MEASURING THE UTILITY OF A CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA) PROCESS FOR MISSION ASSURANCE

THESIS

Christy L. Peterson, Master Sergeant, USAF

AFIT/GIR/ENV/11-M04

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

.

AFIT/GIR/ENV/11-M04

MEASURING THE UTILITY OF A CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA) PROCESS FOR MISSION ASSURANCE

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Christy L. Peterson, BS

MSgt, USAF

March 2011

AFIT/GIR/ENV/11-M04

MEASURING THE UTILITY OF A CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA) PROCESS FOR MISSION ASSURANCE

Christy L. Peterson, BS

MSgt, USAF

Approved:

//signed//	15 Mar 2011
Michael R. Grimaila, PhD, CISM, CISSP (Chairman)	(Date)
//signed//	21 Mar 2011
Robert F. Mills, PhD (Member)	(Date)
//signed//	15 Mar 2011
Michael W. Haas, PhD (Member)	(Date)
//signed//	21 Mar 2011
Gina F. Thomas, PhD (Member)	(Date)

Abstract

Information is a critical asset on which virtually all modern organizations depend upon to meet their operational mission objectives. Military organizations, in particular, have embedded Information and Communications Technologies (ICT) into their core mission processes as a means to increase their operational efficiency, exploit automation, improve decision quality, and shorten the kill chain. However, the extreme dependence upon ICT results in an environment where a cyber incident can result in severe mission degradation, or possibly failure, with catastrophic consequences to life, limb, and property. These consequences can be minimized by maintaining real-time situational awareness of mission critical resources so appropriate contingency actions can be taken in a timely manner following an incident in order to assure mission success.

In this thesis, the design and analysis of an experiment is presented for the purpose of measuring the utility of a Cyber Incident Mission Impact Assessment (CIMIA) notification process, whose goal is to improve the timeliness and relevance of incident notification. In the experiment, subjects are placed into a model environment where they conduct operational tasks in the presence and absence of enhanced CIMIA notifications. The results of the experiment reveal that implementing a CIMIA notification process significantly reduced the response time required for subjects to recognize and take proper contingency actions to assure their organizational mission. The research confirms that timely and relevant notification following a cyber incident is an essential element of mission assurance.

Acknowledgement

First of all, I thank my family and friends for their unconditional love and support of my career and countless sacrifice while I attend AFIT.

I especially thank my thesis advisor Dr. Michael R. Grimaila, for his enthusiasm, expert insight, and guiding me throughout the thesis process. His dedication and work ethic went beyond the call of duty. I would also like to convey my sincere thanks to Dr. Robert F. Mills, Dr. Michael W. Haas and Dr. Gina F. Thomas, for their commitment and guidance in my research.

Additionally, I would also like to express my sincere appreciation to Brig Gen Paula G. Thornhill and Lt Col Shane Knighton, for giving me the opportunity to attend AFIT. And, finally, thank you to my fellow students for their teamwork; my many professors for providing an invaluable education and making my academic journey truly enjoyable.

Christy L. Peterson

Table of Contents

List of Figures

FIGURES PAGE

List of Tables

TABLES PAGE

MEASURING THE UTILITY OF A CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA) PROCESS FOR MISSION ASSURANCE

I. Introduction

Information is a critical asset, on which organizations depend to meet mission objectives. Military organizations, in particular, have embedded Information and Communications Technologies (ICT) into their core mission processes as a means to increase their operational efficiency, exploit automation, improve decision quality, and shorten the kill chain (Grimaila et al., 2009a). However, the increasing dependence upon ICT has resulted in an environment where an incident involving a cyber resource, hereafter called a "cyber incident," can result in severe mission degradation or failure with catastrophic consequences to life, limb, and property (Grimaila et al., 2010). Even organizations that build and maintain robust security capabilities will enviably experience a cyber incident resulting from external attacks, insider attackers, natural disasters, human errors, infrastructure degradation, or equipment failure (Grimaila et al., 2007). When a cyber incident occurs, it is essential to notify all decision makers whose missions are potentially affected in a timely and relevant manner in order to assure mission success.

1.1 Background

In a military context, information is continuously being collected, processed and analyzed, aggregated, stored, and distributed for multiple purposes, including support of situational awareness, operations planning, and command decision making (Grimaila et al., 2008a). Military organizations exhibit unique attributes such as high levels of

sustained information interaction among multiple entities, distributed time sensitive decision making, and the criticality of consequences that may result from ill-informed decision making. In some cases, operations have critical time interdependencies which require significant planning and coordination to ensure the success of the mission objectives. The timeliness of the information used in the decision making process dramatically impacts the quality of command decisions. Hence, the documentation of information dependencies is essential for the organization to gain a full appreciation of its operational risks (Grimaila et al., 2009b; Grimaila et al., 2010). Information dependencies encompass not only the information itself, but also all of the ICT systems and devices used to store, process, transmit, or disseminate the information. Further, one must understand how the information supports the organizational objectives and how the information value changes as a function of time in relation to other mission activities. While eliciting and documenting this information is not a trivial task, it is an essential prerequisite for mission assurance so that mission risk management can be performed (e.g., architect missions to be more resilient to cyber attacks prior to mission execution and inform contingency decision making when the mission is underway) (Grimaila et al., 2010).

Unfortunately, military organizations today struggle to maintain awareness of the ICT systems they depend on for day-to-day operations. Several underlying problems have been identified: 1) lack of dynamic risk assessment process, 2) lack of documentation that explicitly identifies information assets and their mission value, 3) lack of timely and relevant notification of downstream information consumers following an information incident, and 4) poor to non-existent knowledge continuity (Grimaila et

al., 2009b). Most military organizations do not collect, document, maintain, refine, disseminate, and exploit knowledge of mission-to-information dependencies effectively. However, the ability to efficiently identify, quantify, document, and maintain a formal understanding of mission-to-information resource risk is of paramount importance to provide decision makers with actionable information needed to evaluate their mission risk as a function of their ICT dependency. This insight is needed to proactively design robust missions, develop and maintain situational awareness following an incident, take appropriate contingency measures to assure mission success, and to retain and exploit the "lessons learned" gained from experience (Grimaila et al., 2010; Hale et al., 2010).

1.2 Problem Statement and Purpose of Research

This research seeks to measure the utility of timely and relevant notification following a cyber incident in a model operational setting. The underlying premise of the research is that timely and relevant notification will enable appropriate contingency actions to be taken sooner, improving operational outcomes and mission assurance. This research is part of the Cyber Incident Mission Impact Assessment (CIMIA) project sponsored by the Air Force Research Laboratory which is focused upon improving the timeliness and relevance of cyber incident notifications within the USAF through the development of an incident notification Decision Support System (DSS). The objectives of the research will be attained through human subject experimentation conducted in a model hypothetical operational Air Force unit. This research seeks to objectively evaluate the effectiveness and efficiency of cyber incident notifications both in the "as is" case and in the presence of a proposed CIMIA incident notification process. In doing so,

the focus is upon understanding how information dependency knowledge can be used following a cyber incident to improve incident response and decision making to assure mission operations.

1.3 Hypothesis

The primary goal of the CIMIA project is to provide timely, accurate, secure, and relevant notification from the instant an information incident is declared, until the cyber incident is fully remediated (Grimaila et al., 2009a). There has been no quantitative research that has been conducted to measure the effect of timely and relevant notification for cyber incident response on mission objectives. The purpose of this experiment is to remedy this deficiency by designing an experiment in a realistic mission environment that will provide the empirical evidence necessary to test the main hypothesis. The main hypothesis for this research was developed based on the notion that it is important to promptly notify decision makers within an organization about cyber incidents in a timely manner so they can take appropriate contingency measures and assure their mission. The null and alternate hypotheses are as follows:

H_o: There is no statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

H_a: There is a statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

If there is a statistical difference between the existing and CIMIA incident notification processes, it is expected that the proposed CIMIA incident notification process will result in a reduction in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents improving mission assurance.

1.4 Research Goals

The primary goal of this research is to determine how the proposed CIMIA DSS would impact mission objectives by evaluating its impact upon the time required to identify a cyber incident and take appropriate contingency measures to assure the organizational mission. This research goal complements other CIMIA research elements focused upon identifying ideal candidate DSS technologies conducive for incident notification (Woskov, 2011) and developing an incident notification architecture that links together mission dependent entities (Miller, 2011). Lastly, this research seeks to demonstrate the importance of explicit documentation identifying information resources and their mission value. One result of this research would be to replace the manual effort required to coordinate with the affected system owners and custodians to determine which organizations are potentially affected by the incident. As a result, this research effort can be operationalized by infusing a reliable DSS into the workplace, where deemed appropriate. By doing so, organizations could potentially benefit from real-time notification following an information incident. In addition to improved decision making, the DSS may also provide knowledge continuity for mission owners.

1.5 Thesis Structure

This research is organized into five chapters with the first chapter providing the introduction. Chapter 2 is a literature review of pertinent background information related to this research. It then discusses the proposed CIMIA incident notification process, the USAF incident notification process, and some key concepts that support the CIMIA methodology. Chapter 4 presents an analysis of the experiment of the study that is used to determine that the value of the proposed CIMIA incident notification process within military environments. Chapter 5 provides the conclusion of the research and offers areas for future study in the research domain.

II. Literature Review

2.1 Introduction

This chapter acquaints the reader with several key concepts and issues pertaining to the research. First, definitions and perspectives on situation awareness, decision making and human performance are reviewed. Next, the current Air Force (AF) cyber incident notification process and proposed alternative incident notification process, CIMIA, are discussed. Finally, this chapter concludes by discussing the key concepts that support the proposed CIMIA methodology.

2.2 Situation Awareness

The concept of Situational Awareness (SA) has its roots in the fields of air traffic control, airplane cockpit control, military commands and control, and information warfare. SA can be traced back to World War I, where it was recognized as a crucial component for crews in military aircraft (Endsley 1996; Endsley & Jones, 1997, 2001; Endsley & Garland 2000). Today, SA is one of the most prominent research topics in the aviation Human Factors field; this interest grew in the mid-1980s and increased through the 1990s partially through advancements in technology (Endsley & Garland, 2000). SA can be achieved by people alone, while the human factors approach often requires the integration of a specific technology, like automation. Although technology can be useful to detect and report incident indictors or intuitions, Endsley argues that people are frequently slow in detecting that a problem has occurred which necessitates human intervention (1996). The author identified that additional time is spent figuring out the

situation and course of action, ultimately delaying human performance that can result in slight delays to catastrophic failures with major consequences (Endsley, 1996).

While several limitations have been identified and discussed regarding problems with automation and automation failures, (Ephrath & Young, 1981; Kessel & Wickens, 1982; Wickens & Kessel, 1979; Young, 1969; Endsley 1996) Endsley (1996) points out that the use of automation can also be beneficial to achieving a higher level of SA with several new approaches to automation. One daunting challenge is to keep the "human in the loop" (Endsley, 1995). Endsley suggests one approach would be "to optimize the assignment of control between the human and the automated system by keeping both involved in the system operation" (1996). Furthermore, to reduce negative impact on the operator's SA (lower levels), a level of automation should be determined while keeping the human actively involved in the decision making loop (Endsley, 1996).

According to Endsley, decision makers' SA is a major factor driving the quality of the decision process (1997). In other words, SA influences the decision making process; it is "represented as the main precursor to decision making" (Endsley & Garland, 2000, p. 8). Although SA may mean many things to many people, simply put, SA is being aware of what is going on in one's surroundings, in the context of the individuals' objectives. Endsley's definition is widely recognized and defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" (Endsley, 1988, p.97). The "elements" of SA "vary widely between domains, the nature of SA and the mechanism used for achieving SA can be described generically" (Endsley, 2000, p.5). SA is described as being dynamic, hard to maintain, and easy to lose. Although SA is a

challenging to maintain, it is central to good decision making and performance (Endsley, 2000). In cyberspace, decision makers face the challenge of maintaining a high level of situational awareness to function in a timely and effective manner following a cyber incident. SA in cyberspace is crucial to mission success to allow decision makers to understand what matters. They must be able to continuously depend on critical ICT and avoid working with tampered, corrupt, or missing information. Therefore, SA in cyberspace must be maintained in order to ensure information dominance in cyberspace.

2.3 Maintaining Situation Awareness

A number of factors have been shown to influence the process of acquiring and maintaining SA. Endsley describes three processes: perception, comprehension, and projection (Endsley, 1995):

- Level 1 SA - Perception of the elements in the environment
- Level 2 SA – Comprehension of the current situation
- Level 3 SA – Projections of future status

SA provides "primary basis of for subsequent decision making and performance in the operation of complex, dynamic systems." At the lowest level, perception is considered fundamental to the process to reduce the odds of developing a model of a given situation; "it involves perceiving critical factors in the environment" (Endsley, 1988, 1995). At level 2 SA, a mental model is developed which are observations that correspond with knowledge and experience: "understanding what those factors means, particularly when integrated together in relation to the person's goals (Endsley, 1988, 1995). In level 3 SA, understanding from the previous level enables projections of a future state of the

environment: “an understanding of what will happen with the system in the near future” (Endsley, 1988, 1995). Endsley (1998) reported that “these higher levels of SA are critical for allowing a decision maker to function in a timely and effective manner” (p. 2).

SA is strongly related to the decision making process (Endsley, 2000). The theoretical model of SA shows the relationship between SA and decision making (Figure 1). Endsley says that SA must precede decision making because the operator has to perceive a situation in order to have a goal. Adams et al (1995) suggest an inter-relationship between SA and the processes used to achieve that knowledge. Smith and Hancock (1994) argue, but emphasize that “SA is up-to-the minute comprehension of the task relevant information that enables appropriate decision making stress” (p. 3).

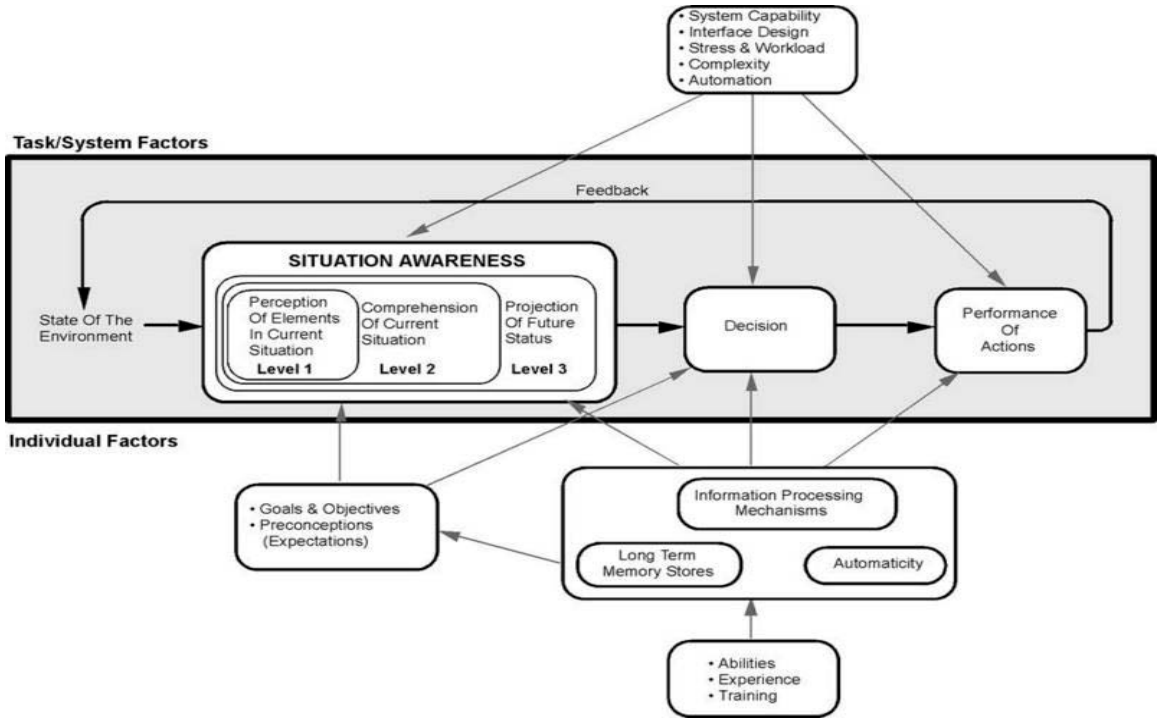


Figure 1. Theoretical Model of Situation Awareness (adapted from Endsley & Garland, 2000)

2.4 Cyber Attacks and Situational Awareness

A cyber attack that compromises the protection of information can have catastrophic affects to mission objectives if the attack goes undetected, or the attack is interpreted as business as usual (e.g. software glitches, computer crashes, ordinary maintenance, frequent unavailability, etc.) which seems normal (Endsley & Jones, 2001). Endsley (2001) proposed a model that "incorporates the ways in which information attacks can effectively disrupt human decision making at various points in information processing" (p.6) (Figure 2). By carefully examining not only the cues that might depict an attack to information systems, but also how human observers will be affected by such cues, one can develop more robust systems for protecting against disruptions and information attack (Endsley & Jones, 2001). The model helps to explain the effects that disruptions can have on SA and decision making in four major categories: 1) disruptions that affect information pre-processing; 2) disruptions that affect prioritization and attention; (3) disruptions that affect confidence in information, and (4) disruptions that affect interpretation (Endsley & Jones, 2001). Although disruptions can range from information overload to cyber attacks or malicious activity, "the intention of the model is to help direct efforts at creating systems for supporting decision makers in effectively comprehending and dealing with information attacks and normal disruptions" (Endsley & Jones, 2001). Further, the author explains that the model "is being used to develop decision support tools for detecting such attacks within the context of normal disruptions and interruptions" (Endsley & Jones, 2001).

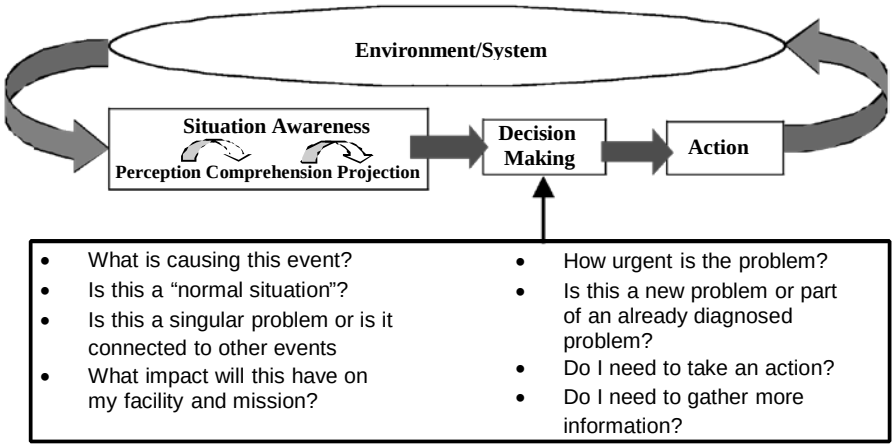


Figure 2. Decision Content for Detecting and Diagnosing Information Attacks (adapted from Endsley, 2001)

2.5 Human performance and automation

Automation shifts human performance from a physical workload to a more cognitive and perceptual activity which raises a host of human factor issues dealing with situation awareness, vigilance, stress and workload (Endsley, 1996; Parasuraman, 1987; Wickens & Carswell, 1997). There are several cases in which operators do not detect critical state changes when acting as monitors of automated systems for a number of reasons (Ephrath & Young; 1981; Kessel & Wickens, 1982; Wickens & Kessel, 1979; Young 1969). Monitoring failures have occurred irregardless of the complexility level of the tasks. According to Wickens and Carswell (1997), information processing lies at the heart of human performance. As humans interact with systems, "the operator must perceive information, transform that information into different forms, and take actions on the basis of the percievd and transformed information" (p.90). Information processing occurs in stages from perceptions in the environment to acting upon that envirnoment.

Wickens' model (1992) in Figure 3 depicts the stages that develop in an operators perception of the environment based on sensory processing to attend to, select, organize, and interupt information in order to meaningfully recognize objects and events in the environment. Wickens' explains operators selectively focus on and attend to specific stimuli that are most relevant to their goals or purpose (1992; Wickens and Carswell, 1997). Attendion initaties information processing and short-term/working memory. Information which is attended to enters either short-term or working memory where thinking occurs from external stimuli. Internal thought processes generate reason, problem solve or make decisions to initate responses and actions. Decision making requires the decision maker to make a choice between several alternatives.

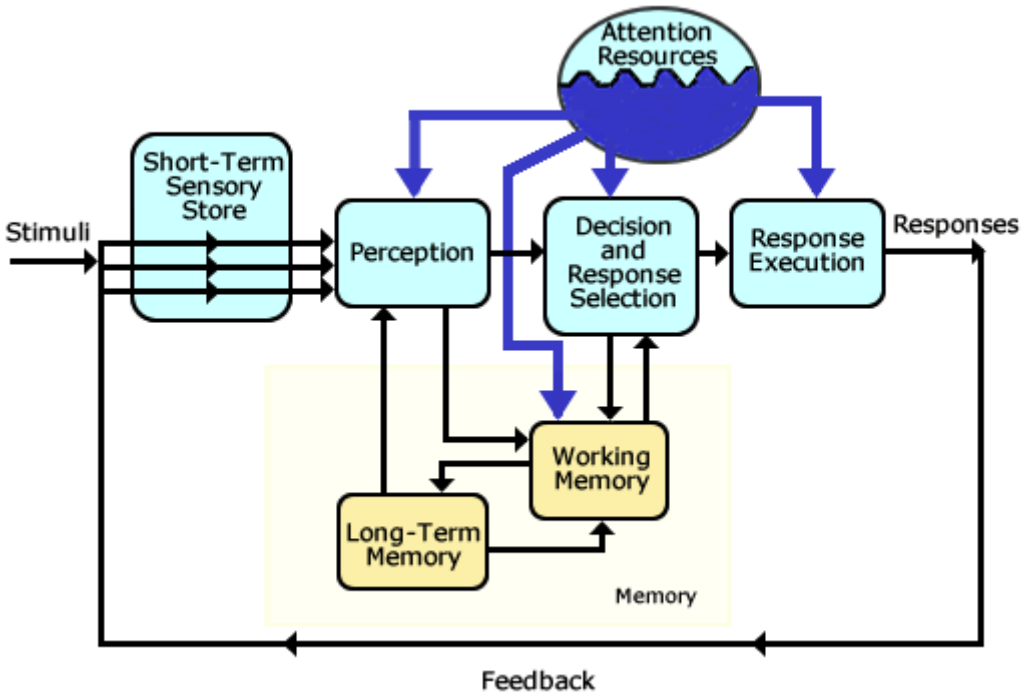


Figure 3. A model of human information processing (adapted from Wickens, 1992)

2.6 Human Decision Making

Decision making is a subset to the information processing that draws upon sensory inputs. A paper by Lehto, "Decision making," discusses that as decisions grow more complex, information processing actually becomes part of decision making and methods of decision support that help decision makers process information become of growing importance (1997). Therefore, if automation is used to aid higher levels of SA for decision makers to avoid undesirable consequences, the effects of automation support must be carefully considered relative to information processing. The CIMIA incident notification process is an alternative methodology to the incident notification process utilized within the USAF to assist decision makers' to maintain awareness of critical ICT following a cyber incident.

