Information Security Outcomes and Summative Assessment for ABET-Accredited IS and IT Programs

Jeffrey P. Landry
jlandry@southalabama.edu

Angela M. Clark
amclark@southalabama.edu

Rhonda L. Lucas
rhondalucas@southalabama.edu

Department of Information Systems & Technology
University of South Alabama
Mobile, AL 36688, USA

Abstract

While there is heavy demand for skilled and educated cybersecurity professionals, there are few standards for assessment provided by ABET's computing criteria, except for its cybersecurity degree program criteria. This paper provides an approach for defining and assessing cybersecurity program outcomes for ABET-accredited information systems (IS) and information technology (IT) degree programs. We use the ABET general criteria for IS and IT programs, along with the ABET cybersecurity degree outcomes, to map items covering IT security issues. These items are given as part of a summative assessment exam to students in the capstone course. Results show that students in IS and IT demonstrated a higher and statistically significant level of mastery of the 23 security-related items than on the overall 100-item exam mean.

Keywords: Information Security, Cybersecurity, ABET, Accreditation, Assessment

1. INTRODUCTION

The seriousness of today's cybersecurity threats, such as Ransomware attacks (Ekta & Bansal, 2021) and the demand for cybersecurity professionals stress the need for an educated cybersecurity workforce. A 2020 ISEDJ paper reports that 60% of cybersecurity job ads at Dice.com require a bachelor's degree, and 24% prefer a graduate degree (Marquardson & Elnoshokaty, 2020).

ABET-accredited computing programs, including those in Information Systems, Information Technology, and Computer Science, bear a responsibility for preparing the future cybersecurity professional. Following best practices for accreditation and the scholarship for teaching and learning (Dickson & Treml, 2013), computing programs should approach cybersecurity education by such practices as defining learning outcomes, addressing constituent needs, mapping outcomes to courses, performing assessment, and instituting program improvements on a continuous basis (Saulnier, 2014).

The purpose of this paper is to describe our process for assessing the aspiring cybersecurity professional. Following the Saulnier (2014)

approach, we emphasize the use of learning outcomes, course and assessment item mapping, and summative assessment. The remainder of this paper describes our use of outcomes in information security for our ABET-accredited information systems (IS) and information technology (IT) programs, and then demonstrates how we assessed these outcomes using a summative assessment exam.

2. ABET STUDENT OUTCOMES

We use ABET-specified outcomes as an overarching framework for student learning. We also use these outcomes for mapping questions on our summative assessment exam. ABET defines a set of exit criteria for graduates of computing programs which are called Student Outcomes (ABET Computing Accreditation Commission, 2020). These outcome statements define what graduates in computing programs should be able to know or do by the time of graduation. Five of these outcomes are common to programs in IS, IT, and computer science (CS). They are as follows:

Graduates of the program will have an ability to:

1. *Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.*
2. *Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.*
3. *Communicate effectively in a variety of professional contexts.*
4. *Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.*
5. *Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.*

The ABET outcome statements are broad and not explained further by ABET documentation. We interpret these outcomes in a way that suits the particular aims of our three local computing programs. For our information systems program, we followed a practice started in prior years by giving each ABET outcome a one-word, descriptive label that was easy to remember and captured the essence of each outcome for IS (Landry, Daigle, Longenecker, & Pardue, 2010). We thus labeled these outcomes, in order, as ANALYSIS, DEVELOPMENT, COMMUNICATION, ETHICS, and TEAMWORK. These are not ABET terms but our own. We will use them throughout the rest of the paper as a short-hand for each outcome.

3. OTHER SOURCES OF CYBERSECURITY OUTCOMES

Broadly written, the common ABET student outcomes do not mention cybersecurity specifically, so we therefore sought out other sources of outcomes to guide us. These included two other ABET sources, our own program educational objectives, and a national cyber defense source. ABET lists "principles and practices for secure computing" as one of three topics that computing programs "must include" (ABET Computing Accreditation Commission, 2020, p.4). Our own set of program educational objectives (PEOs—what the program's graduates will be able to achieve 3 to 5 years after graduation—an ABET requirement) for IS makes two references to cybersecurity. It states that "information security" is one of six specialty areas and that "safeguarding information assets" is an important ethical issue for IS graduates.

Our IT program, furthermore, has mapped its curriculum to the National Center for Academic Excellence in Cyber Defense (CAE-CD) standards (https://public.cyber.mil/ncae-c/), and the institution has been designated as a CAE-CD since 2011. Much like ABET, the CAE-CD program criteria defines a set of elements which is comprised of program-level learning outcomes (PLOs) which "serve as a key measure of graduates' success from the program of study and should be assessed by the identified program outcomes assessment indicators" (NSA, 2021).

