Cybersecurity Capstone Case Study: Closing the Loop on Technology Competency Literacy

Lethia Jackson
Department of Technology & Security
Bowie State University
Bowie, MD, USA
ljackson@bowiestate.edu
hteymourlouei@bowiestate.edu

Velma Latson
Department of Technology & Security
Bowie State University
Bowie, MD, USA
vlatson@bowiestate.edu

Haydar Teymourlouei
Department of Technology & Security
Bowie State University
Bowie, MD, USA
hteymourlouei@bowiestate.edu

Abstract – The evolution of the exchange of resources through network computers exploded in the 1990s with introduction of user-friendly web browsing to surf the World Wide Web. As more organizations opted to add their networks to the infrastructure, it became known as cyberspace. Through this network of computers, data breaches to networks have become common occurrences. Innovative instructional environments are needed to ensure a capable workforce to protect resources and data in cyberspace. In 2017 NIST released a draft NISTIR 8193, which defines a framework that provides capability indicators to describe and organize the cybersecurity workforce knowledge, skills, and abilities. Using the NIST framework, the faculty members in the Department of Technology & Security at Bowie State University use various instructional environments across courses in the curriculum for the Computer Technology Program. Case-study research was conducted to examine the outcomes in a cybersecurity capstone course. Used to improve professional skills, capstone courses evaluate final achievement, culminating the work and experience in the program. The findings from the research study support a new pedagogy for teaching cybersecurity content in different instructional environments: a) direct instruction, b) active learning, c) experiential learning, and d) competency-based learning, which combine programming theory, skills-application, and internships. The results of the study support a new literacy landscape, Technology Competency Literacy (TCL) specific for cybersecurity and computer technology professionals.

Keywords: cybersecurity, cybersecurity education, learning environments, capstone course

1 Background

The evolution of the exchange of resources through network computers exploded in the 1990s with introduction of web browsing to surf the World Wide Web. This innovation became known as cyberspace as organizations opted to add their networks to this infrastructure. Through this network of computers, data breaches to networks are common occurrences. A data breach occurs when private and personal information is comprised. The number of data breaches are increasing as technology is becoming an integral part of the workplace. Presently there are laws that require organizations to report data breaches that contain personal and private information (Teymourlouei & Jackson, 2016). Innovative instructional environments are needed to train and teach a capable workforce to protect resources and data in cyberspace. As result, many papers have been published that address the challenges to develop a cybersecurity curriculum at colleges, institutions, and universities.

Bowie State University's (BSU) is designated as a National Center of Academic Excellence in Cyber Defense (CAE-CD) and offers a bachelor’s degree in Computer Technology (CTEC). BSU’s CTEC program has been in existence since 1998 and graduated the first of many network security professionals starting in 2000.
The CTEC program is accredited by the Accreditation Board for Engineering and Technology, Inc. (ABET), which bolsters the high quality and rigor of the department’s program. Given the national shortage of cybersecurity workforce, the CTEC program produces skilled cybersecurity workers with a different approach to cybersecurity education and outreach. The degree is centered on network security which is now one of the significant components of cybersecurity. Students that earn a degree in CTEC have a strong background in programming, network infrastructure, and security. The learning theories embedded in the CTEC program curriculum enhance problem-solving, problem-based learning, critical, analytical and computational thinking as well as computational-based learning. The program is grounded in theory, applied and skill based courses. The required core courses in the CTEC program’s curriculum include:

- Secure Programming in Java
- Data Structures
- Statistics
- Networking
- Calculus or Elements of Calculus
- Discrete Structures
- Building a network from the scratch without any earlier work (Networking)
- Breadth of knowledge in Database Administration and Data Science

