



**COMPARING INFORMATION ASSURANCE AWARENESS TRAINING:
A CONTENT ANALYSIS EXAMINATION OF AIR FORCE AND DEFENSE
INFORMATION SYSTEMS AGENCY USER TRAINING MODULES**

THESIS

John W. Fruge'

AFIT/GIR/ENV/08-M07

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/08-M07

COMPARING INFORMATION ASSURANCE AWARENESS TRAINING:
A CONTENT ANALYSIS EXAMINATION OF AIR FORCE AND DEFENSE
INFORMATION SYSTEMS AGENCY USER TRAINING MODULES

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

John W. Frugé

March 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

COMPARING INFORMATION ASSURANCE AWARENESS TRAINING:
A CONTENT ANALYSIS EXAMINATION OF AIR FORCE AND DEFENSE
INFORMATION SYSTEMS AGENCY USER TRAINING MODULES

John W. Frugé

Approved:

//signed//
Dr. Dennis D. Strouble (Chairman)

24 Mar 08
Date

//signed//
Dr. David P. Biros (Member)

24 Mar 08
Date

Abstract

Today, the threats to information security and assurance are great. While there are many avenues for IT professionals to safeguard against these threats, many times these defenses prove useless against typical system users. Mandated by laws and regulations, all government agencies and most private companies have established information assurance (IA) awareness programs, most of which include user training. Much has been given in the existing literature to laying out the guidance for the roles and responsibilities of IT professionals and higher level managers, but less is specified for "everyday" users of information systems. This thesis attempts to determine the content necessary to educate system users of their roles and responsibilities for IA. Using the NIST Special Publication 800-50 as a guide, categories of threats and knowledge areas are established and the literature is analyzed to verify these categories. The thesis closes with a comparison of the IA awareness training modules of the United States Air Force and Defense Information Systems Agency and a discussion of areas of further research concerning IA awareness training.

Acknowledgments

I would like to thank my advisor, Dr. Strouble, for all his advice and guidance. I would also like to thank my classmates for their support and friendship through some very trying times, not counting the thesis and coursework we all slogged through! My time at AFIT was a great experience.

Finally, I must give thanks to God, for His “peace that passes all understanding.”

Furthermore, to His blessings here on earth in the form of my wonderful children – you guys amaze and inspire me every day with your questions, thoughts, and love; and my loving, patient wife – you mean the world to me and I know I wouldn’t have gotten through this without your unwavering love and support. SHMILY!!!

John W. Fruge’

March 2008

Table of Contents

	Page
Abstract.....	iv
Acknowledgments	v
Table of Contents.....	vi
Table of Figures	viii
Table of Tables	ix
Introduction.....	1
Research Question.....	4
Training Requirements	5
Information Assurance and Awareness Defined	7
Thesis Layout	8
Literature Review	10
Federal Information Security Management Act	10
National Institute of Standards and Technology	11
Current IA Awareness Literature	15
Methodology	21
Introduction	21
Content Analysis	21
Summary	25
Analysis of Results	27
Introduction	27
Background	27
Results	29
Summary	31
Conclusion	32
Introduction	32
Discussion	32
Limitations.....	34
Areas of future research.....	35
Summary	36

	Page
Appendix A. Codebook	38
Section 1 – Coding Instructions	38
Section 2 – Glossary	40
Section 3 – Code Sheet.....	43
Appendix B. AF Information Protection Module	44
Bibliography	56

Table of Figures

	Page
The IT Security Learning Continuum (Wilson & Hash, 2003)	13
USAF Module - Example of Link Slide	28
DISA Training - Example of Roll-overs.....	28
USAF Module - Slide 17	39

Table of Tables

	Page
Awareness Topics (Wilson & Hash, 2003).....	15
Topic Coverage.....	29
Concept Occurrence Results.....	30
Similar Concept Occurrence.....	31
Zero Concept Occurrences.....	31

COMPARING INFORMATION ASSURANCE AWARENESS TRAINING:
A CONTENT ANALYSIS EXAMINATION OF AIR FORCE AND DEFENSE
INFORMATION SYSTEMS AGENCY USER TRAINING MODULES

Introduction

Within the past several years, there have been many high profile examples of governmental and corporate data loss. The Department of Veterans Affairs made headlines when, in May 2006, an analyst's home was broken into and an agency laptop, containing information (including social security numbers) on over 26 million veterans, was stolen (The Associated Press, 2006). The analyst responsible was in violation of agency policy. In January 2007, retail giant TJX Companies, parent company of TJ Maxx, Marshalls and other retail stores, admitted to having lost customer information to hackers. The company estimates 94 million (more than double the original figures of 45 million) credit and debit card numbers were taken from a company system by an unknown number of intruders (Vijayan, 2007). The company's wireless systems were left unsecure and the thefts went unnoticed for over 18 months (Vijayan, 2007).

Other retailers have felt the sting of indirect data breaches as well. In October of 2007, a backup computer tape was discovered missing from a warehouse run by Iron Mountain Inc, the backup storage provider to GE Money. GE Money handles credit card operations for J.C. Penney and many other retail stores. Information on the backup tape includes personal information for about 650,000 customers and Social Security numbers

for about 150,000 customers (The Associated Press, 2008). The backup tape is still missing.

Neither is the problem of data breaches confined to the United States. In England, two CDs, containing the entire database of child benefits, were lost in the mail. HM Revenue and Customs, the responsible office, reported information in the database included children's names, addresses, birthdates and National Insurance ID numbers as well as bank account information of parents and guardians (McCue, 2007). While the discs were mailed out on October 18, 2007, it wasn't reported internally until November 8, 2007; the public wasn't notified until November 20, 2007 (McCue, 2007). The bright spot in this story is the information on the discs was encrypted.

Sometimes the attacks originate from within the organization, rather than outside. In 2007, Fidelity National Information Services suffered a data breach in the form of a "rouge and dishonest employee" stealing records (The Associated Press, 2007). Most of the records stolen included individuals' bank account and personal information. The employee worked at a subsidiary, Certegy, and had stolen the information to sell to marketing companies through a self-owned company (The Associated Press, 2007).

Attackers are refining their form of operations too. The US Federal Bureau of Investigations released a warning concerning e-mail based attacks with a Valentine's Day theme (Keizer, 2008). In the past, attackers have utilized attachments, which, when opened by the user, pass along malicious code, such as Trojan horses or viruses. The newer method uses an IP-address-only link in the e-mail, in this case purporting to be a link to an e-card, leading to an infected computer on the botnet which then infects the target computer (Keizer, 2008).

With the frequency of attacks and data breaches, the actual financial cost is incredibly high to organizations. In 2006, companies responding to a survey from CSI/FBI reported an estimated \$52.49M lost to information security incidents (Gordan, Loeb, Lucyshyn, & Richardson, 2006). The respondents represented all areas of industry, ranging from medical to government to retail to financial to information technology. These incidents included computer viruses, laptop theft, denial of service, system penetration, financial fraud, and unauthorized access to information other various methods of attack. Methods used to combat these cyber-security incidents include firewalls, anti-virus and anti-spyware software, intrusion detection systems, access control lists (server based), encryption of data in storage and transit, and other defensive technologies (Gordan et al., 2006). With the consequences of losing or mishandling data shown to be so great, what can be done to protect an organization's data? Firewalls, intrusion detection software, penetration testing, anti-virus/anti-spyware software, among other things, can all provide layers of defense against data loss and intrusion (Gordan et al., 2006). But these methods really only provide a partial defense against the hackers, spies, and social engineers; in other words, the outside attackers working to get inside an organization's information systems. But that is only half the battle. Users represent a greater threat because of the trusted access given by the organization (Schou & Shoemaker, 2007). According to the CSI/FBI survey, over 65% of respondents contributed some organizational data loss to authorized users (Gordan et al., 2006). The survey also indicated respondents considered security awareness of employees to be very important to the overall security of the organization (Gordan et al., 2006).

Users make up the largest group within an organization and, as such, can be the difference between success and failure in an IT security program (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, Information Technology Security Training Requirements: A Role- and Performance-Based Model - NIST SP 800-16, 1998). To combat this ever-present problem, the organization must make users aware of the threats and vulnerabilities to maintaining information assurance and security. Beyond the basic need for IT security is government legislation, mandating organizations to establish IT security programs within certain guidelines (United States Congress, 2002). This legislation, in the form of either the Federal Information Security Management Act (FISMA) of 2002 or the Sarbanes-Oxley Act, also requires organizations to inform users of their rights and responsibilities when using information systems (United States Congress, 2002).

Research Question

Using the NIST SP800-50 as a guide, this thesis will compare two IA awareness training modules. Both training modules are specific to the Department of Defense (DoD), as opposed to private organizations. The first, developed by the US Air Force (USAF), is a web-based training program, utilizing graphics, sound and user interaction. The second, developed by DISA, has actually been adopted by the DoD for implementation by all sub-agencies. The DISA training is also web-based and includes the use of graphics, sound and user-interactivity. The research question can be broken down into three parts:

RQ 1: Does the AF IA awareness training module comprehensively cover the topic list put forth in the NIST SP 800-50?

RQ 2: Does the DISA IA awareness training module comprehensively cover the topic list put forth in the NIST SP 800-50?

RQ 3: Does one module incorporate more of the NIST topic list than the other module?

Training Requirements

Air Force Instructions (AFIs) concerning information assurance are governed by federal and Department of Defense (DoD) policies. These policies stem from the Federal Information Security Management Act (FISMA) of 2002 and from DoD Directive 8500.1, which required compliance with FISMA. DoD Directive 8500.1, *Information Assurance*, is instrumental in assuring that “all DoD information systems shall maintain and appropriate level of confidentiality, integrity, authentication, non-reputation, and availability that reflect a balance among the importance and sensitivity of the information and information assets” (DoD Directive 8500.1.) DoD Directive 8570.1, *Information Assurance Training, Certification, and Workforce Management*, sets the stage for our network security directives by requiring every DoD member to complete Information Assurance training before they are allowed to access the network (DoD Directives 8570.1.)

