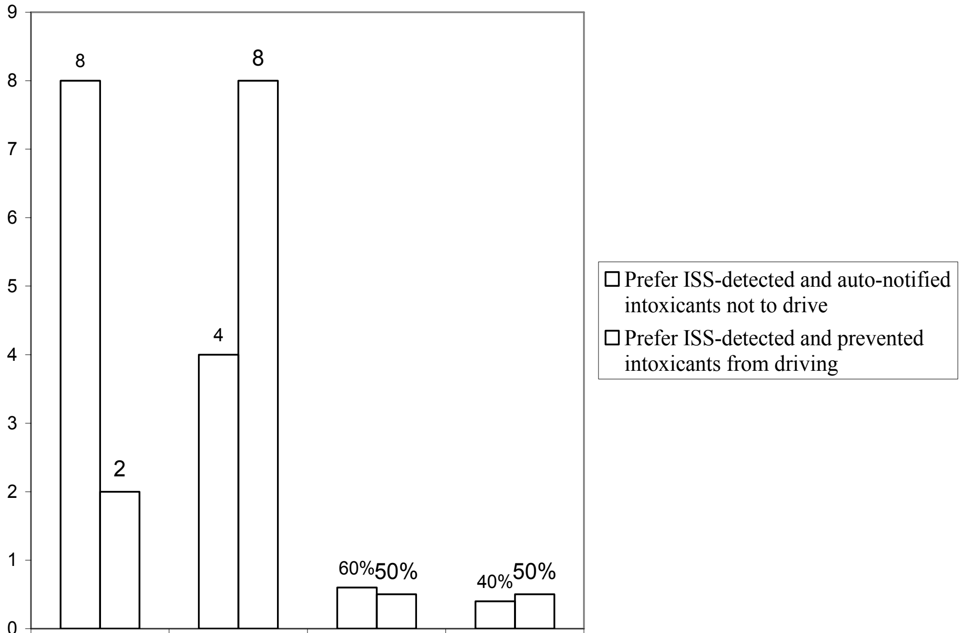
The participants strongly suggested the need for ongoing intoxication prevention and mechanisms for intoxicated drivers to be restrained when necessary. The data suggest sufficient technology access and support must exist in order for problems to be addressed immediately. In addition, frustration from lack of support plays a major role in abandonment of some technologies. As a result, prior information security systems remediate weaknesses to support intoxication prevention, which is why this study maintains its underlying mechanisms into three critical findings in the data collection, detecting, identifying, and preventing.

ISS-Preventer

When it comes to ISS-preventer, the data indicate participants wanted to have convenient ways to activate ISS intoxication prevention as seen fit, which is not in the best interest of an intoxicated individual or ISS. The data derived from the participants is useful in setting guidelines for developing comprehensive methods and providing information for successful integration to stop vehicles from starting. There was strong consensus among the participants that ISS could be utilized to prevent individuals under influence of alcohol from driving, and the three areas of focus must be detecting, identifying, and preventing. Unfortunately, none of the three mechanisms can uncover all the vulnerabilities alone, which is why real-time ISS monitoring is essential to prevent an intoxicated individual from driving.

Data Analysis

The interview questions provided specific data from participants that have been summarized in the data analysis figures. The responses were very constructive; data suggest that ISS should utilize detector devices rather than prevention devices to stop individuals under influence of alcohol from driving. However, the responses and percentages of data (see Table 8) show that there is more than one preferred method to delivery ISS services. As shown in Figure 6, twelve participants, or 60% of the respondents, indicated that a method that detects and alerts intoxicated individuals is a better concept. Ten participants, or 50%, indicated that ISS that detect driver intoxication and prevent vehicles from moving were the most important ways to save lives. Two participants, or 10%, indicated that combinations of these concepts would be the most effective. Data suggest of the male participants, four, or 40%, indicated that the primary factor for deciding whether to buy a vehicle with such technology is the cost; six of the male participants, or 60%, stated they would never buy a car with such technology.

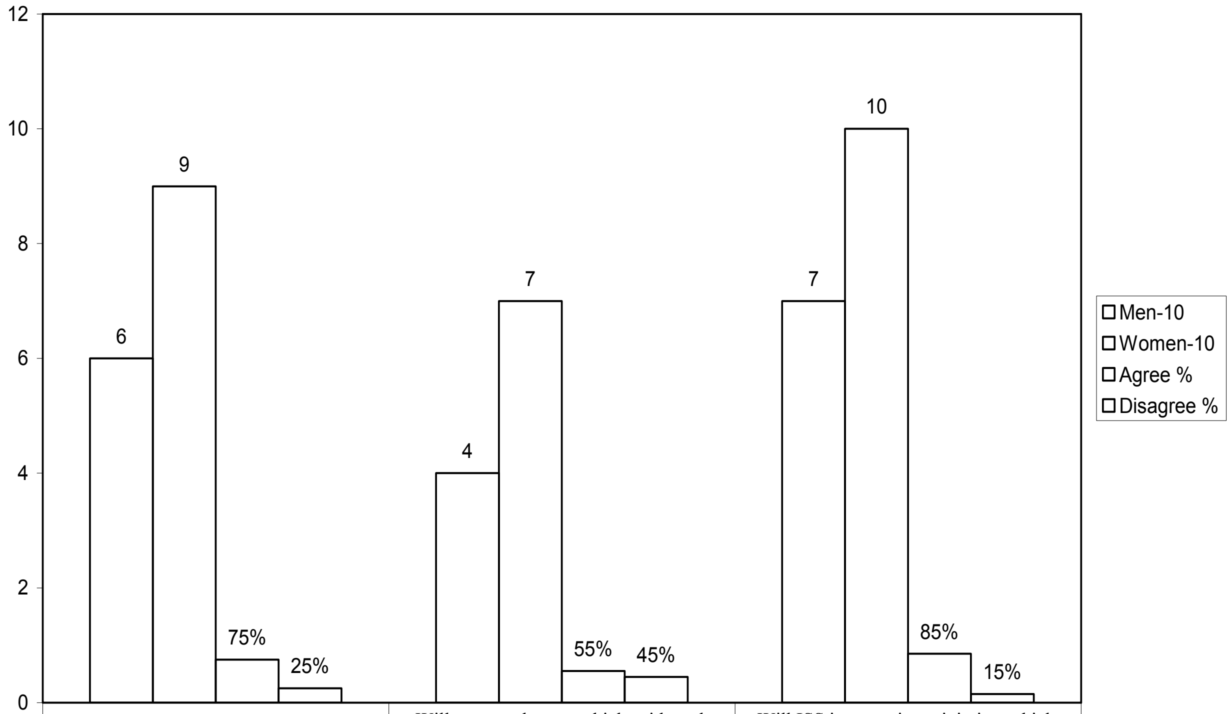


	Men-10	Women-10	Agree %	Disagree %
Prefer ISS-detected and auto-notified intoxicants not to drive	8	4	60%	40%
Prefer ISS-detected and prevented intoxicants from driving	2	8	50%	50%

Figure 6. Participant data analysis of ISS detect and prevent.

Seven of the women participants, or 70% of the female respondents, indicated that the primary factor for deciding on buying a vehicle with such technology was the ability of the technology to protect them and save the lives of others; and three, or 30%, stated they would buy a car with such technology as long this feature did not increase the cost of the vehicle. Sixteen participants, 80%, indicated that individuals who have been convicted of DUI should have such technology implemented in their vehicles all the time, and there should be a mandatory law enforcement requiring such systems to be placed in those individuals' vehicles. Four participants, or 20%, stated such a system should be installed in a vehicle based on the individual DUI conviction.