After completion of the core courses, students choose one of three course tracks: a) Internet Technology and Multimedia, b) Data Science and Database Administration, or c) Computer Networking and System Network Administration. Beginning fall 2018 semester, the required core courses for CTEC majors will contain five cybersecurity courses, to include a cybersecurity capstone course. Capstone courses are an important aspect of the CTEC program, and are used to evaluate final achievement culminating from previous work and used to improve professional skills (Ward, 2012). For the CTEC program, the capstone course is vital to producing cybersecurity and computer technology professionals. The curriculum for cybersecurity continuously shifts as increased threats and vulnerabilities invade the workplace, households, industries and the way we live and interact with technology. As documented in NIST NISTIR 8193 and the NIST Cybersecurity Framework, standards, guidelines, and practices are needed for organizations to continually assess an organization’s posture to cybersecurity incidents (NIST, 2018). In addition to the CTEC curriculum, students who demonstrate mastery skills (at any academic level) are provided experiential learning opportunities from industry partners through industry-driven tasks, national hackathons, research opportunities, presentations, panel discussions, and internships. The course sequence in the program allows for integration, connection, progression, adherence to prerequisites and application of the theories into practice. The hypothesis is that the Computer Technology Program’s curriculum prepares students for work as a Cybersecurity and Computer Technology professional by offering a diversity of learning approaches.

2 Introduction

The CTEC program’s instructional environments are grounded in the theory of constructivist-learning. Constructivist learning places learners at the center of instruction. The role of the teacher is to create a suitable environment for learners to be engaged, reflective, and able to resolve real-world problems (Jonassen, 1999). The CTEC curriculum is structured to support constructivist learning where students are actively involved in their own learning and construction of knowledge. More specifically, the courses offered by the program emphasize the following learning approaches: experiential learning, active learning, computational-based learning, and direct instruction, which include computational thinking. In this environment students are expected to actively engage and lead the way in their own learning.

2.1 Experiential Learning

The capstone course and real world problems provide experiential learning experiences to students in CTEC. CTEC cybersecurity courses include experiential-based opportunities within the curriculum where students utilize sandbox environment’s to complete hands on active learning. The sandbox environment utilizes a real-world approach and offers a virtualized environment using both software and hardware. A sandbox environment affords students the
opportunity to learn, analyze, synthesize and implement a wide range of technology-based concepts and topics using a “hands-on” approach. Experiential learning environments include classroom-based learning (e.g., capstone courses) and field-based learning (e.g., internships) (Lewis & Williams, 1994). This environment serves as a test bed in which students have the ability to explore and experiment. There are several models for experiential learning environments that share common characteristics including a mixture of content, absence of excessive judgement, engagement in purposeful endeavors, encouraging the big picture perspective, the role of reflection, creating emotional investment, re-examination of values, presence of meaningful relationships, and learning outside of one’s perceived comfort zones (Schwartz, 2012).

2.2 Active Learning

The goal of active learning is to provide practice for mastery of practical problems in the real-world as well as developing the student’s ability to research and implement self-study. The sandbox environment is how the student learns, replicates, verifies and solves the assigned tasks in the Computer Technology Program. It serves as the foundational component for all courses taught in the Computer Technology Program. All CTEC courses make full use of daily experiences in the sandbox environments which allow the students to learn and do. Continual practice and learning in the sandbox environment builds a skill set necessary to work in cybersecurity and other technology-based jobs. Active learning is a key element of the courses taught in the CTEC program. Specifically, at the end of each course, students are expected to be able to install, configure, and manipulate applications and operating systems. As described in experiential learning the sandbox environment is a major attribute of the active learning environment in the CTEC program. Ruder, Stanford, and Gandhi (2018) report active learning environments can introduce skills to students that are in high demand in the workplace. Active learning environments create a learning atmosphere that promotes team collaboration, creative thinking, problem-solving, leadership, and communication skills.

2.3 Competency-Based Learning

Competency-based learning is not assessed through scores from exams or testing (Chavez, 2012), but a “combination of skills and personal attributes (behaviors) gained through experience, practical application and continuous learning” (p. 1). Through the demonstration of established benchmarks at each core course in the CTEC program, students successfully participate in experiential designed learning environments such as the capstone courses and internships. Competency-based learning happens in the program when students are asked to produce a product that involves putting all the pieces that contain the content and practice together to demonstrate a complete understanding of how their knowledge is applied.

