ISSN: 1545-679X

Information Systems Education Journal

Volume 5, Number 11 http://isedj.org/5/11/ May 18, 2007

In this issue:

Redesigning an Information System Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends

Belle S. Woodward
Southern Illinois University
Carbondale, IL 62901 USA

Travis Young
Southern Illinois University
Carbondale, IL 62901 USA

Abstract: Information technology's integration into the world has afforded cyber criminals the opportunity to exploit societal entities on an epic scale. The ability to mitigate these attacks becomes a must if current and future professionals intend to survive in a tightening job market. In order to meet this ever-increasing need for protection, educational institutions are pressed to develop a new age of cyber security specialists. Information security curriculum development continues to be challenged today to support a dynamically changing workplace. Information security's rise in importance following the burst of the Internet bubble in 2000 has called for some unique ways to prepare undergraduate students for the workplace. The requirements for more "hands on" experience for students at the university level, along with information security's status as having the greatest job-growth potential over the next three to five years. This has required the researchers to significantly reduce lecture based course content and increase "hands on" instruction through the principles of active learning. This paper details changes to an information security program at a midwestern university. Beginning with the theories of Kolb, the researchers combined traditional pedagogy and modern business trends to shift from one course in network security and two courses in networking to a more comprehensive program of three classes in network security and three classes in networking. Students exposed to this new course curriculum validated the relevance of these changes, ultimately receiving a first place win against seven other educational institutions in the 2006 Midwest Regional Collegiate Cyber Defense Competition.

Keywords: curriculum development, pedagogy, information security

---

Recommended Citation: Woodward and Young (2007). Redesigning an Information System Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends. *Information Systems Education Journal, 5* (11). http://isedj.org/5/11/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2006:* §2332. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/5/11/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Redesigning an Information Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends

Belle Woodward, Assistant Professor
bellew@siu.edu

Travis Young
youngtg@siu.edu

School of Information Systems and Applied Technologies
Southern Illinois University
Carbondale, IL 62901

ABSTRACT

Information technology's integration into the world has afforded cyber criminals the opportunity to exploit societal entities on an epic scale. In order to meet this ever-increasing need for protection, educational institutions are pressed to develop a new age of cyber security specialists. Information security curriculum development continues to be challenged today to support a dynamically changing workplace. Information security's rise in importance following the burst of the Internet bubble in 2000 has called for some unique ways to prepare undergraduate students for the workplace. The requirements for more "hands-on" experience for students at the university level, along with information security's growing status as having the greatest job-growth potential within the Information Technology (IT) field over the next three to five years, have required the researcher to significantly reduce lecture based course content and increase "hands-on" instruction through the principles of active learning. This paper details changes to an Information Security program at a mid-western university. Beginning with the theories of Kolb, the researchers focus shifted from one course in network security and two courses in networking that relied largely on abstract conceptualization and reflective observation to a more comprehensive program of six. Students exposed to this new course curriculum validated the relevance of these changes, ultimately receiving a first place win against seven other educational institutions in the 2006 Midwest Regional Collegiate Cyber Defense Competition.

Keywords: curriculum development, pedagogy, and information security

1. INTRODUCTION

It has been said that the best offense is often a good defense. This is particularly true in the cyber defense industry. The 2005 CSI/FBI Computer Security Survey has shown a tremendous growth in both the probability and severity of attacks on the information systems containing vital corporate informational assets. The origin of these attacks is not only from external threats, but also from internal threats, accidental and intentional. The increased dependence on computer systems to support critical business applications has drastically increased the need to be able to quickly and proactively defend against threats.

The methods and means of protecting critical computer systems have had to evolve during the past few years to provide increased access to networks, while continuing

to keep them secure from attacks. As a comparative example, a bank would not be considered viable without incorporating security that accommodates people going into and out of the bank. Designing today's networks also requires the incorporation of security while allowing access to the system. With this fundamental requirement for access to networks within a world of interconnected systems, it is no longer a feasible security measure as it once was to just hide details of computer operations from potential attackers. This evolution of requirements in network design has been a driving force for the reorganization of the security education market. The focus is now being shifted to educating graduates to proactively defend the interests of a corporation's informational assets, all this while conforming to the key tenets of confidentiality, integrity, and availability.