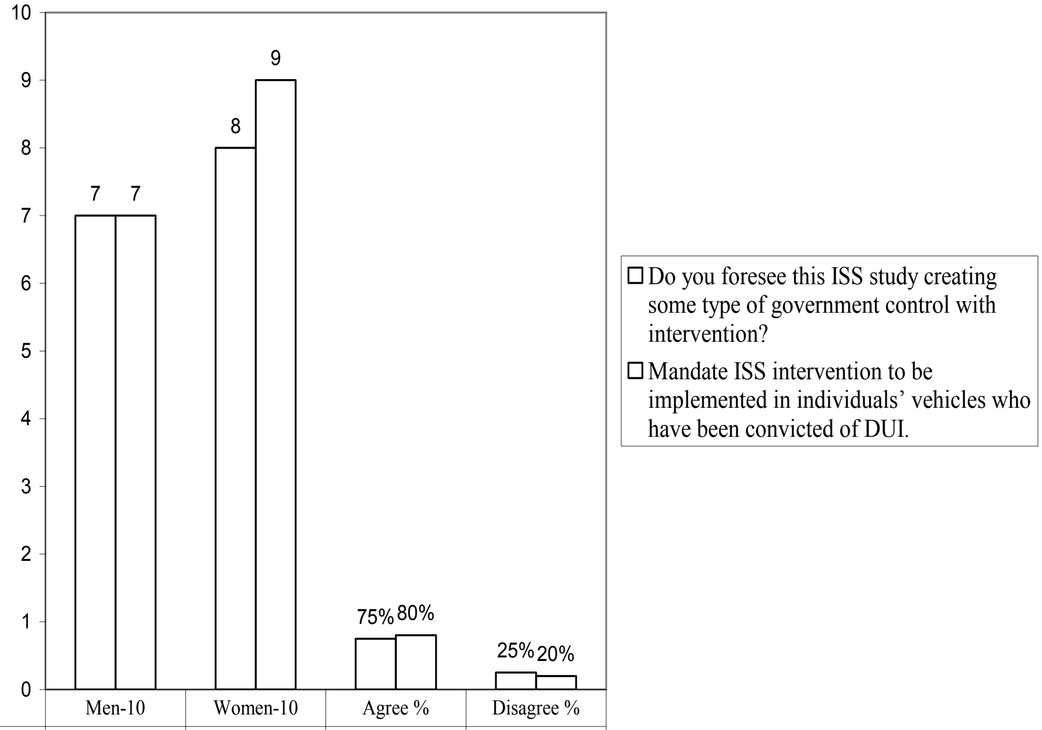
As seen in Figure 7 and Figure 8, 75% of the respondents indicated that some form of integrating new technology into motor vehicles to prevent individuals under influence of alcohol from driving is necessary, but should not be used as an opportunity for government to take over peoples' lives. One participant indicated, there should be a joint effort between ISS and instructional methods to help intoxicated individuals heal themselves from excessive alcohol consumption.



	Will such intervention add significant value to you and others?	Will you purchase a vehicle with such intervention to prevent you from driving while you are under influence of alcohol?	Will ISS intervention minimize vehicle crashes or death toll related to individuals under influence of alcohol?
Men-10	6	4	7
Women-10	9	7	10
Agree %	75%	55%	85%
Disagree %	25%	45%	15%

Figure 7. Data analysis on significant value of vehicle purchase.

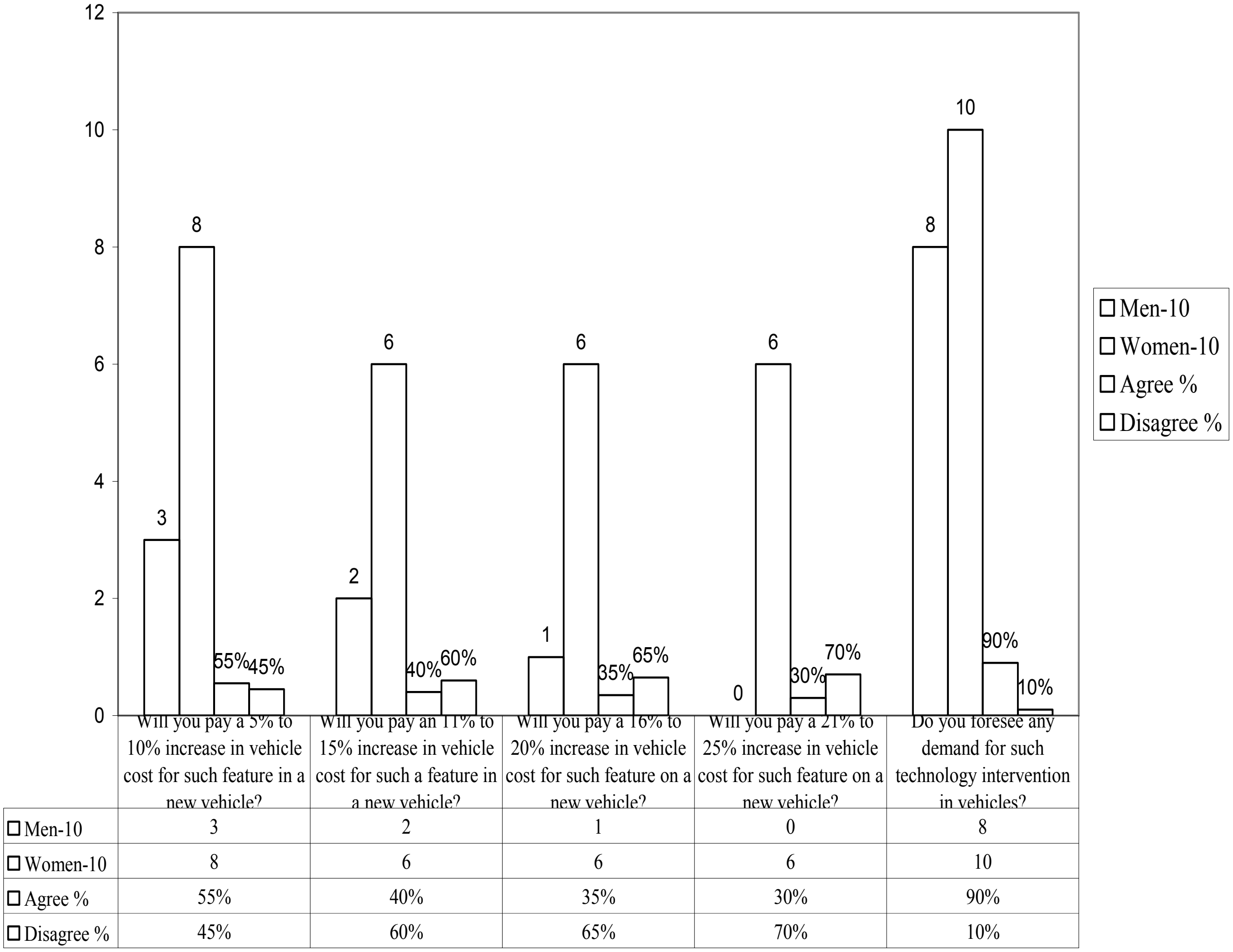
The last question in the interview asked participants in what way an ISS feature for preventing intoxicated individuals from driving would be beneficial to the public. Seventeen of the participants, 85% of respondents, indicated that it would significantly minimize motor vehicles crashes.