2.3.1 Direct Instruction

Direct instruction maximizes the effectiveness and efficiency of instruction, while simultaneously recognizing students’ skill levels for them to receive appropriate instruction (National Institute for Direct Instruction, n.d.). The programming courses in the CTEC program are designed to utilize the direct instruction approach. Students are introduced to this type of instruction during their freshmen and sophomore levels, where the curriculum is delivered in modules with established objectives that give students an opportunity to practice the programming concepts. Each module serves as a building block to the next module (Jackson, Latson & Gross, 2011).

2.3.2 Computational Thinking

Computational thinking is a problem-solving approach focusing on decomposing the problem, recognizing and analyzing repetition of patterns, connecting the student with what they already know to what they are learning. Computational thinkers solve problems, design systems, and understand human behavior by drawing on the concepts, such as problem decomposition, data representation, and modeling pursuing less familiar spaces and abstraction. (Barr, Harrison & Conery, 2011, p. 1). During class in the sandbox, learners design and refine the problem using a step by step approach that also requires thinking strategically and allows for trial and error which produces big thinking. Solving problems related to cyberspace and cybersecurity require this type of
thinking. The CTEC curriculum supports this type of thinking, encouraging students to utilize the iterative process to solve problems.

3 Methodology

A case study approach was used to evaluate the outcomes of CTEC capstone course. Case studies examine real-life events in the context of current environments (Ridder, 2017). Although case studies have non-random participants, they allow the researcher to investigate cases of interest to identify patterns and relationships for creating a theory.

3.1 Description of Capstone Course and Project

The capstone course was offered spring 2018. The course contained 15 senior level students and 1 junior level student. The entire department was involved in the culmination of this course. There were three instructors for this course all of which published cybersecurity-related documents and have taught programming and technology-based courses in the department for over seven years. For the capstone project, students were required to research cybersecurity measurement techniques and to measure the effectiveness of cybersecurity solutions. The project topic was offered by one of the department’s technology industry partners. The industry partner, which will remain unnamed, has been in existence for over 60 years, employs 8,000, and has revenue of one billion dollars. The mission of the project is to provide insight on policies and procedures to the National Institute of Standards and Technology (NIST).

3.2 Participants

The students were tasked to provide a user case that assesses a fictitious organization. The mock organization helps the students to understand the technology and connectivity between the various components of how the organization operates and does business. The students were asked to demonstrate the measurement techniques performed with examples of inputs, analysis, and output results. To guide students, the instructor divided the project into five learning modules that had separate objectives: 1) analyze existing techniques on measuring cybersecurity effectiveness, 2) outline the advantages and disadvantages of each technique, 3) suggest improvements on existing techniques, 4) discuss how the improvements provide additional value, and 5) suggest new methodologies for measuring cybersecurity effectiveness.

3.3 Instructional Modules

3.3.1 Module 1

For the first module, students were required to research cybersecurity measurement techniques. Students used self-study learning videos called Massive Open Online Courses (MOOCs) to reinforce concepts, topics, and knowledge. The topic of the first MOOC covered IT fundamentals, which consisted of learning IP addressing, IPV6, packet delivery, and network routing. A best practice for implementing MOOCs before assigning them to the students is to have the faculty review them first. This technique ensures that the content is relevant for the student’s understanding of technology as it relates to the project’s objectives (Latson, Jackson, Lamar, & Gross, 2015).

The students were divided into two groups to create two fictitious organizations. Each group was tasked to create an overview presentation that describes a fictitious organization. Each presentation had to include the organization’s mission/vision of the company, stakeholders (employees, customers), the cybersecurity problem and solution, the market opportunity for the organization, the product, technologies used, and comparable company’s competition. This helped them to understand how the fictitious organization worked. At the completion of the mock scenario presentations, the class voted to select one of the fictitious organizations to use for the duration of the capstone course. The selected organization included four entities: 1) warehouse, 2) headquarters, 3) transportation, and 4) 3 storefronts. The students worked together to diagram a WAN topology of each to describe how they were interconnected. One of the last steps for this module was to divide the students again into four groups. Each group was assigned to one of the aforementioned entities.
3.3.2 Module 2

