Editorial Preface

Information Assurance and Security

Corey D. Schou, Idaho State University, USA
Kenneth J. Trimmer, Idaho State University, USA

Welcome

Welcome to the first special edition of the *Journal of Organizational and End User Computing on Information Security*. Four articles form the core of this special edition. The articles focus on items of interest to the end user and range from conceptual work to empirical studies and bridge the gap between basic information security and the emerging discipline of information assurance.

Background

Information assurance contains all the elements of information security (confidentiality) but also includes elements of availability, and integrity[1]. Information assurance provides a view of information protection that includes defensive measures in all three states — processing, storage, and transmission. To defend information and data there are three fundamental countermeasure categories:

1. technology,
2. operations,
3. awareness, training and education.

Fifteen years ago, the U.S. government identified these as the three primary countermeasures to protect Critical Information Infrastructure (CIP). It is important to remember that in an electronic era, information must be defended not only for national security but for legal reasons such as FERPA and HIPPA[2]. In a recent article, Maconachy[3] points out that the end user is the first line of defense.

The Threat

Security holds both national and international attention; frequently, one loses site that our information security is more than physical. Global commerce relies on computers and an associated electronic infrastructure. E-commerce, business to business, Internet, and e-mail are just a few of the tools that have entered the vocabulary of the end user in the past decade. Many individuals would not know how to make their lives work nor their enterprise profitable without these tools. Consider how much would your life change if you no longer had access to the internet and its myriad services?

Now, expand your thinking to include those other critical functions that are supported by that same electronic infrastructure. Hospitals, airlines, power, food distribution, schools, libraries, agribusiness, and

manufacturing are a sample of critical information infrastructure components that support a modern economy and society. These systems have become so complex that no one understands all their interactions. This complexity combined with closely coupled systems operations creates fragile critical systems. In these systems, failure of a single component may adversely affect the integrity, confidentiality, and availability of many critical systems. In addition being fragile, they are brittle — they may break unexpectedly into a nonrecoverable state. Any national or international security effort cannot afford to place the security of their economy and society on the backs of fragile systems.

Although languages and specifics may differ by discipline, there is now general recognition that information technology security is a core business process. Integral to establishing a core process is building a competent information technology security work force — a people based countermeasure. This security workforce facilitates both industry and government in establishing integrated information security systems relying on multidimensional approaches. The multidimensional approach deals with technologies such as biometrics, cryptographic systems, and smart cards; operations issues such as HIPAA, transborder data flows, procedures, software property rights, privacy, auditing, personnel, and risk assessment; as well as people development which goes beyond just education and training into professional development and recognition through certification.

In the final analysis, either our economy is directly or indirectly under attack; this attack has been termed as network centric warfare. "The organizing principle of network-centric-warfare has its antecedent in the dynamics of growth and competition that have emerged in the modern economy".[4] Information assurance protects critical information infrastructures and provides for homeland security[5].

Information Assurance & the End User

Information assurance relies on a triad of countermeasures; this triad is a defense in depth model. The most obvious and expensive countermeasure is technology. Technology includes everything from operating systems to routers, switches, and electronic intrusion detection systems. No matter how well designed these technical countermeasures are, they are ineffective if they are not supported by well-designed operational plans, policies and goals. However, in the final analysis, all of this fails if one does not have end users who are aware of information assurance issues, trained to operate systems appropriately.

Like the iceberg, the majority of information assurance supports the small, visible portion at the top and like the iceberg; one must worry about the parts that are unseen.

Guidelines for Users

From an end user perspective, the education awareness and training are the important countermeasures. In the U.S., the federal government took training the end user seriously enough to demand that all federal employees using sensitive systems receive annual training. The Computer Security Act (PL 100-235) also delineated the responsibility for information assurance standards between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). However, how does one know

Figure 1: Defense in Depth Pyramid

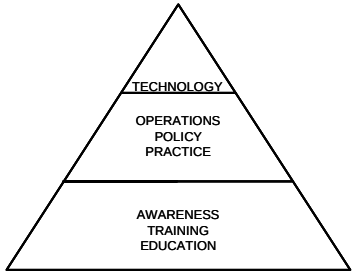
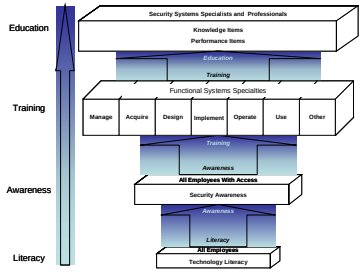


Figure 2: Information Assurance Learning Hierarchy



were to start building compliance and good practice?

In addressing where to start the building process, two main standards were developed to aid managers in determining the end user needs for awareness, training, and education countermeasures. The NIST Standard 800-16 and Committee on National Security Standards (CNSS)[6] standards 4011 through 4016 detail the training contents.