	Men-10	Women-10	Agree %	Disagree %
Do you foresee this ISS study creating some type of government control with intervention?	7	8	75%	25%
Mandate ISS intervention to be implemented in individuals' vehicles who have been convicted of DUI.	7	9	80%	20%

Figure 8. Data analysis of government control and mandate.

Three participants, or 15% of the respondents, mentioned that ISS may diminish vehicle accidents related to drunken drivers, but it would not motivate individuals to stop drinking. As see in Table 8 and Figure 9, eighteen participants, 90% of the respondents, indicated more demand and flexibilities would require ISS to respond rapidly within a limited time to prevent drunken drivers from starting motor vehicles.



	Will you pay a 5% to 10% increase in vehicle cost for such feature in a new vehicle?	Will you pay an 11% to 15% increase in vehicle cost for such a feature in a new vehicle?	Will you pay a 16% to 20% increase in vehicle cost for such feature on a new vehicle?	Will you pay a 21% to 25% increase in vehicle cost for such feature on a new vehicle?	Do you foresee any demand for such technology intervention in vehicles?
□ Men-10	3	2	1	0	8
□ Women-10	8	6	6	6	10
□ Agree %	55%	40%	35%	30%	90%
□ Disagree %	45%	60%	65%	70%	10%

Figure 9. Data analysis of percentage of participants willing to pay for ISS features

Summary Results

The analysis of the articles revealed that ISS has no comprehensive framework to prevent individuals under influence of alcohol from driving. However, there were relationships and construct approaches based on the descriptive and qualitative aspects of the articles to determine the extent to which ISS may detect intoxicated individuals while starting motor vehicles. As part of this study, the researcher attended an Alcoholics Anonymous (AA) meeting to get participants who experienced alcoholism issues and voluntarily embraced this research study to tell their histories. Their experiences have provided significant value to shifting the paradigm of ISS as seen in the data analysis in Table 8. The inputs from participants in the AA meetings in two counties in South Florida have shown that a strong focus exists to minimize vehicle crashes and deaths toll related to drunken drivers.

With that in mind, there is an increasing demand for more research on this topic. People expect a rapid response and greater flexibility from ISS in preventing individuals under influence of alcohol from driving. Participants in this research also indicated that the future of ISSP is essential in meeting the need to minimize death tolls related to intoxicated drivers, which includes training individuals to control excessive alcohol consumption. In an ISSDA, an integrated detector system for a vehicle would be comprised of a sensor having a sensing surface that is capable of retrieving intoxication data in whatever format (skin, eyes, breath, air, sweat) desired and storing data associated with predetermined characteristics. At that point, ISSD is to determine if the individual exceeded BAC level from the vehicle sensor signal outputs.

In ISSDB, an integrated identifier system for a vehicle would be compromised of a sensor that is capable of monitoring reflected and emitted patterns from data and comparing the detected patterns to reflected characteristic patterns. At that point, ISSI would triangulate the indication of location position if the individual was too intoxicated to operate the vehicle.

In ISSDC, an integrated prevention system would be comprised of data from the intoxicant's BAC level in reference to the integrated vehicle monitoring system. At that point, ISSP would determine what methods would be implemented to prevent the identified individual from driving. Prevention can be based on substantial BAC level matches found between the derived data and the stored data, or it may determine if the intoxicant is not authorized to drive the vehicle when no substantial match is found between the derived data and the stored data (Couper & Logan, 2004).

In ISSD, an integrated monitoring system would be comprised of processors for deriving data corresponding with the predetermined characteristics of the individual in whatever format (skin, eyes, breath, air, and sweat) desired from the signal outputs. Simultaneously, vehicle sensors present data on the intoxication of the individual during the monitoring process. At that point, ISSM would compare the derived data with the stored data associated with pre-characteristic data for substantial matches between all processes level, which include detector, identifier, preventer, and monitor.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Discussion

In developing a system to prevent individuals under influence of alcohol from driving via ISS, one has to assume the theory should be clearly specified before design and implementation. Failing to follow defined requirements, design approaches can cause delays, failures, and high costs. Many research studies confirm the fact that most critical decisions are usually made during the early development phases (Welander, 2007). Therefore, an upfront investment in conducting a proper analysis will pay off during the later phases of development. In this study, 14 articles on information security practices were the main focus for this research.

Moreover, in the information security industry, there is significant pressure to deliver solutions that protect peoples' privacy at any cost. In this analysis the facts showed that with all the new applications and services brought about by networking technologies, information security is faced with the challenge of building successful ISS that would prevent people under influence of alcohol from driving. Since the devices that make-up the ISS would require other products to meet this demand, it must adopt a solution approach that can be implemented with traditional network communication providers, such as phone service providers, detector devices, and other public services.

The research results show there is a need for ISS to adopt a specific perspective approach to prevent individuals under influence of alcohol from driving. However, it requires conjoined efforts to provide the best fit detection/prevention devices and applications from multi-networking products with the primary concern being the need to meet requirements and satisfy the desired goals that minimize the challenges of preventing intoxicated individuals from driving (Wen et al., 2007). It is now a known fact that people want more to be done to minimize vehicles crashes and deaths caused by intoxicated drivers. It has been evident in the past couple of years that there is not enough being done to help people implement and manage ISS to better meet their needs. Today, people want services that apply technology to transform information to minimize risk and to prevent intoxication related accidents.

Implications

To develop ISS that will prevent intoxication related accidents requires knowledge, experience, and expertise across communication networking environments; it involves understanding the changes that are taking place in detection devices and how other public services are responding to intoxication events across the information security industry. This is vital since integrated communication networks in this era are incorporated applications and devices. The ISS environment becomes more distributed in businesses that dictate enhanced end-user capabilities; it also sees the evolution through network communications (Welander, 2007). Therefore, network theories/methods that seek to address ISS and its support applications, which prevent individuals under influence of alcohol from driving, as shown in the Figure 1 and Figure 10, could represent a paradigm shift in ISS.