The key goal of network design is to counter Cyber attacks, which threaten a networks confidentiality, integrity and availability and must be prevented or quickly mitigated. Cyber attacks consist of attacks both on the physical infrastructure and the digital information. The capability of defending against cyber attacks, therefore, must be included in any modern day information security educational program.

In the interest of preparing students to defend against these attacks, The National Science Foundation, the Center for Infrastructure Assurance, The University of Texas, and Texas A&M, sought to create a computer security competition. This coalition created what would come to be known as the Collegiate Cyber Defense Competition (CCDC). The CCDC was designed to give students the opportunity to participate in a business like environment while competing with other student groups. The Midwest Regional Collegiate Cyber Defense Competition is one of the preliminary competitions that leads to the national level finals. IT professionals and educators commit a significant amount of time and resources to ensure the competition is relevant to today's workplace.

If graduates are going to effectively defend corporate networks in the 21st century, such as the one portrayed at the CCDC, then they need the intellectual tools to understand and conduct security audits against the systems they intend to protect. Since the field of information security is still in its infancy, developing a curriculum must prepare future security professionals to not only survive, but also thrive in this environment. A question for academia is how to best prepare future professionals in information security to defend their critical information systems. Focusing only on information security techniques denies the student an understanding of how these techniques woven into system development and implementation can provide an integrated defense. Because information security always involves weighing user access against security, costs, and the threat, the professional should thoroughly understand the nature of the threat and what the attacker is trying to gain whenever creating and implementing an effective defense.

Currently, a trend followed by academia and industry is to take a reactive approach to information security. This reactive approach can be flawed because the security professional is one step behind the attacker. To promote a proactive approach, information security knowledge should be embedded into undergraduate level network design courses. The courses should train network engineers to implement security practices during the design stage of development. These practices should be considered when writing requirements and specifications, throughout the entire process of system design and implementation. These changes would shift the views of the security community from a reactive approach to a proactive approach.

Security cannot be thought of as a follow-on process that is only considered after the project is complete. The incredible growth of our society's deployment of computing has too often been conducted with concerns for speed or lowest cost rather than with concern over issues of privacy, security, and reliability. Much of the established infrastructure is not designed with security in mind and most personnel do not have the necessary level of security awareness (Cyber Security, 2001). Just as a house would not be built without locks, a network should not be built without proper defenses in place from the ground up. Securing an existing structure that was built without security in mind presents many challenges.

All of these forces combine to be a major driving force for relevant change not only

within the security industry, but also within the academic setting. According to an Information Technology Association of America (ITAA) survey, 43% percent of respondents say job candidates lack sufficient hands-on experience (ITAA 2003). Morneau (2004) considers most information security programs lacking in a hands-on component and emphasizes the need for undergraduate information security programs to focus on a hands-on component as they prepare learners for the workplace. According to ITAA (2005), employers determined information security to be the area with the greatest job-growth potential over the next three to five years. These two perspectives combined create a need that should be addressed at the undergraduate level.

This academic change should effectively integrate theory with real world experience. Since there is a lack of a general consensus for an ideal IT security program at the undergraduate level, many different programs were compared (Steel, Stojkovic, & Zaveri, 2004). An academic program can only succeed through the blending of traditional academic pedagogy and newer progressive teaching styles. It is only through this blending that an incoming student can be shaped into a well rounded professional (Schön, 1987).