For the second learning module, students had to simulate the warehouse, headquarters, transportation and storefronts as working networked components using a computing system with removable hard drives. Each group had to draw a network operation typology diagram as well as research examples of data breaches recently reported in the news as it related to their assigned entity. The students provided diagrams for two kinds of topologies: WAN and the topology specific to each entity. The WAN displayed how all of the entities are connected to each other. The individual topology diagrams for each entity included firewalls, wireless access points, Internet, switches, IDS systems, Proxy servers, software and hardware. Students provided three examples of data breaches. The first example discusses how intruders were able to gain access via an out of date WordPress application. The second example discusses how an intruder was able to gain access through the company’s API. The last example discussed how an intruder was able to gain access through poor learning algorithm. Also, each group was required to install a host operating system (Windows 10) and virtualization software VMWare/Virtualbox) on the assigned hard drive. Guest operating systems were installed (Kali Linux, Windows XP, Windows 7, and Windows Server 2016) to simulate enterprise resources. This module also included MOOCs in which students learned about the internet of things (IoT), security topics, securing the IoT secure architecture, securing the IoT, designing and testing, security of IoT foundations, and standards and ecosystems.

3.3.3 Module 3

For the third module, students had to demonstrate the measurement techniques performed with dummy inputs, analysis, and output results. Gray box testing methodology was used to simulate insider threats. To reinforce their knowledge of ethical hacking, the students were required to review several MOOCs, which included topics such as ethical hacking exploits, perimeter defenses, penetration testing, computer security investigation, and response and Microsoft cybersecurity stack. Students were also required to review the National Institute of Standards and Technology Special publication. The groups were instructed to exploit each other’s computing system using the following processes:

- Reconnaissance - to locate, gather, identify, and record information about the target;
- Scanning and Enumeration - to actively probe a target machine or network for vulnerabilities that can be exploited;
- Gaining Access - to exploit vulnerabilities in order to enter into the system;
- Maintaining Access - by installing backdoors in order to enter into the system in the future; and
- Reporting by documenting risks and recommendations.

3.3.4 Module 4

For the final module, the entire class presented their work for the capstone project including findings and recommendations to seven industry professionals, who were invited to attend the presentation. At the completion of the presentation, the invited industry professionals ask the students the following questions:

1. So, which are the two main tools, would you recommend?
2. For scoping a pen test engagement, would you want to include questions about whether the human testing elements, i.e., social engineering, are in scope?
3. How would you approach testing in your environment if you were the company? Would you use internal people only from a different sub-component of the company, or engage third parties (completely external to the company) to perform the testing?

The aforementioned questions would normally be posed in a professional environment as part of a continued discussion of the presented results. The students were not asked traditional college level questions such as: how were the group dynamics, how were the task divided among the group, how did you select the team lead. In conclusion of the presentation, the students were able to answer all questions without hesitation. Their answers to the questions were considered a contribution to the presentation as well as a significant part of the final product.
As part of the analysis, each invited professional was asked to complete a survey assessing the student’s presentation. In addition, students were also given a reflective survey to assess their preparedness to implement, complete and present a real-world task.

4 Analysis

The analysis of this study is derived from the final project presentation specifically based on the rubric scores from the professionals and the reflective survey completed by the students.

4.1 Industry Professional Rubric

To rate the presentations, the invited professionals were given a scoring rubric (Table 1). The purpose of the rubric was to see if the professional thought that the presentation covered the project’s objectives. The rubric consisted of six questions: Question 1, was the presentation organized? Question 2, did the presentation address whether the students surveyed the advantages and disadvantages of existing techniques on measuring cybersecurity effectiveness? Question 3, did the presentation offer suggestions of improvements on existing techniques and discuss how the improvements provide additional value? Question 4, did the presentation provide suggestions of new methodologies for measuring cybersecurity effectiveness? Question 5, did the presentation discuss a use case that assesses an example organization to show how the measurement techniques perform with example inputs, analysis, and output results? Question 6, did the students respond to the questions asked by the professional with a full understanding of what was presented? Each question presented in the rubric received a rating from 0 to 5, where a score of 1 or 0 was unacceptable, as score of 3 or 2 was satisfactory and a score of 5 or 4 was exemplary. The overall scores as provided by six industry professionals rated the student’s presentation as exemplary for all six standard areas (Table 2). The results of the work performed by the students as well as the rubric scored by the professionals demonstrate that the CTEC curriculum prepares students to perform the work needed as well as answer work related questions for real world tasks.