The AF, utilizing the guidance and authority from the DoD directive, has adapted a series of Air Force Policy Directives (AFPD) and Air Force Instructions (AFI) to

encompass network security for AF networks and information systems. AFPD 33-2, “Information Assurance (IA) Program,” provides overarching scope and direction for all things related to information security within the AF. AFPD 33-2 also implements IA policy that is based “on fact-based operational risk assessments; total risk avoidance is not practical in many cases and, therefore, risk assessment and management is required” (AFPD 33-2, 2007, p. 3.) This policy directive also clarifies the terms “information assurance” (as used in DoD and AF IA programs) and “information security” (per FISMA) as being synonymous in meaning. Specific instructions, roles, responsibilities and requirements for policy developers, commanders, information professionals and users are found in AFI 33-202, Volume 1, “Network and Computer Security.”

Though the AF has policy in place to establish information assurance awareness training, much of it is vague and all-encompassing in scope. AFPD 33-2, Section 4.6 discusses the education and training for IA professionals, indicating DoDD 8570.1, *Information Assurance (IA) Training, Certification and Workforce Management*, as the guide for IA programs. However, it is left to IA managers to develop programs to educate and make aware the users of policies and risks to the information systems, “commensurate with an individual’s respective responsibilities” (AFPD 33-2, 2007, p. 3.) The AF has implemented several iterations of information assurance awareness training required of the entire force. This training is required for initial access to AF network systems and then required annually (and in many cases, upon a permanent change of station) in order to maintain system access.

Information Assurance and Awareness Defined

Information assurance is concerned with protecting information as well as ensuring the availability of the systems and information used for access when needed (Conklin, White, Cothren, Williams, & Davis, 2004). The Air Force definition of information assurance is the “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.” (Air Force Information Protection Module, accessed Dec 2007) Schou and Trimmer (2004) reiterate this idea, but they cite only confidentiality (which includes all aspects of information security), availability and integrity. However, they expand the proposal of protecting and defending information by categorizing the methods into three fundamental countermeasures: technology, operations and awareness, training and education (Schou & Trimmer, 2004.) For purposes of this paper, the focus will be on the final category.

In his book “Information Security: Protecting the Global Enterprise,” Donald L. Pipkin (2000) devotes an entire chapter to awareness, discussing the importance of a user awareness program to overall system security. His perspective considers awareness in four parts: defining appropriate use, the makeup of the program, the design of the program and the implementation of the program (Pipkin, 2000.) The program should be relevant to each user in their capacity as it is very important to convey the roles and responsibilities to the users of an information system in order to protect the rights of both the company and the individual. Pipkin (2000) cites an example of a user in England who was fired for using an organizational computer inappropriately, but was reinstated when

the courts ruled the user was not appropriately made aware of the policies and the consequences of violating the policies.

The awareness program should be the first step for a user obtaining access to the organization's information systems and should be a continuous requirement as long as the user requires access. The program should not only pertain to the technological aspects of the environment, but should also focus on all aspects of information assurance. The program should communicate the importance of information security in a way that is readily understood by all users and should do so in a manner cost effective to the organization (Pipkin, 2000.)

Designing the program, Pipken (2000) says, should focus on the delivery methods, actual content of the message and the timeliness of the information within the training. Implementation is the final step for an awareness program. There are several options to implement the program, which could vary by organization. Keeping cost in mind, awareness can be executed across the entire user community, focused on smaller user groups or even by the individual (Pipken, 2000.) But beyond the value added of informing users of the importance of information security and appropriate system use, the Air Force has the force of law behind assurance awareness training.

Thesis Layout

Chapter 1 has introduced the topic and research questions. It also provided the background and definitions to be discussed within the thesis. Chapter 2 will provide an examination and discussion of the literature and lay the basis for the content analysis.

Definitions of information assurance, awareness, training and other key terms will be taken from the existing literature. This thesis will also explore the differences in training levels required for different user types, i.e. end-users, senior management, IT professionals. The threats to information assurance and security will also be examined as this presents some of the framework for required content in training programs. Though the focus of this thesis is on specific computer-based training programs, other methods of delivering IA training will be discussed, mostly to add to the content base to educate users, but also to discuss different ideas concerning IA programs.

The comparison of the two training modules will follow a modified content analysis research methodology, which will be discussed in greater detail in Chapter 3. Chapter 4 will review the results of the research, discussing the findings and the limitations of the methodology used in this thesis. Chapter 5 will offer conclusions based on the research and recommend areas of further research concerning the topic of information assurance awareness.

Literature Review

In 2002, the Federal Information Security Management Act (FISMA) was passed and dictated how information technology was to be viewed, used and managed within the federal government. FISMA tasked the National Institute of Standards and Technology (NIST) with establishing the standards organizations should use to fulfill FISMA requirements. Therefore, this research will review FISMA and NIST documents and requirements for information assurance training. In order to establish the authority and influence of the NIST standards, this thesis will provide examples from the literature applying these same ideas and, in some cases, specifically referencing NIST documents.

Federal Information Security Management Act

According to NIST SP 800-39, the E-Government Act of 2002 (Public Law 107-347) recognizes “the importance of information security to the economic and national security interests of the United States” (Ross, Katzke, Johnson, Swanson, & Stoneburner, 2007, p. 2). Title III of this act is what is commonly referred to as “FISMA”, the Federal Information Security Management Act. In FISMA, Congress stated that all national agencies would implement and report on information security programs. It is further stated an effective program would include, among other facets of information security, “...(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— (A) information security risks associated with their activities; and (B) their

responsibilities in complying with agency policies and procedures designed to reduce these risks;” (United States Congress, 2002, p. 53). FISMA can be viewed as an extension of the Computer Security Act of 1987, which was similar in scope and intent and required the recurring training in computer security awareness for “...all employees who are involved with the management, use, or operation of each Federal computer system...” (United States Congress, 1987, p. 3). The Computer Security Act of 1987 also established the authority of the National Bureau of Standards (NBS) in matters concerning standards and guidelines for computer systems in federal agencies. The next year, with PL 100-418, Congress changed the name of the NBS to the National Institute of Standards and Technology (United States Congress, 1988).

National Institute of Standards and Technology

It is through FISMA that the NIST is tasked with the general mission of developing “...standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency...” (United States Congress, 2002, p. 59). Given this mission, the NIST has published many documents concerning information security, including Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*; SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective (Draft)*; SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*; and, SP 800-50, *Building an*

Information Technology Security Awareness and Training Program. Each of these publications discusses the importance of raising user awareness in regards to system security and information assurance. NIST SP 800-50 is of particular interest to this thesis because it provides an authoritative list of topics and concerns relating to information assurance awareness training. It also establishes the difference between awareness, training, and education, as defined in NIST SP 800-16.

According to NIST SP 800-50, an organization should focus security awareness and training for all information system users. The purpose of this is two-fold: one, it provides the method of communicating security requirements and news across the organization; two, it describes the rules and regulations for using the IT systems and information (Wilson & Hash, 2003). It is important to distinguish between awareness, training, and education (See Figure 1) because each contributes differently to the security learning continuum (Wilson & Hash, 2003). NIST 800-16 defines the three terms as:

Awareness: “Awareness is not training. The purpose of awareness presentations is simply to focus attention on security.” (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998, p. 15)

Training: “The “Training” level of the learning continuum strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing).” (Wilson et al., 1998, p. 16)

Education: “The “Education” level integrates *all* of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles

(technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response” (Wilson et al., 1998, p. 16).

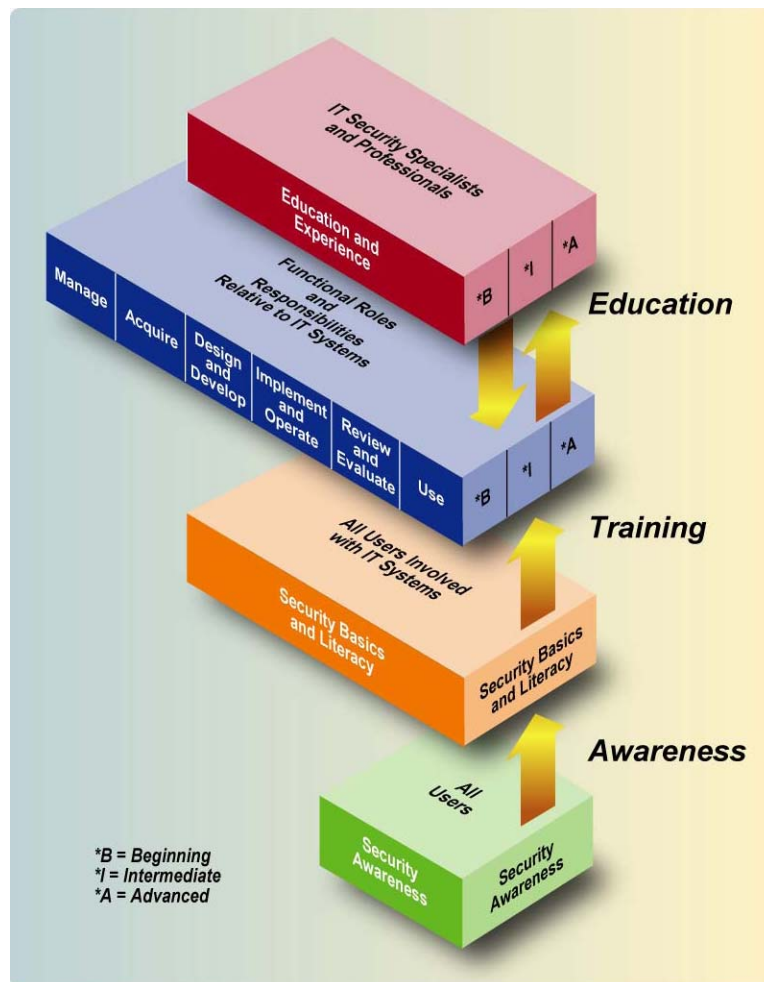


Figure 1 - The IT Security Learning Continuum (Wilson & Hash, 2003)

Awareness “campaigns” are used to simply establish user recognition of information security. Whether in the form of posters, computer log-on notices or weekly security e-mails, the goal is to reinforce a behavior in the users (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998). The user is simply a recipient of information.