2. PEDAGOGICAL THEORIES

For the researchers, the design of the IT course curriculum began at a foundational level upon which an educational environment conducive to the development of reflective problem solvers was constructed. The theoretical writings of Dewey (1938/1997) and Vygotsky (1986) poured the foundation for the IT program's redesign, while the research of Schön (1983; 1987) supplied the construction materials for the basic structure. The essence of Dewey's "genuine education" (1938/1997, p. 25) is one of connectedness in learning. Dewey explains that it is the interaction of the environment and the individual that contributes experiences leading to growth, and that maximizing the use of physical and social surroundings will enhance the experience, thus making it a more worthwhile, educative experience. Dewey's theories hold that school should engage students in an educational process that meets them at their cognitive level, and using developmentally appropriate instructional principles, provide students a problem solving environment that prepares them for the impending work world. Dewey's emphasis on problem solving and critical thinking skills are still vital today. In addition to Dewey's theories it is important to integrate Vygotsky's social learning theory and his theory on the Zone of Proximal Development (1978) as it plays out in collaborative settings. Vygotsky's research found that to fully develop a learner's cognitive abilities, social interaction is required. It is the use of language in this social interaction that plays such a fundamental role (1934/1986). At any given age however, a learner's cognitive development is limited to a certain range of skill. It is through the articulation of knowledge (skills, concepts and processes) by a more senior guide or peer collaborator that this range can be increased or developed to surpass what the learner would otherwise be able to accomplish alone. Using this theory, it is clear that IT students would benefit from greater in-class opportunities to work collaboratively to solve real world problems, thus more pervasively employing the zone of proximal development. The incorporation of these real world problems needs to include challenges that rise above simplistic applications of programming code. Instead, these problems need to propel students into the realms of higher order critical thinking skills: analysis, synthesis and evaluation (Bloom, 1956).

Building upon this concrete foundation is that of an instructional approach facilitating "reflection-in-action" (Schön, 1983). Upon examination of professionals at work in their fields, Schön determined that a competent professional inquires into a problem, attempting to find a solution to the problem, as it is initially set. The professional, remaining open to the possibility that incongruence might develop with the original problem's setting, steps directly into the problematic situation for the purpose of imposing a "reframe", in essence a critical review of the problem and potential re-definition. All the while the professional is cognizant of any consequences that could occur due to this reframe, and is willing to reflect during this action (reflection-in-action), formulate new hypotheses, and test these hypotheses through further action (followed by further reflection). These actions function to frame and re-frame the problematic situation as

well as explore new junctures or phenomena as they surface for further consideration and reflection until the problem is adequately solved. This "professional artistry" (Schön, 1987, p. 22) is the type of proficiency exhibited in "unique, uncertain, and conflicted situations of practice" (p. 22). Developing these professional skills in novices is accomplished using the "reflective practicum" (Schön, 1987, p. 157) during which the instructor facilitates learning through coaching techniques that embody and model reflection-in-action. The instructional tools ideally suited for these theories are case method and problem-based learning (PBL). Case method with its roots in law, medicine and business schools provides a descriptive narrative based on a real life situation or event. This balanced, multi-dimensional perspective represents the participants, context and issues comprising this real world scenario. These cases are used to assist novice practitioners in honing their decision-making and problem solving skills. By portraying a practitioner's work as context-specific, problematic situations that are tangled and complex, the novice learns to reflect-in-action in order to generate solutions. Cases stimulate analytical thinking, the development of professional knowledge as well as reflection skills.

In a PBL approach, problems are set into highly contextualized situations. Learners work collaboratively while actively investigating these situations. They build new knowledge upon prior knowledge while striving to find the most appropriate solutions. This type of meaningful learning task encourages independent investigation as it fosters the ability to adapt quickly to novel situations. The fluid landscape of internet technologies will continue to accelerate and morph while the cyber learning curve becomes steeper. This leads us to another important consideration put forth by Dewey in applying his principle of continuity to instruction, "the future has to be taken into account at every stage of the educational process" (1997, p. 47).

The researchers drew from another useful model of learning style presented by Kolb (1983). Kolb suggests four stages that must be included when designing a successful curriculum. If any of the four stages are missing, incomplete learning results. The stages include abstract conceptualization, active experimentation, concrete experience, and reflective observation. Each stage produces unique knowledge that when applied provides an understanding of a given topic. Although each stage is required, different types of students may gain more knowledge on a topic in one stage than in other stages based on their particular learning styles.

The first stage that needs to occur is abstract conceptualization. In this stage the student begins to learn the theory associated with the given topic. This sets the foundation from which all other knowledge is built upon. Students who learn best in this stage need to know as many details as possible about the intricate inner workings of the topic.

Active experimentation follows the abstract conceptualization stage. In the active experimentation stage the student works with the knowledge gained in the conceptualization stage, by applying the theory, regardless of the outcome. This allows the student to be able to better understand the inner workings of the topic through a "black box" approach, where the outputs of different inputs are analyzed to be able to generalize about the internal process.