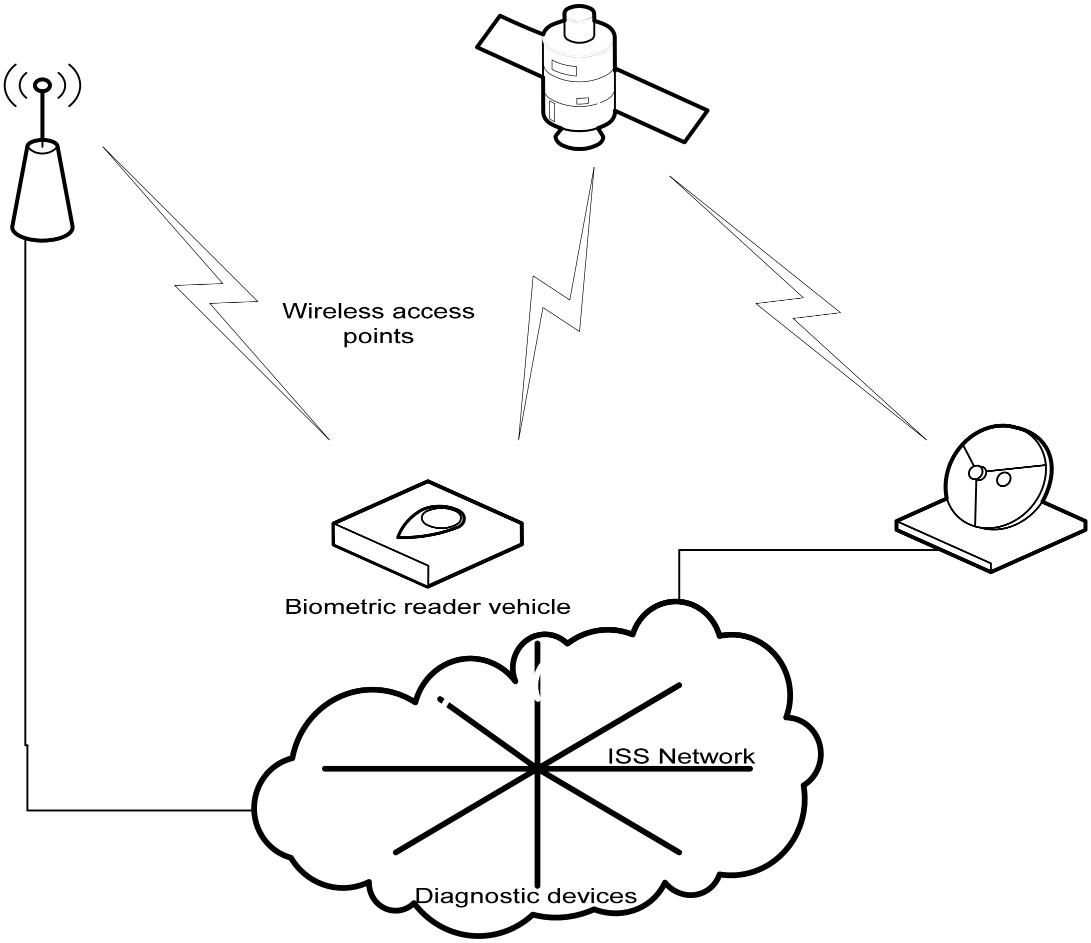


Figure 10. ISSD wireless network

These applications seek to leverage the core ISS that enables the organization to enhance process efficiencies, ISS workflow management, and ISS intoxicant communication (Taylor, 2005). There are benefits that have driven information security to migrate to complex voice and data infrastructures and away from reliance on heavy contact center usage and large numbers of remote and mobile operators. Here is where this research approach would be beneficial. In integrating or migrating ISS with intoxication detector devices, it would be easier to properly retrieve intoxication data

(Kantrow, 1980). Evaluating individuals who are under influence of alcohol and at the same time providing data to make good decisions would allow operators to keep pace with emerging prevention techniques to stop vehicles from moving.

Recommendations

Detecting Intoxication via ISS (ISSP1)

An overwhelming case has been made to build integrated network solutions that embrace multi-products from service providers to new network requirements. It is not only integration with legacy communications hardware, although it would not make good sense to replace old technologies, but also the incorporation of wireless technologies and other vendor devices more suitable to meeting the needs of data retrieval. Therefore, the goal of detector communications is to keep pace with emerging technologies and the opportunities to adapt with new demands. Nevertheless, this approach would require proper analysis of requirements and evaluation based on the individual intoxicant cases.

ISS detection of BAC levels is a promising method that could prevent intoxicated drivers from driving if integrated into a vehicle ignition interlock system. However, previous research has shown significant time delays between alcohol ingestion and detection using any of the formats, which makes real time data estimation of BAC level sensor measurements difficult to retrieve (Couper & Logan, 2004). Part of the significant time delays have been due to body weight and variances in individual ability to metabolize alcohol. In many instances drinkers underestimate the amount of time needed to burn the alcohol they have ingested. Theoretically, the average rate is 0.015% metabolized BAC per hour (Couper & Logan, 2004).

The alcohol content evaluation of individuals can be estimated based upon of weight, gender, and amount of alcohol consumed using the Widmar formula (Couper & Logan, 2004). The Widmar formula (E = W x R x AC x 0.2) estimates the amount of alcohol in the body by E = fluid ounces of alcohol, W = body weight, R = factor (0.65 for males, 0.55 for females), and AC = alcohol concentration (Couper & Logan, 2004). When the percentage of alcohol is reached between .05 to .10%, the body has reduced muscular coordination and judgment to make a correct decision. Driving a motor vehicle at these levels is considered legally intoxicated; in addition, intoxication is federally mandated at the standard of .08% in most states. As a result, ISS would be positioned to detect BAC at .05% and automatically alert the individual; beyond the legal limit, ISS would automatically prevent the individual from driving.

The single intoxicant detector end-to-end network solutions approach has to meet the needs of the emerging applications to adopt with this new ISS paradigm. The four-intoxication solution (detecting, identifying, preventing, and monitoring) is essential to meeting the challenges of building a successful ISS that can prevent intoxicated individuals from driving (Feeny & Willcocks, 1998).

Identifying Intoxication via ISS (ISSP2)

Identifying intoxicated individuals requires the determination of distance and duration of changes since alcohol consumption has already been detected as abnormal through ISS-detector. Knowing that each network segment has to be at the highest speeds, connection links have to be dedicated within bandwidth that is considered more than needed. This efficiency provides ISS infrastructure with flexibilities that would not tie up ISS resources. Information became a reality with the stability of the ISS protocol and adjusted input data type as needed (Scott & Davis, 2007). The incoming data has to provide the position of the vehicle to inform the coordinator and enable preventative action.

If positioning delivers vehicle location, it could be mapped onto a descriptive location in order to be interpretable by the ISS operators. The ISS in turn would have to distinguish between the levels of intoxication received and body weight to deal with the intoxicated individuals, and it also has to make the results of the data available to external emergency services as needed. Since the transmit data rates may have to be increased significantly while transmitting intoxication data, ISS wireless networks could outperform wired networks. As a result, ISS may wire network infrastructure to support Gigabit Ethernet on its backhaul connections for building high performance while securing its wireless networks within a high speed triangulation process to transmit data.

