Utilizing a Virtual Laboratory to Implement Standards Based Ethical Decision Making in Information Assurance Courses

By

Dan Likarish, Assist Prof
Regis University/MSCIT
3333 Regis Blvd
Denver CO 80222
dlikaris@regis.edu

Abstract

In response to an increased demand for graduate level Information Assurance (IA) education, the SPS/MSCIT (School for Professional Studies/Masters of Science in Computer Information Technology) at Regis University, Denver developed a series of IA courses in late fall of 2003. In addition to the technical, policy and management course content, modern ethical decision making techniques were integrated into the classroom courses. The courses were developed with the intent to deliver them to online students via the WebCT platform. The course development work was divided into three phases; phase 1, selection of appropriate ethical practices and decision-making techniques from content experts, professional organization, and standards bodies, phase 2, design, development and construction of supporting instructional labs associated with the standards using the MSCIT virtual laboratory at Regis University, and finally phase 3, implementation of the supporting classroom and online Vlabs.

Keywords: Instructional Design, Distance education, Virtual Lab, Information Assurance, Information Technology, Applied Ethics,
Introduction
Due to the increased demand for Information Assurance (IA) courses that contain rich technical content and offer good governance practices, the Masters in Science Computer Information Technology (MSCIT) program at Regis University has developed a pedagogical methodology for implementation of adult decision making models, tools and evaluative methods within IA courses, see figure 1. The methodology follows a constructivist approach for adult experiential learners based on the work by M. Knowles, see Knowles (1990). Our framework follows Knowles’ constructivist recommendation that the adult learner should be presented work with increasing complexity and rigor based on acquired skills through interactive and personalized exercises. The three steps within the pedagogical framework are, first acquisition of specific moral models and their influence on ethical decision making (initiation to the use of moral decision making), secondly application of ethical concepts through the use of best of breed analysis software and hardware (formation of a moral center), and finally the evaluation of case studies using the analytical tools (determination of an action plan).

The moral models, referred to as the Deontological, and Teleological moral models from work by Richard Spinello, see Spinello (1997) and additionally the Relationality-Responsibility moral model by Charles Curran, see Curran (2002) exposed our students to a moral frameworks based on law, goals and the larger business community. Because of our participation in a variety of academic alliances with major software vendors, MSDN, OAI, OPnet, Rational, IBM etc. and our own enterprise network Academic Research Network (ARNe), we were able to offer applications that provided our students with hands-on experience with design tools for modeling and simulation of ethical exercises. Finally, the highest complexity level achieved in our pedagogy allowed student to use previous skills to perform an evaluation of security policy, code of ethics and operational/organizational structures from case studies provided by Thomson Course Technology, see Reynolds (2003), Tipton (2000) and Whitman (2004). The varied course offerings from simple to complex in nature would not have been possible without an organizational structured framework developed by Sam Conn, see Conn (2004) the Informational Systems Learning Cycle (ISLC). The ISLC maps the cognitive and applied instructional course material to specific online browser enabled technology: MSCIT’s Virtual Laboratory (Vlab), see figure 2. The Vlab component of the ISLC is hosted and delivered to our worldwide student body through MSCIT’s Academic Research Network enterprise (ARNe). The other components of the ISLC (reading, review questions, research, discussions, presentations and the Vlab) interact with each other and the adult learner at various stages of their learning cycle to map the course terminal and weekly objectives into their learning experience. The resulting pedagogical methodology provides a structured interactive curriculum based on established traditional moral models that allow our student to analyze and evaluate complex adult ethical decisions using a variety of common information systems tools.

Background and basis for our Information Assurance courses
Information security and assurance personnel who have a balance between technology and good management skills possibly represent the new management tier of critical business and government resources. The constant need for technology savvy employees has been supplemented and in some cases supplanted
by the need to understand good governance, best practices and good policy construction. From review of standards groups (BSA 17799, ACM, CISSP etc)\textsuperscript{1,2,3} that represent the former topics, codes of ethics and ethical decision making are not surprisingly materially important to successful implementation of assurance plans. DoD has recently coined the phrase “IT warrior” to describe the latest battlefield of the present and its reliance on real-time IT for successful execution of its mission. The NSA CAE program has expanded and is adding schools at a very quick rate, as of 2004 there are over fifty programs that have qualified for CAE status.