2.7 CIMIA Incident Notification Process

The CIMIA project has proposed a different approach to deal with incident notification following cyber incidents (Grimaila et al., 2009a). CIMIA proposes a conceptual methodology for a defensive cyber damage and mission impact assessment to provide decision makers situational awareness of the impact to mission capability following a successful cyber incident; impact is a function of CIA (Fortson, 2007; Fortson et al., 2007; Grimaila et al., 2007; Grimaila et al., 2008a; Grimaila et al., 2008b; Grimaila et al., 2009a; Grimaila et al., 2009b; Grimaila et al., 2010; Hale et al., 2010). Instead of a technology-based focus, an information asset-based focus is more conducive to document mission-to-information dependencies. Organizations must employ a robust

risk management strategy that accounts for the mission, the information that is required for mission success, and the ICT used in mission fulfillment in order to support risk tradeoffs and contingency decision making. The use of a risk management process allows decision makers to explicitly identify and document critical ICT systems (Grimaila et al., 2009a; NIST, 2002; NIST, 2010; AFI-33-138, 2010). This is extremely important when decision makers need an accurate assessment of how a cyber incident impacts their mission.

By accomplishing a risk assessment, decision makers would achieve pre-incident activities identified in the CIMIA incident notification process (Figure 4). These pre-incident activities deliberately identify and document all critical information processes and assets that affect mission accomplishment for the organization. As Fortson (2007) noted, this research advocates an asset-focused approach that takes into account the information assets impact to the mission long before an incident occurs**.** According to Grimaila et al. (2008b):

> The identification and valuation of information dependencies must occur before an incident occurs. Identification of an information dependency inherently implies there is a supplier (source) of the information and a consumer (sink) of the information. In some cases, both the information supplier and consumer may be within the same organization, in others they may be in different organizations. Regardless, each organization must first identify, document, and value its information dependencies. This can be accomplished through an information asset-focused risk assessment or using other similar information asset profiling techniques. (NIST 2002; Alberts and Dorofee, 2003, 2005).

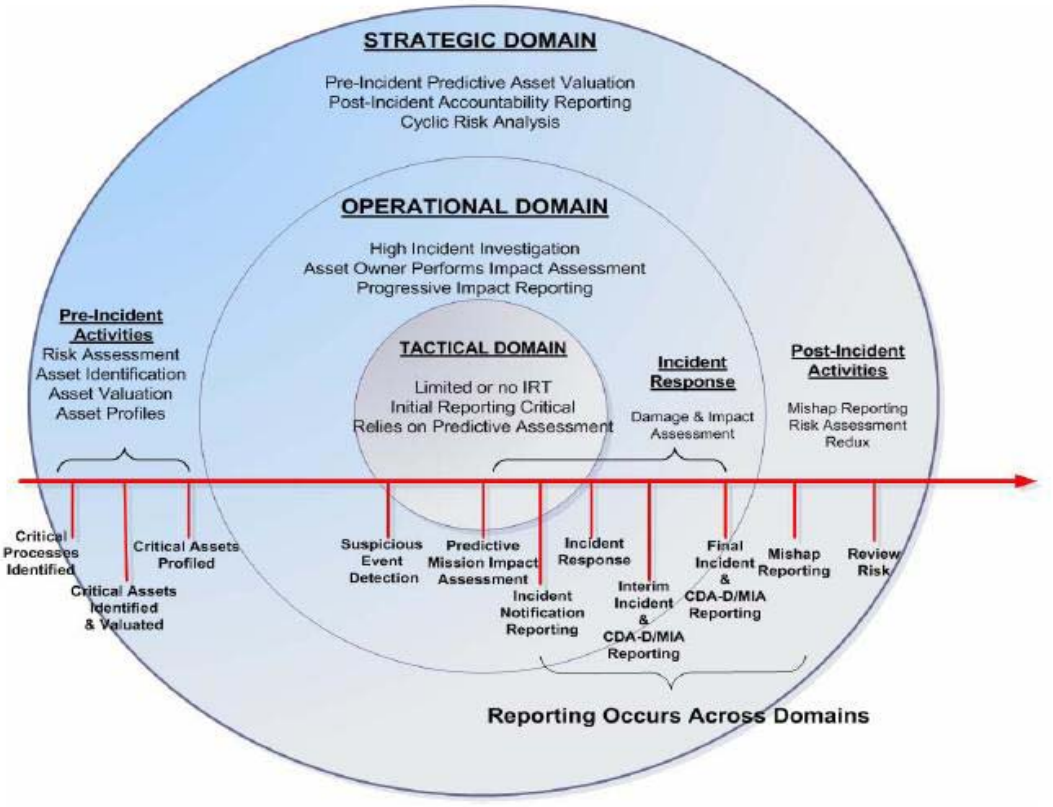


Figure 4. Defensive Cyber Damage and Mission Impact Assessment Time (Fortson, 2007)

While the USAF notification process focuses on pushing cyber incident notifications to all organizations in the Air Force Network Operations hierarchy, the CIMIA incident notification process is focused on enabling downstream consumers to discover and directly subscribe to the status of the mission critical ICT systems they depend on to attain their mission objectives. In the proposed CIMIA incident notification process, when an information incident occurs, the downstream consumers are notified in near real-time that an event has occurred that may impact their missions as a consequence of the loss, or potential loss of, information security (Grimaila et al., 2009a). The notification will "supply meaningful mission impact assessment and enable accurate

predictive situational awareness, and develop a timely understanding of possible adversarial intent during a cyber incident" (Grimaila et al., 2008b, p.9). Unfortunately, the existing USAF cyber incident notification process does not provide the ability to uniquely identify and notify decision makers who are critically dependent on the affected ICT systems. Table 1 presents a comparison chart of the two incident notification processes.

Table 1. Incident Notification Process Comparison Chart

Incident Notification Process	**NOTAM (USAF)**	**Pop-up (CIMIA)**
Methodology	Pushes incident notifications to all organizations in the Air Force Network Hierarchy	Enables downstream consumers to discover and directly subscribe to the status of mission critical ICT systems
Timeliness	Disseminates to subordinate organizations within 24 hours	Disseminates to downstream consumers in near real-time that an event occurred
Relevance	Incident notification is informative in nature; primarily limited to technical metrics	Provides meaningful mission impact and potential mission impact to decision makers following cyber incident
Process	Focus upon the protection of systems and network infrastructure elements	Focus upon information stored, processed, and transmitted within the infrastructure
Means of communications	C4 NOTAM disseminates via email	Cyber incident notification disseminates via a mockup pop-up

2.8 Current Cyber Incident Notification Process

When a cyber incident occurs, it is essential to notify decision makers whose missions are affected in a timely and relevant manner to assure mission success. AFI 33-138 explains the process used by Air Force Network Operations to generate, disseminate, acknowledge, implement, track, and report network compliance end status information. This document details the use of Time Compliance Network Orders for communicating downward-directed operations, security and configuration management-related orders issued by the Air Force Network Operations Security Center. Notification following a cyber incident occurs using a Command, Control, Communications, and Computers Notice to Airmen (C4 NOTAMs). C4 NOTAMs are informative in nature and are the primary means for notifying organizations that a network incident has occurred which may impact their mission operations. C4 NOTAMs are disseminated via email to organizations required to be notified in accordance with AFI 33-138. The C4 NOTAM, in Figure 5, is broadcast to all organizations identified as potentially affected by the incident. As a consequence, some organizations may be notified who are not dependent upon the affected ICT systems (Grimaila et al., 2009b). Worse, some organizations may not be identified as dependent on the affected resource even though they are directly or indirectly critically dependent upon the affected ICT systems. Thi1s situation prevents a decision maker from acquiring a meaningful level of SA on the status of critical ICT.

UNCLASSIFIED//FOR OFFICIAL USE ONLY
ACKNOWLEDGEMENT DATE: 13 JAN 2011
INTITAL RELEASE TIME: 13 0455Z JAN 11
TCNO TRACKING NUMBER: NOTAM C4-N AFNOC 2010-100-001
ORIGINATING AGENCY: 663 OC/CYCC
TYPE: INFORMATIVE
CATEGORY: NOTAM
PRIORITY: SERIOUS
SUBJECT: VULNERABILITY IN INTERNET EXPLORER COULD ALLOW REMOTE CODE EXECUTION (981374)
MISSION IMPACT: LOSS OF SYSTEM AVAILABILITY/INTEGRITY
EXECUTIVE SUMMARY:
VULNERABILITY EXISTS IN MICROSOFT INTERNET EXPLORER THAT COULD ALLOW A REMOTE ATTACKER TO RUN CODE OF THE ATTACKER'S CHOICE OR PERFORM A DEINAL-OF-SERVICE (DOS) AGAINST A VULNERABLE SYSTEM. MS INTERNET EXPLORER IS A WEB BROWSER FOR MICROSOFT SYSTEMS.
SYSTEM(S) AFFECTED:
WINDOWS XP SP 2 AND WINDOWS XP SP 3
WINDOWS XP PROFESSIONAL X64 EDITION SP 2
WINDOWS SERVER 2003 SP 2
WINDOWS SERVER X64 EDITION SP 2
INTERNET EXPLORER 6 SP 1 FOR WINDOWS XP SP 2
INTERNET EXPLORER 7 FOR WINDOWS XP SP 2
INTERNET EXPLORER 7 IN WINDOWS VISTA, WINDOWS VISTA SP 1, WINDOWS VISTA SP 1
ACTION:
PATCHES ARE NOT AVAILABLE AT THIS TIME. ORGANIZATIONS MAY APPLY THE MS ADVISORY WORK AROUNDS TO TEMPORARILY ALLEVIATE THIS PROBLEM. A TCNO WILL BE RELEASED ONCE MS ISSUES PATCHES FOR THIS VULNERABILITY.
NOTE: ALL WORK AROUNDS WILL IMPACT OPERATIONS IN SOME WAY. PLEASE READ THE WORK AROUNDS CAREFULLY.
RISKS ASSOCIATED WITH UNPATACHED SYSTEMS: UNAUTHORIZED ACCESS TO COMPROMISED SYSTEMS.
REPORTING REQUIREMENTS:
NONE
REMARKS:
PLEASE CONTACT 663 CS HELP DESK - IF YOU HAVE QUESTIONS AND/OR CONCERNS AT 6503

Figure 5. C4 NOTAM

Instead of utilizing email, the proposed CIMIA incident notification process is disseminated via a pop-up to downstream consumers who subscribe and pull the status of the critical ICT they depend on. Pop-ups are known to visually capture that attention of an operator while using a computer. They are a form of an interruption that captures the attention of an operator. Some research suggests that interruptions (e.g. warnings, alerts, reminders, notifications, etc.) (Bailey et al., 2000) slows an operators' performance on interrupted tasks; however, some evidence exist that an interruption may actually speed up the completion of a task (Zijlstra et al., 1999). Hence operators are affected by interruptions in different ways. For this reason, it is important to identify key features that may impact the effectiveness of the interruption. Fischoff et al. (1998) paper, "What Information Belongs in a Warning?" suggests design of messages should focus on the "critical gaps between what consumers know and what they need to know" (p. 664). Because interruptions are typically viewed as communications whose purpose is to inform and influence behavior, the mockup of the pop-up was based on Laughery and Wogalter's (1997) eight criteria for design and assessment of warnings. They are:

1) Attention – should be designed to attract attention;

2) Hazard information – should contain information about the nature of the hazard

3) Consequence information –should contain information about the potential outcomes

4) Instructions – should instruct about appropriate and inappropriate behavior

5) Comprehension – should be understood by the target audience

6) Motivation – should motivate people to comply

7) Brevity – should be brief as possible

8) Durability – should last and be available as long as needed (p. 1195)

In addition to this criterion, the challenge was to make the pop-up salient, attract the operator's attention, and to make the information seem relevant. Therefore, special consideration was given to the size, color, signal words, and content of the pop-up shown in Figure 6. The reminder of this Chapter discusses some of the key concepts that support the CIMIA methodology.

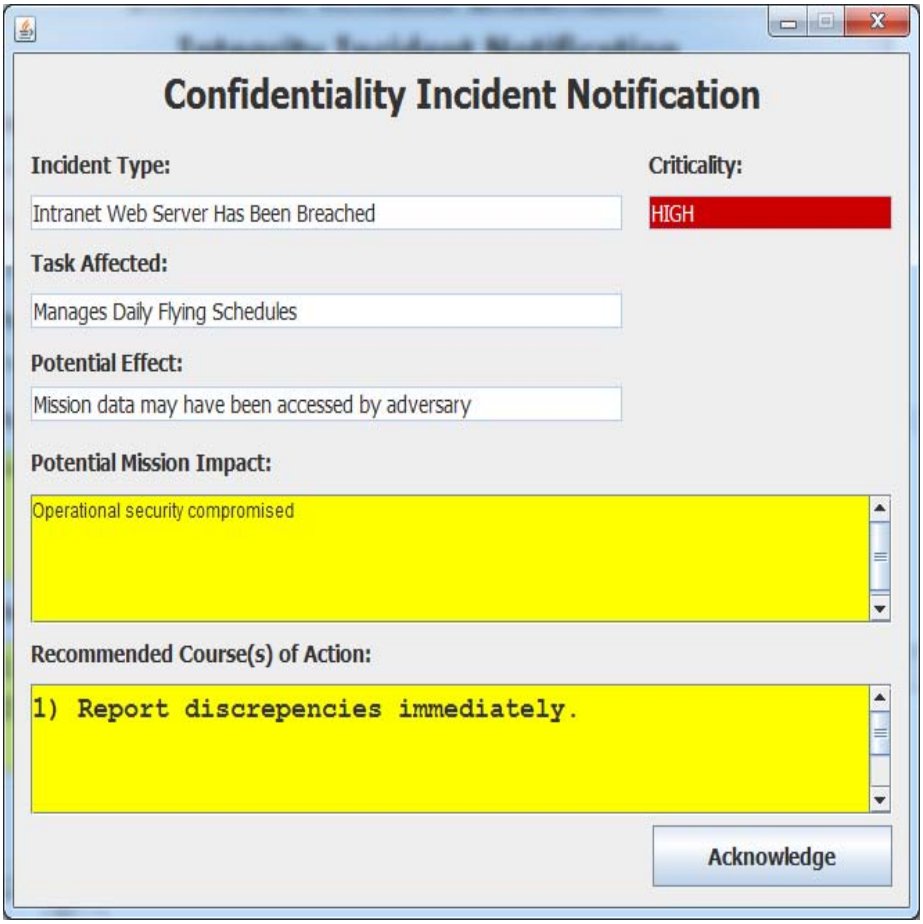


Figure 6. CIMIA incident notification

2.9 Information Security

The widespread use of information and communications technology (ICT) has revolutionized the communication process and with it the significance and implications of information security. Today, information has become more crucial than ever for decision makers to maintain mission awareness. Decision makers depend on information to meet their mission objectives; they make decisions based on the information available at the time. Mission objectives cannot be achieved with erroneous information. Clearly, information must be protected, but knowing what information to protect is a challenge. Although information is a basis for decision making, all information cannot be deemed critical. Because critical information is valuable, organizations must recognize information security as a top priority and carefully consider protecting critical information that supports mission objectives.

The Air Force uses security measures to protect and defend information and information systems through both OPSEC and information assurance (Department of the Air Force, 2002). Joint Publication (JP) 3-54, *Operations Security*, 1997, defines OPSEC as a "process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) indentify those actions that can be observed by adversary intelligence systems; b) determine what indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation" (1997, p.26). It explains that planning and

execution occur as part of the commander's command and control warfare efforts in focusing on identifying and protecting critical information to increase mission effectiveness (DoD, 1997). Information assurance, on the other hand, is defined as "those measures to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation" (Department of the Air Force, 1998, p.17). This definition is closely related to the definition of information security, which is an event that appears to be a breach of the organization's information security countermeasures (i.e. systems that can prevent or mitigate the effects of, threats to a computer, server, or network). In International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) Information Security Management 27000, information security is defined as the "preservation of confidentiality, integrity and availability of information" (2009, p.3). Information security is the process of protecting information. It is the protection of information and ICT against unauthorized access or modification on information. "The adverse impact of a security event can be described in terms of loss or degradation of any or a combination of any, of the following three security goals: availability, integrity, and confidentiality" (NIST, 2002, p.22). These three security goals, Confidentiality, Integrity, and Availability (CIA) are considered the core principles of information security, and are commonly referred to as the CIA triad. The National Institute of Standards and Technology (NIST), *Special Publication 800-37 rev 1*, Appendix B Glossary, defines CIA as:

- Confidentiality – Preserving authorized restrictions on information access and disclosure to prevent disclosure to unauthorized individuals, entities or processes, including

means of protecting personal privacy and propriety information

- Integrity – Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity

- Availability – Ensuring timely and reliable access to and use of information (2009)

Information can reasonably be called secure when confidentially, integrity, and availability of information are present. Mutually, information security and information assurance share the common goal of protecting the CIA of information. However, "information assurance process is applied through technology-based activities" (Department of the Air Force, 1998, p.17) while information security should be asset-based focused.

2.10 Information Asset

The CIA of information is critical to organizations' missions. Therefore, organizations cannot form protection strategies that are focused solely on infrastructure. Instead, an information asset-based focus is more conductive to protecting critical information that supports the mission. "Information should be the central focus in understanding mission impact because it holds relevance and value as knowledge to decision makers in the organization" (Grimaila et al., 2009a). An information asset is "knowledge or data that has value to the organization" (ISO/IEC, 2009, p.3) or "any information that has enterprise value and is created, managed, or accessed during the operation of the organization" (AFPD 33-3, 2010, p.9). Having an information asset-

based focus allows organization to control risk with respect to protecting its information assets. Achieving comprehensiveness in identification of assets is important because perpetrators often look for assets and vulnerabilities that defenders have not recognized (Parker, 2008). Hence, vulnerabilities in one area can have significant impact to related mission interdependencies.

2.11 Criticality of Information

The value of any information is determined by the person using the information; it does not necessary have to be the decision maker. AFI 31-401, *Air Force Information Security Program*, advocates for protection of Air Force information by "delegating authority to the lowest level possible" and "focusing on identifying and protecting only that information that requires protection" (2005, p.7). Delegating authority down to the lowest level places the responsibility of protecting information on the information owners. According to the Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, 2006, an information owner is an "official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal." Along with many others, information owners must be involved in this process to specify the criticality of information to ensure the appropriate information security countermeasures (Pipken, 2008). The type and amount of protection required depends on the nature of the information and its usage. As appropriate, the protection of information varies between organizations; therefore, information owners should determine what protection their information requires based on criticality. It is

important for owners of information to inform those who access, use, and depend on their information to understand the level of protection required, to implement appropriate security countermeasures, and to recognize information incidents when they occur, in order to take action. In addition, the determination of criticality is not solely based on the information owner; instead, information consumers also must determine the criticality for the ICTs on which they depend on.

According to AFI 33-129, *Web Management and Internet Use*, 2010, critical information is "sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information." Information alone may not seem important, but every little bit of information is a puzzle piece. In order to protect mission-to-information dependencies, organizations must use a risk-based approach to determine the consequences of having inadequate protection before an information incident occurs. All ICT must include security controls that reflect the value of critical information processed on the system. The DoD and the Air Forces have done a commendable job in establishing directives, policies, procedures, and guidance for protecting information. However, despite these efforts, ICT are far from being secure. Protecting against an information incident even on a small scale is challenge for organizations to accomplish.

Organization cannot reply on a small set of protective technologies to protect critical ICT that support mission objectives. ICT are constantly at risk of cyber attacks that compromise confidentiality, integrity, and availability. An adversary would like nothing more than to gain access to critical ICT on which decision makers depend to maintain mission success. Therefore, organizations must employ a robust risk

management strategy that accounts for the mission, the information that is required for mission success, and the ICT used in mission fulfillment in order to support risk tradeoffs and contingency decision making.

The scope of the problem with protecting critical information is identifying what information to protect. Therefore, organizations must look at the information that directly supports mission objectives to apply adequate protection countermeasures. This can be achieved by using a systematic approach, including risk management principles, to identify critical information and associated risks. Otherwise, the lack of awareness could lead to information incidents that could compromise the mission. Although insufficient resources exist to fully secure ICT, organizations can take steps to mitigate risks and improve their current state.