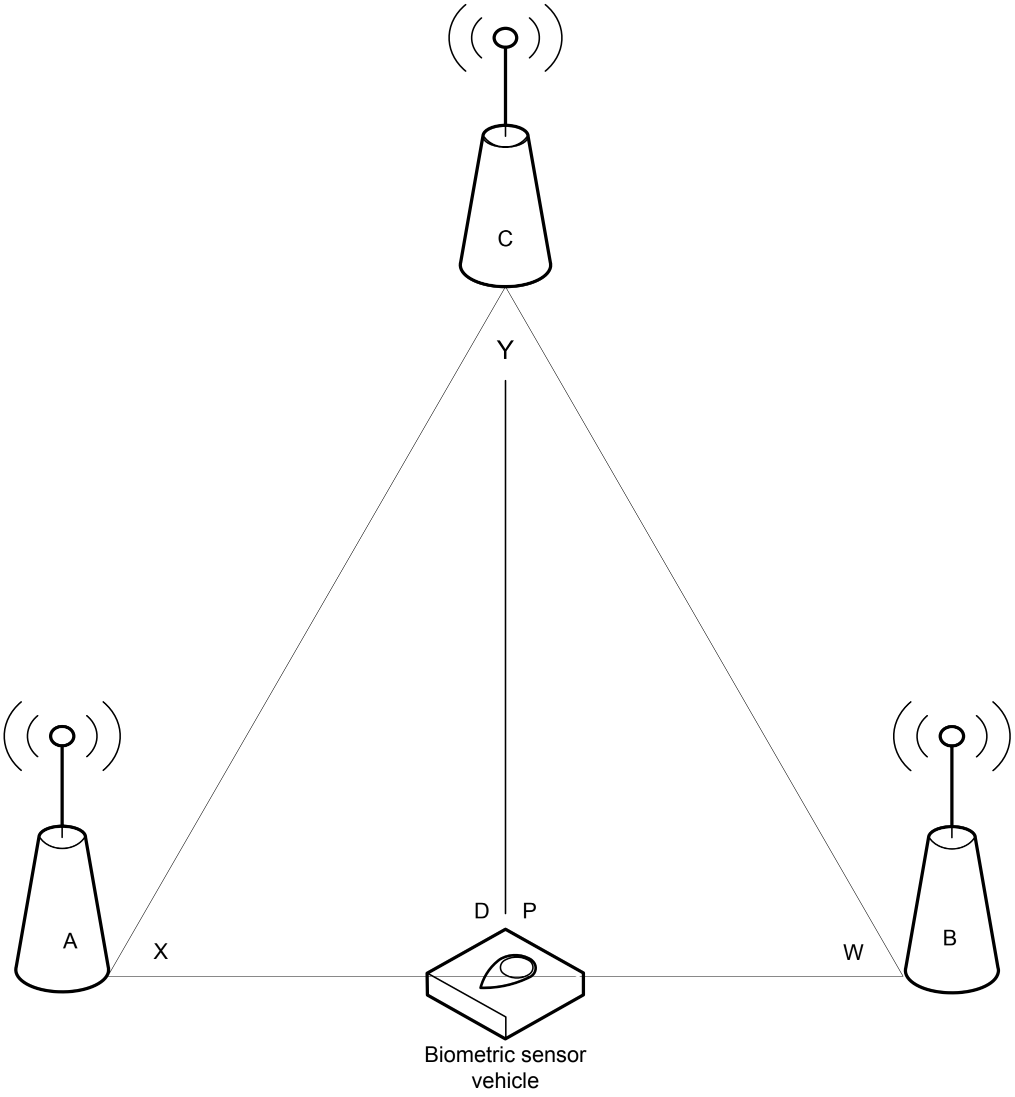
Thus, it is essential to ensure adequate bandwidth exists for all required applications. As show in Table 9, the minimum bandwidth requirements for most major applications such as voice, video, and data for any given link should consume no more than 75% of the total bandwidth available in that link. This 75% rule assumes that some bandwidth is required for overhead traffic to keep alive the ISS monitoring process and additional application transfer protocol traffic routing (Mehta & Hirschheim, 2004). The capacity planning on a data, voice, and video network requires at least a video data rate of +20% to meet the bandwidth demanded.

Table 9.

Minimum Bandwidth Requirements

ISS Routing Applications Rate Minimum Rate	ISS Routing Bandwidth Required Bandwidth Require	Traffic format type
512kbps-ISSD, ISSI, ISSP, ISSM	614kbps-ISSD, ISSI, ISSP, ISSM	Voices
786kbps-ISSD, ISSI, ISSP, ISSM	921kbps-ISSD, ISSI, ISSP, ISSM	Data
1.5Mbps-ISSD, ISSI, ISSP, ISSM	1.8Mbps-ISSD, ISSI, ISSP, ISSM	Video

The triangulation process can be used for positioning vehicles by measuring arrival data between the given individual's vehicle and reference location points. The arrival data is triangulated through multiple wireless network points in the array of the signal output transmission (Kantrow, 1980). Many schemes have been developed for estimating received signal output and location points, such as the proposed approach illustrated in Figure 11, to determine output power, likelihood estimation point, and area base approach location.



Calculation point formula

$$\frac{\text{Sin}(X)}{BC} = \frac{\text{Sin }(W)}{CA} = \frac{\text{Sin}(Y)}{AB}$$

$$\frac{\text{Sin }(P)}{BC} = \frac{\text{Sin }(W)}{CD} = \frac{\text{Sin }(pi\text{-}P\text{-}W)}{DB}$$

Figure 11. Triangulate position.

Preventing Intoxication via ISS (ISSP3)

The first step of ISS is to detect and to identify intoxicant data based on BAC level and to send the results to the prevention phases. Preventing intoxicated individuals from driving may rely on several types of data features such as voices, data, and video over the same ISS network infrastructure to allow operators to use different paths to communicate with the identified intoxicant, to bypass some of the public networks, and to minimize bandwidths to obtain specific data required to prevent one from starting a motor vehicle. Once a stream of data packets is sent, computing resources are freed up. That allows monitoring between two parties over the ISS infrastructure.

The ISS sever has to identify each individual data in sequence in order for the information to travel toward the monitoring solution. That sequence data range would provide possibilities for ISS data centers positioning the intoxicated vehicle through the triangulation concept of wireless technologies, which relatively determines the area where the intoxicant is located from two or more reference points as shown Figure 11.

Monitoring Intoxication via ISS (ISSP4)

Monitoring intoxication of individuals allows operators to integrate all the different services into one ISS infrastructure center (Oh & Pinsonneault, 2007). In this environment, new information on locations should be online in less than minutes. Not only does this ISS network allow operators to build redundancies and eliminate the single point of failures, it allows for internetworking with non-internet protocol (IP) based on the ISS network. When analyzing the case presented in the 14 articles for an integrated ISS network solution, it is revealed that all the different access networks may have to inter-work with the ISS solution to prevent an intoxicated individual from driving.

Therefore, in the theory of integrated ISS solutions, the need for an approach that allows operators to explore access choices may enable seamless communications between the two different network environments (Feeny & Willcocks, 1998). That is why core features of monitoring require full data switch coverage as shown in figure 12 in the threat of management lifecycle of data flow to both internal and external communications. It is also provides external communications over the WAN or a carrier-class IP network that may not be related to the ISS intoxicants prevention network.

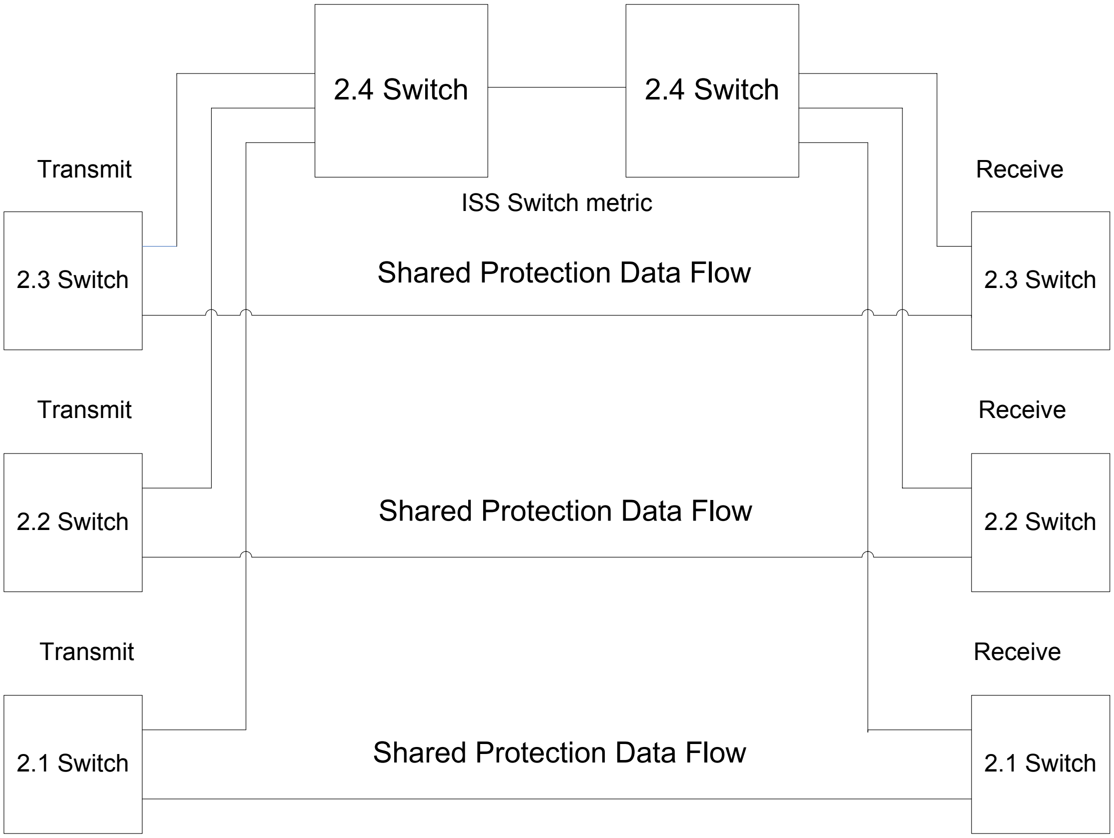


Figure 12. ISS switch data metric.