Training, on the other hand, has the goal of “building knowledge and skills to facilitate the job performance” or specific skill(s) users should be able to apply (Wilson & Hash, 2003). As shown in the continuum model, NIST SP 800-16 recommends “a bridge or transitional stage between awareness and training...” (Wilson & Hash, 2003) This bridge is the security basics and literacy material, consisting of “a core set of terms, topics, and concepts” (Wilson & Hash, 2003).

To establish a security awareness and training program, a plan must identify the material to be covered. The list identified for each organization will provide the foundation for the entire security program (Wilson & Hash, 2003). However, not all organizations will necessarily require the same topics for security awareness and training; though many will be similar to all programs, the topics should be tailored to an organization’s policies, requirements and goals (Wilson & Hash, 2003). To aid in this, NIST 800-50 has provided a list of awareness topics that can be used (See Table 1). While an awareness program can consist of simple posters or e-mail messages, it is consistent with the literacy level of the learning continuum model, to incorporate more information on each topic (Wilson & Hash, 2003).

Table 1 - Awareness Topics (Wilson & Hash, 2003)

Password usage and management	Desktop security
Protection from malicious code	Incident response
Policy – implications of noncompliance	Shoulder surfing
Unknown e-mail/attachments	Changes in system environment
Web usage and monitoring of user activity	Inventory and property transfer
Spam	Personal use and gain issues
Data backup and storage	Handheld device security issues
Social engineering	Use of encryption
Supported/allowed software on organization systems	Laptop security
Access control issues	Personally owned systems/software at work
Individual accountability	Configuration management
Use of acknowledgement statements	Software license restriction issues
Visitor control and physical access to spaces	Protect information subject to confidentiality concerns
	E-mail list etiquette

Current IA Awareness Literature

In order to demonstrate the comprehensiveness of the awareness topics developed by NIST, the rest of this chapter will review books, articles, conference papers, and commercial white papers. This review will discuss the correlations between the academic and corporate literature and government publications in regards to information awareness training. This will provide the basis for using the NIST awareness topics as the tool for analyzing the Air Force and DISA IA training modules.

In the article, *Users Are Not the Enemy* (1999), Adams and Sass report on a comparative study conducted with two companies, one in the technology sector and the

other in construction. Concentrating on the confidentiality aspect of the security triad, the study focused on password issues, especially user behavior and password memorability. The study found “four major factors influencing effective password usage” (Adams & Sasse, 1999). These factors were related to multiple passwords, password content, perceived compatibility with work practices, and user perceptions of organizational security and information sensitivity (Adams & Sasse, 1999).

The problem associated with multiple passwords was the difficulty users had in remembering several different passwords without circumventing security policy, such as writing passwords down. Password content was a problem because of poor user knowledge of content requirements for passwords. The study also showed that some users would bypass security policies out of a perceived incompatibility with work practices, specifically dealing with groups and group passwords. Another reason the study gave for poor password usage among users was a lack of user knowledge of real security risks and threats. Adams and Sasse (1999) blamed this on “the authoritarian approach” that led to unwillingness on the part of security departments to share threat and risk information with users. Also, the security departments poorly educated users of security classification information, causing a disparity in how users treated sensitive information.

Adams and Sasse saw two problems for effective password usage among users: system and external factors. System factors are policies or requirements users feel the need to circumvent. External factors are centered on compatibility (or incompatibility) with working procedures. Both factors stem from a lack of communication between users and security. The authors make four recommendations, with all but one (the second)

consistent with the awareness topics in NIST 800-50: 1) Provide users better instruction/training for password content; 2) Reduce the need for multiple passwords or move to single sign-on for multiple systems; 3) Increase user visibility of system security and existing/potential threats; and 4) Provide system/information sensitivity (classification) guidance to users.

In the article “Security awareness: Switch to a better programme,” Everett C. Johnson, the immediate past international president of ISACA, discusses the need to inform users and develop and maintain a good security program (Johnson, 2006). (ISACA is an international organization focused on IT governance. It was formerly the Information Systems Audit and Control Association, but now is known solely by its acronym. (ISACA, 2008)) Though a defense for IT security expenditures, especially training for IT professionals, Johnson presents reasons for maintaining an IT security plan similar to those provided in NIST publications. Johnson (2006) asserts a good security program begins by changing the organization’s mindset. With more than 30% of IT security related incidents beginning from the inside of organizations, there is a definite need to make all users aware of good security practices (Johnson, 2006). The article also proposes a list of awareness topics common to any organization. This includes the security policy, major risks to info security, countermeasures, security incident reporting, and the basics of the security organization, such as functions, departments, and responsibilities (Johnson, 2006). The author also recommends including topics concerning physical access, classification guidance, viruses/Trojans, backup procedures, and proper use of equipment, Internet, and e-mail (Johnson, 2006). This list includes roughly half of the topics recommended in NIST 800-50.

Ives, Walsh, & Schneider (2004) also discuss password usage and management. In their article, “The Domino Effect of Password Reuse”, they note the problem with users reusing passwords on multiple systems is that all systems are now as unsecure as the least secure (Ives, Walsh, & Schneider, 2004). The article provides the following example: if a hacker captures passwords from a poorly secured system within an organization, there is a definite threat to the breached system. But if users have reused the same passwords for access to other, more secure systems, those systems are now exposed to the same threat (Ives, Walsh, & Schneider, 2004). The authors propose IT security should move away from passwords to Public Key Infrastructure/Encryption (PKI/PKE) in order to abate this potential risk to information assurance (Ives, Walsh, & Schneider, 2004). Ives et al. (2004) also recommend security training for users should be improved and even include technologies such as biometrics, smart cards, PKI, and PKE.

In the editorial preface to the initial edition of the *Journal of Organizational and End User Computing on Informational Security*, Schou and Trimmer discuss the importance of IA awareness training in the overall scheme of information security (Schou & Trimmer, 2005). They depict IA as being a triad of means, projecting a defense in depth, with technology and policy making up the top two levels. The third level, largest and most important, is the people within the organization, the users of the information (Schou & Trimmer, 2005). Though the editorial does not specify topics to include in IA awareness training, Schou & Trimmer (2005) cite NIST and the Committee on National Security Standards (CNSS) as the main standards for developing awareness, training, and education programs.

In a paper presented to conference proceedings for the Journal of Information System Security, the authors proposed ten domains for IA awareness training. The topics they recommended to emphasize in training are passwords, social engineering, e-mail, physical security, proper computer security (locking/logging off), internet usage, phishing and handling storage media and portable computers (Mellor & Noyes, 2005). Using NIST SP 800-16 as a guide, Mellor and Noyes (2005) created an IA awareness training model which utilizes a checklist to incorporate personal accountability in the training. The importance of this, according to the authors, is “it literally transforms the trainee from a passive learner to an active learner as they become individually accountable for the material presented.” (Mellor & Noyes, 2005) Each of the ten domains is a NIST recommended topic for awareness training and individual accountability, also an awareness matter, is applied in a distinct style.

There are also many organizations implementing IA awareness programs based partly or wholly on the standards laid out in NIST SP 800-50. The Department of Veteran Affairs covers the following topics in its VA Cyber Security Awareness Course: identification of information security officer, passwords, privacy and confidentiality, backups (data), viruses, incidents, infrastructure protection, social engineering, and authorized use of information systems (U.S. Department of Veterans Affairs). Each of these is included in the recommended awareness topics in NIST 800-50.

The state of Nebraska has published guides also using principles from NIST publications. Formed under the state’s Chief Information Officer’s office, the Nebraska Information Technology Commission (NITC) offers a handbook for information security officers as well as templates for writing an organization’s security policy, to include an

awareness program for employees (NITC, 2001). This guide stresses the importance of establishing security rules for system usage and recommends the following categories to be covered: access control; network security; e-mail, internet and e-commerce; workstation/office; physical/people security; copyright; acceptable use. The document also covers incident reporting, risks and threats, such as hackers, viruses, and social engineering (NITC, 2001).

To conclude, information assurance awareness training is vital to successfully defending an organization's information system. While there is much written about the issue of educating users, there is little in the way of a definitive catalog of essential awareness topics. The literature and current training programs seem to point to the same general themes important to user awareness. As discussed earlier in this chapter, these themes are neatly captured in NIST 800-50. This provides the basis for comparing the AF and DISA training modules as it is currently the most comprehensive and authoritative guidance on raising user awareness.

Methodology

Introduction

The purpose of this research was to determine the comprehensiveness of two information assurance awareness training modules. To do this, an initial baseline had to be determined. The literature review in Chapter Two established the baseline as the awareness topics laid out in NIST SP800-50. To compare the baseline and the training modules, a content analysis methodology was used. What follows in this chapter is an explanation of how this methodology was applied to the data. The chapter concludes with a review of the advantages and limitations of conducting content analysis research.

Content Analysis

As a methodology, there are several definitions of content analysis. Krippendorff defines it as “a research technique for making replicable and valid inferences from data to their context” (Krippendorff, 1980, p. 21). He describes it as a tool one can use to provide new knowledge, insights and representation of “facts” (Krippendorff, 1980). Neuendorf, on the other hand, says content analysis is “a summarizing, quantitative analysis of messages that relies on the scientific method...and is not limited to the types of variable that may be measured or the context in which the messages are created or presented” (Neuendorf, 2002, p. 10).