2.12 Risk Management

No organization is immune to risk; in fact, risks are constantly changing, which requires organizations to have a proper balance of control to achieve risk management. An organization implements a risk management program to reduce negative impact on its ability to perform the mission (NIST, 2010). The goal of the risk management process is to help organizations manage their risks to an acceptable level. It is recognized as a tool that organizations can use to protect invaluable critical information and better manage ICT and their risks. "Risk management is the process that allows IT managers to balance operational and economic cost of protective measure and achieve gains in mission capability by protecting IT systems and data that support their organizations' missions" (NIST, 2002, p.4). Decision makers must make a commitment to understand and include

risk management in their decision making process to determine the extent of potential threats and risks associated with IT systems (NIST, 2002). While this process is complex and constantly changing, it must be an organization wide effort. The rapid growth in technology and information sharing has increased the risk to critical information being compromised. Obviously, if decision makers decide not to execute risk management principles because the cost outweighs the gain, they are exposing the organization to risk. Organizations use risk management to identify what risks the organization is exposed to then decide which risks need immediate attention and which risks are acceptable.

There are several different definitions of risk. According to ISO/IEC 27000, risk is the "combination of the probability of an event and its consequence" (p.4). NIST 800-30, *Risk Management Guide for Information Technology Systems*, 2002, describes risk as the net "negative impact of the exercise of a vulnerability, considering both the probability and the impact of the occurrence" (p.1). Finally, risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset) (NIST, 2002). While there are many different meanings of risk, risk-related events either have a positive or negative deviation from what is expected. Although organizations should assess risk to determine the extent of potential threats and risks associated with ICT, the process can be extremely labor intensive, time consuming, and require periodic updates when mission objectives change.

2.13 Risk Assessment

While risk management processes are challenging, they are crucially important to identify risks and determine optimal protection strategies. The implementation of risk

management in every organization is different. Organizations must develop strategies that can be translated and tailored to their organizational mission. The risk assessment process selected must provide an accurate assessment of the mission risk. According to DoDD 3020.40, *DoD Policy an Responsibilities for Critical Infrastructure*, 2010, risk assessment is a "system examination of risk using discipline processes, methods, and tools." From this perspective, it is the necessary actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities. Conducting the assessment provides an environment for decision makers to evaluate and prioritize risk continuously and to recommend strategies to remediate or mitigate those risks (DoD, 2010). NIST 800-30 describes risk assessment as the first process in the management methodology. It is a process that identifies risk, assesses risk and takes steps to reduce risk; it encompasses identification and evaluation of risk and risk impacts, and recommendation of risk-reducing measures. Using this approach produces a value for IT assets and resources effect based on the potential mission impact (e.g. the criticality, and sensitivity of the IT system components and data) (NIST, 2002). ISO 31000 recognizes that organizations operate in an uncertain environment. Every decision made by a decision maker involves some level of risk. It defines risk assessment as a process that is made up of three processes:

- risk identification, a process used to find, recognize, and describe risk that could affect mission objectives;
- risk analysis, a process that is used to understand the nature, source, and causes of identified risk and estimate level of risk; and
- risk evaluation, a process used to compare analysis results with risk criteria to determine whether or not a specific

> level of risk is acceptable or endurable to mission objectives (ISO, 2009 p.18)

As information continues to become a critical asset in organizations, it must be protected against various sources of unwanted access, external attacks, malicious insiders, natural disaster, accidents and/or equipment failure and from within, or external to, the organizational boundary (Grimaila et al., 2009a). All the information held within organizational boundaries is subject to cyber attacks. Organizations must prepare for and operate through cyber degradation or attack. A risk assessment can better prepare an organization for an information incident. The quality of the assessment depends on the accuracy of information collected in each step. NIST advocates for a risk assessment methodology, discussed above, that incorporates nine primary steps (Figure 7). Although the risk assessment process is extensive, at a minimum, organizations should complete the first step, System Characterization, to manage risk. In the first step, an organization can identify critical ICT resource dependencies, the downstream consumers on these ICT resources, and the valuation of systems in terms of how they support mission objectives. This information plays a vital role analyzing the impact of an information incident on the organization's mission. More specifically, when an information incident occurs, decision makers at all levels whose missions are affected can be notified in a timely and relevant manner to maintain awareness of their critical ICT resources and assure mission success.

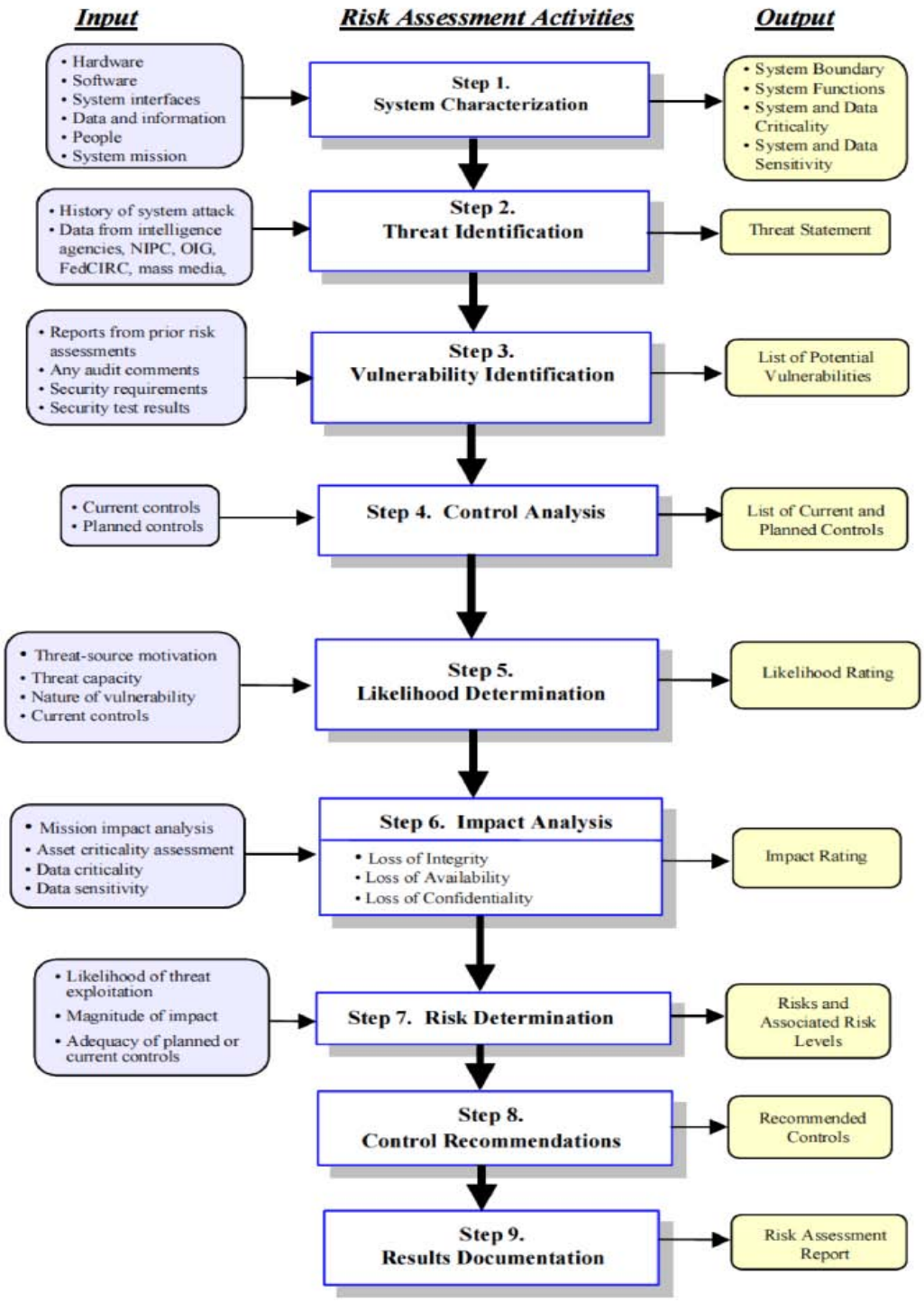


Figure 7. Risk Assessment Activities (NIST, 2002)

2.14 Mission Assurance

As risks to ICT have steadily increased, the growing threat has led to increased focus on mission assurance. According to mission assurance doctrine, mission assurance consists of measures required to accomplish essential objectives of missions in a contested environment, entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities (Department of the Air Force, 2010, p.7). Mission assurance ensures that organizations are able to provide assurance for those ICT on which they depend to meet mission needs, even when compromised. When a mission has been compromised, it does not have to result in mission failure; instead, the mission is degraded to an acceptable level where operations can continue. Therefore, organizations must constantly revisit their risk management strategies to ensure critical ICT that support mission objectives are secure (Grimaila et al., 2010). Although organizations cannot prevent every attack, they must be able to defeat an adversary when a cyber attack occurs and sustain their missions. Mission assurance means ensuring that ICT can support mission objectives in times of uncertainty: "a deficiency of information and leads to inadequate or incomplete understanding" (ISO, 2009).

Today, organizations have a dependence on critical information embedded in IT systems which can be exploited by an adversary as a weakness. Defending critical ICT resources from an adversary is a serious challenge, especially with the use of commercial-off-the-shelf products. "The proliferation of commercially available technology will allow adversaries to develop niche capabilities that will threaten, in

varying degrees, the successful conduct of operations in areas where the US forces were previously unchallenged" (Department of the Air Force, 2010). Cyberspace operations doctrine states that:

> Adversaries in cyberspace are exploiting low-entry cost, widely available resources, and minimal required technological investment to inflict serious harm, resulting in an increasing complex and distributed environment. They are fielding sophisticated cyberspace systems and experimenting with advanced war-fighting concepts.

As sophisticated adversaries continue to exploit vulnerabilities of critical ICT resources which organizations depend on for mission success, organizations must prioritize the organization's mission objectives, determine critical information assets that support these objectives, and come up with a plan for mitigating cyber threats to critical ICT resources. In 2008, the DoD Inspector General published an audit of 436 DoD mission critical IT systems and found:

- 264 system (61 percent) lacked a contingency plan or their owners could not provide evidence of a plan
- 358 systems (82 percent) had a contingency plan that had not been tested or for which their owners could not provide evidence of testing

The audit concluded that "DoD mission-critical systems may not be able to sustain war-fighter operations during disruptive or catastrophic event" (DoD, 2008). Ensuring organizations can accomplish the mission while in degraded information environment requires a wide range of protection measures. Finally, these protection measures must be coordinated within and across organizational boundaries where interdependencies are inherently created by reliance on critical information to support mission objectives.

2.15 Summary

This chapter summarized the literature that is necessary to understand and conduct the research presented in this thesis. Recognizing that humans interact with systems in their own way and information processing occurs in stages that draws upon sensory inputs, Figure 8 shows the research model that will be used to compare the existing USAF incident notification process which uses incident notification dissemination via email, with the proposed CIMIA incident notification process which achieves incident dissemination via pop-up notices.

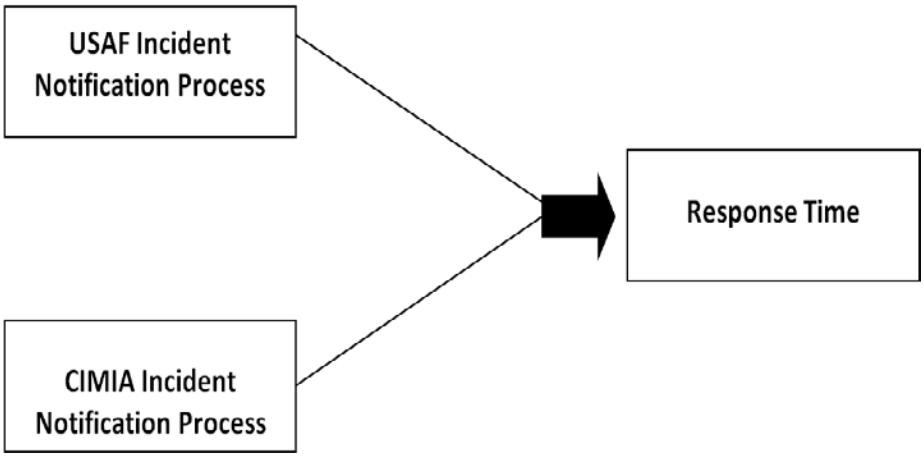


Figure 8. Research Model

The purpose of this model is to provide the empirical evidence necessary to test the main hypothesis identified in this research that it is important to promptly notify decision makers within an organization about cyber incidents in a timely manner so they can take appropriate contingency measures and assure their mission. It is upon this model that the experiment methodology in Chapter 3 is based.

III. Methodology

3.1 Introduction

The purpose of this chapter is to describe the hypothetical real-world environment in which the research experiment is conducted, explain the experiment design, and discusses the statistical methods that were used to analyze the collected data.

3.2 Research Objective

No quantitative research exists to measure the effect of timely and relevant notification for cyber incident response on mission objectives. The purpose of this experiment is to remedy this deficiency by designing an experiment in a realistic mission environment that will provide the empirical evidence necessary to test the main hypothesis. The null and alternate hypotheses are as follows:

H_o: There is no statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

H_a: There is a statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

The main hypothesis for this research was developed on the notion that it is important to promptly notify decision makers within an organization about cyber incidents in a timely manner so they can take appropriate contingency measures and assure their mission.

3.3 Experimental Environment Description

Research personnel comprised of both military and civilian personnel met regularly over a six month period to consider a potential environment to evaluate the utility of the proposed CIMIA incident notification process. The first discussions centered on the nature of potential experiments, and what needed to be done to ensure that the experiment was not biased. The initial task was to ensure that the experimental results would provide the necessary data to test the given hypothesis. During brainstorming sessions, a variety of different experiments were considered to test the hypothesis. Several meetings were held to consider the best operational environment that had critical mission-to-information dependencies and could be easily abstracted so that test subjects could be drawn from the general population. The outcome of these meetings helped shape the experimental environment and resulted in the selection of the Maintenance Operations Center (MOC) as the experimental environment in which to conduct the research.

The realization that it will be difficult to model and simulate the full extent of the MOC environment led to the design tradeoffs to identify and select only a subset of the MOC tasks for use in the experiment. The aspects used in this experiment are only superficially accurate; the operational environment is not accurate in great detail. However, the concept of the scenario is based on the organizational setting and aspects of the real-world operational environment. Adelman suggests that the more accurate the simulation along all dimensions, the greater the external validity of the experiment (1991). Accurate representation of the operational environment is particularly important

for future experiments as the CIMIA incident notification process is fully developed (Adelman, 1991). The experiment focused on information incidents that involved an internal server, and two external databases that are representative of the systems used in the MOC along with several aspects of the operational environment.

The research personnel focused on developing the appropriate case study based on the information obtain from the MOC to exploit critical mission-to-information dependencies. Yin has defined a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context; using multiple sources of evidence; and striving to explain how or why something happened by logically linking the data to the propositions supporting one rival hypothesis versus others" (1984, p. 23). Using this definition, the case study measured the proposed CIMIA incident notification process by demonstrating the feasibility for developing an incident notification process to improve the USAF's incident notification process. Adelman argues that developers of decision support systems (DSS) lack the empirical data supporting the merits of their system (1991). Therefore, to evaluate whether the CIMIA incident notification process improves the push method utilized in the USAF, the research personnel created a hypothetical scenario to generalize some aspects of the MOC's operational environment.

The MOC operates under the maintenance group; it is considered the eyes and ears of the maintenance group commander. The MOC operates around-the-clock, and is continuously dependent on information and communications technologies (ICT) throughout day-to-day operations to exchange information between numerous units. To do this, MOC personnel work day, swing, and mid shifts where they plan, schedule, and manage actions for assigned aircraft. This information-rich environment must maintain

awareness of competing resources based on daily flying schedules and maintenance priorities (AFI 21-101, 2010; AF1 21-102, 2010; AFI 21-103, 2010). MOC personnel are responsible for maintaining aircraft readiness per AFI 21-101; they "monitor and coordinate sortie production, maintenance production, and execution of the flying and maintenance schedules" (p.114). Aircraft maintenance data collection and documentation are tracked in the Maintenance Management Information System (GO81) (AFI 21-101, 2010). This system is highly integrated with a global system called Global Decision Support System (GDSS). Both systems push and/or pull information, and are not totally reliant on each other. Either system is capable of maintaining aircraft maintenance data separately if needed should one become unavailable. For instance, GO81 may push/pull aircraft discrepancies and aircraft status to GDSS while GDSS pushes/pulls missions, launch, and landing times to GO81. GDSS is primary utilized to check aircraft availability, discrepancies, and monitor the status of the USAF's fleet of aircraft. Higher levels of command utilize this system for status conditions that affect aircrafts ability to perform assigned missions.

The MOC ensures that the information is accurately entered into the GO81 in a timely manner so higher levels of command can determine aircraft availability for mission tasking (AFI 21-101, 2010). If information is not accurately updated in a timely manner, it could impair the military mission. Real-time data updates help reduce ground times and improve management of base support functions. It is apparent that the MOC's mission depends on information that is accurate to conduct operations. To obtain a better understanding, research personnel had the opportunity to visit a MOC. With the support of the MOC's superintendent, military personnel were interviewed and provided

substantial input on the most critical aspects of their operations. This input was used to develop a case study providing a framework for evaluating the proposed CIMIA incident notification process. Based on these findings, two mission objectives were used to develop an experiment: 1) ensure aircraft status is reported accurately, and 2) ensure all GO81 information is entered accurately and timely.

Focusing on an information incident, research personnel examined how the MOC dealt with the loss of CIA. Surprisingly, the MOC had excellent contingency measures to deal with the loss of availability. The MOC is not solely dependent on the GO81; in contrast, documentation is maintained in parallel to system entries for unanticipated availability. Having the appropriate contingency measures in place when the loss of availability occurred would not result in mission failure or severe degradation. Instead, when GO81 was not availability, the MOC documented maintenance information in a log book and/or phoned another unit with GDSS access to update the system to ensure information was accurately reported. MOC personnel are used to experiencing the loss of availability, but had no knowledge of the loss of either integrity or confidentially. However, the mission's impact was discussed if loss of integrity or loss of confidentially occurred. Consequently, the loss of either CIA would have some impact on the MOC's mission objectives. Based on this situation, a simple experimental scenario was created in which the methods of both cyber incident notifications processes could be evaluated.

3.4 Equipment and Facility

The experiment was conducted in a room at the Air Force Institute of Technology on Wright-Patterson AFB, Ohio. The room was configured to resemble the operational environment of a MOC, as shown in Figure 9.

A small local area network (LAN) was configured for the experiment using a router. The LAN consisted of two Hp Compaq dc5858 Microtowers with 3.48 Gbytes of RAM and 2.69 GHz of hard disk drive. Each microtower ran independently with Windows XP operating system. The first microtower was used as the workstation for subjects. The workstation included two 20-inch monitors, one Video Graphics Array (VGA) and one Digital Visual Interface (DVI) connection. The subject's workstation hosted email and a graphical interface (GUI) for the database. The second microtower was used as a server for the Domain Name System (DNS), email server, and host system for two databases. Two 30-inch monitors were connected, one VGA and DVI connection.

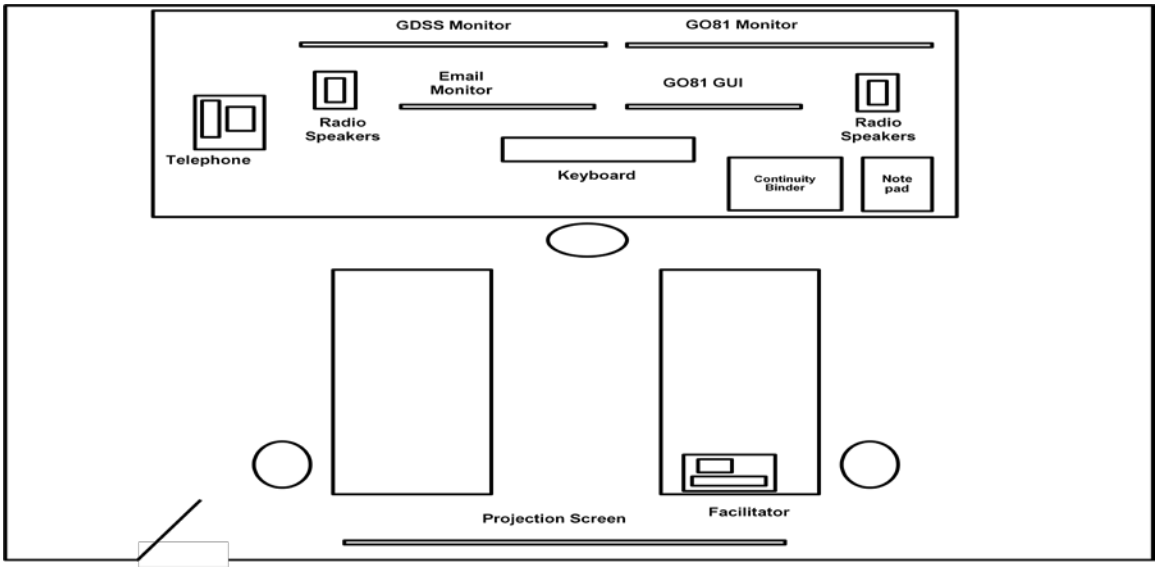
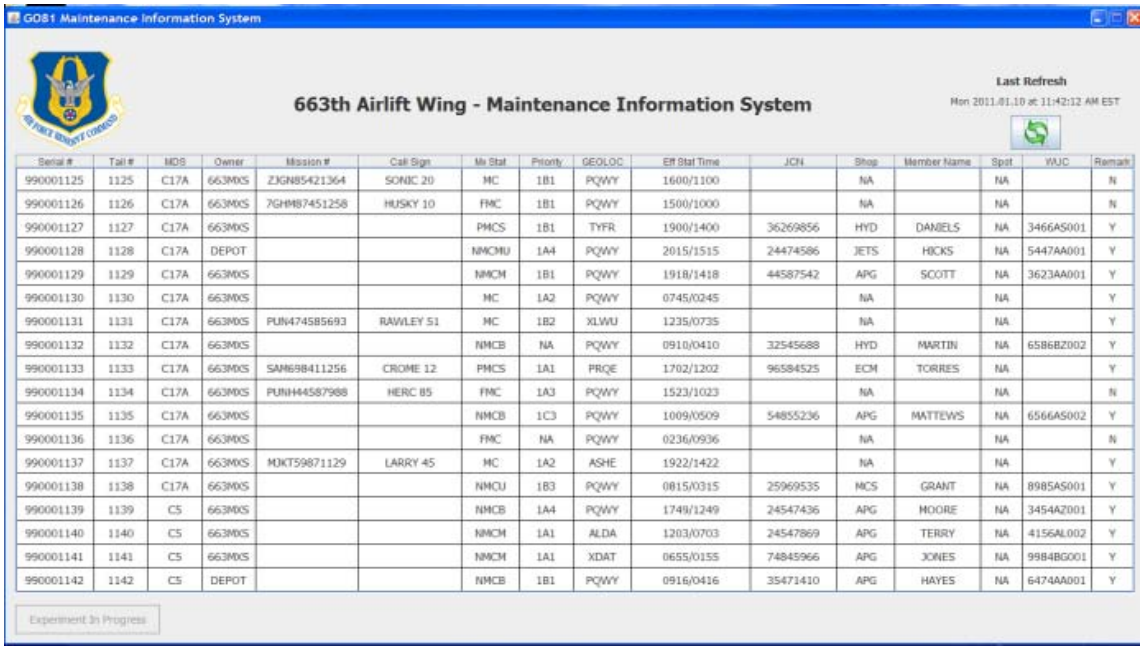


Figure 9. Experimental Environment

3.5 Software Description and Procedures

Oracle Database 10g Express Edition for Windows was the database of choice because it was free to develop, easy to deploy and distribute, and fast to download. This platform is well documented and has many accessible books, forums, blogs, and articles for troubleshooting problems. The first database developed was GO81. The MOC utilizes GO81 to document aircraft information and exercise related missions to ensure 100 percent reporting accuracy on aircraft mission capability (AFI 21-101, 2010). The development of the GO81 database focused only on maintenance aspects of timely and accurate reporting within the assigned aircraft function of the system. As shown in Figure 10, sixteen fields were selected for the case study scenario to provide relevant information about the aircraft's current mission capability. The second database, GDSS, was designed with the same look and feel of the GO81.



