Submission to the
5th National Colloquium for Information Systems Security Education
May 22-24, 2001

TITLE: ***Information Security University — Web Enabled Learning***
General Track

AUTHOR: **Don Holden, CISSP**
Security Leader, AtomicTangerine, Inc.
23 Manchester Road
Amherst, NH 03031
V: 603 673 8454
F: 603 673 6398
E: DHolden@atomictangerine.com

SPEAKER: **Don Holden, CISSP**
Security Leader, AtomicTangerine Inc.
23 Manchester Road
Amherst, NH 03031
V: 603 673 8454
F: 603 673 6398
E: dholden@atomictangerine.com

ABSTRACT

Information Security University — Web Enabled Learning

How do you provide security training and education to people who cannot travel, are "on the go" or physically distributed? Traditional classrooms and audio/video methods are impractical or fall short of a high-quality educational experience. Have you ever received a bunch of talking-head PowerPoint charts? It's not education!

There is an effective method to train information security professionals or end users, using only a web browser. This paper discusses how we created Information Security University (InfosecU), what it does, how it does it, and how it can be used to educate both end users and professionals.

In response to the need for quality in-house, online information security education for both end users and security practioners, DuPont set out to build Information Security University (InfoSecU). DuPont and Atomic Tangerine, a spin-off of SRI International and SRI Consulting, designed and delivered the basic information security courses in a period of a few months, and Information Security University went live at DuPont in the fall of 1999. Using only a web browser, a student can access the university from any computer anywhere in the world, register for a course and begin learning. Courses can be started and stopped at anytime, and progress is constantly tracked. Courses range in duration from an hour to a few days. Five levels of courses have been defined beginning with the 0 level awareness training courses for end users through the 100 basic introduction courses to the specialized 400 level courses for managers. InfoSecU employs interactive audio and video, case studies and fast-paced interactive question and answer dialogs to test the student's retention. Through a partnership with ISC^2 we are able to provide students with continuing professional education credits for their CISSP re-certification.

The initial core curriculum based upon a common body of knowledge defined by ISC^2 has been expanded to 14 courses with more in development.

BIO

Don Holden, a security leader at AtomicTangerine, specializes in information security architecture and policy. He has more than 20 years of experience in information systems, security, encryption, business continuity and disaster recovery planning. Don has written numerous white papers and given presentations on information security management and technology issues such as

intrusion detection, firewalls, biometric authentication and digital watermarking. He is on the staff of the AtomicTangerine s Information Security University and a subject matter expert for several of the courses. He is also currently the co-chairman of the IEEE Computer Society working group on recommended best practices for Internet security. He is also participating in the development of security standards for the financial industry. Before joining AtomicTangerine, Don was a senior consultant for SRI Consulting, where he was a project leader for an Internet startup assignment to plan a revolutionary secure electronic commerce portal-based business. Don previously served as program manager for Compaq s Security Program Office and as the director of operations research at a major Boston bank. Don holds an M.B.A. from Wharton and a B.S. in business and accounting from Georgetown University. He is a Certified Information System Security Professional (CISSP) and a member of the IEEE Computer Society, the Computer Security Institute, and the Information Systems Security Association.

Information Security University — Web Enabled Learning

It has long been known that the weakest link in the information security chain is people. The billions of dollars that are forecast to be spent on information security technology will be wasted without security training and awareness. As information technology becomes pervasive throughout organizations, proper usage of this powerful capability becomes a part of everyone s job. The Computer Security Act of 1987 recognized this link when it required periodic security training for everyone one in the Federal government who operates, manages, or uses a computer system. The challenge is how do we provide effective, low cost, and easy to take training for non-technical users as well as for IT and security professionals who have a need to stay abreast of the rapid advance in technology and security attacks. The security professionals were familiar with the routine work of raising awareness, managing access to computers, protecting proprietary information and investigating the occasional theft of a laptop. Many performed clerical or administrative functions. But as we leave the 20th century, the nature and degree of risk facing organizations is changing dramatically. Malware is on the rise, while hackers, crackers, and hacktivists are knocking at the organization s perimeter with hundreds of new attack vectors. Many infosec professionals are ill-prepared to cope with these new attacks, vulnerabilities and countermeasures.

While the need for more training is clear. The challenge is how do you provide security training and education to people who cannot travel, are "on the go" or physically distributed? Traditional classrooms and audio/video methods are impractical or fall short of a high-quality educational experience. Many training courses are a series of PowerPoint slides with little explanatory material. These presentations are often put together by different people, many of who have little or no teaching experience. Additionally there is a shortage of trainers. Tasking existing security professionals who are already stretched to also do training is seen as interrupting their real job.