Carley, in her 1993 article, states simply, “content analysis focuses on the frequency with which words or concepts occur in texts or across texts” (Carley, 1993, p. 81). The purpose is to take a list of concepts and analyze a set of texts for the number of times each concept occurs within the texts, the intent being to gain some insight and understanding into the texts (Carley, 1993).

There are also two types of content analysis a researcher can use, conceptual and relational. Relational content analysis focuses on the relations between concepts in the text. In this type of study, the researcher takes the view that individual concepts have no meaning without the semantic, or meaningful, relationships to other concepts (Busch, et al., 2005). Conceptual analysis is more traditional and uses established concepts and analyzes the texts for quantifying/tallying the presence of the chosen concepts (Busch, et al., 2005).

This study is not concerned with concept relations, but rather the tallying of concepts within the texts. As such, this research followed the steps of content analysis laid out by Carley (1993) and Busch et al. (2005). In the following paragraphs, these steps are outlined and include the specific actions taken for this study.

1. Decide level of analysis. Are single words or phrases/word groups being coded?

For this analysis, both single words and phrases are used. This is because the study is based upon a specific list of awareness topics and the concepts are established.

2. Decide what to do with “irrelevant” information. Should it be ignored or re-examined and used to possibly change the coding scheme?

Carley (1993) states it is the researcher's decision as to what to do with irrelevant information. In this study, the definition for irrelevant information is any information not explicating pertaining to the topic at hand, i.e. information assurance awareness. Because this is a relatively narrow topic and the concepts are well-defined, there was little expectation on the part of the researcher to encounter similar topics not already included in the study. Therefore, irrelevant information was disregarded for the purposes of this thesis.

There are two types of irrelevant information, meaningless and meaningful. Meaningless information can be considered to be common words, such as “the”, “and”, “to”, “of”, “be”, etc. These words are common to most, if not all, texts and, as such, do not add to the analysis of the concepts. Meaningful information is considered to be concepts, either similar to those under examination, or important in its own right. For example, “constitution” is a concept with great meaning, but because that meaning is not directly applicable to this study, it would be considered irrelevant information and ignored.

3. Decide how many concepts to code for. This step is also concerned with whether the concepts will be pre-defined or interactive. Pre-defined concepts are established from a specific, rigid set of categories. Interactive concepts allow flexibility in adding new categories as the coding progresses.

This study will code for a pre-defined set of concepts. These concepts have been established by NIST SP 800-50, as discussed in Chapter Two. Please see the codebook (appendix something) for the specific definitions and exceptions for coding each concept.

4. Decide how to distinguish between concepts, i.e. the level of generalization.

Will similar terms be coded the same or will the terms warrant separate coding?

Busch et al. (2005) gave the example of “expensive” and “expensiveness”. Do the words mean the same or are the meanings different enough to be considered different terms? Because this study is utilizing a pre-existing set of concepts, the level of generalization is accepted as established in NIST SP 800-50. Instances in which compromises of the topic list can be made are discussed in the next step, rules for coding.

5. Develop rules for coding the selected texts.

These are the translation rules. These rules explain the decisions in step 4 so data is coded the same throughout study. This also provides the groundwork for replication of the study. The translation rules are contained in the codebook, found in Appendix A.

6. Decide whether to code for existence or frequency of each concept. Existence relates to whether or not the word/phrase appears in the text. Frequency, on the other hand, is derived from how often the word/phrase appears.

It was decided to use a combination method of existence and frequency when coding the two training modules. As each slide was examined, the existence of a concept would warrant a tally. The concept was tallied only once per slide, even if the concept appeared multiple times on the slide. But, if the concept appeared on more than one slide, it was tallied for each slide it appeared on. This thesis placed an exception upon tallying the frequency of concepts. As an awareness and training tool for personnel, the modules being examined may have slides which list several different concepts, but have no definitions or explanations of the concepts. Because this analysis is attempting to measure the comprehensiveness of the training modules, a simple mentioning of a

concept would not raise either security awareness or user training. For example, if a slide were to contain the word “virus” with no explanation, a user could misinterpret this as a physical human virus that causes illness, not as a computer virus that presents harm to information assurance on information systems. In such an instance, user awareness is not raised as intended and the training has failed at that particular occurrence of the concept. Also, each module contains summary and question slides which were not tallied for this analysis as the information on these slides was previously counted.

7. Code the texts.

The texts were two information assurance awareness training modules, one created by the USAF, the other by DISA. Both are geared toward DoD usage, to include military, civilians, and contractors who use DoD information systems. Both modules are administered in the form of computer based training and are viewed similar to PowerPoint presentations.

8. Analyze the results.

After coding of the texts is complete, the researcher will examine the data, making observations, in order to formulate conclusions and generalizations based on the content analysis. The results will be provided in Chapter Four and the analysis and conclusions will be discussed in Chapter Five of this thesis.

Summary

Content analysis has been shown to be an effective methodology for analyzing textual content and context (Carley, 1993; Busch et al., 2005; Neuendorf, 2002;

Krippendorff, 1980). Carley (1993) and Busch et al. (2005) provide a content analysis framework that fits this type of study very well. The steps taken for this study and outlined in this chapter provide the basis for future research on this topic. The next chapter will discuss the results of the content analysis.

Analysis of Results

Introduction

This chapter discusses the findings of the content analysis of the two IA awareness training modules. To provide for a better understanding of the results, a basic description of each module will be offered. Following the background, the results will be provided, as well as identifying some of the more significant findings.

Background

Both the USAF and DISA training modules are completed by users online. The DISA module is accessible by the general public at <http://iase.disa.mil/eta/>. The USAF module is accessible only to authorized users of AF systems who have a valid user logon for the Advanced Distributed Learning Service (<https://golearn.csd.disa.mil/kc/login/login.asp>) system. In order to facilitate future research, the USAF module used in this study has been replicated through the use of screen captures and can be found in Appendix B.

The AF module utilizes roll-overs, using the mouse and cursor to bring up more information on a topic. The DISA training is similar, but requires a mouse-click to display the added content. The DISA module makes use of audio, using a narrator to convey the training, and visual, employing transitions of information on single slides. The AF training is static, other than the aforementioned roll-over use, and provided links

to extra material, typically policy guidance or regulations (See Figure 2). The DISA training offers similar links and roll-overs for extra materials (See Figure 3).

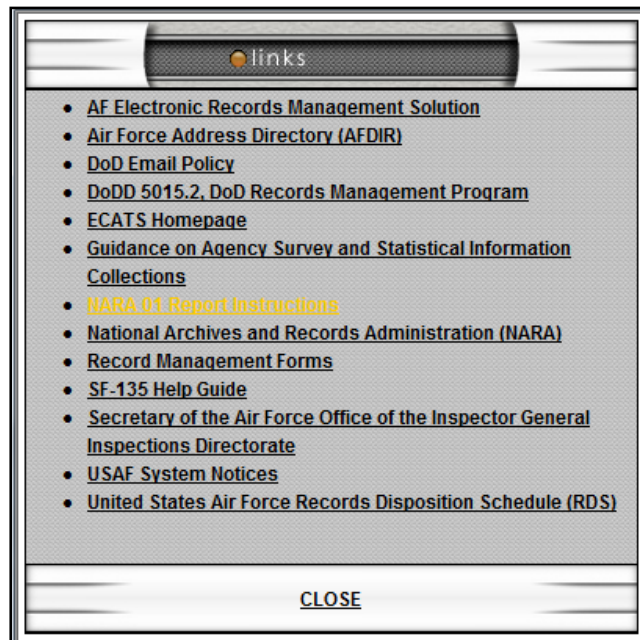


Figure 2 - USAF Module - Example of Link Slide



Figure 3 - DISA Training - Example of Roll-overs

The entire AF module contains 47 slides, but, as explained in Chapter 3, this study examined only 27. The DISA training has 75 slides, nearly three times as many. Both modules insert test-like questions after each section of training. All questions relate to material previously covered and require a response from the user. However, neither module scores the user or employs a grading scale for wrong answers. Regardless of a user's performance on the questions, a certificate of completion is given at the end of the training, the only requirement having been to view each slide of the presentation.

Results

In this study, there were a few ways to display the results. The DISA training covered 93% of the NIST recommended topics, while the USAF training covered 56% of the topics (See Table 2).

Table 2 - Topic Coverage		
Concept	USAF	DISA
Topics covered	15	25
Topics not covered	12	2

Though the number of topics covered throughout the training provides some insight, the actual frequency of each topic within the training gives the study more information (See Table 3). There are several topics which the DISA training seems to have covered more in depth than the USAF training. Some of these are malicious code, unknown e-mail attachments, web usage and monitoring of user activity, individual accountability, and laptop security. These results are noteworthy because of the disparity

of training coverage, with the DISA training spending a minimum of four more slides than the USAF training.

Table 3 - Concept Occurrence Results

Concept	USAF	DISA
Password usage and management	1	1
Malicious code, protection from	1	7
Policy – implications of noncompliance	2	5
Unknown e-mail/attachments	0	4
Web usage and monitoring of user activity	1	5
Spam	0	0
Data backup/storage	1	2
Social engineering	1	3
Software, supported/allowed on organization systems	1	1
Access control issues	2	4
Individual accountability	1	5
Use of acknowledgement statements	0	2
Visitor control/physical access to spaces	0	2
Desktop security	1	1
Incident response	3	6
Shoulder surfing	0	0
Changes in system environment	1	1
Inventory and property transfer	0	1
Personal use/gain issues	1	2
Handheld device, security issues	0	2
Use of encryption	1	3
Laptop security	0	5
Personally owned systems/software at work	0	1
Configuration management	0	1
Software license restriction issues	0	1
Protecting information, confidentiality concerns	4	6
E-mail list etiquette	0	3

Despite the difference in the number of occurrences of some concepts, there were several concepts both modules covered equally or nearly equally. These include password

usage/management, data backup/storage, software (supported/allowed on organization systems), changes in system environment, personal use/gain issues (See Table 4). Each of these concepts was covered in one or two slides in both the USAF and DISA modules. Two concepts, spam and shoulder surfing, were not covered at all by either training module (See Table 5).