<table>
<thead>
<tr>
<th>Standards</th>
<th>5 - 4 Exemplary</th>
<th>3 – 2 Satisfactory</th>
<th>1 - 0 Unacceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Has a clear opening statement that catches audience’s interest; maintains focus throughout; summarizes main points.</td>
<td>Has an opening statement that is relevant to the topic and gives outline of speech; is mostly organized.</td>
<td>Has no opening statement; gives the listener no focus or outline of the presentation.</td>
</tr>
<tr>
<td>Survey existing techniques on measuring cybersecurity effectiveness.</td>
<td>The Survey shows a large amount of original thought.</td>
<td>The Survey shows some original ideas and new insight.</td>
<td>The Survey is not original and uses basic information.</td>
</tr>
<tr>
<td>Suggest improvements on existing techniques.</td>
<td>The suggested improvements to the case study are valuable and useful.</td>
<td>The suggested improvements to the case study are valuable and useful to some extent.</td>
<td>The suggested improvements to the case study are not useful and would not work in the real world.</td>
</tr>
<tr>
<td>Suggest new methodologies for measuring cybersecurity effectiveness.</td>
<td>The suggested new methodologies are complete and accurate.</td>
<td>The suggested new methodologies are somewhat complete and accurate.</td>
<td>The suggested new methodologies are do not appear to be complete.</td>
</tr>
<tr>
<td>Provide a use case that assesses an example organization to show how the measurement techniques perform with example inputs, analysis, and output results.</td>
<td>The use case scenario assesses an example organization that demonstrates how the measurement techniques perform with example inputs, analysis, and output results.</td>
<td>The use case scenario assesses an example organization that somewhat demonstrates how the measurement techniques perform with example inputs, analysis, and output results.</td>
<td>The use case scenario assesses an example organization that does not demonstrate how the measurement techniques perform with example inputs, analysis, and output results.</td>
</tr>
<tr>
<td>Response to Questions</td>
<td>Demonstrates full knowledge of the topic; explains and elaborates on all questions.</td>
<td>Shows ease in answering questions; does not elaborate.</td>
<td>Demonstrates little grasp of information; has undeveloped or unclear answers to questions.</td>
</tr>
</tbody>
</table>

Table 1 CTEC 450 Case Study Presentation Scoring Rubric

<table>
<thead>
<tr>
<th></th>
<th>Q #1</th>
<th>Q #2</th>
<th>Q #3</th>
<th>Q #4</th>
<th>Q #5</th>
<th>Q #6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional #1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Professional #2</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Professional #3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Professional #4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Professional #5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Professional #6</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 2 The final rubric ratings by the professionals
4.2 Student Self Reflective Survey

All students participated in completing the self-reflective survey. The survey contained 10 questions. Question 1, are you employed? Question 2, do you have any certifications? Question 3, which of the MOOCs did you find useful? Question 4, did the capstone projects give you insights of what to expect in a real work scenario? Question 5, how comfortable are you using open source tools to perform penetration testing? Question 6, what courses/experiences did you find most helpful in performing this case study? Question 7, which activity or activities did you enjoy the most? Check all that apply. Question 8, which activity or activities did you not enjoy the most? Check all that apply. Question 9, did implementing the Case Study help you? Please check all that apply. Question 10, would you recommend this capstone course to another student?

Questions 1 and 2 gather some background information about the student as it relates to his/her level of work experience and prior professional knowledge. Question 3 specifically targets the MOOCs which is considered on the job training within the capstone course. Questions 4, 5 and 9 respond to the student’s confidence in solving the capstone project. Questions 6 and 7 relate to the core courses offered in the CTEC program. Question 10 asks the students would they recommend this course to others. The majority of the students found the MOOCs mostly useful especially as it related to penetration testing.

The results of the survey show that the majority of the students did not have any professional experience or prior knowledge of work. According to question 8 they least enjoyed working with the MOOCs. All of the students thought that the capstone project did give them insight to a real world experience. The majority of the class can use open source tools for penetration testing. The penetration testing may take a couple of tries, but eventually, I can get into the network.