Failures of Traditional ISS Approach

Traditional ISS failures are due to the fact that its services need a vehicle that emphasizes a solution that must to be scalable, flexible, easily managed, and cost effective in securing sensitive information (Hong et al., 2003). However, assuring consistent quality of services has not been deployable in ways that evolve and remain interoperable with the existing infrastructure. There have not been any approaches that would take physical control of an asset via ISS. This sturdy prospective was based strictly on the extent to which ISS can be utilized to prevent an individual under the influence of alcohol from driving. It is interesting to note that this research study has revealed within a comprehensive approach to ISS using biometric devices, ISS could prevent an intoxicant from driving while still protecting against cyber attacks and misuse. However, the ISS solution must not overburden its capacity. It should also be reliable and provide redundancy for failsafe capability (Naisbitt, 1982).

Summary

Finally, the research articles analysis revealed the extent to which ISS could be utilized to prevent individuals under influence of alcohol from starting motor vehicles through sensors, which are capable of collecting data from skin, eyes, breath, air, and sweat of the individual. However, the mindset of 70% of the participants in this study focused more on the limitation of the ISS from taking control over their lives. Simultaneously, the participants wanted the ISS to help in minimizing vehicle crashes and deaths related to intoxicated drivers. Moreover, 30% of the participants did not care about ISS pricing or control, as long it was a safe system that would detect intoxicated drivers and automatically shut down their vehicles. There may not be right or wrong ISS theories or methods for preventing intoxicated individuals from driving; for different situations, different techniques may have to be implemented. This study does not suggest a theory or method for building ISS networks; rather, it presents an approach to shifting the paradigm for building ISS to prevent individuals under the influence of alcohol from driving (Trochim, 2006).

Currently, ISS does not have any established theories or methods to evaluate BAC levels and to make the determination to stop a motor vehicle from moving (Couper & Logan, 2004). It is recommended that mandated alcohol consumption average .05 to .08 gram BAC. Nevertheless, ISS architecture has to be generically designed in a manner that can be flexible to meet other ISS objectives while securing and sharing its environment to provide the enabling capabilities for intoxication prevention. ISS operators must be engaged in the analysis of the incoming information, having a clear understanding of the individual's vehicle direction, current position, and immediate future. ISS operators need to be competent enough to determine the best technical solution given an understanding of all the problems of preventing intoxicated individuals from driving.

The four approaches seek to resolve this concern by detecting individuals under the influence of alcohol when starting a vehicle, identifying the position of a vehicle, preventing the vehicles from moving, and monitoring the vehicle from the first minute intoxication was detected. There may be reputable incoming information from each process approach; nevertheless, the solutions will not be generic due to different situations. It is specifically for this reason that this study presents the four approaches: ISS-detector, ISS-identifier, ISS-preventer, and ISS-Monitor (ISS-DIPM). The researcher recommends further investigation of ISS, which would be valuable to allow for more generalization of this study's findings. Finally, gaining a better understanding of the relationship of ISS and biometric devices may reveal methods that are useful in eliminating the significant time delay of data retrieval.

References

Ameri, A. (2004). The five pillars of information security. *Risk Management*, *51*(7), 48.

Arbnor, I., & Bjerke, B. (1997). *Methodology for creating business knowledge* (2nd ed.). Thousand Oaks, CA: Sage.

Backerville, R. (1994). Research directions in information systems security. *International Journal of information Management*, *14*(5), 385-387.

Baets, W. (1992). Aligning information systems with business strategy. *Journal of Strategic Information Systems, 1*(4), 205-213.

Barton, B., Byciuk, S., Harris, C., Schumack, D., & Webster, K. (2005). The emerging cyber risks of biometrics. *Risk Management*, *52*(10), 21-31.

Bharadwaj, A. (2000). Information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, *24*(1), 169-196.

Bielski, L. (2007). Security is still a study of the basics. *ABA Banking Journal*, *99*(4), 56-57.

Biometric Technology, Inc. (2004). *Biometric technology assessment*. Retrieved August 21, 2009, from http://www.bio-tech-inc.com

Chan, Y.E., Huff, S.L., Barclay, D. W., & Copeland, D. G. (1997). Business strategic orientation, information system strategic orientation and strategic alignment. *Information Systems Research, 8*(2), 125-150.

Choe, J. (2003). The effect of the environmental uncertainty and strategic applications of IS on a firm's performance. *Information and Management*, *40*(4), 257-268.

Collaborative Institutional Training Initiative. (2009a). Research with protected population-vulnerable subjects: an overview. Retrieved April 15, 2010, from https://www.citipropram.org/members/laernerII/moletext.asp

Collaborative Institutional Training Initiative. (2009b). Group harms: research with culturally or medically vulnerable groups. Retrieved April 15, 2010, from https://www.citipropram.org/members/laernerII/moletext.asp

Collaborative Institutional Training Initiative. (2009c). HIPAA and human subjects research. Retrieved April 15, 2010, from https://www.citipropram.org/-members/laernerII/moletext.asp

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings.* Chicago, IL: Rand McNally.

Cooper, D. R., & Schindler, P. S. (2006). *Business research methods* (9th ed.). Boston, MA: McGraw-Hill Irwin.

Couper, J., & Logan, K. (2004). *Drugs and human performance fact sheet*. (DOT HS 809-725). National Highway Traffic Safety Administration.

Creswell, J. (2003). Research design: *Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. (2007). *Qualitative inquiry & research design choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Denzin, N. K. (1978). *The research act: A theorized introduction to sociological methods* (2nd ed.). New York, NY: McGraw-Hill.

Denzin, N., & Lincoln, Y. (1994). *Handbook of qualitative research*. Thousand Oaks, CA: Sage.

Feeny, D.F., & Willcocks, L. P. (1998). Core IS capabilities for exploiting information technology. *Sloan Management Review*, *39*(3), 9-21.

Harvard Medical School (2008). *Trusted advice for a healthier life*. Retrieved August 19, 2009, from http://www.health.harvard.edu

Harvard Medical School (2008). *Special Health Report on Alcohol Use and Abuse*. Retrieved August 19, 2009, from http://www.health.harvard.edu

Hoffman, L., Jenkins, L. K., & Blum, J. (2006). Trust beyond security: An expended trust model. *Communication of the ACM, 49*(7), 95-101.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management and Computer Security*, *11*(5), 243-248.

Huberman, A. M., & Miles, M. B. (1994). Data management and analysis methods. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 428-444). Thousand Oaks, CA: Sage.