These standards evolved from a series of studies over more than a decade that established their content. Figure 2 shows[7] the relationships among literacy, awareness, training, and education.

Awareness Training & Education: End User Solutions

To illustrate the need for training and education, the healthcare environment provides an example. By implication, every healthcare worker needs to have a common understanding that allows all individuals involved in biomedical informatics and their associated critical information infrastructure systems to work together in an environment of trust.[8] It is essential that these individuals be interoperable and work from the same knowledge base to insure robust, reliable, and resilient systems.

A broad effort to assist in facilitating information in the United States was fueled in 1997 when the President's Commission on Critical Infrastructure Protection called for:

"NIST, NSA, and the U.S. Department of Education work in collaboration with the private sector to develop programs for education and training of information assurance specialists and for the continuing education as technologies change."[9]

The previous statements indicate a strong need for a structured model for literacy, awareness, training, and education to all employees.[10]

Awareness

Awareness is at the lowest level of the solution to information assurance. It is designed to affect short-term memory. It is composed of stimulation, focus, attention, decision, and assimilation (examples are presented in Table 1). A successful program will begin by meeting these five requirements.

Table 1: Awareness Characteristics

STIMULATION	FOCUS	ATTENTION	DECISIONS	ASSIMILATION
Security only colors	Change Locks	Bulletin Boards	Read Security Reg.	Key ring with message
Security only music theme	Reminders	Flyers	Read Magazines	Short Seminars
		Posters	Attend Lecture	Video Tape Programs

Table 2: Literacy Examples

Definitions	Distinctions
Virus, Trojan horse, worm	Authentication vs. passwords
Insider threat	Certification vs. accreditation systems

Table 3: Training Characteristics

ACTIVE KNOWLEDGE SEEKER	LONG TERM MEMORY
Self Paced Course	Computer Based Instruction
OJT	Multi- Session Seminar
Conferences	

Literacy

Information assurance literacy places fundamental working knowledge and principles into the minds and actions of a work force. Examples of literacy include those presented in Table 2.

Training

There is a gray zone between awareness and training. A gross distinction between them is that in awareness activities the learner is a passive recipient of material, while in the training environment the learner assumes an active role in the learning process. A primary role of awareness programs is to motivate employees/learners to move into a training mode and actively seek more knowledge. Examples of strategies and goals of training efforts are illustrated in Table 3. One fundamental goal of training programs is motivation of learners to move knowledge and skills from short-term memory into long-term memory. Often, these knowledge and skills are chained sequences of behavior that require higher level mental processing.

Education

The distinction between training and education can be made by examining the intent and scope of the instruction. In a training environment, the employee learns to use specific skills as part of exacting job performance. In education, the employee is encouraged to examine and evaluate not only skills and methods of work but fundamental operating principles and tenants based upon job skills. The employee is using internalized concepts and skills to perform operations such as analyses, evaluation, and judgment to reach higher cognitive level decisions. This leads to accommodation of newly integrated knowledge and skills. Accommodation is an end process in which the learner makes a conscious decision to modify existing ways of thinking and responding to satisfy new experiences and knowledge. Table 4 shows examples of exercises to increase knowledge integration and accommodation.

Standards for Professionals

At the higher end, private industry was not silent on the importance of profes-

Table 4: Education Characteristics

INTERNALIZATION	ACCOMMODATION
Point Papers	Long Term Training
Study Groups	Research and Deliver Briefing

sional standards as a countermeasure. Recognizing this as a critical issue, the Joint Security Commission on Redefining Security pointed out in a 1994 report that … *Uniformity in skills and knowledge taught to security professionals is needed not only to ensure the quality of work, but also to foster a common understanding and implementation of security policies and procedures.*[11]

A non profit organization the International Information Systems Security Certifying Consortium[12] [(ISC)^2] established 10 domains of knowledge every information assurance professional should master. These 10 domains for certified professionals (CISSP) are:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

They believe that all professionals need to understand all aspects of these ten learning domains. They believe that end users should be at least aware of these subjects.

Information Assurance & Academia

Information assurance was identified as a national priority in the United States for the protection of the critical information infrastructure. Even before PDD-63 was established, the *National Infrastructure Assurance Council* was drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan[13], as the federal government was proactively addressing the problem. The US government established the NIETP[14] to, among other functions; create Centers of Academic Excellence in Information Assurance Training and Education. This created an academic infrastructure to support the critical information infrastructure. Establishing NIETP demonstrates the insight of government leaders in information assurance. In the United States, the federal government established an ROTC (Reserve Officers Training Corps) type scholarship program to increase the size of the information assurance workforce. These Scholarships for Service (SFS)[15] provide full tuition and stipends to support both undergraduate and graduate studies in information assurance at centers of excellence schools. Upon graduation, the student is required to work for the federal government for two years. Such programs are necessary in order to create a pool of professionals, educated in standard practices to help insure organizational information assurance.