Concern for information security has reached exponential proportions in government and industry. As recently as March 16, 2004, the House Government Reform Committee Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, reported to Congress progress in government information security since the creation of the Federal Information Security Management Act in 2002 (FISMA). Its chairman, Robert F. Dacey stated: “For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences. Further, since 1997, we have identified information security as a government wide high-risk issue in reports to the Congress-most recently in January 2003\textsuperscript{4}. Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, in October 2000 the Congress passed and the President signed into law the Government Information Security Reform provisions (commonly known as GISRA) to strengthen information security practices throughout the federal government. With GISRA expiring in November 2002, FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies by GISRA. FISMA added important new requirements, such as mandating that the National Institute of Standards and Technology (NIST) develop minimum information security requirements for information systems.

Government agencies have been the early adopters of Information Assurance (IA) programs, but recently the private sector has recognized the usefulness of IA personnel, techniques and processes The National Security Agency (NSA) is actively recruiting Information Assurance Specialists. Ongoing attacks against computer systems have prompted the Federal government to comply with a mandate to protect the sensitive personal information of its citizenry. The Federal Bureau of Investigation (FBI) has responded to the need to protect the critical assets of the nation by creating the InfraGard.org; a security awareness organization of government, industry and private sector individuals. In addition, the Gramm-Leach-Bliley Act (1999)\textsuperscript{5} mandated that all banking and finance institutions follow a rigid guideline to comply with information assurance. The Health Insurance Portability and Accountability Act (HIPPA, 2002) mandates that the Health Care Profession agree with similar guidelines for the sensitive personal health information of its patients\textsuperscript{6}. The BSA 17799, considered the foremost security specification document in the world, the code of practice includes guidelines for all organizations, no matter what their size or purpose\textsuperscript{7}. Recent revisions of the guideline have produced documents that encompass ethical behavior of persons responsible for developing, maintaining and supporting IA standards at companies.
Due to the demands by government and industry for competent IA technologists, many institutions of higher learning have instituted IA programs. From a study of the current state of the art in IA curriculum programs appear to either focus on technology, firewall installation and monitoring, Active Directory Services, etc. or management and governance of policy and practice. The first subset of students with excellent technical skills is very employable, because of the obvious need for students with the knowledge of data security and infrastructure protection. The later group has the ability to not only accomplish technological protection of business systems but institute ethical practices that provide a consistent and well ordered business. Significantly, conversations with NSA personnel, fellow faculty at similar institutions and industry leaders resulted in the surprising but not unexpected request that our adult learners should be security technologists but also well versed in ethical decision making. Upon assimilation of this data MSCIT has produced an IA program that has two principle components, the first, enterprise security job task technology training, and secondly, governance of information. MSCIT, because of two significant factors, our tradition and interest in applied ethics and the availability of our virtual lab (Vlab) has taken a balanced approach to the curriculum. Job task training provides for training in increasingly complex systems environments.

- securing of devices; routers, switches, firewalls
- systems access: authentication, authorization and intrusion detection
- enterprise systems security, through policy management of operational and organizational groups

Our students receive both the technology and ethical components of IA governance. In addition because of the existence of our Vlab technology, MSCIT uses it within its instructional systems life cycle (ISLC) to further reinforce and support our adult learners both in the classroom and online.

The other key component in establishing a vital online program was a delivery system. As such, MSCIT established a feasibility study of an enterprise network that would allow for development and production of curricular materials in support of our online and classroom classes. The resulting network, ARNe (Academic Research Network, enterprise) provides the delivery of our Vlab course materials developed using the ISLC. ARNe provides our MSCIT students with a safe environment to develop, plan and test the next generation of OS, applications and curriculum in support of our online and classroom classes.