Finally, we eventually sought out ABET guidance again, this time looking at its cybersecurity program criteria, for which there is a set of eight student outcomes (ABET Computing Accreditation Commission, 2020, p.8). While our IS and IT programs are not subject to the standards for an ABET cybersecurity accreditation, these program outcomes nevertheless might be useful for describing, by comparison, what we do expect of our IS and IT graduates to know about cybersecurity.

Our assessment purposes were closely aligned with our ABET-mandated program of continuous improvement. As such, ABET SLOs and its cybersecurity guidance was paramount. However, one additional cybersecurity education framework (CSEC2017 Joint Task Force, 2017) not considered by this effort may have proven to be useful. The Cybersecurity Curricula 2017 (CSEC2017) guidelines include IS and IT programs, provides for six knowledge areas (Component Essentials, Connection Essentials, System Essentials, Human Essentials,

Organizational Essentials, Societal Essentials), and is very detailed, going down to the level of multiple outcome statements per knowledge area. The outcome statements in particular would be useful for driving course content and question item coverage.

4. MAPPING TO COURSES

The IS and IT programs at our institution share a lot of courses in common and others that have overlap. Those providing coverage of information security related topics include:

Lower division

- introductory courses (separate but similar)
- the programming sequence
- system architecture

Upper division

- data communications and networking
- data management
- information technology in society
- project management

Also in the upper division is an IS course in IS strategy and policy. While relevant to cybersecurity with its emphasis on security policy, IT students take it as an elective course, and so it was not used in our mapping.

Elective courses also covered cybersecurity, but were not included in the mapping either. Two four-course IT focus tracks cover networking and digital forensics, respectively. A focus track of four courses in web development, networking, or digital forensics is required to be taken by IT majors. IS majors may take an IT focus track or mix and match courses. There are also special topics courses offered such as cloud computing infrastructure and penetration testing. Despite the extensive coverage of cybersecurity in all these elective courses, they were not mapped for assessment because not all majors would take them. Thus, our assessment objective was to define what *any* computing (IS/IT) student should know about cybersecurity at the time of graduation, and so only required courses common to IS and IT—shown in the lower and upper division lists above—were used for populating the shared assessment exam.

5. CIS EXIT EXAM

The origin of our cybersecurity assessment items is related to the assessment of graduating seniors from multiple majors within our School of Computing (SoC), formerly the School of Computer and Information Sciences (CIS). The CIS Exit Exam, as we call it, has been used for summative assessment of the five ABET outcomes at our institution. It is an online, 100-item, 75-minute, multiple choice test given to IS and IT majors in their last semester. It is proctored by the instructor of our senior capstone experience and senior seminar course. This exam was based on the Information Systems Exit Exam developed as part of a national effort to assess the readiness of IS graduates (Landry, Reynolds & Longenecker, 2003; Reynolds, Longenecker, Landry & Pardue, 2004).

The original exit exam was validated by a recognized computing certification organization. Passing scores of 50% and 70% were established for professional "Information Systems Analysis (ISA)" certifications at the associate and certified levels, respectively (McKell, Reynolds, Longenecker, Landry & Pardue, 2005). Schools participating in the project could compare student mean scores against grand means at both business and non-business institutions. A spin-off 25-item Database Exam (Landry, Pardue, Daigle & Longenecker, 2013) used at our institution, demonstrated how such an exam could be used to assess ABET outcomes, provide an instructor-independent assessment of learning, enable course assessment, and serve as a placement exam. After the relationship between university faculty and the exam's sponsoring organization ended, the institution retained the rights to use items locally in perpetuity.

The full exam underwent modification over the years, leading up to its current form. The original exam was shortened from its 3-hour, 258-item format to a 92-question, 90-minute length. Obsolete questions, such as those on old JCL language, and items that did not perform well statistically, were dropped. More current items were added.

Most notably, two efforts were made to create a set of security-related items based on our 2014 ABET program assessment. Under the ABET criteria in 2014, we were only partially assessing "the impact of computing on individuals, organizations, and society including ethical, legal, security, and global policy issues." Our exit exam which was used for outcomes mapping and assessment, lacked a sufficient number of security questions. Based on this ABET accreditation review, a set of 12 additional test items were created in 2014 and added to the exam.

In 2018, more items were added to the exit exam. At that time the faculty conducted a periodic review of the PEOs and Student Learning Outcomes (SLOs) and decided to adopt the new ABET SLOs version 2.0 (https://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf). An assessment committee also scheduled a review of the current exam. A committee of instructors from systems architecture, project management, and data communications and networking worked together in 2019 to add, delete, and revise items. They wrote items according to their specialty and reviewed each other's items. The current 100-item exam is the result of that effort.