The results reveal that the learning environments along with the core courses were considered helpful in achieving the results of the project. The students gained confidence in penetration testing, a component of cybersecurity, to detect vulnerabilities and risk. Overall the students thought this experience helped them to prepare for a real world task. They felt successful in creating the mock scenario, understanding and completing the objectives of the project and had a good experience working as a team.

<table>
<thead>
<tr>
<th>Survey Questions</th>
<th>Responses/Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you currently employed?</td>
<td>40%-- were employed, while 60%-- were not employed</td>
</tr>
<tr>
<td>Do you have any certifications?</td>
<td>14%-- held certifications such as Center of Academic excellence, CISSP, GPEN, and Security + While 86% -- did not have any certifications</td>
</tr>
<tr>
<td>Which of the MOOCs did you find useful?</td>
<td>66%-- Fundamentals of IT</td>
</tr>
<tr>
<td></td>
<td>60%-- Security Videos</td>
</tr>
<tr>
<td></td>
<td>66%-- Ethical Hacking</td>
</tr>
<tr>
<td></td>
<td>60%-- Malware</td>
</tr>
<tr>
<td></td>
<td>80%-- Penetration Testing</td>
</tr>
<tr>
<td>Did the capstone project give you insights of what to expect in a real work scenario?</td>
<td>100%-- replied yes</td>
</tr>
<tr>
<td>How comfortable are you using open source tools to perform penetration testing?</td>
<td>.06% --- 1 - I still do not understand and do not know how to use open source tools to perform penetration testing</td>
</tr>
<tr>
<td></td>
<td>13% --- 2 - I can use open source tools to perform penetration testing; I still have problems understanding how to use some of the open source tools to perform penetration testing</td>
</tr>
<tr>
<td></td>
<td>46% --- 3 - I can use open source tools to perform penetration testing, I have to ask my mentor for help or refer to the other resources. The penetration testing may take a couple of tries, but eventually, I can get into the network.</td>
</tr>
<tr>
<td></td>
<td>20% --- 4 - I can open source tools to perform penetration testing. The penetration testing may take a couple of tries, but eventually, I can get into the network.</td>
</tr>
<tr>
<td></td>
<td>13% --- 5 - Very comfortable – I don’t have to refer to my mentor or other references for help</td>
</tr>
<tr>
<td>What courses/experiences did you find most helpful in performing this case study?</td>
<td>53%-- stated courses were helpful</td>
</tr>
<tr>
<td></td>
<td>66%-- stated applied learning and research were helpful</td>
</tr>
<tr>
<td>Which activity or activities did you enjoy the most? Check all that apply</td>
<td>60%-- Building the Mock Profile Scenario</td>
</tr>
<tr>
<td></td>
<td>53%-- Working with the Enterprise Architecture</td>
</tr>
<tr>
<td></td>
<td>26%-- Testing the Methodology</td>
</tr>
<tr>
<td></td>
<td>53%-- Presentation Skills</td>
</tr>
<tr>
<td></td>
<td>66%-- Working as a Team</td>
</tr>
<tr>
<td></td>
<td>40%-- MOOCs</td>
</tr>
<tr>
<td></td>
<td>.06%-- None of the above</td>
</tr>
</tbody>
</table>
5 Conclusion

The cybersecurity capstone case study is based on a constructivist-learning environment. The results of this study give a synopsis of the students’ acquired knowledge and learning. The evidence of this study supports the new conceptual framework, Technology Competency Literacy (TCL) for instructional environments.

The results revealed that the majority of the students learned how to complete the capstone project through course work, MOOCs and applied learning and research experience. Furthermore, through direct instruction enhanced with computational thinking, the majority of the students were able to think outside the box for solutions, learn from each other, and gain confidence in their knowledge of cybersecurity, and use open source tools to perform penetration testing.

The results from the industry professional’s survey competency-based learning assessed through the student responses to the three questions posed by the industry professionals during the Q&A session of the presentation. The industry professional’s overall rating of the presentation was exemplary. The findings give verification that the department should continue to offer a real world capstone experience at the senior level with an additional capstone course offered at the sophomore level to address innovation early in the students’ academic career.

6 References