The Vlab has several advantages over traditional simulation environments. The virtual nature of the laboratory as an Internet-based tool ultimately allows all Regis students, and potentially those of other institutions, access to its facilities virtually all of the time. The virtual laboratory isn’t limited to one specialized domain. It provides an environment in which numerous students, in various disciplines, can practice with state-of-the-art technology using a multitude of applications. For example, a student in a database course can practice configuring a large database used by other students at the same time that a software engineering student can be updating the requirements or design of a service community project being worked on by fellow students. Simultaneously, students taking network administration and e-security courses could be configuring the network policies and security associated with the
laboratory. Finally, as part of a project management course, several business
students could be using the laboratory to extend an existing project plan for a large
fictitious corporation. All of this taking place in a save, risk-free environment that
encourages student participation and collaboration.

The Vlab is capable of delivering applications via the Internet using Citrix “thin client”
technologies over the Regis University/ARN (Academic Research Network). With
access to the Internet, students all over the world can use their browser to connect to
the Vlab and the lab applications that support their coursework. The goal of the ARN
is to create a research and academic support network with global connectivity that
could be jointly managed by Regis University students studying in the Database
Technologies and Network Lab Practica.

MSCIT online and classroom student census
The United States Department of Education reports that the number of degree-
seeking students taking online courses has grown at a compound rate of 33% over
the last several years; reaching 2.2 million students by the end of 2004. The
National Information Assurance Education and Training Program (NIETP), in its
criteria for Centers of Academic Excellence, places emphasis on distance learning
as the most effective means to meet the needs of the global work force. Currently
54% of all Regis University School for Professional Studies students are enrolled in
online courses – up from 9% in 1999/2000. MSCIT has over 1230 enrolled student
with more than 60% taking online classes. As an early adopter of online education,
in 1999 MSCIT began offering a limited subset of our curriculum to our distance adult
learners.

Our typical student population has changed over the past few years. Before the
collapse of the dot.com industry our students tended to be bi-normally distributed
between career changers and IT professionals; a challenging teaching environment
at best. The most recent student census indicates that we are maintaining our bi-
normal distribution, the career changes have been supplanted by IT workers that are
in need of retooling with the latest IT technology, architecture and business
intelligence. Additionally, the ratio of online to classroom based students was 1 to 5,
as of the spring semester in 2004 MSCIT taught 4 online students to 1 classroom
student. Online or in the classroom, MSCIT students have consistently requested
more “hands-on experience” (experiential learning) with technology. Recently, a
large subset of the student body has express much interest in Information
Assurance, of course, with the usual request for lab experience with routers, firewalls
and policy development. Through attendance at national conferences the MSCIT
faculty has recorded an increase in higher education IA programs. The change in
our student population in concert with consistent demand for hands-on experience
necessitated the development of techniques and methods to address the student
desires. It is MSCIT position that the course offerings consisting of a balance
between job task training and management of governance and policy would best
meet the needs of our student in the short term and for their career.

The movement of our courses to the online arena has resulted in the necessity to
develop delivery strategies for lab materials to the classroom and online students.
Online learning has become a preferred learning mode among adult learners with
demanding work lives, especially those who work in fields of information technology.
Regis University is uniquely positioned for this growth. Due to the increase in online student population Regis University proposed and implemented a distance learning solution utilizing the WebCT delivery system with course materials developed by MSCIT faculty. Currently, the MSCIT student whether online or classroom based, their class laboratory work is delivered to their desktop at work, home or on travel through our Vlab. As the course development system has become more complex, MSCIT developed the ISLC framework for classroom and online course development, support and maintenance, see Conn 2004. In addition four IA courses were developed for the 2004 calendar year to provide a foundation in IA in the enterprise. Their accompanying course descriptions are listed below:

- **Introduction to Enterprise Information Assurance** introduces students to the elements of the basic Information Assurance (IA) model and its components; security of the database, the application and the network. Current security standards and best practices, such as the security development lifecycle, NSTISSC\textsuperscript{10} security model, NSA security standards, and government/commercial sector security standards and auditing practices will be examined with respect to enterprise IA components.

- **Managing a Secure Enterprise** is designed to provide the student with the knowledge of designing and managing a secure enterprise. This course will focus on many aspects of enterprise security to include physical security, hardware and software, security, operating system security, email security, and personnel security.

