

In this issue:

- 4. Teaching Cybersecurity Incident Response Using the Backdoors & Breaches Tabletop Exercise Game**
Jacob Young, Bradley University
Sahar Farshadkhah, University of Illinois Springfield
- 18. Going Beyond Considering the Use of Competency-based Education for Designing a Cybersecurity Curriculum**
Fred L. Strickland, University of Maine at Presque Isle
- 29. Preparation for a Cybersecurity Apprenticeship Program (PCAP)**
Jonathan Lancelot, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Grace Smith, University of North Carolina Wilmington
Chris Nichols, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Ron Vetter, University of North Carolina Wilmington
William Wetherill, University of North Carolina Wilmington
- 40. Rubber Duckies in the Wild: Proof of Concept Lab for USB Pen Testing Tool (Teaching Case)**
Anthony Serapiglia, Saint Vincent College
- 44. An IoT Based New Platform for Teaching Web Application Security**
Zhouzhou Li, Southeast Missouri State University
Ethan Chou, Southeast Missouri State University
Charles McAllister, Southeast Missouri State University
- 54. Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C)**
Jeff Greer, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
- 66. Identity Attributes in Teaching Privacy (Teaching Case)**
Yaprak Dalat Ward, Fort Hays State University
Li-Jen Lester, Sam Houston State University

The **Cybersecurity Pedagogy and Practice Journal (CPPJ)** is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (<https://cppj.info>). Our sister publication, the proceedings of the ISCAP Conference (<https://proc.iscap.info>) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal. Currently the target acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2022 ISCAP Board of Directors

Eric Breimer Siena College President	Jeff Cummings Univ of NC Wilmington Vice President	Jeffry Babb West Texas A&M Past President/ Curriculum Chair
Jennifer Breese Penn State University Director	Amy Connolly James Madison University Director	Niki Kunene Eastern CT St Univ Director/Treasurer
RJ Podeschi Millikin University Director	Michael Smith Georgia Institute of Technology Director/Secretary	Tom Janicki Univ of NC Wilmington Director / Meeting Facilitator
Anthony Serapiglia St. Vincent College Director/2022 Conf Chair	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor	

Copyright © 2022 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
St. Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina
Wilmington

Paul Witman
Associate Editor
California Lutheran
University

Thomas Janicki
Publisher
University of North Carolina
Wilmington

Teaching Cybersecurity Incident Response Using the *Backdoors & Breaches* Tabletop Exercise Game

Jacob Young
jayoung@bradley.edu
Bradley University
Peoria, Illinois

Sahar Farshadkhah
sfars2@uis.edu
University of Illinois Springfield
Springfield, Illinois

Abstract

In this paper, we describe an in-class cybersecurity exercise based upon the tabletop incident response game, *Backdoors & Breaches* (B&B), developed by Black Hills Security and Active Countermeasures. Instructors present students with a cybersecurity incident scenario and then task them with selecting appropriate defensive measures and analysis techniques to mitigate the threat. First, we provide background discussion on business continuity, incident response, and tabletop exercises. Second, we explain B&B and provide an example incident scenario. Third, we describe how we utilized the game in an Executive Master of Business Administration program and a junior-level information security course. Fourth, we discuss feedback that we received from students. Fifth, we discuss additional game development that has occurred since we employed B&B in our courses. Sixth, we provide recommendations for others interested in replicating the exercise. Lastly, we outline future research directions.

Keywords: Incident response, Business continuity, Tabletop exercise, Cybersecurity, Pedagogy.

1. INTRODUCTION

In this paper, we describe our implementation of an in-class security exercise based upon the tabletop incident response game, *Backdoors & Breaches*. The game was developed in 2019 by the cybersecurity firm Black Hills Information Security and Active Countermeasures (Black Hills Information Security & Active Countermeasures, 2021). *Backdoors & Breaches* was originally intended to help organizations review and improve incident response procedures, but we felt that it would also translate well to the classroom. Although *Backdoors & Breaches* has been mentioned in two articles (Puchkov et al., 2021; Straub, 2020), none of the extant pedagogical research has focused specifically on employing the game as an in-class exercise. Therefore, we piloted the game to assess how well *Backdoors & Breaches* (B&B) would be received by students.

First, we discuss business continuity and the importance of tabletop exercises in incident response planning. Second, we explain B&B and provide an example incident scenario. Third, we discuss how we used the game in our course. Fourth, we discuss the feedback that we received from students. Fifth, we discuss additional game development that occurred after our study. Sixth, we provide suggestions for instructors to consider when utilizing the game in their courses. Lastly, we outline future research directions involving B&B.

2. BACKGROUND

In this section, we discuss the importance of business continuity planning, the implementation of incident response procedures, and how the use of tabletop exercises can improve organizational preparedness.

Business Continuity

Business leaders and information technology professionals must ensure that their organization can withstand and recover from a wide variety of operational disruptions, such as cyber-attacks, extreme weather events, and global pandemics. When a disaster happens, all organizations want to mitigate its disruptive impact and get back to normal operations as quickly as possible. Developing, testing, and refining organizational processes to prepare for abnormal scenarios improves their business continuity.

Business continuity is the ability of an organization to maintain operations under disaster conditions. Business Continuity Planning (BCP) involves recognizing potential threats and their likely impact to an organization's operations, then developing a collection of procedures for the various business units (Wilson, 2000) that will mitigate the disruption on key functions (Rezaei Soufi et al., 2019).

Incident Response

One aspect to ensuring continuity of operations at a time of crisis, especially when a cybersecurity attack occurs, is incident response. Core activities involved in incident response are detection, containment, eradication, and recovery. It is also important for organizations be agile in addressing emerging threats (Naseer et al., 2021). Any response to potential or ongoing cybersecurity incidents needs to happen in a timely and cost-effective manner (Cichonski et al., 2012).