Serial #	Tail #	MDS	Owner	Mission #	Call Sign	Mx Stat	Priority	GEOLOC	Eff Stat Time	JCN	Shop	Member Name	Spot	WUC	Remark
990001125	1125	C17A	663MXS	ZJGN85421364	SONIC 20	MC	1B1	PQWY	1600/1100		NA		NA		N
990001126	1126	C17A	663MXS	7GHM87451258	HUSKY 10	FMC	1B1	PQWY	1500/1000		NA		NA		N
990001127	1127	C17A	663MXS			PMCS	1B1	TYFR	1900/1400	36269856	HYD	DANIELS	NA	3466AS001	Y
990001128	1128	C17A	DEPOT			NMCMU	1A4	PQWY	2015/1515	24474586	JETS	HICKS	NA	5447AA001	Y
990001129	1129	C17A	663MXS			NMCM	1B1	PQWY	1918/1418	44587542	APG	SCOTT	NA	3623AA001	Y
990001130	1130	C17A	663MXS			MC	1A2	PQWY	0745/0245		NA		NA		Y
990001131	1131	C17A	663MXS	PUN474585693	RAWLEY 51	MC	1B2	XLWU	1235/0735		NA		NA		Y
990001132	1132	C17A	663MXS			NMCB	NA	PQWY	0910/0410	32545688	HYD	MARTIN	NA	6586BZ002	Y
990001133	1133	C17A	663MXS	SAM698411256	CROME 12	PMCS	1A1	PRQE	1702/1202	96584525	ECM	TORRES	NA		Y
990001134	1134	C17A	663MXS	PUNH44587988	HERC 85	FMC	1A3	PQWY	1523/1023		NA		NA		N
990001135	1135	C17A	663MXS			NMCB	1C3	PQWY	1009/0509	54855236	APG	MATTEWS	NA	6566AS002	Y
990001136	1136	C17A	663MXS			FMC	NA	PQWY	0236/0936		NA		NA		N
990001137	1137	C17A	663MXS	MJKT59871129	LARRY 45	MC	1A2	ASHE	1922/1422		NA		NA		Y
990001138	1138	C17A	663MXS			NMCU	1B3	PQWY	0815/0315	25969535	MCS	GRANT	NA	8985AS001	Y
990001139	1139	C5	663MXS			NMCB	1A4	PQWY	1749/1249	24547436	APG	MOORE	NA	3454AZ001	Y
990001140	1140	C5	663MXS			NMCM	1A1	ALDA	1203/0703	24547869	APG	TERRY	NA	4156AL002	Y
990001141	1141	C5	663MXS			NMCM	1A1	XDAT	0655/0155	74845966	APG	JONES	NA	9984BG001	Y
990001142	1142	C5	DEPOT			NMCB	1B1	PQWY	0916/0416	35471410	APG	HAYES	NA	6474AA001	Y

Figure 10. Maintenance Management Information System (GO81)

Headquarters Air Mobility Command utilizes GDSS to have visibility of available resources to meet mission requirements. Communication interfaces between GO81 and GDSS allows the exchange of real-time data updates on aircraft status conditions. The design of the GDSS database is similar to the actual system utilized in the Air Force. However, only a portion of the information about aircraft owned by the hypothetical airlift wing was utilized in the experiment.

Information contained in the aircraft summary display on GDSS was obtained from the GO81 Maintenance Management Information System through user-entered data. In the experiment, GO81 pushes updates to GDSS 2 within minutes the information has been entered into the database. Each database has a total of 16 fields, of which only 12 are the same between the two systems. The aircraft summary displays provide visibility to monitor aircraft resources. The displays for GO81 and GDSS reflect aircraft owned by

the hypothetical airlift wing regardless of the aircraft's location. A description of the fields in both databases is provided in Appendix D.

A GUI was developed using NetBeans Integrated Development Environment (IDE) 6.9.1. This free open source IDE provided a JavaFX Composer tool to create and layout a GUI to interact with the GO81.

The email agent used to manage email during the experiment was Mozilla Thunderbird, a free open source email client, was installed on the subject's workstation. The email server hMailServer, a free email server for Microsoft Window that supports POP3 email protocol, was installed on the server workstation. The server workstation also hosted the DNS server which was Dual DHCP Server 6.72.

3.6 Experimental Scenario

A military scenario was developed that described the mission to be accomplished and the tasks that were expected to be performed. The 663rd Airlift Wing, a fictitious organization, at Rickenbacker AFB in Columbus, Ohio, was the operational environment for the scenario. The subjects were presented a power point presentation which provided background information about the wing's mission and how the MOC helps the wing as a whole by ensuring the mission is accomplished. The presentation provides the in information in the mission brief script shown in Figure 11.

663rd Mission Brief Script
The 663 AW supports a worldwide global mobility mission to provide trained maintenance specialist for the U.S Air Force's largest cargo transport aircraft, the C-5 Galaxy and C-17 Globalmaster III cargo aircraft. These aircraft move valuable supplies and people in support of Global Reach for America. The 663rd Maintenance Squadron Maintenance Operations Center (MOC), under the direction of the maintenance group commander, manages scheduled maintenance to the fleet on a near 24/7 basis to accomplish all operational commitments with minimal impact to maintenance personnel, facilities and equipment while ensuring optimal use of both time and resources. They coordinate and control scheduled and unscheduled aircraft maintenance to ensure readiness for 18 assigned aircraft. As the MOC coordinates maintenance operations, they ensure timely and accurate support of everyday and exercise related missions, implementing daily flying and maintenance schedules to ensure optimum utilization of hundreds of maintenance group personnel. The more than 400 members of the squadron streamline their technical expertise in supporting C-5 and C-17 aircraft. Their mission is to provide global response, world-class systems, support equipment, and aircraft maintenance. All team members of the 663rd Maintenance Squadron play a pivotal role in maintaining aircraft and equipment in mission-ready status to ensure Headquarters Air Mobility Command's ability to maintain Global Reach for America.

Figure 11. 663rd Mission Brief Script

Once the subjects understood the wing's mission, they were told what tasks were expected of them. Each subject in the experiment assumed the role of a Shift Supervisor on swing shift who was responsible for ensuring Rickenbacker's fleet of aircraft was maintained. In this role, the subjects were instructed to keep track of every assigned aircraft and the aircraft's current mission capability. They ensured timely and accurate support of everyday and exercise related missions while managing computer-based platforms to include GDSS and GO81. They were tasked with the crucial responsibility of flawless orchestration of maintenance operations which ensures timely and accurate support to Headquarters Air Mobility Command. Figure 12 shows the experiment scenario that each subject was briefed.

Experiment Scenario Script
You have just reported to the Maintenance Operations Center (MOC) for swing duty. The day-shift Shift Supervisor has just briefed you on the daily events and gives you a backlog of updates to enter into GO81. The database was unavailable part of the day for scheduled maintenance. As a result, several updates need to be entered into the database for accurate status reporting on the 663rd fleet of aircraft. The scheduled system maintenance on GO81 was advertised in advanced and all system users are aware that the system is back online. Your objectives in this study are to accurately enter all data from the data sheets into GO81 and ensure the information is accurately pushed to GDSS, monitor email, listen for and write down radio communications and answer any calls that come into the MOC based on your understanding of the mission.

Figure 12. Experimental Scenario Script

Each task was described and subjects received training to ensure they understood their role in the experiment. The training provided is discussed below under the pre-experimental activities.

3.7 Experimental Design

The experimental design approach focused on the selection of the appropriate case study to represent the different treatment conditions. According to Keppel, "an experiment consists of a carefully work-out and executed plan for the data collection and analysis. Treatment conditions are chosen to focus on particular features of the testing experiment" (1982, p. 4). Furthermore, he explains that "conditions are administrated to subjects in such a way that observed differences in behavior can be unambiguously attributed to critical differences existing among the various treatment conditions" (Keppel, 1982, p. 4).

This experiment was tailored from factorial experimentation which "permits the manipulation of more than one independent treatment in the same experiment" (Keppel,

1982, p.20). Specifically, a 2 x 2 mixed factorial design with a combination of within-subjects and between-subjects variables was used. The term "mixed" refers to the elements of both within-subject and between-subject designs (Keppel, 1982). This design uses the same subjects with every condition of the research, including the control. Keppel explains that subjects serve more than once in the experiment, repeated measurements are taken, and treatment effects are associated with differences observed within each subject.

In the 2x2 Mixed Factorial Design shown in Table 2, the design consists of one within-subject variable (type of incident notification), with two levels (NOTAM and Pop-up), and one between-subjects variable (incident notification order), with two levels (NOTAM/Pop-up and Pop-up/NOTAM).

Table 2. 2x2 Mixed Factorial Design

		Factor C **Type of Incident Notification**	
Factor A **Initial Notification**	**Factor B** **Subjects**	**Session 1**	**Session 2**
NOTAM	S_1 S_2 S_3 S_8 S_9 S_{10} S_{11} S_{16} S_{17} S_{18} S_{19} S_{24} S_{25}	NOTAM	Pop-up
Pop-up	S_4 S_5 S_6 S_7 S_{12} S_{13} S_{14} S_{15} S_{20} S_{21} S_{22} S_{23}	Pop-up	NOTAM

In this case, the USAF incident notification process (NOTAM) was one of two independent variables, compared to the proposed CIMIA incident notification process (Pop-up) being the second independent variable.

Subjects who participated in the experiment received random assignment to the between-subject variable. This procedure guaranteed that the treatment condition had an equal opportunity of being assigned to a given subject and whatever other uncontrolled factors might be present during any testing (Keppel, 1982). "The critical features of random assignment, then, are that each subject-session combination is equally likely to be assigned to any one of the treatment and that the assignment of each subject is independent of that of the others" (Keppel, 1982, p.16).

3.8 Pilot Study

A pilot study was conducted approximately four weeks before the first experiment. The pilot study was performed with 20 volunteer Air Force Institute of Technology graduate students at Wright-Patterson Air Force Base, Dayton OH. Because experiments involving humans are difficult to design and control, the pilot study was used to establish which variables could be controlled and measured, and to reveal any deficiencies in the design of the proposed experiment. Patten states that pilot studies are designed to obtain preliminary information on how new treatments and instruments work (2009). That is to say, they can potentially reveal errors in design as well as allow for refinement and correction before the actual experiment. Specifically, the pilot study was used to check experimental procedures, operation of equipment to include hardware and software (GO81 and GDSS), data collection techniques, and the questionnaire.

The pilot study gave the researcher the opportunity to practice and receive notable remarks from the pilot group. The lessons learned in the pilot study were weaknesses in the experimental procedures related to training and clarification issues in the

questionnaire. The pilot study group received a training session that included all the expected tasks to be performed. The training session was not originally divided into sessions to allow practice and complete understanding before receiving instruction on the next task. Modifications to the experimental procedures resulted in the subjects receiving training in stages to allow for practice after instruction on each task.

The most notable remarks received from the pilot group referred to the questionnaire. Originally, the questionnaire asked open-ended questions. Many of the responses received did not answer the intended question and several subjects asked for clarification before responding. As a result, several questions were modified to improve clarity and the open-ended questions were changed to an 8-point Likert scale response.

3.9 Subjects

The subjects used in this experiment were drawn from the graduate student population at the Air Force Institute of Technology and undergraduate student population at Wright State University located in Dayton, Ohio. Participation was completely voluntary.

3.10 Experiment Procedures

Prior to their arrival, the subject's were randomly assigned a subject number which determined the experimental design block for the experiment, as shown in Figure 9. Subjects did not know in advance about the experimentation process, nor did they have any prior knowledge of what was expected of them. They were told that the

purpose of the experiment was to evaluate a prototype software tool investigating an Air Force program in a simulated real-world situation.

3.10.1 Pre-experimental Activities

The first pre-experimental activity was the administration of the consent form. The consent form was reviewed in detail to ensure each subject understood. Next, the experiment scenario was conveyed and a short presentation (mission brief discussed above) was presented which provided background information about the scenario.

Another pre-experimental task explained the experimental environment. Subjects received training on the tasks they were expected to perform. The training was segmented into stages that explained each task to be performed. This allowed subjects the opportunity to practice what was instructed immediately which prevented them from receiving too much information at once. In the first portion of training, they were introduced to GO81.

Operation of the GO81 database for subjects was relatively straightforward. The subjects needed to understand how to bring up the data entry screen, enter data from a data sheet (Appendix F), and change data. These topics were fully addressed and discussed during a "hands-on" training session. After specific instruction, the subjects spent eight minutes in a training session to become familiarized with the data sheets and data entry screen. They were instructed to locate every field between the data sheet and data entry screen, and verify the information on the entry screen was correct before saving the information in GO81. In order to enter data into GO81, the subject had to select the aircraft tail number (from data sheet) that required an update. This was

accomplished by clicking on any part of the row with the aircraft's tail number. Once clicked, the data entry screen would pop-up for that tail number. After the subject entered all the data from the data sheet into the entry form and clicked save, the information was immediately saved in GO81. Within two minutes, the information was pushed to GDSS 2. Once the subject was comfortable with the task, the second training stage instructed was how to verify information between GO81 and GDSS.

The process of verifying information between the two systems was simple. The two 30-inch monitors connected to the server displayed GO81 and GDSS respectively. The subjects were instructed to visibly compare the information in GO81 and GDSS. By looking at the row of the tail number in GO81 and the same tail number in GDSS, the subject could verify that the information was accurately pushed from GO81 to GDSS. This portion of the training session was intended to familiarize the subjects with the common fields between the databases and verify the information they previously entered was accurate in GDSS. The next training stage was instruction on how to use email.

The subjects received instruction on how to use the basic functions of Mozilla Thunderbird email client. These functions included how to open, send, delete and read email. The last training stage included the use and operation of the telephone and radio.

The operation of the telephone and radio were both straightforward. Telephone instructions were given and a list of frequently called numbers was available on speed dial. The radio was simulated through the desktop speakers for one-way transmission. The subjects did not have to interact with the radio; they were instructed to listen for and write down all radio transmissions. All transmissions were broadcast twice. If the

transmission was unclear or not recorded in a timely manner, the subjects were asked to write the time of the broadcast.

Finally, subjects received detailed instruction on how to complete the NASA workload assessment. They were given the opportunity to practice and ask any questions on how to complete the assessment.

In addition, the subjects received a continuity binder (Appendix D) that included information covered in the training session. The continuity binder also included a graph of all the ICT that the subjects depended on during the experiment. Each of the tasks was accomplished with one of the available resources.

3.10.2 Experimental Session

The subject's objectives were to complete all given updates from a datasheet into GO81, monitor email, listen for and write down radio transmissions, and answer any calls that came into the simulated MOC environment. Subjects were asked to input the information from the datasheets into GO81 and verify that the information was successfully updated. The subjects had to actively monitor the accuracy of GO81 and, within two minutes, ensure the same information was updated and reflected accurately in GDSS. Some information that subjects entered was manipulated, changed or altered, and made unavailable as part of the experiment. The subjects experienced three types of information loss or modification by manipulation, representing losses of confidentiality, integrity, and availability (CIA). These manipulations took the form of notices directly to the subject from the two incident notification platforms. The USAF incident notification process utilized a push method process in the form of an email. The CIMIA incident

notification process utilized a subscribe and pull process (discussed in Chapter 2) in the form of a pop-up notification following a cyber incident.

The experiment was divided into two sessions in which subjects were required to complete the same set of tasks. Each session of the experiment included the three types of manipulation. To induce cyber attacks that resulted in the loss of integrity and loss of availability, incorrect information was deliberately presented, information between the two systems was deliberately mismatched, and/or either system was made unavailable. The loss of confidentiality resulted in a breach to the intranet web server by an adversary. The server contained a weekly flying schedule. The subjects were not informed that some of the information they updated in the database was manipulated, altered, and not available as part of the experiment. At the conclusion of the experiment, the true intent of the experiment was debriefed to all subjects.

Once the experiment started, the subjects were presented with the three types of manipulation in each session based on their progress of completing the datasheets. Additionally, each subject was presented distracting information in the form of emails, radio updates, and calls that had to be acknowledged and, in some cases, required a course of action. The manipulations and distractions were applied in the same sequence and at approximately the same time during each session as shown in Figures 13 and 14.

In each session, subjects were given 30 minutes to complete all given tasks. Immediately following the first session of the experiment, subjects completed a rating (NASA TLX) workload assessment. Upon completion, subjects were given a 10-15 break before starting the next session. In the second session, subjects were asked to

complete the same tasks followed by two additional workload assessments, one rating and weights.

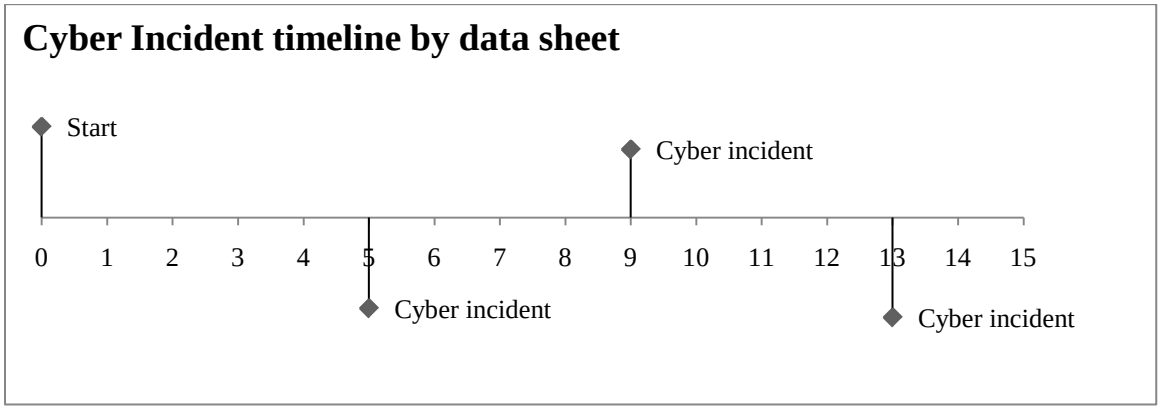


Figure 13. Cyber Incident timeline by data sheet

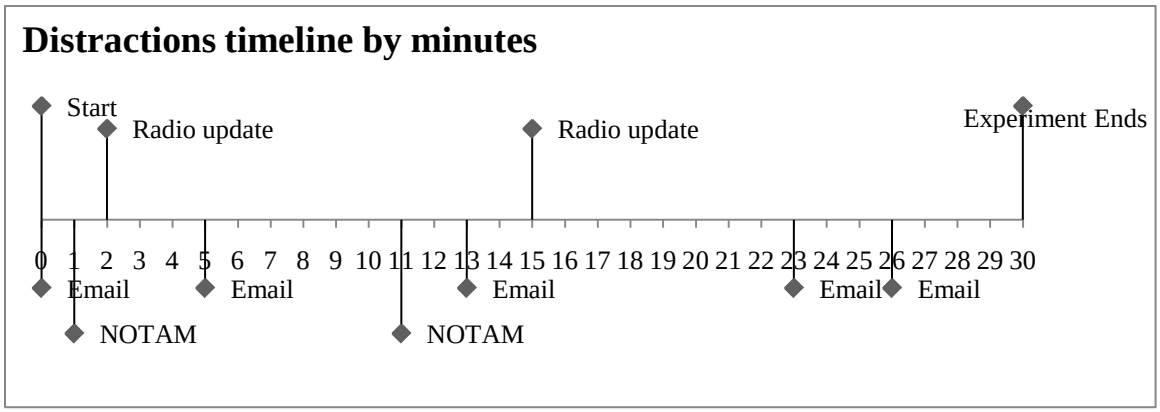


Figure 14. Distractions timeline by minutes

3.10.3 Post-experimental Activities

At the completion of the experiment all subjects completed a questionnaire identical to that shown in Appendix B. The post-experimental questionnaire was administered to garner information in the following areas:

(1) Gather some demographics of the subjects in terms of age, gender, academic level

(2) Subjects self-assessment evaluation of their performance

(3) Evaluation of the incident notifications usefulness

(4) Indirect measures of situational awareness

Subjects were debriefed and their questions about the experiment were answered. The experiment concluded when the questionnaire was completed and the subject's questions were answered. In total, each experimental session required approximately 2 hours per subject.