To meet this challenge DuPont and AtomicTangerine, a spinoff of SRI International and SRI Consulting, designed a web enabled training called DuPont InfoSecU. The initial courses were delivered after only a few months in late 1999. Using only a web browser, a DuPont employee can access InfoSecU from anywhere in the world, register for a course, and begin learning.

Building on this successful project, DuPont and AtomicTangerine then formed a venture to further develop InfoSecU into a full security curriculum covering the security common body of knowledge as currently defined by ISC^2. The Information Security University (ISU) curriculum covers the learning spectrum starting with some basic awareness courses that are applicable for all employees: Information Security Fundamentals, Privacy, and Identity Theft. These are at the

0 level. Information Security Fundamentals also serves an entry course for all the other courses in the 10 security domains. The ten domains are the following:

- Access Control and Methodology
- Security Management Practices
- Telecommunications and Network Security
- Application and System Development Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Business Continuity Planning and Disaster Recovery
- Law, Investigations, and Ethics
- Physical Security

The next level is the 100 level which is basic training for the major areas of the common body of security knowledge. We expect that IT professionals as well as general users with an interest in security will take 100 level courses. To take the course the student should have completed the introductory course (050) or have equivalent knowledge. The student can also take a pre-course test to determine if he or she already knows the material to be covered and areas where additional training would be useful. The student should be able to perform the following types of actions upon completion of a 100 level course:

- Describe an operation
- Identify and explain
- Recognize correct answers

An end of course test will evaluate the ability of the student to

- Recognize basic terms and concepts
- Classify terms based on taxonomy
- Able to list 3 benefits of sound security
- Know what you don't know
- Able to list and define x examples of course content
- Explain info sec in non-technical level
- Identify appropriate next steps for knowledge development

The next level course (200 level) is the beginning of application-oriented training. Students taking 200 level courses will be IT and security professionals whose job requires security training. The student will have taken one or more 100 level prerequisite course or have equivalent knowledge. For example course 231 Access Controls for Networks has Course 130 Access Controls Systems and Methods as a prerequisite. After taking the course the student should be able to

- Describe range of alternatives for doing an operation
- Identify factors for choices

The end of course test will evaluate some or all of the following

- Given a list of alternatives, learner is able to select one alternative and make a case for its use in a given situation
- Judge suitability of technique for achieving goal (job specific)
- Identify choices to complete the project
- Use information to bring it to brain to make decision. Customize solution.
- Provide management with concrete suggestions for company specific security practices in existing
- Recognize common security vulnerabilities/threats
- Assess implications
- Make recommendations

The 300 level courses are designed to provide training for complex procedures, applications or product security. For example, Course 331 Access Controls for Windows 2000 is another course in the Access Control Domain. Upon completion of a 300 level course the student is expected to be able to

- Implement and perform security tasks at highest level of performance
- Anticipate problems
- Deduce from evidence, potential problem, synthesize alternatives, select course of action/solutions for preventing problems from reoccurring

The highest level courses, the 400 level, are designed for managers and specialists where insight is needed for integration of strategic planning and enterprise security management. In the learning spectrum, 400 level courses fit into the education area. The focus is on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the IT security profession and to keep pace with threat and technology changes. Some potential courses could include Managing Risk Assessment and Business Continuity Planning and Intranet and Extranet Security Management . The desired outcomes could include some of the following:

- Able to articulate importance of information security in strategic planning
- Able to apply information security
- Able to make optimal decisions on implement, maintenance evaluation and revision on information security programs
- Explain value of operations, benefits, roles, financial implications of information security
- Understand and define next steps in personal and professional development plan.

Learner Profile Survey

A survey of existing and potential students was conducted after the initial InfoSec U training was done at DuPont to help us build the expanded Information Security University. The survey was designed to collect data that would help answer the question, Who is the potential ISU audience? The characteristics measured in the survey included: several demographic factors; previous training; available training-related hardware; frequency of and proficiency in job tasks; and learning preferences.˚

The survey conducted by SRI International was done in three parts. Part 1 surveyed the DuPont information security coordinators who attended the DISO World conference in May, 2000, during which 71 valid surveys were completed. Part 2 surveyed a national audience of Security Portal users, during which another 71 valid surveys were completed. Part 3 surveyed information technology practitioners from SRI International who perform information security functions as part of their jobs. A total of 6 valid surveys were completed. A total of 148 combined surveys comprise this report.