Table 4 - Similar Concept Occurrence

Concept	USAF	DISA
Password usage and management	1	1
Data backup/storage	1	2
Software, supported/allowed on organization systems	1	1
Desktop security	1	1
Changes in system environment	1	1
Personal use/gain issues	1	2

Table 5 - Zero Concept Occurrences

Concept	USAF	DISA
Spam	0	0
Shoulder surfing	0	0

Summary

The results of analyzing the content of the two training modules reveal differences in the amount of topic coverage. The DISA training covered more topics from the NIST awareness topic list than did the USAF training module. The DISA module also had more slides discussing each concept. The next chapter will, based on these results, offer some conclusions and recommendations for IA awareness training and future research in the topic area.

Conclusion

Introduction

The purpose of this research, as established in the first chapter, was to answer three research questions. Based on the analysis written in Chapter 4, this final chapter will answer these questions. These questions were:

RQ 1: Does the USAF IA awareness training module comprehensively cover the topic list put forth in the NIST SP 800-50?

RQ 2: Does the DISA IA awareness training module comprehensively cover the topic list put forth in the NIST SP 800-50?

RQ 3: Does one module incorporate more of the NIST topic list than the other module?

Discussion

The answer to RQ 1 is, simply, no. The USAF training module included just over half of the topics recommended in NIST SP800-50. Neither did the training spend much time, as measured in the number of slides given to each concept, on any but one concept (protecting information/confidentiality concerns). It should be taken into account this list is a suggested list (Wilson & Hash, 2003) and not a strict requirement for inclusion in all training programs. Though each topic has importance and value for information

assurance awareness among users, the length of the training must also be taken into account.

The answer to RQ2 is yes, in the opinion of this researcher, the DISA IA awareness training comprehensively covered the NIST topics. Because the DISA module contained more slides covering most of the concepts and included all but two of the topics, the training is more inclusive, based upon the NIST recommended topics, for raising user information security awareness levels.

In answer to the last research question, yes, one training module incorporated more of the NIST topic list than the other. As noted above, the DISA module covered more of the topics and with more depth than did the USAF module. This research concludes the USAF training should incorporate more of the concepts recommended in NIST SP800-50 in order to provide a more robust and in depth IA awareness training module for its users. Being a DoD component agency, the USAF could also simply implement the DISA training.

It should be noted that as recently as 2007, the USAF used an IA awareness training program that was more robust and intensive than the current iteration. This study did not compare the current and past training modules or attempt to ascertain why the changes were affected. Nevertheless, with the myriad of training required of USAF personnel, it is quite possible several of the IA awareness topics omitted in the researched training module are included in other required training.

A last observation and recommendation is that of both modules' use of interactivity with the user. Both modules satisfy federal requirements of annual user IA awareness training and users receive a certificate upon completion of the training

attesting to this. Both modules also “quiz” users sporadically throughout the training session. However, neither module requires users to answer the questions correctly in order to “pass” the training. This research recommends some form of user accountability, beyond the simple “clicking-through” of training slides, to ensure better awareness among users.

Limitations

The content analysis portion of this study was based upon the special publications of the NIST, specifically SP 800-50 and SP800-16. Both of these documents provided the basis for the concepts used in the analysis of the two training modules. However, there was still room for researcher bias. As a researcher, personal knowledge and opinions of the studied topic can introduce bias into the research process and the analysis of the results (Mehra, 2002). To mitigate researcher bias in this study, the definitions developed for the various concepts were mostly taken from the glossary used in NIST publications, found in SP 800-16, Appendix C. Even though steps were taken to lessen the researcher bias in this study, it is inevitable some bias still exists. What is important in qualitative research is to recognize the presence of bias and the implications that stem from the bias (Mehra, 2002).

Coder bias is another area of bias in this study. When coding, it is left to the coder to interpret the concepts and the text. Though rules and instructions are provided, there is still room for differences of interpretation to arise. Also, there was only one coder (the primary researcher) of the content. This further exacerbates the possibility of coder bias.

To mitigate this form of bias, multiple coders should have been used, each receiving a portion of the texts to code. This would have established better validity of the study.

Another limitation of this research is the number of training programs analyzed. Though there is no hard and fast requirement for the number of texts used in content analysis, it is normally accepted to use greater than 20 texts (Carley, 1993; Krippendorff, 1980; Neuendorf, 2002). This research confined itself to the two selected training programs because of the significant similarities between user populations and policy. Additional texts (i.e. IA awareness training programs) would have provided a larger basis for comparison, both of the concepts covered and the organization's perceived value of those concepts.

Areas of future research

This study focused on the inclusion of specific content in two training programs. There are several areas stemming from this thesis to be explored in future research. The first is the possibility of utilizing a similar content analysis of other training programs, seeking similar results. This type of study could validate or refute the findings of this study. Considering the changing nature to information systems and assurance, new security threats emerge on a regular basis. A future study of this type may uncover some of the new concepts that will play a vital part in raising user IA awareness.

Another area of future research is to measure the effectiveness of the different IA training modules. Though this study made no claims as to the value added by either module examined, an experiment using pre-test and post-test methods could make

reasonable conclusions as to training effectiveness. This could explore the idea more content equals better training.

Finally, further research should be undertaken into the different types of IA awareness training in different agencies. Whether as comparative case studies or content analysis research, future studies exploring the concepts discussed in multiple training programs would be useful in providing a complete taxonomy of IA awareness topics. This research used the NIST publications as the standard of measure for the training modules, but there are several standards of information management being used around the world today. COBIT (Control Objectives for Information and related Technology, created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)), ISO/IEC 27002 (published by the International Organization for Standardization and International Electrotechnical Commission), ITIL (Information Technology Infrastructure Library) also provide frameworks and recommendations for IA awareness programs and training. Organizations implementing training programs under these standards may discuss concepts not examined in the NIST or this study. By expanding the accepted concepts for IA training, organizations can extend the scope of users IA awareness.

Summary

In summary, this thesis looked at two information assurance awareness training modules, used by DoD agencies. Using a topic list published by the NIST and employing a content analysis of both modules, the study was able to reach certain conclusions about

the comprehensiveness of the content in each module. It is the hope of this researcher that this study and the conclusions drawn from it will help in the creation of more comprehensive IA awareness user training in the future.

Appendix A. Codebook

This codebook is intended to provide coders all necessary instructions required to code information assurance awareness training modules. It is divided into three sections to aid in readability and understanding. Section 1 is coding instructions and includes a brief description of the modules to be coded. Section 2 is a glossary of the concepts (terms) the coder is analyzing. This can be used as the coder examines the texts as an aid for defining concepts. Section 3 is a sample code sheet.

Section 1 – Coding Instructions

The texts were two information assurance awareness training modules, one created by the United States Air Force (USAF), the other by Defense Information Systems Agency (DISA). Both are geared toward DoD usage, to include military, civilians, and contractors who use DoD information systems. Both modules are administered through web-based training and are to some extent comparable to PowerPoint presentations. Because of the similarity to PowerPoint presentations, further reference to the viewable screen within the modules will use the term “slide”.

The text of the USAF module is provided because the module requires a system log-in, available only to users (military, civilian, and contractor) of USAF information systems. Screen captures of the training module is provided, however, this did not always provide all the information contained on each slide. For this reason, some slides are duplicated, in order to capture all data. The USAF module is found in Appendix B. It

should also be noted here that this study only looks at a portion of the USAF module. This is because the entire module contains topics other than information assurance and security. The slides not used in this study cover records management, Privacy Act, and Freedom of Information Act. Also not included in the appendix are the question and answer slides, as these are not to be coded.

As the coder proceeds through the text, count each concept as it appears on each slide. The exception to this method is if the concept appears in a list and is not defined or explained on that slide (See Figure 4).



Figure 4 - USAF Module - Slide 17

Section 2 – Glossary

Password usage and management: A password is a protected/private alphanumeric string used to authenticate an identity or to authorize access to data. Usage and management is concerned with how and when users are expected to maintain and protect passwords.

Malicious code, protection from: Malicious code is software or firmware capable of performing an unauthorized function on an IS. Viruses, Trojan horses, worms, etc. are included in this concept. Protection topics include scanning IT systems and updating virus definitions for anti-virus software.

Policy – implications of noncompliance: This concept is related to explaining the organization's policy and the consequences for operating information systems contrary to said policy.

Unknown e-mail/attachments: Policy informing users of what actions to take upon receiving unknown e-mails or attachments.

Web usage and monitoring of user activity: Informing users of organization policy concerning web usage and informing users of consent to monitor policies.

Spam: Unwanted e-mail, usually excessive in nature. The problem for organization information systems

Data backup/storage: Provides users information concerning the organization's data backup/storage procedures and policies.

Social engineering: A term for non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – used to attack information systems.

Software, supported/allowed on organization systems: Information relating to users the requirements for software on organization systems. This is related to software assurance, which is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

Access control issues: Access control is limiting access to information system resources only to authorized users, programs, processes, or other systems.

Individual accountability: The ability to associate positively the identity of a user with the time, method and degree of access to an IS. This is similar to monitoring of user activity.

Use of acknowledgement statements: Policy informing users of situations/systems that require user acknowledgement.

Visitor control/physical access to spaces: Policies controlling visitor access to workspaces and information systems.

Desktop security: Actions users can take to keep their desktops secure, especially when visitors/outsideers are in the workplace.