3.11 Questionnaire Design

This research sought to not only objectively measure the temporal aspect of an cyber incident notification required for mission personnel to recognize and respond, but also to measure through more subjective means the perceptions of the subjects, self-assessment. According to Endsley, the most commonly used means of subjectively evaluating operator's concepts on SA involves direct questioning. Thus, "the measurement of SA provides a useful index for evaluation system design and training techniques and for better understanding human cognition" (Endsley & Garland, 2000, p. 24). In addition,

> *One of the chief reasons for measuring SA has been for the purpose of evaluating new system and interface design in order to determine the degree to which new technology or design concepts actually improve or degrade operator SA, it is necessary to systematically evaluate them based on a measure of SA, thus providing determination of which ideas have merit and which have unforeseen negative consequences.*

The questionnaire was employed to establish the subjects perception of critical aspects of environmental elements in the experiment to determine their level of SA and to perform comparative analysis of responses associated with each session. The intent was to use an ordinal scale similar to the Likert 7-point scale. Although the Likert scale is commonly understood and well known, the survey instrument used is not a validated measuring device for SA or DSS. Instead of the traditional 7-point Likert scale, an 8-point scale was used for ease of analysis. The development phase of the questionnaire was extracted from guidance in the U.S Army Research Institute for the Behavioral and Social Sciences' Questionnaire Construction Manual and the human factors and ergonomics field of study on questionnaires.

In addition to the ordinal scale questions, multiple choice questions were also administered in the questionnaire. These questions were administrated to obtain a single answer response for demographic information such as gender, age group and academic level and multiple answer selections.

3.12 Data Collection Techniques

During each session of the experiment three log files were used to record time stamps of the events that occurred. The first log file recorded the data entered in GO81. This log provided the time stamp of every data sheet entered, as well as what data was entered and shared between the two databases. It also provided the start and end of the experiment for each subject. The researcher used this information to measure part of the subject's performance outcome that included the number of sheets completed during each

session of the experiment, accuracy of the information entered by the subject, and to ensure the order of the sheets entered were consistent among subjects.

The second log was an automated telephone file log. This log provided the time stamp of each call placed and destination of the call. The researcher used this information to record the response time. The response time was calculated from the time the cyber incident occurred (which was a predefined time previously discussed in Figure 13) to the time the subject took a course of action.

The last log was a two-part evaluation file that contained the results of the NASA TLX workload assessment. The NASA TLX workload assessment is a subjective technique that relies on a multidimensional construct to derive an overall workload score based on weight averages of ratings on six subscales: mental demand, physical demand, temporal demand, performance, effort, and frustration level. Slick et al. (2005) comment that:

> *As defined, workload is task-dependent, because it generally refers to some part of the relationship between an operator and the task being performed. There three are key issues associated with measuring workload: First, workload is subjective in the sense that individuals may use different criteria to judge their own workload, so there is no way to compare subjective workload across individuals. Second, individuals' criteria for judging workload may change over time, as the individual becomes more proficient at the primary task. Third, given that workload is subjective, there is no way to assess whether individuals' subjective ratings include all pertinent aspects of the task.*

The NASA TLX consists of two-parts: ratings and weights. Ratings for each of the six subscales are obtained from the subjects following the completion of each session. A numerical rating ranging from 0 to 100 is assigned to each scale. Weights are determined by the subjects' choices of pairwise comparisons between all possible combinations of the subscales, approximately 15. Weights are collected at completion of

session 2. The ratings and weights are then combined to calculate a weighted average for an overall workload score. The workload assessment was used to assess the subjective ratings of workload between the presents and absence of the treatment. The first part of the file provides the subjects individual ratings of session 1 and 2 respectively. Part two of the file provided the weights evaluation that pertained to the workload experience of the subject during both sessions of the experiment.

The data collection processes was standardized across all subjects by implementing a Data Collection Form (Appendix E). The form was used to record the logged information discussed above. In addition, the form was used to record observed behavior that contributed to the subject's decision making activities.

The questionnaire asked specific questions that related to the decision making process of the subjects, as well as pointed questions that dealt with the conditions. For this reason, a pre-process questionnaire was not used. The researcher did not what to sensitize the subjects to the treatment. This problem is what Patten refers to as pretest sensitization (2009). The pretest sometimes causes problems by exposing subjects to what would be covered in the experiment (2009). To overcome this problem, only a post-process questionnaire was used.

3.13 Statistical Analysis

According to Keppel, one of the important tasks in summarizing the outcome of the experiment is by means of statistical indices and procedures (1982). Keppel suggests that the goal is to extract as much meaningful information as possible from the experiment. Although several statistical techniques were utilized in this study, one

method used for evaluating the primary outcome examined the distribution of the data to determine whether these distributions were significantly different. For instance, should data from the CIMIA incident notification process result in a significantly different distribution compared to the USAF's incident notification process, one would conclude that the treatment had a significant effect on the outcome variable being evaluated. Based on the results of the sample statistical test, one could then make inferences about the feasibility of the proposed CIMIA incident notification process being utilized within the USAF. Hypothesis testing was used to determine the results of the data collected.

A hypothesis is a "prediction of the outcome of a study" (Patten, 2009, p. 15). It asserts that the treatment will generate some type of effect. In this study, a null hypothesis and alternative hypothesis are considered for hypothesis testing. According to Keppel, the research hypothesis is "translated into a set of statistical hypothesis, which are then evaluated in light of the obtained data" (1982, p.24). He explains that the statistical hypothesis "consists of a set of precise hypothesis about the parameters of the different treatment populations." The null and alternative hypotheses are two examples of the statistical hypothesis which "are mutually exclusive or incompatible statements about the treatment parameters" (Keppel, 1982, p.24). The hypothesis statement is the null hypothesis, H_o, which will be tested and rejected as false. The alternative hypothesis, H_a, will in turn be accepted as true when the H_o is rejected (Keppel, 1982). Comparing the difference between means to the variability within contestant distribution is the basis for analysis of variance.

3.14 Test Selection

An analysis of variance, abbreviated as ANOVA, is a method for hypothesis testing that compares differences between two or more means to determine if the averages are likely to be the same, or likely to be different. An ANOVA is an analysis of the variation present in an experiment. It is a test of the hypothesis that the variation in an experiment is no greater than that due to the normal variation of individuals' characteristics and error in their measurement (Keppel, 1980). Keppel (1982) discusses that the tests in an ANOVA are based on the F-ratio which is the variation due to an experimental treatment or effect divided by the variation due to experimental error. ANOVA is considered a parametric test which is "one that requires data from one of the larger catalogue of distributions that statisticians have described and for data to be parametric certain assumptions must be true" (Field, 2005, p. 63). The major assumptions of ANOVA are:

- Normally distributed
- Homogeneity of variance
- Independence

Keppel argues that violating the normality of distribution, homogeneity of variance and independence of score in treatment conditions does not appear to have any practical significance for statistical analysis of an experiment because they apply equally to the factorial design. However, when data is not normal, remedial measures for non-normality is data transformation which is applied so that the data appear to more closely meet the assumptions of a statistical inference procedure (Field, 2005). Homogeneity of

variance is that the variance of the populations is equal. "ANOVA works well even this assumption is violated except in the case where there are unequal numbers of subjects in the various groups" (Fields, 2005, p.97). Violations of independence produce a non-normal distribution, which results in invalid F ratios. However, independence assumption is met through the random assignment of subject to conditions (Keppel, 1980).

3.15 Summary

This chapter presented the research methodology for this study. The conceptual framework was defined and the research objective, case study and experimental design were summarized. The data collection procedure and data analysis methods were also discussed. Finally, this chapter concluded with the test selection used in the experiment to be analyzed in the following chapter.

IV. Results

4.1 Introduction

The previous chapter identified the methodology for the collection and analysis of data in order to test the hypothesis stated in chapter 1. This chapter applies the research methodology and discusses the results. Specifically, this chapter provides an overview of the demographics of the test subjects, presents and analyzes the results of the statistical testing regime, provides a discussion of the interpretation of results, and presents additional related findings.

4.2 Subject Demographics

Data on three demographic variables were collected. These variables included age, gender and academic level (Table 3). These variables were gathered from 13 graduate students at the Air Force Institute of Technology and 12 undergraduate students from Wright State University located in Dayton, Ohio. The majority of the subjects were in the age groups 18-30 (64%). There were more male subjects (76%) than female (24%). Thirty-six percent of the subjects did not have a degree, while 40% of the subjects had a Bachelor.

Table 3. Demographic information on subjects

Demographic Factor (N=25)		Frequency	% of total
Age	18-30	16	64
	30-45	8	32
	45-60	1	4
Gender	Male	19	76
	Female	6	24
Academic Level	No Degree	9	36
	Associate	4	16
	Bachelor	10	40
	Master	2	8

4.3 Deviations in the Methodology

There were a few deviations in the methodology that are discussed below.

- A total of 25 subjects participated in the experiment; however, the expected number of data points was not collected. Each subject was to receive a total of 6 treatment conditions (Integrity, Availability and Confidentiality with and without the treatment) for a total of 150 data points. However, the majority of the subjects only received 4 of the 6 treatment conditions for a total of 96 data points shown in Table 3. The subject's performance of the tasks was self-paced and limited to two 30 minutes sessions. Because of this each subject did not receive the expected number of treatment conditions. Additionally, 1 of the 25 subjects only received half of the treatment conditions; hence, that subject was removed from the sample size leaving a remaining 24. The median response times was taken for all cyber incidents for each subject for the NOTAM (USAF) and pop-up (CIMIA) excluding confidentiality. For example, if subject 4 responded to an integrity

pop-up in 45 seconds and an availability pop-up in 210 seconds, the response time recorded for the CIMIA incident notification process was 128 seconds. If only 1 of the 2 cyber incidents was received, that response time was recorded. Table 4 shows how the data was combined.

Table 4. Collected data points

Type of Cyber Incident	**Treatment Condition**		
	NOTAM	**Pop-up**	**Total**
Integrity	22	21	43
Availability	19	20	39
Confidentiality	5	9	14
Total	46	50	96

Table 5. Combined data points

	Treatment Condition		
	NOTAM	**Pop-up**	**Total**
Cyber Incidents	13	11	24
	13	11	24
Total	26	22	48

- The dependent variable, response time, is not a normal distribution which violates one of the fundamental assumptions of an ANOVA for the test to work properly and yield good results. Therefore, in an attempt to normalize the distribution somewhat, the response variable was transformed. A reciprocal transformation was performed on the response variable for the combined data points based on the formula: $y' = 1/y$. Where y is the value of the original variable and y' is the value of the transformed variable used in the analyses for response time (DeCoster, 2001; Field, 2005).

4.4 Results

The research objective was to compare the USAF incident notification process to the CIMIA incident notification process with respect to the response time to recognize and take proper contingency actions following a cyber incident. Response time was measured in terms of the length of time it took a subject to report that a cyber incident had occurred. The main hypothesis for this research was developed based on the notion that it is important to promptly notify decision makers within an organization about cyber incidents in a timely manner so they can take appropriate contingency measures and assure their mission. The null and alternate hypotheses were:

H_o: There is no statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

H_a: There is a statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

A repeated measures ANOVA was conducted to interpret interaction effects and main effects on response time of the type of incident notification (Type: NOTAM or Pop-up) and the initial incident notification utilized by the subject during the experiment (Initial: NOTAM or Pop-up). The interaction effect is between type of incident notification and initial notification. The main effects are the response time difference between the types of incident notification. Initial notification is the between-subjects variable with two levels (NOTAM and Pop-up) shown in Table 5. The type of incident notification is the

within-subjects variables with two levels (NOTAM and Pop-up) shown in Table 6. These two independent variables had an effect on the dependent variable (response time), called the main effect. Keppel (1980) suggests that the order of testing null hypotheses should be in a rational sequence. The first step is to evaluate is the interaction before analyzing main effects. The significance of this test determines the next step in the analyses. According to Keppel (1980), a significant interaction requires further interpretation of the data where as a non-significant interaction indicates two independent variables. Figure 14 shows a non-significant interaction.

Table 6. Between-Subjects Factors

Between-Subjects Factors

		N
Initial Notification	NOTAM	13
	POP-UP	11

Table 7. Within-Subjects Factors

Within-Subjects Factors

Type of Incident Notification	Dependent Variable
NOTAM	NOTAM Response Time
POP-UP	POPUP Response Time

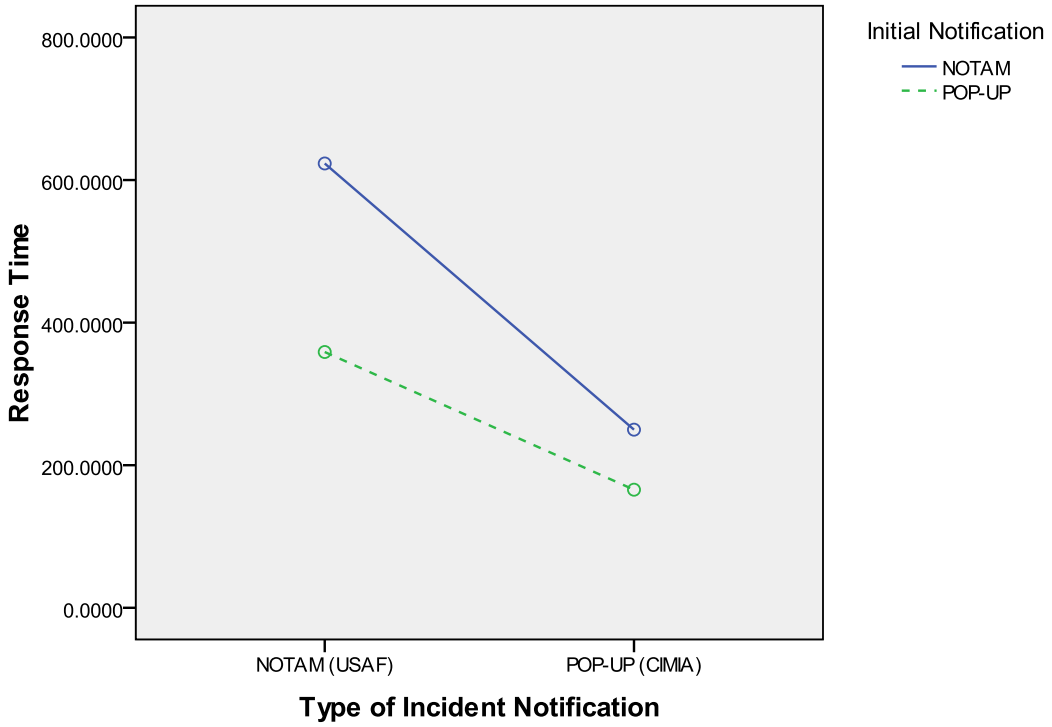


Figure 15. Response Time Initial notification for NOTAM and Pop-up

Table 8. Descriptive Statistics for Response Time

Descriptive Statistics

	Initial Notification	Mean	Standard Deviation	N
NOTAM Response Time	NOTAM	623	322	13
	POP-UP	358	278	11
	Total	502	325	24
POP-UP Response Time	NOTAM	249	179	13
	POP-UP	165	165	11
	Total	211	174	24

Table 9. Levene's Test of Equality of Error Variances

Levene's Test of Equality of Error Variances[a]

	F	df1	df2	Significance
NOTAM	1.179	1	22	.289
POP-UP	.000	1	22	.991

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept + Initial Notification
Within Subjects Design: Type of Incident Notification

Table 10. Analysis of Variance for Response Time

ANALYSIS OF VARIANCE TABLE FOR RESPONSE TIME

SOURCE	DF	SS	MS	F	P
INTIAL NOTIFICATION (A)	1	0.001	0.001	4.593	0.043
SUBJECT (B)					
A*B	22	0.005	0.000		
TYPE OF INCIDENT NOTIFICATION (C)	1	0.001	0.001	7.629	0.011
A*C	1	0.001	0.001	2.771	0.110
A*B*C	22	0.004	0.001		
TOTAL	47	0.012			

Note: ANOVA is based on the reciprocal transformation data

Repeated measures ANOVA found that there was not an interaction between initial notification and type of incident notification ($F(1,22)=2.271$, $p = .110$). This indicates that the two independent variables are representative of simple effect tests. Therefore, the next step in the analysis was to focus on the average effects of the two independent variables and interpret the experimental results in terms of the main effects shown in Table 8 (Keppel, 1980). The dependent variable, response time, was made

more normal by the reciprocal function. There was homogeneity of variance between for the NOTAM and Pop-up as assessed by Levene's test for equality of error variances. Simple main effects analysis showed that initial notification is significant using a significance level of .05 ($F(1,22) = 4.593$, $p = .043$) and there is a difference between the type of incident notification process using a significance level of .05 ($F(1,22) = 7.629$, $p = .011$). Therefore, the null hypothesis was rejected, and it was concluded that there is a statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents.

4.5 Additional Results

4.4.1 Workload Assessment

The NASA TLX workload assessment response variable is a percentage derived from count data which violates one of the assumptions of using ANOVA. The most important assumption is that the data are normally distributed with no imposed limits. Clearly this is not true of percentages, which cannot be less than 0 nor more than 100. Therefore, in an attempt to normalize the data, percentages were converted to arcsine values. The arcsine transformation moves very low or very high values toward the center, giving them more theoretical freedom to vary. An arcsine-square transformation was performed on the response variable to make the percent data normal (Field, 2005). The arcsine value used in the analyses is for amount of workload experienced. The

assessment of subject's workload during the experiment revealed that the overall perceived workload experienced among subjects was consistent.

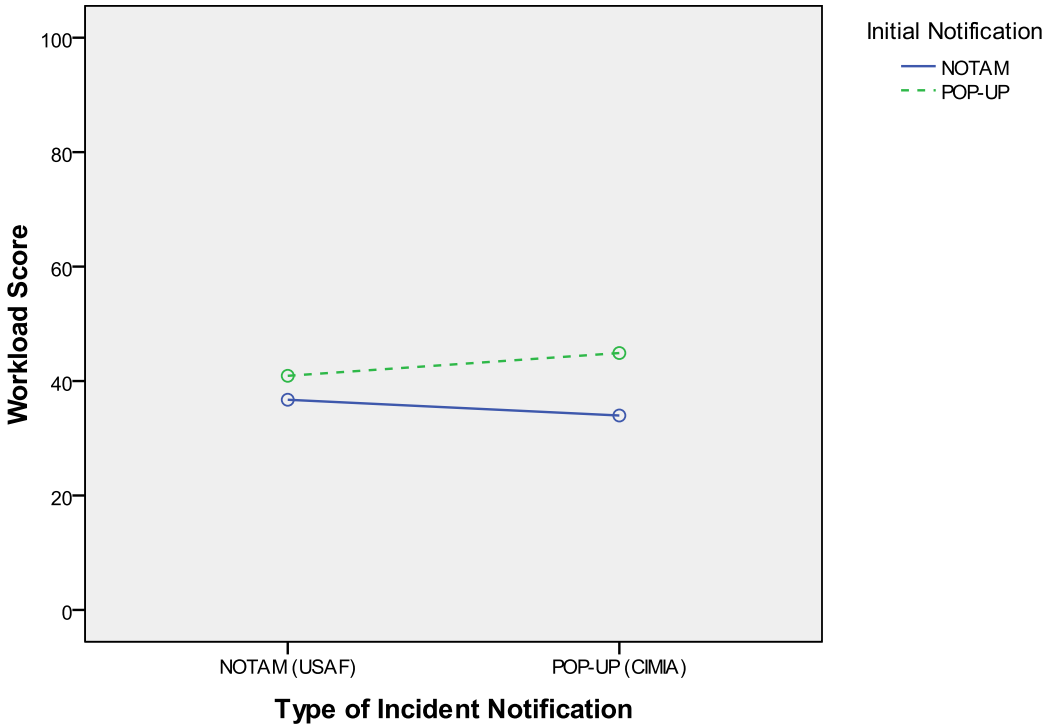


Figure 16. Workload score Initial Notification for NOTAM and Pop-up

Table 11. Descriptive Statistics for Workload score

Descriptive Statistics

	Initial Notification	Mean	Standard Deviation	N
NOTAM Workload	NOTAM	36.7296	13.9583	13
	POP-UP	40.9140	14.4112	11
	Total	38.6475	14.0173	24
POP-UP Workload	NOTAM	33.9759	16.0652	13
	POP-UP	44.8942	10.4745	11
	Total	38.9801	14.6028	24

Table 12. Levene's Test of Equality of Error Variances

Levene's Test of Equality of Error Variances[a]

	F	df1	df2	Significance
NOTAM	.017	1	22	.897
POP-UP	2.104	1	22	.161

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept + Initial Notification
Within Subjects Design: Type of Incident Notification

Table 13. Analysis of Variance Table for Workload

ANALYSIS OF VARIANCE TABLE FOR WORKLOAD

SOURCE	DF	SS	MS	F	P
INTIAL NOTIFICATION (A)	1	679.522	679.522	1.931	0.179
SUBJECT (B)					
A*B	22	7743.074	351.958		
TYPE OF INCIDENT NOTIFICATION (C)	1	4.482	4.482	0.114	0.739
A*C	1	135.096	135.096	3.432	.077
A*B*C	22	866.085	39.368		
TOTAL	47	9428.259			

Note: ANOVA is based on arcsine value

Figure 15 indicates that there is no interaction between the initial notification and the type of incident notification. The dependent variable, workload score, was made more normal by arcsine transformation. There was homogeneity of variance between the NOTAM and Pop-up as assessed by Levene's test for equality of error variances. The ANOVA found that there is not a significant interaction using a significance level of .05 ($F(1,22) = 3.432$, $p = .077$) . Simple effects analysis showed that the main effect of initial

notification on perceived workload was not significant ($F(1,22) = 1.939$, $p = .0179$) and similarly, the main effect of the type of incident notification on perceived workload was not significant ($F(1,22) = .114$, $p = .0739$). The marginal means for the amount of workload experienced in the USAF incident notification process (38.6475) and the proposed CIMIA incident notification process (38.9801) are not statistically different (Table 9).