Some Results of the Survey

- Respondents appear to have relatively little experience with Web-based training
- Respondents showed a strong preference for textbooks and other paper documents as learning media. Web-based courses are ranked in the middle of the distribution of media. E-mail-based courses received particularly low ratings.
- 77% percent either agree or strongly agree to the statement I usually download or print a paper copy of important documents or materials that I find on the web.
- Information security professionals appear to prefer group-based training that results in long-term application of learning outcomes. They appear to be neutral regarding Web-based versus traditional training formats. Information security professionals tend to be slightly more internally motivated than externally motivated to attend training.
- The difference between the importance of various information security tasks and respondents proficiency to perform those tasks varied significantly suggesting areas for greatest need for training. The area of greatest importance was Controlling system access , the area of least proficiency was Developing and administering business continuity plans , while the area with the greatest difference between importance and proficiency was Detecting and responding to incidents .
- Respondents hardware settings vary widely. Internet transmission speeds vary considerably. Over 50% of respondents have T1, DSL or greater connection speed.

Course Design Conferences

New courses have a structured development process. Most new courses will already have an abstract and a place in the overall curriculum map. The Design Conference is a meeting (often a teleconference) of the 3-5 people responsible for "opening" and beginning the creation of an ISU course. This meeting follows a structured process intended to harvest from Subject Matter Experts (SMEs) the information that will comprise the course being developed. The meeting will focus on accomplishing several objectives:

1. Form an efficient team so that course materials can be quickly and cost effectively developed.
2. Characterize the performance environment of learners who will take this course. (type of learner, knowledge level of the learner, difficulty and breadth of the course, etc.)
3. Define the major components of the course:
    a. Course objectives (the major objectives to be covered by the course)
    b. Course content outline (an outline of the subjects covered by the course)
    c. Learning activities (such as readings, simulations, games, scenarios)
    d. Evaluation measures (multiple choice, true/false, matching, short answer, simulations, etc.)
    e. Course specific graphics
    f. Course specific learning aids
4. Create a course-specific schedule that will guide the work of the team.
5. Gain commitment of team members to contribute their time to this effort

The lead SME brings a strawman of the course abstract, objectives, and course outline to the design conference be used to generate discussion. The writer will use the information and ideas generated from the design conference to create a design document (or a detailed skeleton of the course) and will provide this to the SMEs for their input and approval before writing the course. The SMEs and the writer collaborate to produce the course content that is reviewed and sent to the web editors and illustrators

Course Structure:

The following structure applies to courses, modules and lessons across the different levels.

Introduction

- What you will do
- Rationale for Importance
- Sizes the scope of the course
- Estimated completion time
- How the course connects to others in ISU
- How the course connects to information security and your job or company

Learning Objectives

- Define learning objectives in behavioral terms. The student will be able to

- Objectives must be observable, measurable, and concrete.
- List 4-8 objectives.
- Write objectives in declarative statements.
- application/person specific objective (learning transfer)

Self Assessment/Monitoring

- The self-assessment should include parts that are interactive.

Body

The next level of specific content. A course is composed of one or more modules. A module typically takes about 30 to 40 minutes to complete. A module may have one or more lessons covering specific learning objectives. Browser buttons are used to provide straight forward navigation. Hyper-text links are provided to relevant books, articles, news items, glossary of key terms. Engaging examples, illustrations, and animation are employed to make the learning process more enjoyable. Students can hear the experts speaking about security and can see a video clip of the professor . Students are more likely to complete the course if it can hold their attention. Bookmarks are automatically inserted when learners leave courses before completion, making it easy for them to return to the place where they left off. Review quizzes are inserted after each lesson. A subject matter expert is available electronically for questions and clarification.

Terminal Assessment

- Standardized format for all courses
- Records that learner has completed the course and his score
- Tests for mastery of skills
- Gives feedback on progress and results
- Bank of question items, as many as 100. Approximately 25 used for a test.

Summary

- What you have done
- Summary should provide the answers to the objectives

Conclusion

Next Steps

- Applications to work experience
- Additional reading, interactive
- More/Next courses
- Professional development activities

.

Status of Information Security University

Information Security University is now available on the Internet through Security Portal (www.securityportal.com) for individuals and organizations and customized versions are available for corporate intranets. There are two free introductory courses available and an additional 12 courses are on-line with more in development and others in the planning and design stage. Initially we will be filling out the curriculum for the 100 and 200 level courses more rapidly than the 300 and 400 level courses as the higher level courses have a more limited market potential. One exception to this will be courses that help prepare students for the CISSP (Certified Information System Security Professional administered by ISC^2) certification exam. ISC^2 has agreed to accept ISU courses for continuing professional education credits towards re-certification.