Incident response: Informing users how to respond, who to contact, specific actions to take in the case of an information system incident. An incident is the assessed occurrence having actual or potentially adverse effects on an IS.

Shoulder surfing: The act of watching someone input their password for the purpose of capturing the password.

Changes in system environment: Indicators users should watch for that could signal possible breaches in the information system.

Inventory and property transfer: Description of organization policy.

Personal use/gain issues: Description of organization policy and consequences of misuse.

Handheld device, security issues: Any special requirements for securing organization handheld devices or the policies concerning allowing such devices access to information systems.

Use of encryption: Explanation of encryption, how the organization utilizes it, and user responsibilities.

Laptop security: Any special requirements for securing organization laptops.

Personally owned systems/software at work: Discussion of policies for allowing personal systems/software at work or on organization systems.

Configuration management: The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.

Software license restriction issues: Informing users on policies for software licensing and any applicable restrictions.

Protecting information, confidentiality concerns: Policies concerned with confidentiality, which is the assurance that information is not disclosed to unauthorized persons, processes, or devices.

E-mail list etiquette: Policies defining proper use of e-mail.

Section 3 – Code Sheet

Concept	USAF	DISA
Password usage and management		
Malicious code, protection from (includes viruses, Trojans, etc)		
Policy – implications of noncompliance		
Unknown e-mail/attachments		
Web usage and monitoring of user activity		
Spam		
Data backup/storage		
Social engineering		
Software, supported/allowed on organization systems		
Access control issues		
Individual accountability		
Use of acknowledgement statements		
Visitor control/physical access to spaces		
Desktop security		
Incident response		
Shoulder surfing		
Changes in system environment		
Inventory and property transfer		
Personal use/gain issues		
Handheld device, security issues		
Use of encryption		
Laptop security		
Personally owned systems/software at work		
Configuration management		
Software license restriction issues		
Protecting information, confidentiality concerns		
E-mail list etiquette		

Appendix B. AF Information Protection Module

The following slides were taken from the AF Information Protection module of the Total Force Awareness Training. The link for the slides is

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=normal, but it should be noted the link will not

work by itself as the system requires a log-in in order to access the training. The training may be accessed, with proper credentials, through the AF Portal (<https://www.my.af.mil>) or the Advanced Distributed Learning Service

(<https://golearn.csd.disa.mil/kc/login/login.asp>) websites, as provided.



Slide 3 InfoSec

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

INFORMATION PROTECTION

What is Information Protection?

- **Information Protection.** "The collective policies, processes and implementation of risk management and mitigation actions instituted to prevent the compromise, loss, unauthorized access/disclosure, destruction, distortion or non-accessibility of information, regardless of physical form or characteristics, over the life cycle of the information. It includes actions to regulate access to sensitive information, controlled unclassified information and classified information produced by, entrusted to or under the control of the United States Government."



AUDIO SCRIPT STOP AUDIO

STATUS = INCOMPLETE Page 4 of 47 FONT SIZE + Developed by AETC A3IA

Done Internet | Protected Mode: On 100%

Slide 4 InfoSec

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

STATED POLICY REGARDING INFORMATION PROTECTION

"Identify, classify, downgrade, declassify, mark, protect and destroy classified and sensitive information and material consistent with national policy and related executive orders"

Control measures and safeguards:

- Technical
- Physical
- Personnel

DoD contractors legally / contractually obligated to safeguard classified and controlled unclassified information

AUDIO SCRIPT STOP AUDIO

STATUS = INCOMPLETE Page 5 of 47 FONT SIZE + Developed by AETC A3IA

javascript:; Next Page Internet | Protected Mode: On 100%

Slide 5 InfoSec

SCORM Course Window : M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

RESPONSIBILITIES (INDIVIDUALS)

Protect unclassified, sensitive, and classified information processed or stored on information technology (IT) systems

Report to the unit commander or unit security representative:

- Security incidents
- Violations
- Suspicious activity Know / follow security policies for gaining access to facilities / information

Cleared personnel may grant to other persons access to classified information/material for mission essential needs. The person must have:

- Valid clearance
- A signed non-disclosure agreement (NDA) on file
- A need to know

Maintain continued eligibility for a position of trust

- Periodic personnel security background investigations are conducted to ensure a individual's continued reliability and trustworthiness

AUDIO SCRIPT STOP AUDIO

Page 6 of 47

STATUS: INCOMPLETE

FONT SIZE

Developed by AETC A3IA

Internet | Protected Mode: On 100%

Slide 6 InfoSec

SCORM Course Window : M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

RESPONSIBILITIES (COMMANDERS)

Authorize individuals access to classified / sensitive information

- A person's loyalty, reliability, and trustworthiness must be determined prior to granting access

Authorize individuals access to restricted areas and systems

Ensure protection of classified / controlled unclassified information released to contractors

Ensure industrial security requirements are imposed on industry through the contracting process

AUDIO SCRIPT STOP AUDIO

Page 7 of 47

STATUS: INCOMPLETE

FONT SIZE

Developed by AETC A3IA

Done

Internet | Protected Mode: On 100%

Slide 7 InfoSec

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

HANDLING INFORMATION

CLASSIFIED

- Store in a GSA approved vault or container when not in use
- Hand carry as required
- Transmit electronically through secure channels
- Retain for effective and efficient operation as required by law
- Destroy in a manner that eliminates risk of reconstruction
- Electronically processed on approved computer systems

Controlled Unclassified Information (CUI)

- Store in a locked container when not in use
- Destroy when no longer needed

AUDIO SCRIPT STOP AUDIO

STATUS = INCOMPLETE Page 8 of 47 FONT SIZE + Developed by AETC A3IA

Internet | Protected Mode: On 100%

Slide 8 InfoSec

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

NATO SECURITY

- Access to NATO Classified is limited to a need-to-know basis
- U.S. citizens granted NATO access must have a U.S. Security Clearance equal to the level of NATO classified being accessed
- Holder of NATO information is responsible to determine if individual requesting access possesses proper clearance and has need to know

AUDIO SCRIPT STOP AUDIO

STATUS = INCOMPLETE Page 9 of 47 FONT SIZE + Developed by AETC A3IA

Done Internet | Protected Mode: On 100%

Slide 9 InfoSec – NATO

SCORM Course Window - M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

LEVELS OF NATO CLASSIFIED

- COSMIC Top Secret (CTS)—Similar to TOP SECRET
- NATO Secret (NS)—Similar to SECRET
- NATO Confidential (NC)—Similar to Confidential
- NATO Restricted (NR)—Similar to For Official Use Only (FOUO)
- ATOMAL—A term added to a NATO classification meaning the information is provided by the U.S. and U.K. to other NATO components. e.g., COSMIC Top Secret ATOMAL (CTSA)

AUDIO SCRIPT STOP AUDIO

Page 10 of 47

STATUS: INCOMPLETE

Font Size: + -

Developed by: AETC A3IA

Internet | Protected Mode: On

Done

Slide 10 InfoSec – NATO

SCORM Course Window - M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

INFORMATION SECURITY

References:

- [DoD 5200.1-R, Information Security Program](#)
- [DoD 5200.2-R, Personnel Security Program](#)
- [DoD 5220.22-M, National Industrial Security Program](#)
- [DoD 5200.22-R, Industrial Security Regulation](#)
- [AFI 31-401, Information Security Program Management](#)
- [AFI 31-501, Personnel Security Program Management](#)
- [AFI 31-601, Industrial Security Program Management](#)
- [AFI 31-406, Applying NATO Protection Standards](#)

AUDIO SCRIPT STOP AUDIO

Page 11 of 47

STATUS: INCOMPLETE

Font Size: + -

Developed by: AETC A3IA

Internet | Protected Mode: On

Done

Slide 11 InfoSec

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

INFORMATION ASSURANCE

Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation"

AUDIO SCRIPT STOP AUDIO

STATUS = INCOMPLETE Page 15 of 47 FONT SIZE Developed by AETC A3IA

Done Internet | Protected Mode: On 100%

Slide 15 IA

SCORM Course Window :: M7 - Windows Internet Explorer

https://golearn.csd.disa.mil/kc/ilc/scorm_course_launch_frm.asp?strCourseID=C02025&strUserID=FRUGJ003&strCredit=credit&strMode=norm

UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

THREATS TO INFORMATION AND INFORMATION SYSTEMS

<p>Internal Threats. <i>May be intentional or unintentional</i></p> <p>Intentional threats:</p> <ul style="list-style-type: none"> • Deliberate acts by disgruntled employees • Employee espionage <p>Unintentional threats:</p> <ul style="list-style-type: none"> • Carelessness • Poor security procedures 	<p>External Threats. <i>May be natural or deliberate</i></p> <p>Natural threats:</p> <ul style="list-style-type: none"> • Extreme heat and cold • Storms (lightning / flooding) • Earthquakes • Fire <p>Deliberate threats:</p> <ul style="list-style-type: none"> • Phishing • Espionage • Hacking • Malicious Logic (computer viruses) • Social Engineering
--	---