Itakura, Y., & Tsujii, S. (2005). Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. *International Journal of Information Security*, *4*(4), 288-298.

Jones, K., Shinar, D., & Walsh, M. (2003). *State of knowledge of drug-impaired driving*. (DO HS Publication No. 809 642). Washington, DC: Department of Transportation, National Highway Traffic Safety Administration.

Kantrow, A. M. (1980). The strategy – technology connection. *Harvard Business Review, 34*(2), 6-21.

Kaplan, R. S., & Norton, D. P. (1996). *Translating strategy into action: The balanced scoreboard*. Boston, MA: Harvard Business School Press.

Keen, P. G. W. (1991). *Shaping the future: Business design through information technology*. Boston, MA: Harvard Business School Press.

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

King, W. R. (1978). Strategic planning for management information systems. *MIS Quarterly, 2(*1), 27-37.

King, W. R., & Teo, T. (1999). Integrating between business planning and information systems planning. *Information and Management, 30*, 309-321.

King, W. R., & Zmud, R. W. (1981). Management information systems: policy planning, strategic planning and operational. *Proceedings of the Second International Conference on Information Systems*, Boston, 299-308.

Kuhn, T. (1996). *Structure of scientific revolutions* (3rd ed.). Chicago, IL: University of Chicago Press.

LeCompte, W. L. (1992). *Toward an ethnology of student life in schools and classrooms: Synthesizing the qualitative research tradition*. In M. D. Millroy & J. Preissle (Eds.), *The Handbook of Qualitative Research in Education* (pp. 201-223). Orlando, FL: Academic Press.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Thousand Oaks, CA: Sage.
Linder, J. C. (1989). *Integrating organizations where information technology matter*. PhD. Dissertation, Harvard University, Boston, MA.

Malterud, K. (2001). Qualitative research: Standards, challenges, and guidelines. *The Lancet*, *358*(9280), 483-488.

Maxwell, J. A. (1997). Designing a qualitative study. *Handbook of Applied Social Research Methods,* London, England: Sage.

Mehta, M., & Hirschheim, R. A. (2004). *A framework for assessing IT integration decision-making in mergers and acquisitions.* Paper presented at the 37th Hawaii International Conference on System Sciences.

Merali, Y., & McKiernan, P. (1993). The strategic positioning of information systems in post-acquisition management. *Journal of Strategic Information Systems*, *2*(2), 105-124.

Merriam, S.B. (1988). *Case study research in education: A qualitative approach.* San Francisco, CA: Jossey-Bass.

Merriam, S.B. (1998). *Qualitative research and case study applications in education*. San Francisco, CA: Jossey-Bass.

Miles, M., & Huberman, A. (1994). *Qualitative data analysis* (2nd ed.). Thousand Oaks, CA: Sage.

Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage.

National Clearinghouse for Alcohol and Drug Information (2007). *Preventing substance abuse curriculum*. Retrieved September 10, 2009, from http://www.ncadi.samhsa.gov

National Highway Traffic Safety Administration (2006). *Traffic Safety Annual Assessment*. Retrieved September 10, 2009, from http://www.nhtsa.gov

National Institute on Alcohol Abuse and Alcoholism, (2007). *Consequences of treatment on preventing alcoholism.* Retrieved September 10, 2009, from http://niaaa.nih.gov

National Institute on Drug Abuse, (2006), *Treatment and policy on drug abuse and addiction*. Retrieved September 10, 2009, from http://www.nida.nih.gov

Naisbitt, J., & Aburdene, P. (1982). *Megatrends*. New York, NY: William Morrow & Company, Inc.

Oh, W., & Pinsonneault, A. (2007). On the assessment of the strategic value of information technologies: Conceptual and analytical approaches. *MIS Quarterly*, *3*(1), 239-265.

Pettigrew, M. A., Woodman, W. R., & Cameron, S. K. (2001). Studying organizational change and development: Challenges for future research. *Academy of Management Journal*, *44*, 697-713.

Porter, M.E. (1996). What is strategy? *Harvard Business Review*, *85,* 61-98.

Scott, W. R., & Davis, G. F. (2007). *Organizations: Rational, natural, and open systems perspectives*. Upper Saddle River, NJ: Pearson Prentice Hall.

Shanley, M. T. (1987). *Post-acquisition management approaches: An exploratory study*. (Unpublished doctoral dissertation). University of Pennsylvania, Philadelphia, PA.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communication of the ACM, 49*(8), 97-100.

Stake, R. E. (1995). *The art of case \study research.* Thousand Oak, CA: Sage.

Stevens, G. M. (2008). Federal information security and data breach notification laws. *CRS report for Congress*. Retrieved October 19, 2009, from http://www.crs.gov/secrecy-/RL34120.pdf

Straub, D. W., & Welke, R. J. (1998). *Coping with Systems Risk*: Security planning models for management decision making, *MIS Quarterly*, *22*(4), 441-464.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Ground theory procedures and techniques*. Newbury Park, CA: Sage.

Substance Abuse and Mental Health Services Administration (2007). Information on various forms of substance abuse. Retrieved September 10, 2009, from http://www.samhsa.gov

Swanson, M., Bartol, M., Sabato, J., & Graffo, L. (2003). *Security metrics guide for information technology system: Computer security*. Washington, D.C.: National Institute for Science and Technology.

Tan, J., Poslan, S., & Titkov, L. (2006). A semantic approach to harmonizing security models for open services. *Applied Artificial Intelligence*, *20*(2-4), 353-359.

Taylor, D. R. (2005). Five steps to strategic IT management. Retrieved September 13, 2009, from http://esj.com/enterprise/article.aspx?EditorialsID=2090

Tesch, R. (1991). *Qualitative research: Analysis types and software tools.* London: Falmer Press.

Thompson, J. D. (2007). *Organizations in action: Social science bases of administrative theory*. Somerset, NJ: Transaction Publishers.

Trochim, M. K. (2006). *Qualitative Validity*. Retrieved October 24, 2009, from http://www.socialresearchmethods.net/kb/qualval.php

Welander, P. (2007). 10 control system security threats. *Control Engineering*, *54*(4), 38-44.

Wen, J. H., Schwieger, D., & Gershuny, P. (2007). Internet usage: Monitoring in the workplace: Its legal challenges and international strategies. *Information Systems Management*, *24*(2), 185-196.

Wilson, M. (1998). *Information technology security training requirements: A role and performance-based model.* Gaithersburg, M.D: NIST Special Publication 800-16.

World Health Organization (2007). *World report on road traffic injury prevention*. Retrieved September 10, 2009, from http://www.who.int

Ye, N., Newman, C., & Farley, T., (2005). A system-fault-risk framework for cyber attack classification. *Information Knowledge System Management*, *12*(3), 135-151.

Yin, R. K. (2003). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage.

APPENDIX A. LETTER INVITING PARTICIPATION

Joseph D. Pierre
1084 Allamanada Way
Weston, FL 33327

April 1, 2010

I am inviting you to participate in a study that I am conducting in association with the Department of Doctoral Studies, School of Business and Technology: General Business and Technology Program of Capella University. The study is titled Information Security Analysis: A Study to Analyze the Extent to which Information Security Systems can be Utilized to Prevent Intoxicated Individuals from Driving. The study is being conducted to identify the potential of information security systems to help prevent automobile accidents caused as result of driver intoxication.

The study will involve interviews with 20 individuals in the ______ and _______ County region of Florida. I have attached to this letter a preliminary questionnaire and an informed consent form. Please review both documents, and if you are interested in participating in the study, please complete the questionnaire, sign the consent form, and return both documents to me in the stamped, self-addressed envelope.