4.5.2 Questionnaire results

The post-questionnaire was used for a self-assessment to perform comparative analysis of responses associated with each session. The following dependent variables of interest were analyzed with respect to the presents of the CIMIA incident notification process. There was one exception; the first question refers to an overall comfort level of the experiment, not between sessions. A summation is shown using the sample mode and median in Table 8. Overall, subjects were more comfortable during the second session of the experiment, which was expected. In addition, a slight increase in performance is indicated between sessions.

Table 14. Comparison of subject's self assessment

Lickert scale item	Sample mode	Sample median
Subject comfort level with the experiment	7	6
Subject's comfort level with session one	5	5
Subject's comfort level with session two	7	7
Subject's perception of NOTAMs usefulness	1	3
Subject's perception of CIMIA notification usefulness	8	7
Subject's self-assessment of performance in session one	5	5
Subject's confidence of performance rating in session two	6	6
Subject's self-assessment of performance in session two	6	6
Subject's confidence of performance rating in session one	6	6

Part of the questionnaire was also used to obtain an indirect measurement of SA. Because subjective measures of SA are limited in the veracity of self-rating and observer rating of SA (Endsley, 1995), the questionnaire asked questions directed at all three levels of SA. Although, the questionnaire is not a validate technique for measuring SA, it indicates subjects SA level based on their understanding of information available in the experiment environment. A summary of the SA response measures are shown in Table 11.

Table 15. Summary of SA response measures

Response Measure	Session 1 w/o CIMIA	Session 2 w/CIMIA	Session 1 w/CIMIA	Session 2 w/o CIMIA
Subjects detected an error in data	0.8461	1	0.9897	1
Subjects perception of persons affected by cyber incident	3.5384	4.6153	4.4822	4.5333
Subjects notified someone of cyber incident	0.6923	0.923	0.978	0.9585
Subjects notified who they percieved to be affected by cyber incident	1.5384	2.6153	2.75	4.5825

Notes:
1. Mean scores are compared by session.

4.6 Summary

A significant difference in the type of incident notification between the USAF incident notification process and the proposed CIMIA incident notification process was observed. Simple main effects analysis showed that there is a difference between the type of incident notification process using a significance level of .05 ($F(1,22) = 7.629$, $p = .011$). Therefore, the null hypothesis was rejected, and it was concluded that there is a statistical difference between the existing and CIMIA incident notification processes in the length of time required for mission personnel to recognize and take proper contingency actions in response to cyber incidents. The proposed CIMIA incident notification reduced response times by 58 percent. This reduction was a result independent of whether or not the CIMIA notification was the initial notification in the experiment. The additional findings from the NASA TLX workload assessment and post-questionnaire suggest relative performance indicators in regards to the CIMIA incident notification process and indirect measurements of SA. The following chapter will discuss and interpret the results of this research and make recommendations for future research.

V. Discussion and Conclusion

5.1 Review

The result of this research support the Cyber Incident Mission Impact Assessment project, whose purpose is to provide decision makers with timely notification and relevant mission impact estimation, from the instant an information incident is declared, until the incident is fully remediated. This study demonstrated a proof-of-concept in that it provided quantitative research to measure the effect of timely and relevant notification for cyber incident response on mission objectives.

The case study focused on the top two mission objectives representative of those found in an operational Maintenance Operations Center (MOC): 1) ensure aircraft status is reported accurately, and 2) ensure all information is entered accurately and timely into the Maintenance Management Information System (GO81). The case study provided experimental control, but simultaneously allowed enough flexibility to perform operational decision making tasks. This study objective was to compare the USAF incident notification process to the CIMIA incident notification process approach by evaluating both real-time response times following a cyber incident.

A hypothetical scenario was developed using a fictitious MOC to induce manipulations that resulted in the loss of confidentiality, integrity and availability posing a security incident to critically dependent information and communications technologies (ICT). The research evaluated the two incident notification processes by measuring the response time from the time a cyber incident occurred until it was recognized and a contingency action was taken by the subject.

5.2 Findings

The initial notification in the experiment contributed to the performance of the subjects in the second session of the experiment. The initial notification was significant ($F(1, 22) = 4.593$, $p = .043$), which indicates that subjects had a significantly better response time overall with pop-up notification. The subjects that received the NOTAM as the initial notification performed worse than the subjects that received the pop-up first. Perhaps the subjects the received the pop-up first were just better at the task compared to the subjects receiving the NOTAM initially. Alternatively, the pop-up could have been some type of learning stimulus that contributed to improved performances that were observed. Subject's performance in response to the NOTAM in the second session of the experiment was better after being exposed to the pop-up. In each instance, the pop-up had a positive effect on performance, always encouraged better performance.

As predicted in H_a, the proposed CIMIA incident notification process had a statistical difference in the response time for subjects to recognize and take proper contingency actions in response to cyber incidents ($F(1,22) = 7.629$, $p = .011$). The data from the experimental conditions, shown in Table 5, provides insight that differentiates the two incident notification processes. The proposed CIMIA incident notification process reduces the response time as indicated in the mean thresholds. Subjects performed better regardless of when the proposed CIMIA incident notification process was received. The shortest response time was 11 seconds while the longest was 700. There are several reasons that could possibly explain why subjects took longer to respond:

- Subjects perhaps were inattentive because of the distractions in the experimental environment (e.g. emails and radio communications).
- Subjects perhaps did not completely understand the pop-up which required them to investigate the information in their environment before responding. It may have taken some subjects longer to recognize the meaning of the sensation, mental processing time.
- Subjects perhaps were trying to correct the discrepancies themselves before responding.
- Subjects perhaps did not have higher levels of SA immediately; they may not have realized what was happening and what would happen by not responding sooner.

These findings are consists with Ensley's performance-based measures of SA. Performance-based measurements evaluate the real-life actions of a subject and only make inferences to SA. However, using direct testable response gives a more concise measurement of SA, which "requires a discernible, identifiable action from the operator" (Endsley, 2000, p.203). The fact that subjects had to observe what was going on in their environment (information available), make an assessment about the current state (information processing), and understand that an action was required (an alert) is an indication of levels 1 and 2 of SA. According to Endsley, different measures of SA can be defined by the points in the decision making process. Once subjects understood that something was wrong in their environment, they made a decision about the projected future state of the system and perceived a need to take a course of action. The actions

taken by the subjects in response to the proposed CIMIA incident notification process are testable responses that reinforce inferred higher levels of SA.

In response to the four questions that indirectly measured SA, the mean scores increased in the second session of the experiment. As indicated by more errors being detected, number of personnel identified to be affected by the cyber incident, whether someone was notified, and persons actually notified of a cyber incident. Clearly, subjects had higher levels of SA and performed more successfully in the second session of the experiment which consequentially increased the number of discrepancies reported from the induced manipulations of cyber attacks. Subjects that received the NOTAM initially responded only 50 percent of the time to discrepancies, while 92 percent responded after being exposed to the pop-up. Conversely, subjects that were exposed to the pop-up initially responded 92 percent of the time to discrepancies and performance increased in the second session with 100 percent. Having the proposed CIMIA incident notification process initially perhaps alerted the subject to search more closely for discrepancies in the second session of the experiment.

The subjects preferred the proposed CIMIA incident notification process over the USAF incident notification process (rated not very useful). Based on the results from the post-questionnaire (reference Table 10), subject responses to the usefulness of the pop-up was extremely positive. This indicates that the subjects found the pop-up useful to identify discrepancies and improve their level of SA based on their performance and response time.

The NASA TLX workload assessment did not differ between the type of incident notification ($F(1,22) = .114$, $p = .0739$). This indicates that the proposed CIMIA incident

notification process did not manifest as increases or decreases in workload. Although the proposed CIMIA incident notification process improved performance there was no change in subjective measures of workload. The task demand between sessions of the experiment did not change, which in turn would not cause the subject to exert more effort, thereby not affecting their perceived workload. This suggests that the assessment of the workload is not sensitive to the type of incident notification. In addition, subjects could have perceived the tasks as easy and not have associated the type of incident notification with perceived workload. The performance-workload association is interesting in that increased performance is observed but not accompanied by increased workload. It was expected that workload manifest in terms of the amount of information to be processed for subject to have higher levels of SA.

Finally, analysis was conducted on all demographic factors. No demographic factors segregate itself significantly among the sample population (e.g. age, gender or academic level).

5.3 Limitations

Overall, the subjects performed significantly better than expected with the proposed CIMIA incident notification process than the USAF incident notification process. The response rate increased 58 percent with the CIMIA incident notification process. However, this study was limited in several ways because of the scarcity of subjects.

A limitation to this study exists within the sampling population in that only 25 subjects participated, with the majority being freshmen from a civilian institute.

Although the CIMIA project is being developed for a military environment, it is expected to provide utility to any organization that exhibits critical temporal mission-to-information dependencies (Grimaila et al., 2009b). The sample population was not entirely representative of the general public and did not equate to personnel in operational positions.

As stated before, the within-subject design was selected because of the scarcity of subjects. All subjects performed moderately better in the second session than the first session of the experiment, which could have been the result of a carryover effect. Keppel (1980) suggest that the "primary problem is the influence on the subjects' behavior of residual effects from previous conditions combing with the currently administered treatment" (p.177). Therefore, it is not always clearly distinguishable which particular condition may have caused a response. In such a case, the proposed CIMIA incident notification process could have alerted a subject to a sense of urgency. In addition, the use of a within-subject design also limited the number of intended treatments.

The experimental design originally was suppose to test all three adverse events that threaten CIA. However, the majority of the subjects only received the loss of availability and loss of integrity. 78 percent experienced an availability breach while 86 percent experienced an integrity breach. In comparison, only 28 percent received a confidentiality breach. The cyber incidents occurred based on the subject's performance to progress through the datasheets within the 30 minutes for each session. The cyber incidents occurred two minutes after sheets 5, 9, and 13 were entered (see Figure 10). If subjects did not progress through the specific number of datasheets, the cyber incident did not occur.

A final limitation of this study was that only one facilitator was available during the actual experiment. Because subjects were being evaluated on their response times to recognize and take proper contingency actions following a cyber incident, a telephone was used to report discrepancies. Hence, subjects had an option of placing a call to six different extension numbers. However, the same facilitator was the receiver of the call at every extension number in the same room. This was noted as a limitation because it made the experiment seem unrealistic to the subjects.

5.4 Contributions to Research

The data collected has determined the efficacy of having a DSS in place to monitor the status of critical ICT. The results of this research confirm positive empirical results, one future outcome would be to replace the manual effort required to coordinate with system owners and custodians to determine which organizations are potentially affected by a cyber incident. As a result, this research effort can be operationalized by infusing a reliable CIMIA incident notification process into the workplace, where deemed appropriate, improving the push method utilized by the USAF. By doing so, organizations would benefit from real-time notification following a cyber incident.

5.5 Future Research Recommendations

One important direction for research is to conduct more experiments that examine actual SA. This will enable direct evaluation of the effects of the proposed concepts of CIMIA to enhance SA. According to Endsley, without a more direct evaluation it will be impossible to tell if a proposed concept actually helps SA or inadvertently compromises

it in some way. The Situation Awareness Global Assessment Technique is one technique that has demonstrated reliability as a measure of SA in empirical investigation (Endsley, 1995). It is used to capture an operator's SA as an objective means by which to quantify SA. The subjective measures of SA or indirect measures of SA used in this study are not true presentations of actual SA.

A second direction is to more closely examine the nature of the tasks used. There needs to be more research on the results of not receiving or responding to an incident notification to determine mission impact estimation. This will allow further investigation into the concepts of CIMIA in that the length of time required for mission personnel to recognize and take proper contingency action in response to cyber incidents is time sensitive to reduce mission impact.

Because the subjects in this study were novices and did not have operational backgrounds, one could argue that the CIMIA incident notification process adapted the subjects to a sense of urgency to take a contingency action. Subjects could have responded by chance resulting in a lower level of SA, not correctly perceiving pieces of information in the situation. Further research is needed on the CIMIA incident notification process by personnel in a specific domain to evaluate the development of higher levels of cyber SA.

A final recommendation for future research is a more robust experimental design. The experimental design selected in this study examined the mean of within-subjects responses to the two incident notification processes. A fundamental disadvantage of within-subjects designs is carryover effects. Increased performance was observed in the second session of the experiment for subject that received the pop-up initially.

Therefore, further research is needed with a between-subject design to eliminate the possibility of carryover effects.

5.6 Conclusion

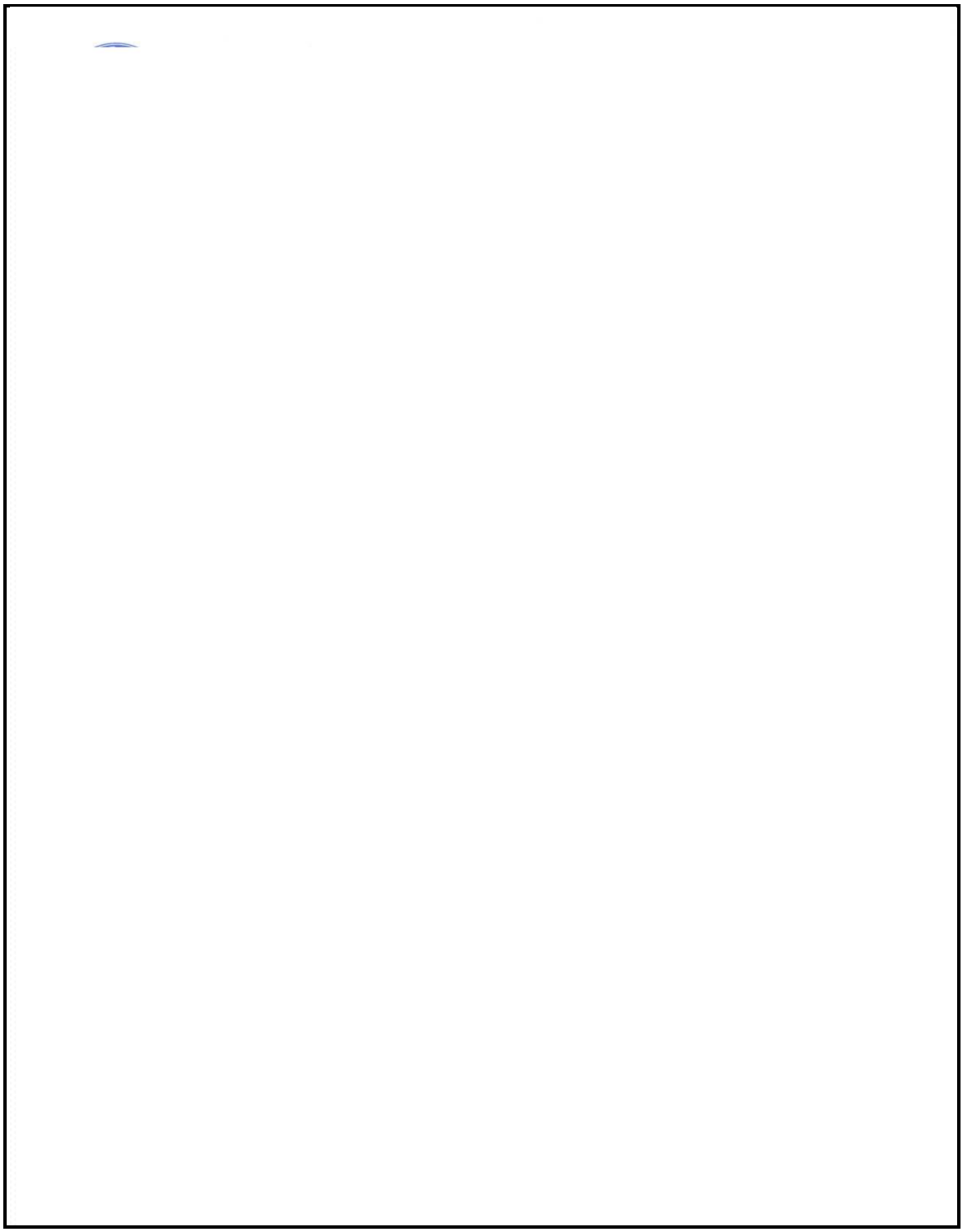
The AF has recognized that it must defend cyberspace from increasing threats and attacks against critical information and communication technologies (ICT) aimed at the manipulation or destruction of information. The Air Force has taken several steps to mitigate these threats and dominate operations in the cyberspace domain by developing cyberspace forces and capabilities to organize, train and equip a full range of defensive operations. Cyberspace combat and support forces have been consolidated under the 24th Air Force component of the Air Force Space Command to protect the information realm which is a central component of the way decision makers fight wars. However, today cyberspace is experiencing a time of increasing threats to information caused by inadequate cyber security. One major problem is decision makers may or may not be notified when a cyber incident occurs and not understand the relevance of received notifications to maintain situation awareness of potential and actual impact to their mission. As a result, ICT are at risk of a cyber attack that compromise confidentiality, integrity, and availability (CIA) of embedded information. These types of threats against the information used by decision makers for day-to-day operations can have real mission impact consequences that range from severe degradation to mission failure. This threat is steadily increasing as adversaries operate in cyberspace. They would like nothing more than to gain access to critical ICT that decision makers depend on for mission accomplishment. Having this dependence requires that decision makers have adequate

status of the critical ICT entrusted to maintain mission objectives. Specifically, preemptive actions are required for decision makers to effectively secure the information assets they depend on and ensure information dominance.

Maintaining information dominance, the ability to collect, control, exploit and defend while denying an adversary the ability to do the same, must be the focus of decision maker's to deny an adversary cyberspace sanctuary. Dominance of information operations is an important strategic characteristic of cyberspace. Thus, it is important to utilize technologies to reduce threats and attacks on critical information assets, and to help allow for decision makers to maintain SA.

The results of this research challenges decision makers to take a closer look their information dependencies and exploit automation to maintain cyber SA. A paradigm shift is required to have a true appreciation for potential mission impacts following a cyber incident. Asset identification must be achieved through some type of risk assessment which explicitly documents and identifies information assets, information valuation, and mission-to-information dependencies. Therefore, the use of a methodology such CIMIA can be implemented improve the timely notification of downstream information consumers following a cyber incident.

Appendix A



Appendix B

Subject #_____

Post-Process Questionnaire

The following information will be used to characterize the individuals participating in this process. The data you provide will be summarized and will not be attributed to any particular individual. Your participation is strictly voluntary, but greatly appreciated.

1) Please provide the following information:
   - Please circle your relevant age group
     - 18 – 30 years
     - 30 – 45 years
     - 45 – 60
     - 60 and above
   - Please circle your gender:
     - Male
     - Female
   - Please circle your Academic Level:
     - No degree
     - Associate
     - Bachelor
     - Master
     - Doctoral/Research

1. How comfortable were you with the experiment, generally? (circle number)

Very uncomfortable Very comfortable

2. How comfortable were you with the first session? (circle number)

Very uncomfortable Very comfortable

3. How comfortable were you with the second session? (circle number)

Very uncomfortable Very comfortable

Subject #_____

4. In session 1, did you find anomalies in the data? (circle yes or no)

   Yes No

5. If you did find anomalies, who would be affected by them? (circle as many as appropriate)

   Self G081 Administrator

   GDSS Administrator 663rd Airlift Wing Commander

   663rd Maintenance Crew Headquarters Air Mobility Command

   Scheduler of Aircraft Pilots

6. In session 1, did you notify anyone of problems with the data? (circle yes or no)

   Yes No

7. If so, who? (circle as many as appropriate)

   663rd Group Commander 663rd Communications Squadron Help Desk

   663rd Squadron Commander G081 Help Desk

   663rd Command Post GDSS Help Desk

8. In session 2, did you find anomalies in the data? (circle yes or no)

   Yes No

9. If you did find anomalies, who would be affected by them?

   Self G081 Administrator

   GDSS Administrator 663rd Airlift Wing Commander

   663rd Maintenance Crew Headquarters Air Mobility Command

   Scheduler of Aircraft Pilots

Subject #_____

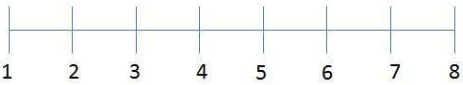
10. In session 2, did you notify anyone of problems with the data? (circle yes or no)

Yes No

11. If so, who? (circle as many as appropriate)

663rd Group Commander
663rd Communications Squadron Help Desk
663rd Squadron Commander
G081 Help Desk
663rd Command Post
GDSS Help Desk

12. How useful were the email NOTAMS? (circle number)

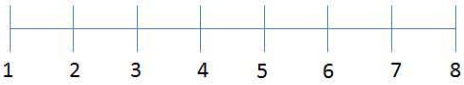


Not useful at all Extremely useful

13. How useful were the pop-up notices? (circle number)

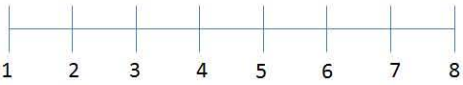
Not useful at all Extremely useful

14. Please rate your performance in session 1. (circle number)



Very poor Very Good

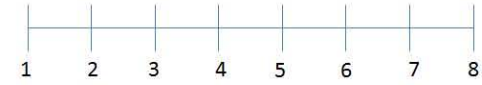
15. How confident are you in this rating? (circle number)



Not at all Extremely

Subject #_____

16. Please rate your performance in session 2. (circle number)



Very poor Very Good

17. How confident are you in this rating? (circle number)

Not at all Extremely

Appendix C

Cyber Incident Mission Impact Assessment Case Study
Instructions for Facilitator

Procedures for Setting up Training Session

Complete the following steps for Training Session:

On the computer marked 1

1. Open command prompt
2. Run P1
3. Minimize command prompt
4. Open another command
5. Run P2
6. Minimize command prompt
7. Open a third command prompt
8. Type cd C:\CIMIA
9. Type Cleanit1

On the computer marked 2

1. Open command prompt
2. Type cd C:\CIMIA
3. Type GO (command prompt should be minimized)
4. Select start experiment
5. Enter Subject ID
6. Select Training Session

Facilitator: General Instructions

Be sure to randomly select subject number before participant arrives.
Databases should be initialized for training session prior to participant arrival.
Do not close database anytime after a session has started. The full 30 minutes must be elapsed.
Set-up database for Session 1 while participant is reviewing the continuity binder.
Set-up database for Session 2 while participant is on break.
Record each subjects experiment file (experiment.dat) and TLX results in subject folder after each session (VERY IMPORTANT).