Some security items are lower-level Bloom taxonomy (Bloom, 1956) questions that assess student recall of basic knowledge of cybersecurity terms. Other questions focus on higher Bloom thinking skills such as the evaluation of a hypothetical situation and applying cybersecurity principles of best practices. An example question from the exam is "An employee of a company has just resigned. Which of the following would be the BEST network security action to take?"

Students must apply their knowledge of best practices to the given scenario of the possible security issues that might occur based on the choices presented. In the above question, the best answer is "disable the user account for a set period of time, then delete", based on recommendations in Chapple, Stewart & Gibson (2018, p. 59).

6. MAPPING TO ABET OUTCOMES

As part of our efforts in documenting the changes to the exit exam, we decided to map our security related questions to the ABET computing outcomes. Of the 100 items on the current CIS Exit Exam, 23 cover information security topics, while also mapping to one of the five common ABET computing outcomes. In this sense, the information security items can be said to be doubly mapped, covering an ABET outcome as well as a cybersecurity outcome. The coverage of security items by ABET outcome area is as follows: ANALYSIS (3), DEVELOPMENT (2), COMMUNICATION (3), ETHICS (15), and TEAMWORK (0). By far the most items are in the area of ETHICS. The ethics theme of IS security is consistent with an applied theme of safeguarding organizational and individual assets. And, it is in alignment with the IT learning outcome of making "informed judgments in computing practice based on legal and ethical principles" and is aligned with our Information Technology and Society course.

7. MAPPING TO ABET CYBERSECURITY

Since the ABET computing outcomes for cybersecurity are written broadly in the Criteria for Accrediting Programs for Information Systems and Information Technology as just discussed, we decided to also perform a mapping of our question set by comparing our written item objectives to the ABET program outcomes for cybersecurity as outlined in the ABET CAC Criteria for Accrediting Computing Programs. Doing so would provide an additional lens with which to view our items. We mapped our 23 items into the set of eight program outcomes defined for cybersecurity programs. The mappings by outcome were as follows:

- Organizational Security (8)
  - Implement technical controls upon employee termination
  - Implement measures to prevent data breach
  - Calculate risk exposure in corporate IT scenario
  - Recognize intellectual property rights in systems development context
  - Choose backup site for disaster recovery, given organization risk
  - Identify security countermeasure for recovery aim
  - Recognize threat to system availability
  - Recognize supply chain security threat
- Human Security (6)
  - Recognize vulnerabilities for identity theft
  - Identify an email message as a spear phishing attack
  - Recognize a suspicious message as a ransomware attack
  - Recognize responsibility to keep information private
  - Identify system access vulnerabilities
  - Assess ethical responsibility to log out an abandoned terminal
- Societal Security (3)
  - Recognize cyber crimes resulting from social media abuse
  - Recognize societal risk of online voting
  - Analyze solutions to the digital divide problem
- Other (6)
  - Recognize need to design UI w/non-volatility for data integrity
  - Recognize that encrypted communication assures confidentiality
  - Implement web-based security countermeasure

- Identify access point collisions in a wireless network
- Recognize use of two-factor authentication
- Recognize means of providing for unique, non-personal id in a database

These mappings made sense to us, because they emphasized areas that were applied and common to IS and IT majors while leaving out areas that were either in electives or not belonging at all. The Organizational Security area is a fit with the applied focus of IS/IT programs, especially the organizational context that is important to IS. The Human Security area represents the individual impacts area of IT security common to IS/IT. Societal Security is important to all computing majors, and our course in IT and Society provides direct coverage. The six Other items focus on technical component security (data/component/systems/software security). This mapping makes sense for IS and IT programs that are very applied, as compared to computer science, computer engineering, and cybersecurity programs which focus more in required courses that cover technical security issues. And given that our technical electives were off-limits for this required-courses only exam, it made sense that so few items mapped to technical areas.

8. RESULTS

The CIS Exit Exam was given during the 2019-20 and 2020-21 academic years with the following results. The assessment items were not ordered consecutively—they were dispersed throughout the 100-item exam. IS majors (n=18) in 20-21 averaged a 75.6% (SD=) and IT majors (n=20) averaged an 80.0% (SD=.1717) on the 23 cybersecurity items. In addition, CS majors (n=34) took the exam in 20-21, averaging an 85.2% (SD=.1311). The grand mean (n=74) was 81.3% (SD=.1499). The InfoSec mean was higher than the overall exam grand mean of 70.1% (SD=.1278) at a statistically significant level (paired t-test, p-value<.0000).