AUDIO SCRIPT STOP AUDIO

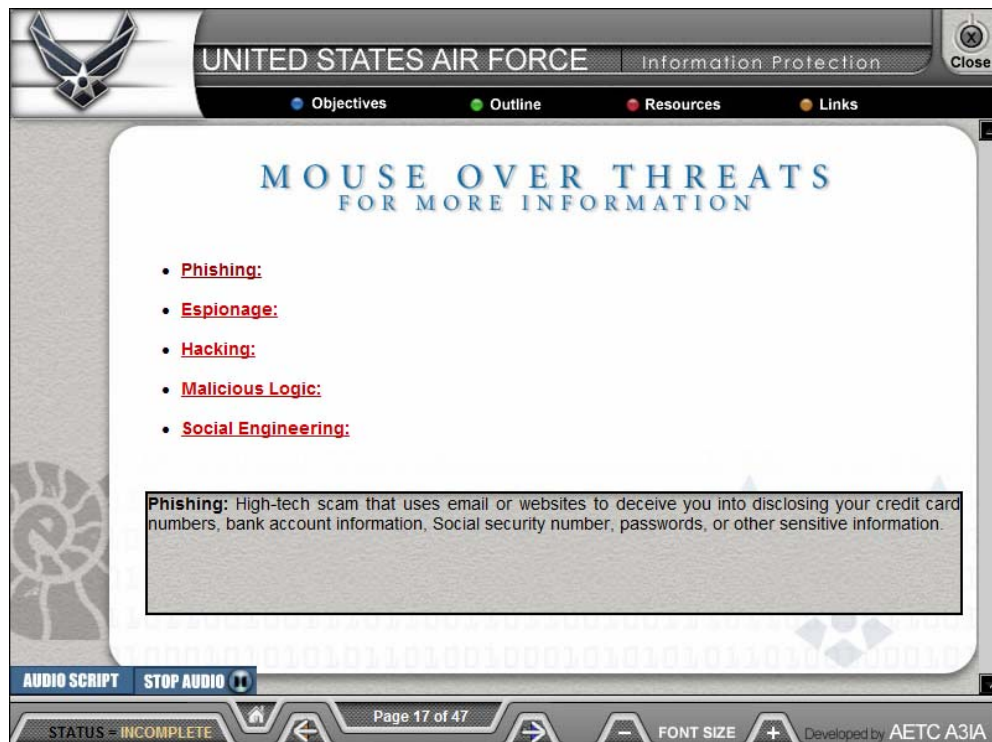
STATUS = INCOMPLETE Page 16 of 47 FONT SIZE Developed by AETC A3IA

Done Internet | Protected Mode: On 100%


Slide 16 IA



Slide 17 IA



Slide 17a IA



UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

MOUSE OVER THREATS FOR MORE INFORMATION

- **Phishing:**
- **Espionage:**
- **Hacking:**
- **Malicious Logic:**
- **Social Engineering:**

Espionage: The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.

AUDIO SCRIPT STOP AUDIO

STATUS INCOMPLETE Page 17 of 47 FONT SIZE Developed by AETC A3IA

Slide 17b IA



UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

MOUSE OVER THREATS FOR MORE INFORMATION


- **Phishing:**
- **Espionage:**
- **Hacking:**
- **Malicious Logic:**
- **Social Engineering:**

Hacking: Illegally accessing other people's computer systems for destroying, disrupting or carrying out illegal activities on the network or computer systems.

AUDIO SCRIPT STOP AUDIO

STATUS INCOMPLETE Page 17 of 47 FONT SIZE Developed by AETC A3IA

Slide 17c IA



UNITED STATES AIR FORCE
Information Protection
Close

Objectives
Outline
Resources
Links

MOUSE OVER THREATS FOR MORE INFORMATION

- **Phishing:**
- **Espionage:**
- **Hacking:**
- **Malicious Logic:**
- **Social Engineering:**

Malicious Logic: Hardware, software, or firmware capable of performing an unauthorized function on an Information System.

AUDIO SCRIPT
STOP AUDIO

STATUS = INCOMPLETE
Page 17 of 47
FONT SIZE
Developed by AETC A3IA

Slide 17d IA



UNITED STATES AIR FORCE
Information Protection
Close

Objectives
Outline
Resources
Links

MOUSE OVER THREATS FOR MORE INFORMATION

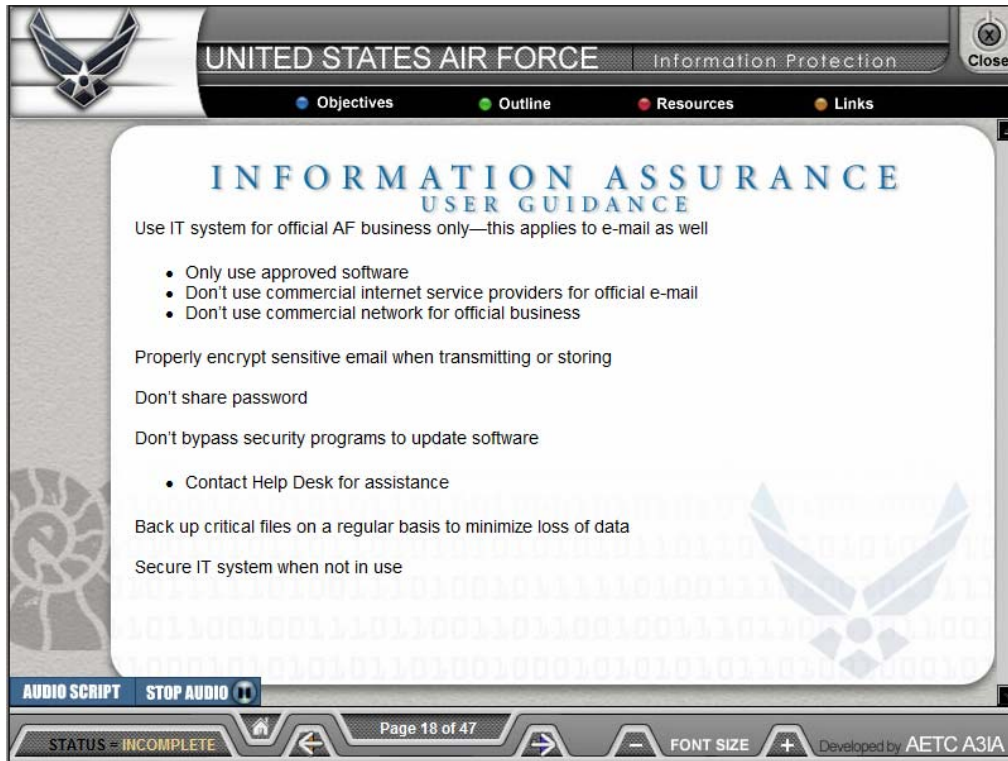
- **Phishing:**
- **Espionage:**
- **Hacking:**
- **Malicious Logic:**
- **Social Engineering:**

Social Engineering: A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems. For example, an unauthorized person who attempts to gain passwords by posing as a service technician with an urgent access problem.

AUDIO SCRIPT
STOP AUDIO

STATUS = INCOMPLETE
Page 17 of 47
FONT SIZE
Developed by AETC A3IA

Slide 17e IA



UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

INFORMATION ASSURANCE USER GUIDANCE

Use IT system for official AF business only—this applies to e-mail as well

- Only use approved software
- Don't use commercial internet service providers for official e-mail
- Don't use commercial network for official business

Properly encrypt sensitive email when transmitting or storing

Don't share password

Don't bypass security programs to update software

- Contact Help Desk for assistance

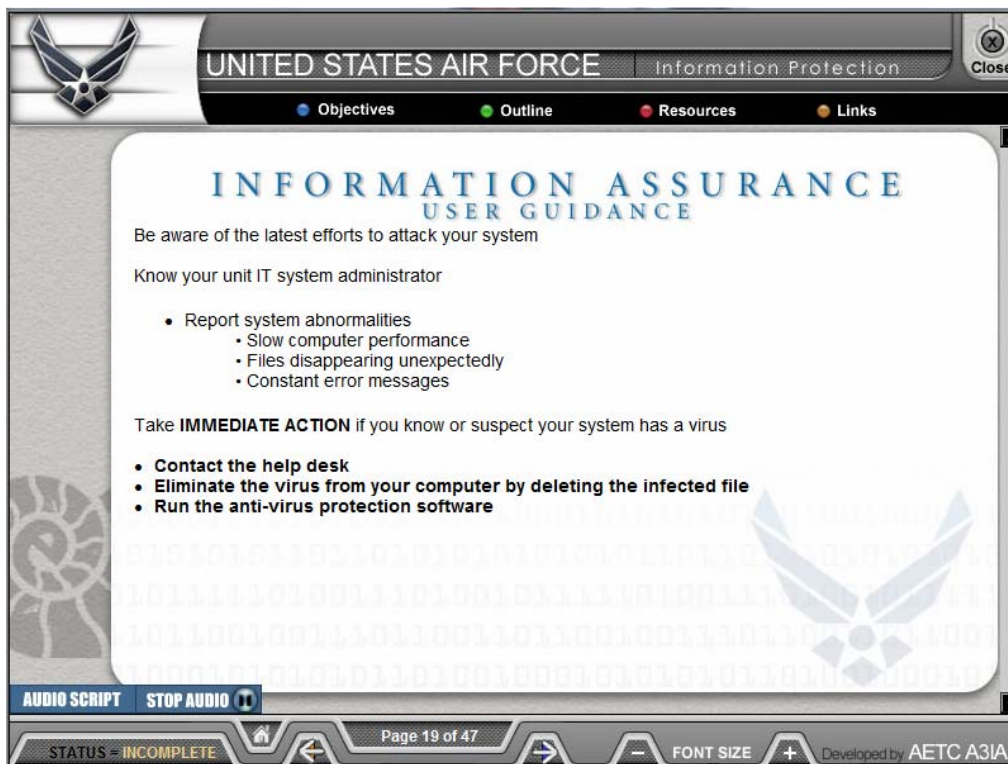
Back up critical files on a regular basis to minimize loss of data

Secure IT system when not in use

AUDIO SCRIPT STOP AUDIO

STATUS: INCOMPLETE Page 18 of 47 FONT SIZE Developed by AETC A3IA

Slide 18 IA



UNITED STATES AIR FORCE Information Protection Close

Objectives Outline Resources Links

INFORMATION ASSURANCE USER GUIDANCE

Be aware of the latest efforts to attack your system

Know your unit IT system administrator

- Report system abnormalities
 - Slow computer performance
 - Files disappearing unexpectedly
 - Constant error messages