Procedures for Completing Consent Form

Have the participant read and sign consent form. Review consent with participant for clarification.

Script for Review:

Thank you for offering to participant in the "Cyber Incident Mission Impact Assessment Case Study" research. The purpose of this research is to evaluate the effectiveness of a proposed prototype software tool.

Here's what you can expect:

- You will be asked to take the role of a Shift Supervisor. Part of your job will be to enter data into a database and verify that it is accurate. This information will be shared between two systems so you should check to verify that the information was accurately pushed to the second system. You will also be asked to monitor email, answer calls and listen for and write down radio communications.
- Your participation is expected to take less than 2 hours. You can take a break any time, but please let me know so I can keep an accurate record of the time you spent on the task. The experiment is divided into two sessions. Each session will last about 30 minutes. After completing each session, you'll be asked to complete a short workload assessment. You will then be given a 10-15 minute break before beginning the second session.
- The second session will be the same as the first. After that session, you'll be asked to take about 5 or 10 minutes to provide some demographic information and answer a few written questions about how you felt about the experiment.
- The risks associated with participation are low – about the same as working in an office. When you are finished with the experiment, you'll be debriefed and given the opportunity to express any concerns you have.
- Your participation is completely voluntarily. You are under no obligation to participate and may choose not to begin the study or to leave the study at any time.
- Your data will be combined with those of others and no personally identifying information will be shared with anyone.

Facilitator: Do you have any questions on the information I just covered?

Facilitator: Sign the consent form and file consent form.

Script for Experiment:

In this experiment you are assuming the role of a Shift Supervisor who is responsible for ensuring Rickenbacker's fleet of aircraft are maintained. The fleet contains a total of 18 aircraft assigned to the 663rd Maintenance Group. In this role, you keep track of every assigned aircraft and the aircraft's current mission capability. You ensure timely and accurate support of everyday and exercise related missions while managing computer-based platforms that include the Global Decision Support System II (GDSS) and the GO81 system. You are tasked with the crucial responsibility of flawless orchestration of maintenance operations to ensure timely and accurate support to Headquarters Air Mobility Command.

You have just reported to the Maintenance Operations Center (MOC) for swing duty. The day-shift Shift Supervisor has just briefed you on the daily events and gives you a backlog of updates to enter into GO81. The database was unavailable part of the day for scheduled maintenance. As a result, several updates need to be entered into the database for accurate status reporting on the 663rd fleet of aircraft. The scheduled system maintenance on GO81 was advertised in advanced and all system users are aware that the system is back online. Your objectives in this study are to accurately enter all data from the data sheets into GO81 and ensure the information is accurately pushed to GDSS, monitor email, listen for and write down radio communications and answer any calls that come into the Maintenance Operations Center based on your understanding of the mission.

Here is a short mission brief about the wing's mission at Richenbacker AFB and how the Maintenance Operation Center helps the wing as a whole by ensuring the mission is accomplished.

Facilitator: Start power point presentation on smart board.

Before you begin the experiment, you will have a training session to get you familiar with utilizing the GO81 database, verifying the accuracy of data between the two databases, and using email, phone and radio.

Now let's go over to the experiment environment to begin your training session.

Script for Explaining Experimental Environment:

Please have a seat and I will go over the experimental environment.

- The two smaller monitors directly in front of you are for the system you will utilize during the experiment. The smaller monitor on your right displays the data you will enter from the data sheets into the GO81 database.
- You will use the smaller monitor on you left to monitor email.

Facilitator: Ensure database is up and running. Demonstrate to participant when giving instructions in script for training session.

Script for Training Session:

- Here are your training data sheets. In order to enter data into the database, click on any part of the row with the aircraft tail number located on the data sheet to bring up a data entry form. All the fields on the data sheets are on the data entry form. However, the fields are not in order.

- You will need to verify the information in each field. If a field is blank on the data sheet and the entry form has information, you will need to delete the information in the editable

fields or select NA in the dropdown field; otherwise, the information in the database will be inaccurate.

- After you have entered all the information provided on the data sheet click save. If you need to go back to the entry form, simply click on the any part of the row that contains the tail number. If you select the wrong row, click close on the entry form.

- The discrepancy field displays in the database under the remarks column. When there is a discrepancy with the aircraft, the remark field is displayed with a Y. When there is not a current discrepancy with the aircraft, the remark field is displayed with a N.

Facilitator: Do you have any questions on the information I just covered?

To begin the training session, please click on the start experiment button in the bottom left-hand corner of the screen. I will enter your subject number and start the practice session. Please let me know when you are comfortable with the data entry part of the task.

Facilitator: Starts training session.
Participant: Completes training session.

Facilitator: Do you have any questions so far?

Script for Training Session (continued):

Now that you are familiar with how to utilize the GO81 database, I will explain how to verify the accuracy of the information between the two databases.

- The two large monitors display the databases that share information. The large monitor on your right shows a summary of the aircraft owned by the 663rd Maintenance Group. The data that you enter from the data sheets should appear in this database, GO81, within a few seconds after you have selected save on the data entry form. This database is the same database that is displayed on the small monitor on the right.

- The large monitor on the left displays the GDSS database. Within 2 minutes after you have entered data into GO81, the information should appear in the GDSS database. This database is used by Headquarters Air Mobility Command to task missions. You should monitor both databases and verify that the information was accurately pushed from the GO81 database, on the monitor on your right, to the GDSS database, on the monitor on your left. In order to verify this information, you'll have to compare the information in each field for each tail number in both databases. Remember, that GDSS should be updated within 2 minutes after you have entered data into GO81.

- Notice when verifying the information that the two databases do not display the same information fields. The databases have 8 columns that are the same; the remaining columns display different information about the aircraft. If you notice inaccuracies, report the discrepancy with a detailed description.

- Let's look at the first data sheet you entered into GO81 and verify that the information was pushed to GDSS.

Facilitator: Demonstrate how to compare the information between the two databases. Point out the tail number and the columns of information that are same between the two database and the columns that are unique.

Facilitator: Do you have any questions on the information I just covered?

Script for Training Session (continued):

During the experiment, you will also be asked to monitor email. The email client is Mozilla Thunderbird which is displayed on the monitor to your left. It has the same basic functions as other email clients such as hotmail, yahoo, and Gmail.

- Your inbox is the organizational email account for your position in the Maintenance Operations Center. This is the icon on desktop to open email. Please do not close the email client at any time.
- You are to read and answer any emails received in a timely manner. When viewing an email you have the option of reading the email in the view pane below your inbox or clicking on the email for it to open in full screen. Emails in full screen open in a tab on the task bar.
- You can organize the inbox any way you like. There are a few subfolders available for you to file an email.
- You can create an email by clicking on write in the upper left-hand corner of the screen. The address book is populated with email addresses available for your use.
- You can also reply, forward or delete any email by clicking the specific option in the upper right-hand corner of the opened email.

Facilitator: Do you have any questions on the information I just covered?

Script for Training Session (continued):

During the experiment you should also answer any calls that come into the Maintenance Operations Center.

- Please answer all calls by stating "663rd MOC, Shift Supervisor".

- You can place a call at anytime during the experiment. Instructions on how to make calls are available in the continuity binder which also has useful phone numbers.

Facilitator: Do you have any questions on the information I just covered?

Script for Training Session (continued):

Finally, during the experiment you should listen for radio updates.

- Radio updates will be heard through the desktop speakers. You will not interact with the radio or be able to have an update repeated. However, the radio updates will always broadcast twice. If you do not record or understand the update, write the time of the update.

Facilitator: Do you have any questions on the information I just covered?
Facilitator: Additional information:

You have a few other resources available to you during the experiment.

- A notepad is provided for you to take any notes and record radio updates.
- Also, on the computer desktop is the Maintenance Snapshot. This schedule includes the flying schedule for the next several days. You will not have to make any changes or updates to the schedule but you may want to reference it. (open file to see if they understand it)
- A continuity binder is provided for your use.

Before you begin the actual experiment, please take a few minutes to look over the information in the continuity binder. Let me know when you are done.
At the end of the experiment, the database will close letting you know that the experiment has ended. Please let me know when this happens so I can begin the workload assessment for you.

Script for NASA TLX Workload Assessment:

The workload assessment is a two-part evaluation procedure consisting of both ratings and weights. The ratings evaluation you are about to perform is a technique that has been developed by NASA to assess the relative importance of six factors in determining how much workload you experienced. This set of six rating scales will be used to evaluate your experience during each session of the experiment (Hand scale sheet to participant).

Please read the descriptions of the scales carefully. If you have a question about any of the scales in the table please ask me about them. It is important that they be clear to you. You may keep the descriptions with you for reference during the assessment.

You will evaluate the session you just completed by marking each scale at the point that matches your experience. Each line has two endpoints descriptors that describe the scale. Note that

"performance" goes from "good" on the left to "poor" on the right. This order has been confusing for some people. Mark the desired location. Please consider your responses carefully in distinguishing among the task conditions. When rating, only reflect on the session you have just completed. Also, please consider each scale individually. Although, the definitions may be similar for two or more scales, try to distinguish them from each other based on my explanations and the definitions provided.

Please practice using the ratings scales.

The second part of the workload assessment is weights. At the completion of the experiment you'll complete a weights workload assessment. You will be presented with a series of pairs of rating scales titles and asked to choose which of the items was more important to your experience of workload in the experiment.

If you have any questions, please ask them now. Otherwise, start whenever you are ready.

Procedures for Setting up Session 1

Complete the following steps for Session 1:

On the computer marked 1

1. From third opened command prompt
2. Type Cleanit1
3. Verify databases are accurate

On the computer marked 2

1. From opened command prompt
2. Type GO
3. Select start experiment
4. Enter Subject ID
5. Select Session 1

Here are your data sheets for Session 1of the experiment. Please click on start experiment button in the bottom left corner of the screen. I will enter your subject number and start Session 1 for you.

Facilitator: Start Session 1.
Participant: Completes Session 1 of the experiment.

Facilitator: Start Ratings Workload Assessment.

Your ratings will play an important role in the evaluation being conducted, thus, your active participation is essential to the success of this experiment, and is greatly appreciated. Please begin and let me know when you are finished.

Participant: Completes Ratings Workload Assessment.

At this time you can take a 10-15 minute break before beginning the Session 2 of the experiment. Please let me know when you are ready to begin.

Facilitator: Save experiment.dat file and ratings.dje file in the subject number folder under CIMIA folder on C drive. Ensure that the files are saved in the folder marked for Session 1 of the experiment for the subject number (VERY IMPORTANT).

Facilitator: Set-up for Session 2 of the experiment.

Procedures for Setting up Session 2

Complete the following steps for Session 2:

On the computer marked 1

1. From third opened command prompt
2. Type Cleanit2
3. Verify databases are accurate

On the computer marked 2

1. From opened command prompt
2. Type GO
3. Select start experiment
4. Enter Subject ID
5. Select Session 2

Session 2

Here are your data sheets for Session 2 of the experiment. Please click on start experiment button in the bottom left corner of the screen. I will enter your subject number and start Session 2 for you.

Facilitator: Start Session 2.
Participant: Completes Session 2 of the experiment.

Facilitator: Start Ratings Workload Assessment.

Here are the scale descriptions for you to reference during your assessment. Please remember to consider responses carefully in distinguishing among the task conditions and only reflect on the session you have just completed. Please click continue.

Participant: Completes Workload Assessment.
Facilitator: Start Weightings Workload Assessment

You will be presented with a series of pairs of rating scales titles and asked to choose which of the items was more important to your experience of workload in the experiment.

If you have any questions, please ask them now. Otherwise, start whenever you are ready.

Facilitator: Enter subject number of questionnaire and give it to participant.

At this time, please take 5-10 minutes to complete this questionnaire and then I will give you a debriefing and address any questions or concerns you may have.

Participant: Completes questionnaire.

Script for Debriefing:

Thank you for participating in this study. This research is supporting an Air Force program that is investigating how military organization can maintain awareness of the information and communication technologies (ICT) they depend on for day-to-day operations. This dependence on ICT systems can place an organizational mission at risk when the loss of availability, confidentially and integrity of a critical ICT system occurs. In order to try to induce manipulations that resulted in the loss of confidentially, integrity, and availability, we deliberately presented you with some incorrect information, caused the information between the two system to be mismatch, and/or presented information that was meant to distract you. In this way, an honest appraisal of the two cyber incident notification processes could be evaluated. If you were frustrated by these manipulations or felt like your performance was worse than you expected or would have liked for it to be, I want to assure you that these responses are perfectly normal.

The goal of this study was to evaluate the utility of a Cyber Incident Mission Impact Assessment (CIMIA) incident notification process. This study focused on a proposed cyber incident notification that contributes to the objectives of the Air Force in that it provides decision-makers at all levels with timely notification and relevant information to maintain awareness of their critical ICT systems. A CIMIA incident notification process will provide real-time incident notification from the instant an information incident is declared, until the incident is fully remediated to downstream consumers. The data collected will be used to help evaluate the

efficacy of having a decision support system in place to monitor the status of critical ICT systems.

If you are feeling anxious or have any other concerns after participating in this experiment you should feel free discuss it with a research assistant today, and/or contact the project monitor at Wright-Patterson Air Force Base (Col William Butler at 937-656-5436 or william.butler2@wpafb.af.mil) to discuss it.

We would appreciate it if you did not talk about the methods used in this experiment or its purpose with others. If the purpose of or methods used in the study are known by future participants, they may not respond naturally to the computer simulations, which could change or bias their data and make the results of the study less reliable or valid.

Again, I appreciate your help and thank you for participating in this study. If you have any questions or concerns, please feel free ask them now or, if you think of anything later that you want to ask, feel free to contact MSgt Christy Peterson at (301) 537-3482 or at christy.peterson@afit.edu or Dr. Michael Grimaila at (937) 255-3636 ext 4800 or michael.grimaila@afit.edu

Appendix D

663rd Maintenance Operations Center
Shift Supervisor Continuity Binder

1.0. Roles and Responsibilities
  1.1. Shift Supervisor

2.0. Office
  2.1. Office Phone Etiquette
  2.2. Office Extension
  2.3. Dialing Instructions
  2.2. Radio
  2.3. Log Book

3.0. Mission Essential Task List
  3.1. Priorities

4.0. Frequently called numbers
  4.1. 663rd Group Commander
  4.2. 663rd Squadron Commander
  4.3. 663rd Communication Squadron Help Desk
  4.4. GO81 Help Desk
  4.5. GDSS Help Desk
  4.6 663rd Command Post

5.0. How to report a discrepancy in GDSS
  5.1 Reporting procedures

6.0. How to report a discrepancy in GO81
  6.1 Reporting procedures

7.0 GO81 and GDSS Database Field Information Table

8.0 Network Resource Map

1. Role and Responsibility

1.1. Shift Supervisor. Monitors and coordinates sortie production, maintenance production, and execution of flying maintenance schedules while maintaining visibility of fleet health indicators.

- Uses GO81 as the primary aircraft management tool to manage assigned aircraft information
- Ensures aircraft information is accurately entered into GO81 and reported in a timely manner
- Ensure aircraft information is accurately updated in Global Decision Support System
- Manages weekly maintenance flying schedule (located on desktop)
- Coordinates maintenance with maintenance unit, base supply, base operations, and command post
- Monitors and updated all owned aircraft regardless of the aircraft's location
- Monitors and records all radio transmission
- Answers all calls received and provides aircraft information as needed

2. Office

2.1. Office Phone Etiquette. Answer all calls as 663rd MOC Shift Supervisor

2.2. Office Extension. Extension number is 4000

2.3. Dialing Instructions.

Local calls:	Last 4-digit extension
Long Distance Toll Calls:	9+98+(area code+number)
DSN calls:	9+94+(region code, if applicable)+(number)
Emergencies:	911 or 9911

2.4. Radio. Radio transmissions are one-way and are broadcasted twice. Listen for and document all radio updates. If a transmission is not clear, document the time and continue with experiment.

2.5. Log Book. The log book is provided to take notes and annotate all aircraft updates.

3. Mission Essential Task List

3.1. Priorities

1) Ensure aircraft status is reported accurately in both GO81 and GDSS

- Aircraft Status: display aircraft status with following information as a minimum: serial number, location, priority, maintenance status and effective status time. Discrepancy narratives should be clear, concise, accurate, and include all pertinent data

2) Ensure all GO81 information is entered accurately and timely

4) Manage, coordinate and monitor aircraft arrivals, departures, parking.

5) Monitor aircraft priorities and direct manpower and support equipment to accomplish mission.

6) Informs affected activities of changes in priorities, plans, and schedules.

7) Coordinates on changes to the flying schedule with applicable agencies.

8) Coordinates on all aircraft engine runs and all aircraft ground movements conducted by maintenance personnel prior to execution.

9) Ensures all deviations to the daily flying schedule are reviewed and accurately reported.

- Flying Schedule: display the individual aircraft scheduled for flight each day with the following information columns, as a minimum: aircraft serial number, scheduled takeoff, actual takeoff, scheduled landing, actual landing, sortie configuration, call sign and remarks (located on desktop).

4. Frequently called numbers

4.1. 663rd Group Commander	x6501
4.2. 663rd Squadron Commander	x6502
4.3. 663rd Communication Squadron Help Desk	x6503
4.4. GO81 Help Desk	x6504
4.5. GDSS Help Desk	x6505
4.6. 663rd Command Post	x6506

5. How to report a discrepancy in GDSS

5.1. Reporting procedures. Report all system problems to the GDSS Help Desk.

When reporting include the following information:

1) Identify self and base location (e.g. MOC Shift Supervisor calling from Rickenbacker AFB)
2) Reason for call
3) Identify Aircraft Tail Number
4) Identify discrepancy (be specific- provide detail information about the discrepancy)

6. How to report a discrepancy in GO81

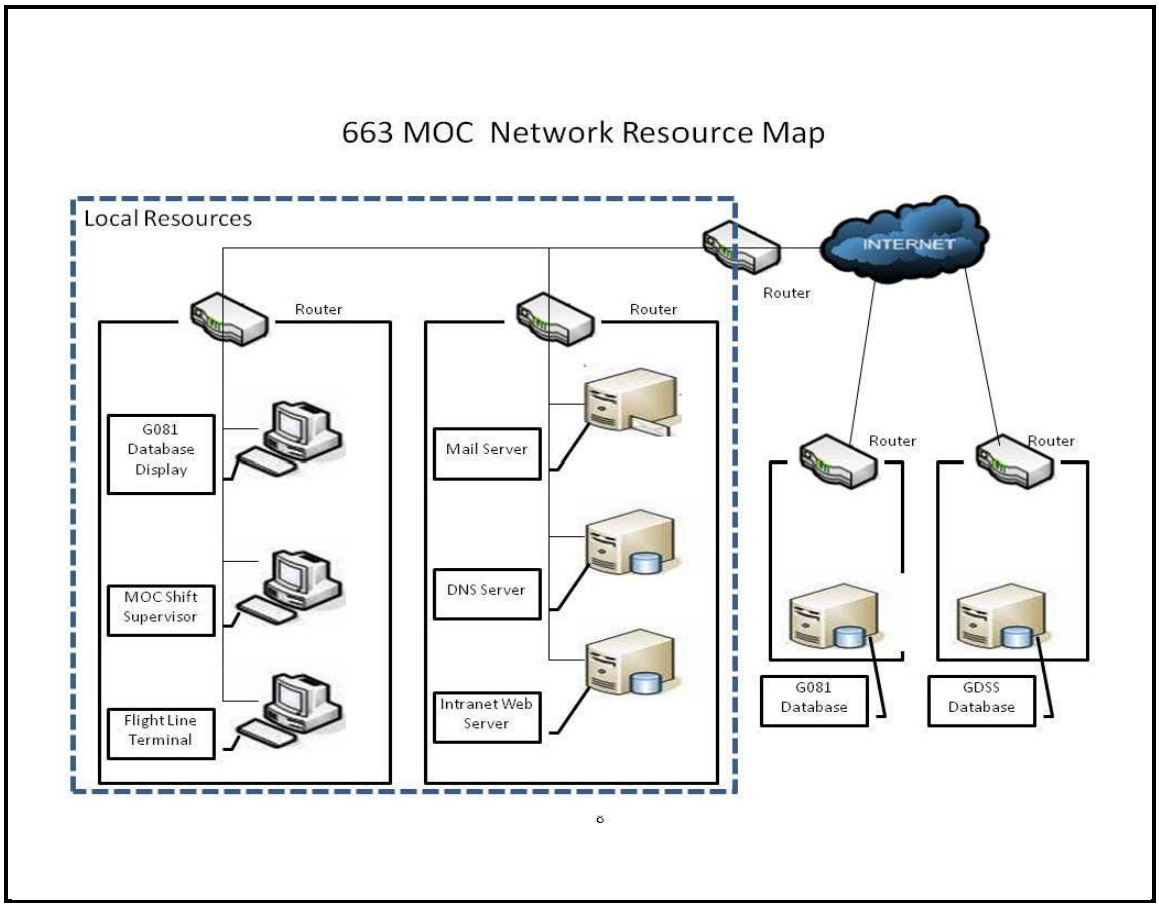
6.1. Reporting procedures. Report all system problems to the GDSS Help Desk.