The active experimentation stage leads to the concrete experience stage. In the concrete experience stage the student works through specific problems that lead to specific solutions. This reinforces the knowledge gained from the previous two stages. Students in this stage learn best by actually performing the tasks.

The final stage is the reflective observation stage. In this stage the student looks back on all of the previous stages in order to try to make sense of all of the information obtained. At this stage the student builds a complete understanding of the topic by integrating all of the information gathered during previous stages to form an understanding of a topic. This stage is called the reflector stage, because it is when the student stops to observe and reflect upon all of the information.

According to Kolb, there are also optimal learning styles that can be broken down into four categories: Assimilative, Accommodative, Convergent, and Divergent Styles. Assimilators focus on abstract concepts concerned primarily with the logical as opposed to the practical aspects of a theory. Assimi-

lators prefer working with concepts versus social interaction. Accommodative style learners work best where precisely following directions, and scrupulous planning are required. Convergent style learners score well on standard conventional intelligence tests, where the need to organize quickly by hypothetical deductive reasoning leads to successful mastery of the learning material. Divergent learners create concrete examples of concepts, where the learner can use these concrete examples to create numerous aspects of the concept, followed by organizing these qualities according to how they are related to each in order to find a solution.

3. APPLICATION OF PEDAGOGY

It is through the application of these theories and instructional methods that a redesigned program in networking and network security was implemented. Before the redesign of the curriculum, the focus was placed almost entirely upon abstract conceptualization and reflective observation stages. According to Kolb (1983) this places the focus on the assimilative form of knowledge. However, students in the applied sciences where the career environment is dynamic, the challenges require them to operate intuitively. This creates a situation where students do not get the most from classes solely designed around the abstract conceptualization and reflective observation stages.

The traditional way of teaching is through reading (or summarizing) the textbook and doing problems or examples through rote memory of either formula or fact. Hands-on experiences are often used only to verify the facts stated in the textbook (Bork, 2000). As previously suggested, in today's university setting, educators in information technology are being challenged to move beyond more traditional methods of instruction (i.e. the lecture mode) to an approach that calls for an increased interactivity with their students about both the subject content and learning strategies of the course content (Bork, 2000). Bork (2000) further noted one of the primary problems with teaching at the college-level is that educational institutions have mistakenly overexposed the information transfer model, where knowledge or information is transferred from the teacher to the student. Bork (2000) also encouraged educators and educational administrators to embrace the newer models of teaching where learning is "fully active, focusing on the student as learner." Many educators stress the importance of active learning (Boggs, 1999; Bonwell and Sutherland, 1996; Conklin, 2006; Felder and Brent, 2003; Young, 1998). Felder & Brent (2003) specifically define active learning as a means of delivering content using hands-on activities that involve the student directly in the learning process. Therefore, some educators may need to get away from a teacher-centered classroom to a student active learning environment (Young, 1998).

The researchers drew from current industry requirements and above listed learning theories to adapt two courses in networking and a single security course into six new courses at a midwestern university. Even though the redesigned program closely follows security priorities drawn from National Security Agency (NSA) guidelines, adaptation was made to allow for the most efficient use of available resources. The content and teaching methodology of the three original courses was also redesigned to relate learning content to corporate situations that may be encountered when working in the IT field. This redesigned content and methodology was intimately embedded into the six new courses within the curriculum. Although the redesigned content and methodology was based upon multiple learning theories (Dewey 1938; Dewey 1997, Vygotsky 1986; Schön 1983; Schön 1987; Bloom 1956; Kolb 1983), the Kolb (1983) model provides the most tangible changes. The original three courses used the assimilative form of knowledge as a teaching method. This made the courses inappropriate for an applied sciences topic such as information security. The changes to the curriculum required a shift in focus from assimilative form of knowledge to the accommodative and convergent forms of knowledge which are a blending of the concrete experience, active experimentation and abstract conceptualization stages which are a more appropriate form of knowledge for the applied sciences field.

In the abstract conceptualization (Kolb, 1983) stage the theory is presented in the form of content lectures. This sets the foundation from which all other knowledge is built upon. Next in the active experimentation stage (Kolb, 1983) the student works with the knowledge gained from the concept

lectures, by applying the theory, regardless of the outcome in an isolated lab environment. This allows the student to better understand the inner workings of the topic through a "hands-on approach".