This Special Edition

The selection of articles for this first special edition covers many of the critical issues of end user computing from both the industrial and academic standpoint.

The special edition begins with a conceptual and definitional work by Gupta, Rao, and Upadhyaya, a discussion of a broad range of security and assurance issues with a focus on electronic banking. This paper provides the Information Professional with little background in IA an introduction to its terminology and principles, as well as a specific topics focusing on banking issues.

The next research paper is an empirical work by Aytes and Connolly that provides a perspective on potential security concerns for organizations. This research focuses on the security behaviors of a population of undergraduate IT majors. The researchers discuss perceived risk and the security precautions emphasized by these future organizational employees.

Warkentin, Davis, and Bekkering present a strategy to provide system users with robust password security. Their empirical study on preferences for competing password strategies presents a new password generation strategy. As with the previous paper, their work also utilizes an important future pool for information assurance, students.

In the final paper of the edition, Stahl conceptually discusses individual responsibility, information assurance, and security. His manuscript develops the argument that individuals have limitations in being totally responsibility for their information assurance activities and that the organization needs to be aware of such limitations.

Closing

If the reader is being introduced to information assurance issues, we hope that you find this set of research manuscripts informative. For the reader experienced in IA issues, our hope is that you find the conceptual and empirical studies presented here to be stimulating to your research, practice, and teaching.

Endnotes

[1] Integrity is the quality of an information system reflecting logical correctness, reliability, and the consistency of the data structures and occurrence of the stored data. Confidentiality is the assurance that information is not disclosed to unauthorized persons, processes, or devices. Availability is the timely, reliable access to data and information services for authorized users.

[2] Family Educational Rights and Privacy Act and Health Insurance Portability And Accountability Act

[3] V. Maconachy, C. Schou, D. Welch, & D. J. Ragsdale (2001). "A Model for Information Assurance: An Integrated Approach." Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, West Point, NY (June 5-6, pp. 306-310).

[4] A.K. Cebrowski & J.J. Garstka (1988, January). Network-Centric Warfare: Its origin and Future. Naval Institute Proceedings.

[5] C.D. Schou & J. Frost (2004). Homeland Security and Information Assurance in Biomedical Informatics Systems. IEEE Engineering in Medicine and Biology, (January/February).

[6] http://www.nstissc.gov/html/library.html

[7] Based on a figure in C. Schou, W. V. Maconachy, et al. (1993). "Organizational Information Security: Awareness, Training, and Education to Maintain System Integrity". Proceedings of the 9th International Computer Security Symposium, Toronto, Canada, IFIP.

[8] C. Schou (2003). Standards, Standards, Standards, Who has the Standards. Proceedings 4th Australian Information Warfare and IT Security Conference– Enhancing Trust, (November 20-21). University of South Australia, Adelaide, Australia.

[9] Critical Foundations: Protecting America's Infrastructures. The report of the President's commission on Critical Infrastructure Protection. Oct. 1997. P71.

[10] C. Schou, W. V. Maconachy, & J. Frost (1993). "Organizational Information Security: Awareness, Training and Education to Maintain System Integrity." Proceedings Ninth International Computer Security Symposium, Toronto, Canada, May.

[11] Redefining Security: Joint Security Commission Report, Feb. 28, 1994, p.124

[12] http://www.isc2.org

[13] http://www.usdoj.gov/criminal/cybercrime/factsh.htm

[14] http://www.nsa.gov/ia/academia/acade00001.cfm

[15] http://www.ehr.nsf.gov/due/programs/sfs/

Corey D. Schou *is the university professor of Informatics, professor of Information Systems, and associate dean of the College of Business at Idaho State University (USA). He has been involved in establishing computer security and information assurance training and standards for 25 years. His research interests include information assurance, ethics, privacy, and collaborative decision-making. Through his research, he was responsible for compiling and editing computer security standards and training materials for the Committee on National Security Systems (CNSS). Dr. Schou serves as the chair of the Colloquium for Information Systems Security Education (CISSE). Under his leadership, the Colloquium creates an environment for exchange and dialogue among leaders in government, industry, and academia concerning information security and information assurance education. In addition, he serves as the editor of Information Systems Security and is on the board of several professional organizations. He has served as the principal investigator on 40 funded research projects and is currently principal investigator on the NSF Scholarship for Service program in information assurance.*

Ken Trimmer *is an assistant professor of Computer Information Systems in the College of Business at Idaho State University (USA). He has a PhD in Management Information Systems from the University of South Florida where his dissertation focused on conflict on cross-functional teams involved in information systems development. In addition to his research interests in systems development, Dr. Trimmer has interests and publications in the management of systems in the healthcare environment, educational issues in information systems coursework, and information systems issues in small to medium organizations, which includes software development as well as the utilization of systems. Dr. Trimmer also has interests in the teaching of information assurance, and security issues in healthcare organizations, particularly with HIPAA.*