As the principal researcher, I agree to protect the confidentiality of the data collected and to ensure that no participant will be individually identifiable. I will share a copy of the final report with you upon written request. Participation in this study is voluntary, and you may withdraw from the study at any time without prejudice or penalty. Moreover, upon your request any information collected from you will be destroyed. If you have any questions or concerns regarding this study, please call or write:

Dr. Samuel Natale
Faculty Mentor; School of Business and Technology, Capella University
225 South Sixth Street, Ninth Floor; Minneapolis, MN 55402
(888) 227-3552

or

Dr. John Whitlock
Faculty Chair for Research, School of Business and Technology, Capella University
225 South Sixth Street, Ninth Floor; Minneapolis, MN 55402
(888) 227- 3552

Thank you for your cooperation,

Joseph D. Pierre

APPENDIX B. PRELIMINARY QUESTIONNAIRE

Please circle your answer.

1. My age is under 30 30 to 50 over 50

2. I am Male Female

3. I am a resident of ________ or _______ County Yes

   No

4. I have been convicted of DUI Yes

   No

5. I have experience with intoxication related driving Yes

   No

6. I would prefer to be contacted by Phone Email

Name
____

Telephone Number ____________________________ Best time to call_______________

Email Address ________________________________

APPENDIX C. INFORMED CONSENT FORM

The main purpose of this form is to provide information that may affect your decision about whether or not you want to participate in this research project. If you choose to participate, please sign in the space at the end of this form to record your consent.

WHO IS DOING THE RESEARCH and WHAT IS IT ABOUT?

Joseph D. Pierre, a doctoral learner under the direction of Professor Samuel M. Natale in the School of Business and Technology at Capella University, is conducting a research study and is inviting you to participate in it. The title of the study is Information Security Analysis: A Study to Analyze the Extent to which Information Security Systems can be Utilized to Prevent Intoxicated Individuals from Driving, and its purpose is to identify the potential of information security systems to help prevent automobile accidents caused as result of driver intoxication.

WHAT DOES PARTICIPATION IN THIS RESEARCH STUDY INVOLVE?

If you decide to participate in this study, Joseph Pierre, the researcher, will interview you. The interview will involve you responding to questions that seek to understand your knowledge relating to intoxication and driving, but are not interested in your dependency on alcohol or your personal history with the abuse of alcohol. This research is solely focused on preventing intoxicated individuals from driving. Your participation will take approximately 30 minutes. You will be audiotaped during your participation in this research, and the tape will be kept the through the official conferring of the doctoral degree.

WHY ARE YOU BEING ASKED TO PARTICIPATE?

You have been invited to participate because of the researcher's belief that you are interested in contributing to the prevention of intoxication related automobile accidents.

ARE THERE ANY RISKS INVOLVED IN THIS STUDY?

Although no study is completely risk-free, we do not anticipate any risks to you if you decide to participate in this study.

ARE THERE ANY BENEFITS TO PARTICIPATION?

The information collected may not benefit you directly; however, what is learned from this study may provide general benefits to information security system studies and business/public practices regarding the operation of motor vehicles.

WHAT HAPPENS IF THE RESEARCHER GETS NEW INFORMATION DURING THE STUDY?

The researcher will contact you if he/she learns new information that could change your decision about participating in this study.

HOW WILL THE RESEARCHER PROTECT PARTICIPANTS' CONFIDENTIALITY?

The results of the research study will be published, but your name or identity will not be revealed. In order to maintain confidentiality of your records, the researcher will use numeric/alpha coding generated by the qualitative software. Moreover, the researcher is the owner of the data and will keep the information secured. This information will be kept confidential and not shared beyond the researchers' Dissertation Committee. The information will be maintained through the official conferring of the doctoral degree.

WHAT HAPPENS IF A PARTICIPANT DOESN'T WANT TO CONTINUE IN THE STUDY?

Participation in this study is voluntary. If you choose not to participate or if you choose to withdraw from the study, you may do so at any time. There will be no penalty. It will in no way influence your present or your future.

WILL IT COST ANYTHING TO PARTICIPATE IN THE STUDY? WILL I GET PAID TO PARTICIPATE?

There are no costs associated with participating in the study.

WILL PARTICIPANTS BE COMPENSATED FOR ILLNESS OR INJURY?

You are not waiving any of your legal rights if you agree to participate in this study. But no funds have been set aside to compensate you in the event of injury. If you suffer harm because you participated in this research project, you may contact Joseph Pierre at 1-954-385-4875, or you may contact the Capella Human Research Protections Office at 1-888-227-3552, extension 4716.

VOLUNTARY CONSENT

By signing this form, you are saying (1) that you have read this form or have had it read to you and (2) that you understand this form, the research study, and its risks and benefits. The researcher will be happy to answer any questions you have about the research. If you have any questions, please feel free to contact Joseph Pierre at 1-888-227-3552 or joseph_pierre@bellsouth.net.

If you have any questions about your rights as a research participant or any concerns about the research process, or if you'd like to discuss an unanticipated problem related to the research, please contact the Capella Human Research Protections Office at 1-888-227-3552, extension 4716. Your identity, questions, and concerns will be kept confidential

Note: By signing below, you are telling the researcher "Yes," you want to participate in this study. Please keep one copy of this form for your records.

Your Name (please print):

____

Your Signature:

____

Date: ______________________________

INVESTIGATOR'S STATEMENT

I certify that this form includes all information concerning the study relevant to the protection of the rights of the participants, including the nature and purpose of this research, benefits, risks, costs, and any experimental procedures.

I have described the rights and protections afforded to human research participants and have done nothing to pressure, coerce, or falsely entice this person to participate. I am available to answer the participant's questions and have encouraged him or her to ask additional questions at any time during the course of the study.

Investigator's Signature:

Investigator's Name: Joseph D. Pierre

Date: April 1, 2010

Capella's IRB Approval

This research has been approved by Capella University's Institutional Review Board. Approval number: ________________; Effective dates: From: __________________ to _____________________. (*This information will be supplied by Capella University's IRB Office upon the approval of the IRB application*.)

APPENDIX D. INTERVIEW QUESTIONS

1. Would you prefer an information security system that detects intoxication or one that prevents a person from operating an automobile when intoxicated?

2. Do you believe that an information security system, which detects intoxication or prevents driving while intoxicated, would have a value to society?

3. What personal strengths and unique experiences do you think you bring to this research study?

4. What factors would influence your decision to implement an information security system in your vehicle?

5. What plan(s) have you used to evaluate your level of intoxication and ability to operate a motor vehicle?

6. What significant changes do you think this study will make in your life and the lives of others?

7. Who are the individuals or groups that you foresee this study to have significant impact on?

8. Would you purchase a vehicle with a new information security system feature that will prevent intoxicated individuals from driving?

9. Which of the following percentage increases would you be willing to pay for a new vehicle that has an information security system feature to prevent intoxicated individuals from driving?

    a) 5-10 percent
    b) 11-15 percent
    c) 16-20 percent
    d) 21-25 percent

10. Why would people want an information security system feature that would identify intoxicated individuals in their vehicles?

11. In the event that an individual is under the influence and the vehicle is ordered by information security system not to start, towing is inevitable. Should a heavy tax be placed on the individual?

12. Have you foreseen any government control as a result of this study? If not, why?

13. Should the installation of an information security system be strongly recommended for those charged with DUI?

14. In what way do you think an information security system feature for preventing intoxicated individuals from driving would be beneficial to the public?