When reporting include the following information:

1) Identify self and base location (e.g. MOC Shift Supervisor calling from Rickenbacker AFB)
2) Reason for call
3) Identify Aircraft Tail Number
4) Identify discrepancy (be specific- provide detail information about the discrepancy)

7. GO81 and GDSS Field Description Table

Field	Description
Serial Number (Serial #)	Aircraft serial number
Tail Number (Tail #)	Aircraft tail number
MDS	The first part is a letter which tells the kind of aircraft and the second part is a number which tells the model of the aircraft.
Owner	Unit aircraft is assigned to
Mission Number (current) (Mission #)	Unique number assigned to a mission
Call Sign	Unique designation for a transmitting station
Maintenance Status (Mx Stat)	Maintenance classification
	FMC - Full Mission Capable NMCB - Not Mission Capable Both Maintenance and Supply NMCM - Not Mission Capable Maintenance NMCMS - Not Mission Capable Maintenance Scheduled NMCMU - Not Mission Capable Maintenance Unscheduled NMCS - Not Mission Capable Supply PMCB - Partial Mission Capable Both Maintenance and Supply PMCM - Partial Mission Capable Maintenance PMCS - Partial Mission Capable Supply
Priority	Mission priority level
Geographical Location (GEOLOC)	Alphabetic designations that represent specific places in the world.
Work Unit Codes (WUC)	Determines subsystem problems and repair actions associated w/piece of equipment or a system
Remark	Determines whether a discrepancy exist
Time	Mission departure time
Next1	Next mission assigned
Next2	Next mission assigned
Next3	Next mission assigned
MDS	Aircraft tasked
Unit	Unit that tasked aircraft
Effective Status Time (EffStatTime)	Time of aircraft status
Job Control Number (JCN)	Maintenance job control number
Shop	Specialist office assigned JCN
	JETS (Propulsion Systems) CND (Communications and Navigation Systems) ECM (Electronic Countermeasure Systems) GAC (Instrument and Flight Control Systems) HYD (Hydraulics Systems) MCS (Mission Communications System)
Member name	Name of specialist JCN is assigned to
Spot	Aircraft parking spot
Discrepancy	Description of maintenance issues or status


663 MOC Network Resource Map
Local Resources
INTERNET
Router
Router
Router
Router
Router
G081 Database Display
MOC Shift Supervisor
Flight Line Terminal
Mail Server
DNS Server
Intranet Web Server
G081 Database
GDSS Database

Appendix E

DATA COLLECTION SHEET

Subject#:

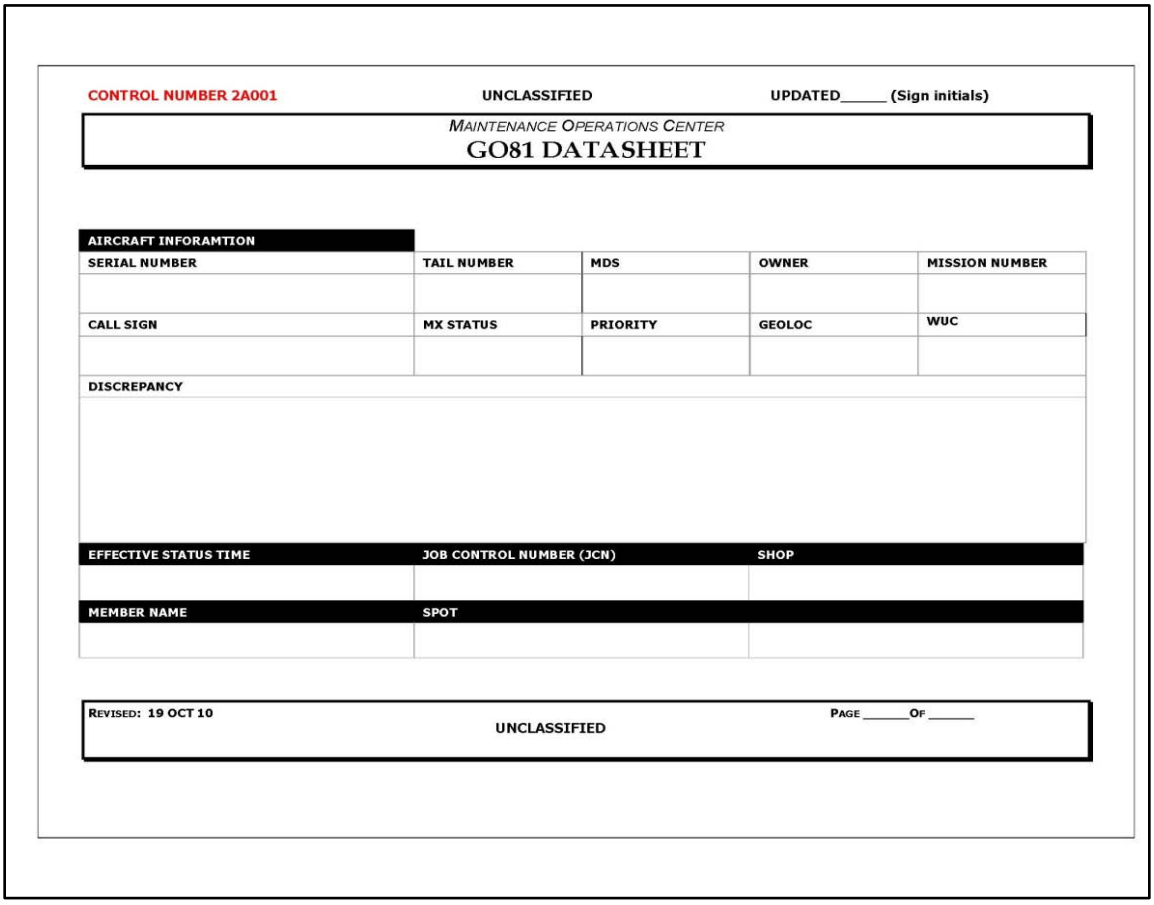
Session 1 Start Time: **Reported Discrepancy Y / N**

Treatment	Sent Email	# of Sheets	# of errors	NOTAM #1 Time	Notified/Time	NOTAM #2 Time	Notified/Time	(A) Time	Notified/Time	(I) Time	Notified/Time	(C) Time	Notified/Time
Y N	Y N												
Additional Calls:													
Remarks:													

Session 2 Start Time: **Reported Discrepancy Y / N**

Treatment	Sent Email	# of Sheets	# of errors	NOTAM #1 Time	Notified/Time	NOTAM #2 Time	Notified/Time	(A) Time	Notified/Time	(I) Time	Notified/Time	(C) Time	Notified/Time
Y N	Y N												
Additional Calls:													
Remarks:													

Appendix F



CONTROL NUMBER 2A001 UNCLASSIFIED UPDATED_____ (Sign initials)

MAINTENANCE OPERATIONS CENTER

GO81 DATASHEET

AIRCRAFT INFORAMTION				
SERIAL NUMBER	TAIL NUMBER	MDS	OWNER	MISSION NUMBER
CALL SIGN	MX STATUS	PRIORITY	GEOLOC	WUC
DISCREPANCY				
EFFECTIVE STATUS TIME	JOB CONTROL NUMBER (JCN)	SHOP		
MEMBER NAME	SPOT			

REVISED: 19 OCT 10 PAGE _____OF _____

UNCLASSIFIED

Bibliography

Adams, M. J., Tenney, Y. J., and Pew, R.W. (1995). Situation awareness and cognitive management of complex systems. Human Factors: *The Journal of the Human Factors and Ergonomics Society Vol 37 Issue 1*, p. 85-104)

Adelman, L. (1991). "Experiments, Quasi-Experiments, and Case Studies: A Review of Empirical Methods for Evaluating Decision Support Systems," *IEEE Transaction on Systems, Man, and Cybernetics, Vol. 21 No. 2*, March/April 1991.

Alberts, C.J., A. Dorofee, J. Stevens, and C. Wooky. (2003). "Introduction to the OCTAVE approach," Pittsburgh, PA, Carnegie Mellon University, 2003.

Alberts, C.J. and A. Dorofee. (2005). "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," Networked Systems Survivability Program, Carnegie Mellon University.

Bailey, B. P., Konstan, J. A., & Carlis, J. V. (2000). "Measuring the Effects of Interruptions on Task Performance in the User Interface." Paper presented at the IEEE Conference on Systems, Man and Cybernetics, Nashville, TN.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers, p. 19.

Committee for National Security Systems. (2010). *National Information Assurance Glossary.* Instruction 4009. 1 June 2010.

DeCoster, J., (2001). "Transforming and Restructuring Data." Department of Psychology. University of Alabama.
Retrieved from
http://www.stat-help.com/struct.pdf

Department of the Air Force. (2010). *Aircraft and Equipment Maintenance Management.* AFI 21-101. Washington: HQ USAF. 26 July 2010.
Retrieved from
http://www.e-publishing.af.mil/shared/media/epubs/AFI21-101.pdf

Department of the Air Force. (2010). *Depot Maintenance Management.* AFI 21-102. Washington: HQ USAF. 19 July 1994.
Retrieved from
http://www.e-publishing.af.mil/shared/media/epubs/AFI21-102.pdf

Department of the Air Force. (2010). *Equipment Inventory, Status and Utilization Reporting*. AFI 21-103. Washington: HQ USAF. 9 Apr 2010. Retrieved from

http://www.e-publishing.af.mil/shared/media/epubs/AFI21-103.pdf

Department of the Air Force. (2005). Enterprise *Network Operations Notification and Tracking*. AFI 33-138. Washington: HQ USAF. 28 November 2005. Retrieved from http://www.e-publishing.af.mil/shared/media/epubs/AFI33-138.pdf.

Department of the Air Force. (2010). *Cyberspace Operations.* AFDD 3-12. Washington: HQ USAF. 10 July 2010.

Department of Defense. (2010). *DoD Policy and Responsibilities for Critical Infrastructure.* DoDD 3020.40. Washington: United States Department of Defense. 14 January 2010.

Department of the Air Force. (1998). *Information Operations.* AFDD 2-5. Washington: HQ USAF. 7 August 1998.

Department of the Air Force. (2010a). *Web Management and Internet Use.* AFI 33-129. Washington: HQ USAF. 3 November 2010.

Endsley, M.R., (1995). "Measurement of situation awareness in dynamic systems." Human Factors, 37 (1), p. 65-84.

Endsley, M. R. (1996). "Automation and situation awareness." *In R. Parasuraman & M. Mouloua (Eds.), Automation and human performance: Theory and applications (p. 163-181).* Mahwah, NJ: Erlbaum.

Endsley, M.R. and Jones, W.M. (1997). "Situation Awareness and Information Dominance and Information Warfare." United States Air Force Armstrong Laboratory. February 1997. http://www.satechnologies.com/Papers/pdf/IW%26SAreport%20.pdf

Endsley, M.R. (1988). "Design and evaluation for situation awareness enhancement." *In Proceedings of Human Factors Society 32nd Annual Meeting (Vol. 1 p. 97-100).* Santa Monica, CA Human Factors Society.

Endsley, M.R. and Garland, D.J. (2000). "Situation Awareness and Analysis and Measurement." CRC Press, Boca Raton, FL.

Endsley, M. R., & Jones, D. G. (2001). "Disruptions, Interruptions, and Information Attack: Impact on Situation Awareness and Decision Making". *Paper presented at the Human Factors and Ergonomics Society 45th Annual Meeting.* Santa Monica, CA.

Ephrath, A. R., and Young, L.R. (1981). "Monitoring vs. man-in-the-loop detection of aircraft control failures." *In J. Rasmussen and W.B Rouse (Eds.), Human dection failures*. New York: Plemun Press.

Fields, A., (2005). *Discovering Statistics Using SPSS*. Sage Publications Ltd, London.

Fischoff, B., Riley D., Kovacs D.C., and Small M. (1998). "What Information Belongs in a Warning? A Mental Models Approach," *Psychology and Marketing*, Vol. 15 Issue 7, p. 663–86.

Fortson, L.W. and Grimaila, M.R. (2007). "Development of a Defensive Cyber Damage Assessment Framework," *Proceedings of the 2007 International Conference on Information Warfare and Security (ICIW 2007*). Naval Postgraduate School, Monterey, CA.

Fortson, L.W. (2007). "Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology," Master's Thesis, AFIT/GIR/ENV/07-M9, Department of Systems and Engineering Management, Air Force Institute of Technology, Wright-Patterson AFB, March 2007.

Grimaila, M.R. and Fortson, L.W. (2007). "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," *Proceedings of the 2007 IEEE Computational Intelligence for Security and Defense Applications (CISDA 2007).* Honolulu, HI, pp. 206-212.

Grimaila, M.R., Mills R.F., Fortson, L.W., and Mills, R.F. (2008a). "An Architecture for Cyber Incident Mission Impact Assessment (CIMIA)," *Proceedings of the 2008 International Conference on Information Warfare and Security (ICIW 2008).* Omaha, NE 2008

Grimaila, M.R., Mills, R.F., and Fortson, L.W., (2008b). "An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mision Impact Assessment," *Proceedings of the 2008 International Command and Control Research and Technology Symposium (ICCRTS 2008).* Bellevue, WA

Grimaila, M.R., Fortson, L.W., and Sutton, J.L. (2009a). "Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process," *Proceedings of the 2009 International Conference on Security and Management (SAM09).* Las Vegas, NV 2009

Grimaila, M.R., Schechtman, G., and Mills, R.F. (2009b). "Improving Cyber Incident Notification in Military Operations," *Proceedings of the 2009 Institute of Industrial Engineers Annual Conference (IERC 2009).* Miami, FL.

Grimaila, M.R., Mills, R.F., Haas, M., and Kelly, D. (2010). "Mission Assurance: Issues and Challenges," *Proceedings of the 2010 International Conference on Security and Management (SAM10)*, Las Vegas, Nevada, July 12-15, 2010.

Hale, B. Grimaila, M.R., Mills, R.F., Haas, M., and Maynard, P., "Communicating Potential Mission Impact using Shared Mission Representations," *Proceedings of the 2010 International Conference on Information Warfare and Security (ICIW 2010)*, WPAFB, OH, April 8-9, 2010.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (task load index): Results of empirical and theoretical research. In P. A. Hancock & N. Meshkati (Eds.) *Human Mental Workload*. North-Holland: Elsevier Science Publishers, p. 139-183.

Keppel, G., (1982). *Design and Analysis: A Researcher's Handbook, Second Edition.* Prentice-Hall Inc., Englewood Cliffs, N.J.

Keppel, G. and Saufley, W.H. (1980*). Introduction to Design and Analysis: A Student's Handbook.* W.H. Freeman and Company: New York.

Kessel, C.J. and Wickens C.D. (1982). "The transfer of failure-detection skills between monitoring and controlling dynamic systems." Human Factors, 24, (1), p. 46-60.

Laughery, K.R., and Wogalter, M.S., (1997). "Warnings and risk perception." In: Salvendy, G. (Ed.), *Handbook of Human Factors and Ergonomics, 2nd Edition*. Wiley, New York, p. 1175–1197

Lehto, M.R., (1997). "Decision Making" *In Handbook of Human Factors & Ergonomics, Second Edition Salvendy, G. (ed*), John Wiley & Sons, NY.

National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems.* NIST Special Publication 800-30. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, March 2008.

National Institute of Standards and Technology. (2004b). *Standards for Security Categorization of Federal Information and Information Systems*. FIPS Publication 199. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, February 2004.

National Institute of Standards and Technology. (2010a). *Guide for Applying the Risk Management Framework to Federal Information Systems.* NIST Special

Publication 800-37, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, February 2010.

ISO. (2009). *Risk management — Principles and guidelines.* ISO 31000. Geneva, Switzerland.

ISO/IEC. (2009). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO/IEC 27000. Geneva, Switzerland. ISSA. (2005*).*

Miller, J.L. (2011), "An Architecture for Improving Timeliness and Relevance of Cyber Incident Notification," Master's Thesis, AFIT/GCO/ENG/11-09, Department of Computer and Electrical Engineering, Air Force Institute of Technology, Wright-Patterson AFB, March 2011.

Parasuraman, R. (1987). "Human-computer monitoring." Human Factors: *The Journal of the Human Factors and Ergonomics Society*, Vol. 29, p. 695-706.

Parker, D. B. (2008). "Diligence-Based Idealized Security Review." *Information Systems Security Association (ISSA).* Retrieved from https://www.issa.org/Library/Journals/2008/January/Parker-A%20Diligence-Based%20Idealized%20Security%20Review.pdf

Patten, M.L. (2009). *Understanding Research Methods: An Overview of the Essentials,* Seventh *Edition.* Pyrczak Publishing. Glendale, CA

Pipkin, D.L. (2000). *Information Security Protecting the Global Enterprise.* Hewlett-Packard Company.

Rosenthal, R., and Rosnow, R. L. (1991). *Essentials of Behavioral Research, Methods and Data Analysis*. McGraw-Hill Publishing. San Francisco, CA. p. 276-300.

Slick, R.F., Cady, E.T., and Tran, T.Q. (2005). "Workload Changes in Teenaged Drivers Driving with Distractions," *Proceedings of the Third International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design,* Rockport, Maine, p. 158-164.

Smith, K. and Hancock, P. A. (1994). "Situation awareness is adaptive, externally-directed consciousness." In R. D. Gilson, D.J. Garland, and J.M. Koonce (Editions), *Situational awareness in complex systems*. Embry Riddle Aeronautical University Press. Daytona Beach, FL. P.59-68.

Sorrels, D.M., Grimaila, M.R., Fortson, L.W., and Mills, R.F. (2008). "An Architecture for Cyber Incident Mission Impact Assessment (CIMIA)," *Proceedings of the 2008 International Conference on Information Warfare and Security* (ICIW 2008), Peter Kiewit Institute, University of Nebraska Omaha.

Title 44 U.S. Code, Chapter 35 – Coordination of Federal Information Policy, Subchapter II – Information Security (3531-3538). 2008. Retrieved from http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35.html

Wickens, C.D. (1992). *Engineering Psychology and Human Performance, 2nd Edition*. New York: HarperCollins.

Wickens, C. D., & Carswell, C. M. (1997). Information processing. In: Salvendy, G. (Ed.), *Handbook of Human Factors and Ergonomics, 2nd Edition*. Wiley, New York, p. 89-129.

Wickens, C.D. and Kessel C. J. (1979). " The effect of participatory mode and task workload on the detection of dynamic system failures." *IEEE Transactions on Systems, Man and Cybernetics*. SMC-9(1), p. 24-34.

Woskov, S. M. (2011), "Improving the Relevance of Cyber Incident Notification for Mission Assurance," Master's Thesis, AFIT/GIR/ENV/11-M06, Department of Systems and Engineering Management, Air Force Institute of Technology, Wright-Patterson AFB, March 2011.

Young, L.R.A (1969). "On adaptive manual control." *Ergonomics*, Vol. 12 Issue *4*, p. 635-657.

Yin, R.K, (1984) "Case Study Reseach: Design and Methods," Beverly Hills, CA: Sage Publications.

Zijlstra, F. R. H., Row, R. A., Leonora, A. B., and Krediet, I. (1999). "Temporal factors in mental work: Effects of interrupted activities." *Journal of Occupational and Organizational Psychology*, Vol. 72, p. 163-185.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
04/2011	Master's Thesis	May 2010 – Mar 2011

4. TITLE AND SUBTITLE

Measuring the Utility of a Cyber Incident Mission Impact Assessment (CIMIA) Process for Mission Assurance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Peterson, Christy L., Master Sergeant, USAF

5d. PROJECT NUMBER
10ENV297

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/11-M04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Douglas Kelly, PhD, Cyber Team Lead
Air Force Research Laboratory
711th Human Performance Wing
Sense-making and Organizational Effectiveness Branch (RHXS)
2698 G Street, Bldg 190
Wright-Patterson AFB OH 45433-7604
Comm: (937) 656-4391

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/HPW/RHXS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT Information is a critical asset on which virtually all modern organizations depend upon to meet their operational mission objectives. Military organizations, in particular, have embedded Information and Communications Technologies (ICT) into their core mission processes as a means to increase their operational efficiency, exploit automation, improve decision quality, and shorten the kill chain. However, the extreme dependence upon ICT results in an environment where a cyber incident can result in severe mission degradation, or possibly failure, with catastrophic consequences to life, limb, and property. These consequences can be minimized by maintaining real-time situational awareness of mission critical resources so appropriate contingency actions can be taken in a timely manner following an incident in order to assure mission success.

In this thesis, the design and analysis of an experiment is presented for the purpose of measuring the utility of a Cyber Incident Mission Impact Assessment (CIMIA) notification process, whose goal is to improve the timeliness and relevance of incident notification. In the experiment, subjects are placed into a model environment where they conduct operational tasks in the presence and absence of enhanced CIMIA notifications. The results of the experiment reveal that implementing a CIMIA notification process significantly reduced the response time required for subjects to recognize and take proper contingency actions to assure their organizational mission. The research confirms that timely and relevant notification following a cyber incident is an essential element of mission assurance.

15. SUBJECT TERMS

Mission Assurance, Cyber Incident Mission Impact Assessment, Cyber incident notification, experiment, risk management.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	18. NUMBER OF PAGES	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Grimaila, Michael R., PhD; AFIT/ENV
U	U	U	UU	126	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 785-3636 x4800 (Michael.Grimaila@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

Form Approved
OMB No. 074-0188