The active experimentation stage leads to the concrete experience stage (Kolb 1983). In the concrete experience stage the student receives business requirements with timeframes that must be met for a successful project. Since working alone is a rare occurrence in business scenarios, students are assigned to teams of three to five. Hardware and software are assigned to the teams to emulate different business situations. Students learn from actually performing the tasks. The scenarios are designed in such a manner that they cannot be completed without the cooperation of every team member. Since roles are not assigned by the instructor the group dynamics force the team to assign roles that benefit each individual and the team as a whole. This begins to challenge knowledge gained by students in the previous two stages.

The reflective observation stage (Kolb, 1983) happens throughout the experience as students are asked to update their project documentation to reflect new end project goals. Project documentation is done in the form of an online forum using WebCT's discussion group forum feature. Team members are required to update this forum on a weekly basis. New intermediate project goals are defined weekly throughout the lectures to give an updated view of the final operating environment. The students must define the steps that they will be required to take in order to reach this objective. This objective can only be reached by integrating the lessons learned in the weekly lectures. By integrating the lectures and lab environment into the documentation, students are forced to reflect on all four stages of learning. Thereby gaining a complete understanding of the materials covered. In this final stage students are asked to present what they have accomplished.

4. CURRICULUM CHANGE – PROOF OF CONCEPT

The researchers were afforded the opportunity to validate the re-designed curriculum at a Regional Collegiate Cyber Defense Competition. A team of eight students (five seniors, one junior, and two graduate students) took part in the competition. Out of the eight, five students had enrolled in all six courses that had been redesigned.

The competition was co-sponsored by the National Science Foundation Regional Center for Systems Security and the Information Security Assurance Site. The focus of the competition for students was on defending networks against a hacker team. In addition to defending against these attacks, the teams were exposed to business oriented injects designed to simulate everyday problems found in a business environment.

Students were evaluated during the competition based on how they maintained their server and host systems, how well they countered the challenges generated from the injects, as well as how well they defended their network against a live and unpredictable hacker team.

A valuable contribution to success during the competition was that the students were already used to working in teams. The team concept was incorporated in 4 of the 6 courses, which broke class populations down into teams early in the course, and designed projects around a business inspired model. These teams were then given course work where an individual's success revolved around the success of the team.

During the competition, simulated business injects were part of the scenarios that teams were exposed to. Because the course curriculum redesign used a business model including simulated injects, the students were familiar with disruptions on IT systems created by injects and were able to react appropriately to the disruptions.

Two of the courses that were redesigned exposed teams to multiple software platforms (UNIX and Windows), which teams were required to use again during the competition. They were therefore not slowed down by the introduction of additional software platforms during the competition. Another strength facilitated by prior active learning used in the curriculum and displayed during the competition was their thorough understanding of infrastructure equipment. This equipment included routers, switches, and firewalls such as Cisco's PIX.

The utilization of active learning principles in the design of the courses was critical to student's ability to internalize the content required to perform well in the competition. Curriculum design initiatives that included working in teams within the classroom, exposure to business style injects during project completion, and exposure to multiple software platforms and infrastructure hardware all revolve successfully around active learning techniques in the classroom. This contributed significantly to the success of the team taking first place.

5. BUILDING IT LEARNING IN PHASES

The revised curriculum was designed with three distinct phases. These phases were intended to expose students to a wide variety of business situations. Many of these business situations can only be resolved through the use of teamwork. It is because of this teamwork model that in all classes, in each phase, isolation is eliminated and students are forced to work together to achieve the desired goals. Each phase consists of a class focused on security along with a class focused on networking fundamentals. This combination allows the student to have an excellent foundation in networking design and administration while also giving students the opportunity to learn how to secure the same network that they have designed and built. All courses included in the curriculum consist of lecture and lab, with an emphasis on hands-on experience.