- **Planning and Implementing Architecture Security** explores security policy development, implementation and standards compliance and testing on corporate systems, application and data. The target architectures include the telecommunications switched and packet-based telephony systems, and the hardened and wireless enterprise corporate data network.

- **Securing and Protecting Systems, Applications and Data** is designed to provide the student with the knowledge of building and protecting their enterprise infrastructure and their company’s proprietary data. This course will focus on many aspects of enterprise security to include risk analysis, security policies, intrusion detection, damage control and assessment, and various technologies to ensure a secure architecture.

The MSCIT students are typical adult learners in that they respond well to a constructivist approach to education, Kolb (2001). The students appreciate individualized teaching materials and hands-on learning. During instructional periods they best respond to opportunities to analyze, evaluate and adapt material to new situations.

In development of the curricular elements of the pedagogy Bloom’s cognitive domain educational theory provided an adaptable methodology for the generation of course materials. Each of Bloom’s hierarchy of learning steps (memorization, understanding, application, analysis, synthesis and evaluation) were a key component in the development of curricular materials. Following the guidelines
established for course development; the course instructors were provided with the learning objectives for the course as well as the weekly objectives. They provided the assessment of the students and determined. The students readily adapt to individualized materials and lab exercises, and respond well to a structured curriculum that first presents introductory concepts and ideas then provide best of breed tools for exploitation of the material. During development of the course material the first step was to introduce the students to the three moral models through material structured by the Bloom’s taxonomy of cognitive learning, see Bloom (1956). As an assessment of student’s ability to use the three moral models in ethical decision making, students were assigned case studies to evaluate and return to the instructor.

**Common moral models and their influence upon adult decision making**

Upon examination of Chapter 3 of Curran’s recent book *The Catholic Moral Tradition Today*, see Curran (2002), three moral models were reviewed and evaluated for their strengths and weaknesses as to their use in the formation of an ethos, see figure 3. The models that were chosen to form the center for the adult decision making pedagogy were the Deontological (law based systematic study of life), Teleological (Goal centered) and Relationality-Responsibility (multiple relationships involving the person, business, community and the resulting affective nature of the relationships) models which will be discussed in detail with respect to their relative importance. Of most importance with respect to adult decision making is the Relationality-Responsibility moral model because it most closely simulates the environment that is represented in typically ill-defined managerial decisions. This is due to its reliance of the affective influences that are commonly found in modern IA decisions. Upon reflection the three models offer our adult students some unique, and some complimentary characteristics that encompass very broad categories. In choosing a model it must be noted that it provides a means of conceptualizing an ethical approach to problem, but that it did not rule out the possible use of a different moral model. The application of a Teleological model to a case study did not necessary exclude legal consideration (Deontological model analysis) of the case. The choice of a moral model describes the method of analysis and an understanding of the moral decision in question.

As shown in figure three, the Bloom’s taxonomical structure with its associated hierarchy of learning in the cognitive domain was used to produce the individual learning cycle elements of the ISLC. The Vlab elements supplement the other elements of the ISLC because of their “hands-on nature”. They are linked through HTML pages and links to tools and applications that are required for completion of the weekly lab work. An example of workshop two for the Introduction to Information Assurance course is listed below. This is an example of a virtual lab that requires the students to research user password and implement the password feature in the Colorado Springs Regis University Virtual Laboratory with respect to the Deontological model. Also, it begins the discussion of the elements of a Code of Ethics:

**Introduction to Enterprise Information Assurance**

**MSC 6941**

**Workshop Two**
Lab: Introduction to the Lab.

Assignment:

Security Policy/password:

- What is a standard recommendation for the length of time before passwords should be changed? Which moral model is best used to determine password modification?
  - Look at MIT’s White Paper: “How to Choose a Good Password”
- Implement this password change in the Security Policy at http://citrix.am.regis.edu.