We have currently conducted some rudimentary item analysis, looking at item difficulty. A total of 13 of the 23 items were in the range of 85% or higher correct percentage, making them "easy" items, according to Lord (1952). Another nine items fell in the range of 51 and 84%, or in the "moderate" category, according to Lord's psychometric scale (University of Washington, 2021). The lowest performing item by correct percentage was an item on "recognize supply chain security threat" with a grand mean of 34%. It was the only item whose mean dipped below 50% correctness, making it the only "hard" item.

9. CONCLUSIONS

In conclusion, this study demonstrates that a set of learning outcomes for cybersecurity can be developed and assessed for all IS and IT majors in ABET-accredited programs. We mapped these outcomes into broad program outcomes, both common to computing programs and specific to relevant cybersecurity standards of ABET. The items developed for these outcomes were given to students in a summative assessment, and the students succeeded in scoring at a high pass rate—higher than the overall test mean.

Given the mapping areas, if we were to define an overarching program outcome to describe the set of information security items we chose to assess, it might be something like *awareness and analysis of important information security implications for systems, individuals, organizations, and society*.

A future direction is to map the exam items to the curricula, so as to be more able to direct program improvements towards specific courses. Another future direction is to review items again, adding items for what are deemed the most crucial to-know issues, such as data mining threats, privacy concerns, or data breach best practices. Students currently learn of their aggregate scores, but do not have a chance to see what they missed. An improvement would be to provide a feedback mechanism while not sacrificing test secrecy.

10. REFERENCES

ABET Computing Accreditation Commission (2020). Criteria for Accrediting Computing Programs 2020-2021. Retrieved April 13, 2021 from https://www.abet.org/wp-content/uploads/2021/01/C001-21-22-CAC-Criteria.pdf.

Bloom, B. S. (1956). Taxonomy of Educational Objectives. Vol. 1: Cognitive domain. New York: McKay, 20(24), 1.

Chapple, Stewart & Gibson. (2018) CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th edition, John Wiley & Sons.

CSEC2017 Joint Task Force. (2017). Cybersecurity Curricula 2017 (CSEC2017): Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Retrieved September 29, 2021 from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

Dickson K.L. & Treml M.M. (2013) Using assessment and SoTL to enhance student learning. *New Directions for Teaching & Learning*, 2013(136):7-16.

Ekta & Bansal, U. (2021). A review on ransomware attack. 2021 *2nd International Conference on Secure Cyber Computing and Communications (ICSCCC),* 221-226.

Landry, J. P., Daigle, R. J., Longenecker Jr, H. E., & Pardue, J. H. (2010). IS 2002 and ABET accreditation: meeting the ABET program outcome criteria. *Information Systems Education Journal*, *8*(67), n67.

Landry, J., Pardue, J. H., Daigle, R., & Longenecker, B. (2013). A database management assessment instrument. *Information Systems Education Journal*, *11*(2), 63.

Landry, J., Reynolds, J., & Longenecker, H. (2003). Assessing readiness of IS majors to enter the job market: an IS competency exam based on the model curriculum, *AMCIS 2003 Proceedings*, 403.

Lord, F.M. (1952). The relationship of the reliability of multiple-choice test to the distribution of item difficulties, *Psychometrika*, 18, 181-194.

Marquardson, J., & Elnoshokaty, A. (2020). Skills, certifications, or degrees: what companies demand for entry-level cybersecurity jobs. *Information Systems Education Journal*, *18*(1), 22-28.

McKell, L. J., Reynolds, J. H., Longenecker, H. E., Landry, J. P., & Pardue, J. H. (2005). Information Systems Analyst (ISA): a professional certification based on the IS2002 model curriculum, *Review of Business Information Systems (RBIS)*, 9(3), 19-24.

NSA (2021). – National Centers of Academic Excellence in Cybersecurity CAE 2021: Proposed Designation Requirements and Application Process For CAE-Cyber Defense (CAE-CD). Retrieved September 29, 2021 from https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-proposed_cae-cd_designation_requirements.pdf.

Reynolds, J. H., Longenecker Jr, H. E., Landry, J. P., Pardue, J. H., & Applegate, B. (2004). Information systems national assessment update: The results of a beta test of a new information systems exit exam based on the IS 2002 model curriculum, *Information Systems Education Journal*, 2(24), 1-10.

Saulnier, B. (2014). A paradigm for student learning outcome assessment in information systems education: continuous improvement or chasing rainbows?. *Information Systems Education Journal*, *12*(1), 4.

University of Washington. (2021). Understanding Item Analysis. University of Washington Office of Educational Assessment, Seattle, WA. Retrieved September 27, 2021 from https://www.washington.edu/assessment/scanning-scoring/scoring/reports/item-analysis/.