Phase I consists of the basic courses needed to introduce the student to networking and security environments. IMS 316 focuses on the ethical and legal responsibilities associated with being an information technology (IT) professional with an introduction to security policy, procedures, and tools. The course covers conceptual and ethical issues as well as practical problem-solving techniques, including security threats and solutions, principles of authentication, security architecture issues, and intrusion detection. Particular emphasis will be placed on the following criteria:

- Ethical IT Behavior and Development of a Code of Ethics
- Legal Responsibilities in Information Systems Management
- Social Engineering
- Security Assessment and Developing a Security Plan
- Security Policies and Procedures
- Introduction to Security Tools Intrusion Detection and Hacking Tools
- Types of Protections and Counter-Measures
- Issues in Wireless Security

At the same time that the student is learning the principles in IMS 316 he/she is also enrolled in ISAT 335. ISAT 335 focuses on the installation and integration of multiple network operating systems in both a local area network and a wide area network (WAN). Students will be introduced to a variety of networking devices, protocols, and procedures for installing and configuring an operational and useful network. A variety of applications and hardware will be used to simulate telecommunication and network functions found in typical business enterprise systems.

Phase II continues to build upon the knowledge obtained in phase I. This knowledge is expanded to include more advanced topics. IST 360 is the next course in the security area. IST 360 focuses on the topic of security within the context of computer networks and inter-networking and will provide students with a foundation for identifying, analyzing, and solving network-related security problems in a lecture/lab approach. The course covers conceptual and ethical issues as well as practical problem-solving techniques, including security threats and solutions, principles of authentication, security architecture issues, intrusion detection, virus detection, and secure network-management practices. Particular emphasis will be placed on the following criteria:

- Security policy design and management
- Security technologies, products and solutions
- Firewall and secure router design, installation, configuration and maintenance
- AAA implementation using routers and firewalls
- VPN implementation using routers and firewalls

ISAT 415 is the next course in the networking track. ISAT 415 examines interior gateway protocols (IGPs) and exterior gateway protocols (EGP). This course includes both routing and switching concepts, covering both Layer 2 and Layer 3 technologies. Routing principles of both distance vector and link-state routing protocols; intermediate switching; advanced IP addressing techniques; the theory behind routing protocols and route redistribution are also discussed. Hands-on lab exercises allow the learner to acquire the skills necessary to configure and troubleshoot various routing protocols in enterprise networks.

Phase III is the final stage in the redesigned curriculum track. At this point in time the student will have all foundation knowledge needed to explore advanced topics. This phase will begin with a review of the enterprise network. Monitoring concepts will be introduced with the implementation of intrusion detection, network monitoring, and syslog analysis processes, in concert with typical business activities. Business "injects" will generate the necessary traffic to establish a network baseline for reference. Detection concepts will begin with the introduction of various anomalies into the enterprise network. Mitigation concepts will begin by splitting internal and external services, implementing software and hardware firewalls (contrast and compare), as well as other advanced configurations throughout the enterprise. Lastly there will be a firm understanding that security is about mitigation of risk while meeting the business requirements. ISAT 416 is a direct extension of ISAT 415. ISAT 416 examines complex networking concepts, troubleshooting tools and techniques, and sophisticated networking configurations. The course focuses on developing skills necessary to implement scalable networks, build campus networks using multi layer switching technologies, create and deploy a global intranet, and troubleshoot an environment using routers and switches for multi protocol client hosts and services. Particular emphasis will be placed on the following criteria:

- Campus Networks and Design Models
- Deploy a global intranet
- Implementing multiplayer switching
- Documenting and base lining networks
- Troubleshooting methodologies and tools

IMS 392 is a lab only course that allows the students to truly be able to test all of the previously learned knowledge. IMS 392 is an advanced undergraduate research course. The investigator intends to address real-world needs of industry through constructing a variety of labs and case studies that will simulate industry scenarios. This will prepare students to become successful team players through hands-on network assessments, network design, network implementations, security assessments, security design, security implementations as well as ethical decision-making. The student will learn how to deliver projects on schedule, within budget and with highest possible quality. Hands-on experience in this lab will enhance successful results in the areas of preparing Statements of Work, effective communication with multiple levels of staff; the ability to make formal or spontaneous presentations to clients and management; and produces timely Project Status Reports. This course will fit into the new Application Development Lab. This lab has been developed for the purpose of developing, testing and deploying application projects.