Analytic tools for decision making

The second element in our pedagogy was to expose students to a variety of tools that provide a toolkit to examine the effect of ethical decisions on organizational structures and the individual within a business organization, see figure four. The selected tools where chosen in response to the student's desire for “hands-on” training and in concert with MSCIT’s academic partnerships with large information technology companies. Thus, a variety of software and hardware based applications were hosted on the ARNe network. The tools represented a variety of common platforms from which students can apply ethical decisions using best of breed software. Some of the typical applications were Microsoft active directory server (operational unit and group policy), OPnet SP Guru (security audit) and OpenBSD firewall platform (VPN technology and ACL). The construction of virtual labs for this segment of the curriculum represented its own set of challenges because of hosting issues related to deliver of the application using a thin client. Only applications that involved less intensive user interfaces were able to be successfully hosted. We have successfully tested Visio, the Rational UML modeling program and the active directory features in Server 2003.

Evaluation complex topics

Spinello’s “Steps for Ethical Analysis” was most helpful in linking the moral models to the ethical decision making process, see Spinello (1997). His seven step process in abbreviated form is:

1. Identify and formulate the basic ethical issues.
2. What are your first impressions or reactions to these issues?
3. Consult the appropriate guidelines.
4. Analyze the issues from the viewpoint of one or more of the ethical theories.
5. Do the ethical theories point to one decision or course of action?
6. What is the normative conclusion about the case?
7. What are the public implications of this case and your normative conclusion?

These seven principles formed the basis for the evaluation of the case studies presented in the courses. They will be presented to the students in the presentation element of the ISLC as resource materials. The virtual lab that will be associated with the evaluation element of the pedagogy will consist of applying the seven step
process to case studies that are concerned with evaluation of security policy implementation, development of code of ethics and design of operational units with emphasis on application of group policy.

Summary and conclusion
The proposed adult decision making pedagogy is grounded in universal moral models with wide applicability to decision making within Information Systems practices and policies. It incorporates accepted standards and procedures from professional and governmental bodies. The model utilizes a variety of applications, software and hardware platforms to demonstrate ethical concepts, allow for hands-on learning, and evaluation of complex ethical issues. The pedagogy relies on the ISLC to provide a structured and iterative process that provides for delivery of instructional material based on an established taxonomy proven to work for adult learners. Only one aspect of the ISLC, the virtual lab, was presented in detail. The virtual lab provides an impressive adjunct to the standard teaching materials, presentations and discussions. Hosting of the virtual labs on the ARNe network provides our students in the Practica with experience in management and support of an operating Information Systems workplace. The ability to present adult learners with a variety of tools for ethical decision making serves to enhance their ability to make proper and useful decisions at work. The evaluation of case studies also increases the experience students have with a variety of difficult situations in a non-threatening learning environment. Upon completion of the virtual labs for all segments of the Information Assurance courses, students will be better able to determine ethical policy for a variety of Information Systems companies.

Endnotes

1 Sources of Ethics Standards for Information Assurance
The course ethics standards and best-practices were derived from the CISSP (Certified Information Systems Security Professional) http://www.cissp.com/cissps/Ethics_Code.html

2 ACM (American Computing Machinery Society) ACM (American Computing Machinery) http://www.acm.org/constitution/code.html


6 www.hep-c-alert.org/links/hippa.html

7 BS7799 (British Standards) were reviewed for incorporation into the course material. http://www.bsi-global.com/Information+Security/index.xalter

9 http://www.nsa.gov/ia/academia/acade00001.cfm

10 NSTI SSC (National Security Telecommunications and Information Systems Security Committee)
Figures

Figure 1 The Adult Decision Making Pedagogy
Figure 2 The IS curriculum online learning cycle, Conn (2004)
Bloom’s taxonomy
Cognitive Domain

Knowledge of terminology

Comprehension
Grasping (understanding) the meaning of informational materials

Application
The use of previously learned information in new and concrete situations to solve problems that have single or best answers

Analysis
The breaking down of informational materials into their component parts

Synthesis
Creatively or divergently applying prior knowledge and skills to produce a new or original whole

Evaluation
Judging the value of material based on personal values/opinions

Moral Models

Deontological

Teleological

Relationality-Relationship

Instructional Design

ISLC

Learning Cycle elements

Readings

Review questions

Research

Discussions

Presentations

Virtual Lab using IS tools, application and development environments

Figure 3 Adult Decision Making Moral Models Framework
Figure 4 Adult Decision Making Analysis Tools Framework
References