Take **IMMEDIATE ACTION** if you know or suspect your system has a virus

- Contact the help desk
- Eliminate the virus from your computer by deleting the infected file
- Run the anti-virus protection software

AUDIO SCRIPT STOP AUDIO

STATUS: INCOMPLETE Page 19 of 47 FONT SIZE Developed by AETC A3IA

Slide 19 IA



UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

PROPERTIES OF SECURE INFORMATION

Confidentiality - measures to prevent unauthorized disclosure of information

Integrity - measures to ensure no unauthorized changes are made to information

Availability - measures to ensure information and systems are accessible to users when they need it

Authentication - measures to ensure the user is who they claim to be

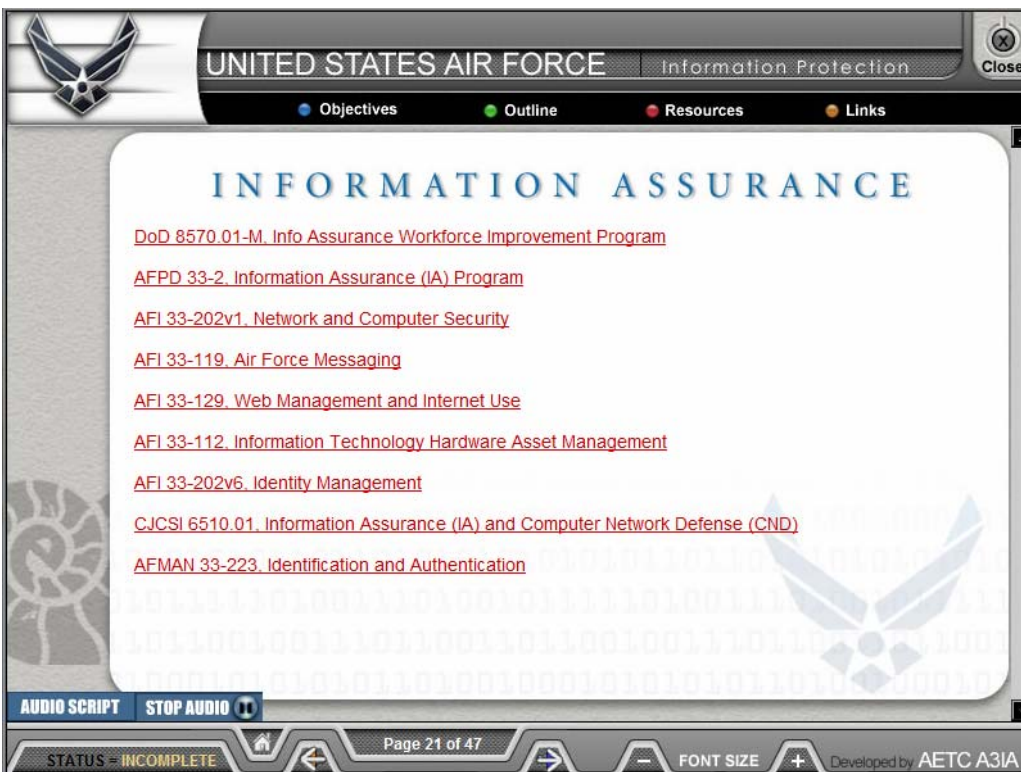
Non-repudiation - measures to ensure the originator cannot deny sending the message

AUDIO SCRIPT STOP AUDIO

Page 20 of 47

STATUS = INCOMPLETE FONT SIZE Developed by AETC A3IA

Slide 20 IA



UNITED STATES AIR FORCE Information Protection

Objectives Outline Resources Links

INFORMATION ASSURANCE

[DoD 8570.01-M, Info Assurance Workforce Improvement Program](#)

[AFPD 33-2, Information Assurance \(IA\) Program](#)

[AFI 33-202v1, Network and Computer Security](#)

[AFI 33-119, Air Force Messaging](#)

[AFI 33-129, Web Management and Internet Use](#)

[AFI 33-112, Information Technology Hardware Asset Management](#)

[AFI 33-202v6, Identity Management](#)

[CJCSI 6510.01, Information Assurance \(IA\) and Computer Network Defense \(CND\)](#)

[AFMAN 33-223, Identification and Authentication](#)

AUDIO SCRIPT STOP AUDIO

Page 21 of 47

STATUS = INCOMPLETE FONT SIZE Developed by AETC A3IA

Slide 21 IA



UNITED STATES AIR FORCE

Information Protection

Close

Objectives Outline Resources Links

CONSEQUENCES OF VIOLATING SYSTEM SECURITY MEASURES

Disciplinary action

Damage to national security

Report incidents immediately to your Client Support Administrator (CSA) or Information Assurance Officer (IAO)

AUDIO SCRIPT STOP AUDIO

Page 22 of 47

STATUS: INCOMPLETE

FONT SIZE

Developed by AETC A3IA

Slide 22 IA

Bibliography

- Adams, A., & Sasse, M. A. (1999). Users Are Not the Enemy. *Communications of the ACM* , 42 (12), 40-46.
- Busch, C., DeMaret, P. S., Flynn, T., Kellum, R., Le, S., Meyers, B., et al. (2005). *Writing Guides: Content Analysis*. Retrieved December 3, 2007, from Writing@CSU: <http://writing.colostate.edu/guides/research/content/>
- Carley, K. (1993). Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis. *Sociological Methodology* , 23, 75-126.
- Conklin, W. A., White, G. B., Cothren, C., Williams, D., & Davis, R. L. (2004). *Principles of Computer Security: Security+ and Beyond*. Boston: McGraw-Hill Technology Education.
- Gordan, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco: Computer Security Institute.
- ISACA. (2008). *ISACA Overview and History*. Retrieved February 15, 2008, from ISACA: http://www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History/Overview_and_History.htm
- Ives, B., Walsh, K. R., & Schneider, H. (2004). The Domino Effect of Password Reuse. *Communications of the ACM* , 4-7.
- Johnson, E. C. (2006). Security awareness: Switch to a better programme. *Network Security* , 15-18.
- Keizer, G. (2008, February 13). *FBI warns of Valentine's Day 'Storm'*. Retrieved February 13, 2008, from Computerworld: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9062538>
- Krippendorff, K. (1980). *Content Analysis: An Introduction to its Methodology*. Beverly Hills: Sage Publications, Inc.
- McCue, A. (2007, November 20). *25M child benefit records lost on 2 CDs sent in mail*. Retrieved February 12, 2008, from Silicon: <http://www.silicon.com/research/specialreports/digitaldefences/0,3800014341,39169217,00.htm>
- Mehra, B. (2002, March). *Bias in qualitative research: Voices from an onlin classroom. The Qualitative Report*, 7(1). Retrieved March 25, 2008, from Nova: <http://www.nova.edu/ssss/QR/QR7-1/mehra.html>

- Mellor, M., & Noyes, D. (2005). *Mellor Security*. Retrieved November 4, 2007, from IA Training Package: <http://www.mellorsecurity.com/iatrainingpackage>
- Neuendorf, K. A. (2002). *The Content Analysis Guidebook*. Thousand Oaks, CA: Sage Publications.
- NITC. (2001). *Nebraska Information Technology Commission*. Retrieved November 25, 2007, from Standards and Guidelines: <http://www.nitc.state.ne.us/standards/>
- Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2007). *Managing Risks from Information Systems - Initial Public Draft*. Gaithersburg, MD: National Institute of Standards and Technology.
- Schou, C. D., & Trimmer, K. J. (2005). Information Assurance and Security. *Journal of Organizational and End User Computing on Information Security* , i-vii.
- Schou, C., & Shoemaker, D. (2007). *Information Assurance for the Enterprise*. Boston: McGraw-Hill Irwin.
- The Associated Press. (2007, July 3). *2.3M Records containing credit card, bank account information stolen, financial processing company says*. Retrieved February 12, 2008, from Fox News: <http://www.foxnews.com/story/0,2933,287862,00.html>
- The Associated Press. (2008, January 17). *Data lost for 650,000 Penney, other customers*. Retrieved February 12, 2008, from CNN Money: http://money.cnn.com/2008/01/17/news/companies/penney_data.ap/index.htm
- The Associated Press. (2006, July 12). *Investigator faults VA, employee for data loss*. Retrieved February 8, 2008, from msnbc.com: <http://www.msnbc.msn.com/id/13819339/>
- U.S. Department of Veterans Affairs. (n.d.). *Cyber Security Awareness*. Retrieved January 14, 2008, from U.S. Department of Veterans Affairs: https://www.cbts.portland.med.va.gov/education/cbt/cyber_sec_fy06/01.htm
- United States Congress. (2002, December). *FISMA Final*. Retrieved January 5, 2008, from Computer Security Resource Center, NIST: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
- United States Congress. (1988). *ITL History Timeline*. Retrieved January 5, 2008, from Information Technology Laboratory - NIST: <http://www.itl.nist.gov/timeline.htm>
- United States Congress. (1987, December 21). *Public Law 100-235*. Retrieved January 5, 2008, from National Institute of Standards and Technology: <http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf>
- US Air Force. (2007). *Air Force Total Force Awareness Training: Information Protection Module*. Retrieved December 7, 2007, from <https://golearn.csd.disa.mil/kc/login/login.asp>

- Vijayan, J. (2007, October 24). *Scope of TJX data breach doubles: 94M cards now said to be affected*. Retrieved February 12, 2008, from Computerworld:
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043944&pageNumber=1>
- Wilson, M., & Hash, J. (2003). *Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology.
- Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model - NIST SP 800-16*. Gaithersburg, MD: National Institute of Standards and Technology.
- Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Gaithersburg, MD: National Institute of Standards and Technology.

REPORT DOCUMENTATION PAGE					<i>Form Approved OMB No. 0704-0188</i>	
<small>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</small>						
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)					8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT						
15. SUBJECT TERMS						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)	