The Application Development Lab is an isolated but connected Distributed Computer Security Lab (DCSL). This lab is sponsored by State Farm to support the infrastructure requirements for the hands-on labs. The intent of this lab is to develop and implement scenario driven exercises to improve a student's ability to perform security management within a team in a realistic environment.

6. CONCLUSIONS

Information security curriculum development continues to be challenged to support a dynamically changing workplace. Information security's rise in importance has called for some unique ways to prepare undergraduate students for the workplace. This study identified a need for a re-design of an information security curriculum taking into account current changes in the discipline. Researchers also used this opportunity to review and incorporate relevant teaching methods into requirements for the curriculum change. The researchers focus for curricular change centered on requirements for more "hands-on" experience along with significantly re-

ducing lecture based course content. This resulted in the researchers developing a course curriculum that ultimately supported a first place win against seven other educational institutions in a regional level competition within the Midwest. Limitations of the study included a small number of students, and a single event being used for validation of the proof of concept portion of the study. Future studies should use a larger sample and measure student success after graduation as they assimilate into the workplace.

7. REFERENCES

Bloom B. S. (1956). Taxonomy of Educational objectives, Handbook I: The Cognitive Domain. New York: David McKay Company, Inc.

Boggs, G. R. (1999). "What the Learning Paradigm Means for Faculty", New Directions for Teaching and Learning, 51(5), 3-5.

Bonwell, C., & Eison, J. (1991). "Active Learning: Creating Excitement in the Classroom", ASHE-ERIC Higher Education Report, Washington, DC.

Bonwell, C., & Sutherland. T. (1996). "The active learning continuum: choosing activities to engage students in the classroom", in Sutherland, T.E., Bonwell, C.C. (Eds),New Directions for Teaching and Learning, Jossey-Bass, San Francisco, CA, 67, 3-16.

Bork, A. (2000). "Learning technology", Educause Review,Vol. 35(1), 74-81.

CSI/FBI. 2005 Computer Crime and Security Survey, Retrieved June 29, 2006, from www.gocsi.com/press/20050714.jhtml

Conklin, A. (2006). "Cyber Defense Competition and Information Security Education: An Active Learning Solution for a Capstone Course," in The Proceedings of the 39th Annual Hawaii International Conference on System Sciences.

Dewey, J. (1938/1997). Experience and Education. NY: Touchstone Book, Simon & Schuster, Inc.

Duch, B., Gron, S., & Allen, D. (Eds.). (2001). The power of problem-based learning: A practical "how to" for teaching undergraduate courses in any discipline. London: Stylus Publishing.

Felder, R. M., & Brent, R. (2003). Learning by Doing. Chemical Engineering and Education, 37(4), 282-283.

Information Technology Association of America (2003). ITAA Workforce Survey. Presented at the National IT workforce Convention May 5, 2003. Arlington, VA.

Information Technology Association of America's (2005), Fifteenth Annual Survey of Federal Chief Information Officers February.

Kolb, D. A. (1983). Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs, NJ: Prentice Hall.

Morneau, K. A. (2004). Designing an Information Security Program as a Core Competency of Network Technologist. Proceedings of the 5th conference on Information technology education, (pp. 29-32).

National Security Agencey. National IA Education & Training Program, Retrieved June 28, 2006, from www.nsa.gov/ia/academia/acade00001.cfm

Schön, D. A. (1983). The reflective practitioner. Boston, MA: Basic Books, Inc.

Schön, D. A. (1987). Educating the reflective practitioner. San Francisco, CA: John Wiley & Sons, Inc.

Steel, G., Stojkovic, V., & Zaveri, J. (2004). An Information System Security Course for Undergraduate Information Systems Curiculum. Information Systems Education Journal, 2(3), 3-14.

Spafford, Eugene H. (2001). Cyber Security – How Can We Protect American Computer Networks From Attack, 107th Cong., 1 Sess. (2001) (Testimony of Eugene H. Spafford).

Vygotsky, L. (1934/1986). Thought and language. (A. Kozulin, Trans.). Cambridge, MA: MIT Press.

Vygotsky, L. S. (1978). Mind and society: The development of higher mental processes. Cambridge, MA: Harvard University Press.

Young, J. R. (1998). Skeptical academics see perils in information technology. Chronicle of Higher Education, 29.