Although many organizations use prevention-oriented strategies to deal with cybersecurity threats, they are more vulnerable to dynamic and unpredictable attacks. Therefore, organizations need to develop a dynamic response capability to detect cyberattack activity in real-time. This approach provides security managers with actionable insights to stop and prevent/mitigate the damage (Naseer et al., 2021).

We believe that employing tabletop exercises in the classroom helps demonstrate the importance of an agile response to disruptive incidents while also developing essential skills for future information technology professionals.

Tabletop Exercises

Cybersecurity educators are using different methods to fill the cybersecurity skills gap that employers are facing. Angafor, Yevseyeva, & He (2020) suggest using tabletop exercises to nurture and enhance practical hand-on skills. These exercises not only improve problem-solving, communication, and teamwork skills, but

also further enhance understanding of business processes. These skills prepare future professionals to perform more effectively as members of cybersecurity incident response teams.

It is important that tabletop exercises improve both technical and nontechnical skills of students. By playing games and scenario-based exercises, educators can simulate the unpredictable nature of cyber incidents (White et al., 2004). This not only demonstrates the importance of time and teamwork in the decision-making process but also gives students the opportunity to learn from unsuccessful outcomes.

3. BACKDOORS & BREACHES

In this section, we describe the requirements and basic gameplay for *Backdoors & Breaches*.

Requirements

Typically, the game would be played with one participant serving as the Incident Master (IM) and up to seven players acting as Defenders. Complete gameplay instructions are available on the *Backdoors & Breaches* website. Black Hills Information Security has also published a helpful tutorial video on YouTube (Black Hills Information Security, 2019).

Instructors will need at least one set of *Backdoors & Breaches* (Spearfish General Store, 2021). Recently, the core deck was refreshed to reflect current practices and an expansion pack was also just released. The original deck contains 52 cards, organized into six different categories: Initial Compromise (10), Pivot and Escalate (7), Persistence (9), C2 and Exfil (6), Procedure (10), and Inject (10). Version two has one additional Procedure card and one fewer Inject card. The first four categories are attack cards. Procedure cards are played by the Defenders and Inject cards are used by the IM to alter gameplay. We provide example cards in Appendix A.

Gameplay

To begin, the IM draws a single card from each of the attack categories (Initial Compromise, Pivot and Escalate, Persistence, and C2 and Exfil) without revealing them to the defending team. The IM would then craft an incident scenario that incorporates the issues described in the cards. A total of 3,780 incidents can be generated.

All Procedure cards are made available to the Defenders, but four cards are randomly selected to serve as written procedure cards. These cards are given a +3 point modifier. After the Defenders

select a Procedure card, they then roll a 20-sided die, also known as a d20. The randomness provided by rolling a die helps demonstrate the unpredictable nature of incident response. If a physical d20 is not available, there are several d20 simulators available online.

If the result of the die roll, plus any applicable modifiers, is greater than ten, then the IM will announce whether the selected Procedure card defeats one of the attack cards. If the Procedure card is successful, then it may be replayed by the Defenders in a subsequent turn. If the die roll is ten or lower, then the turn fails, and the Procedure card cannot be replayed for the next three turns. When a turn fails due to the die roll, the IM should not reveal to the Defenders whether the chosen Procedure card would have been effective against any of the attack cards. Defenders continue to select various Procedure cards to mitigate the incident. The Defenders win if they manage to reveal all four attack cards within 10 turns.

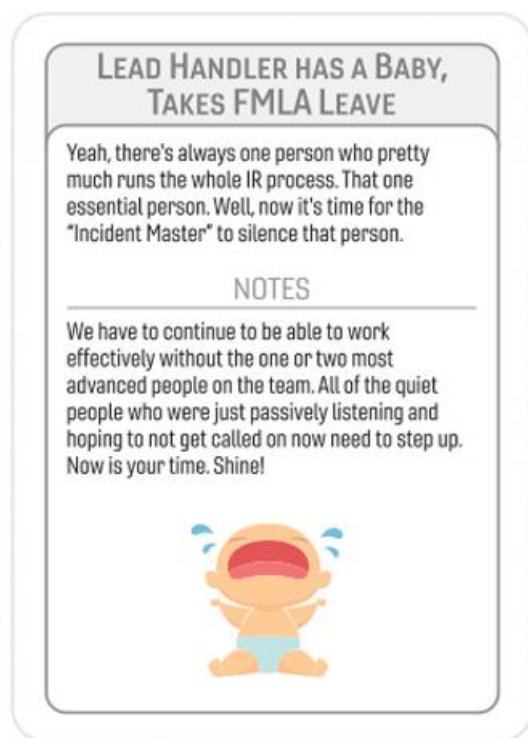


Figure 1: FMLA Inject Card

An optional aspect of the game involves the use of Inject cards. For example, the IM can elect to introduce additional chaos to the incident by selecting an Inject card whenever the Defenders roll a 1, roll a natural 20 (meaning without any modifiers), or roll unsuccessfully 3 times in a row.

Inject cards can impact the incident in a wide variety of ways. Some Injects allow for an attack card to be revealed to the Defenders, others might not impact the game, whereas some could end the game altogether. We provide an example Inject card in Figure 1. Injecting this card would result in silencing the best Defender, as if they were unavailable due to leave protected under the Family and Medical Leave Act.

4. EXAMPLE INCIDENT

In this section, we describe a round of *Backdoors & Breaches*, from dealing Procedure cards, to creating the incident scenario, and playing each turn. We also provide a completed turn tracker worksheet in Appendix B, which can be used to follow along with the gameplay.

Procedure Cards

To begin, the Defenders are dealt all ten Procedure cards, with four randomly selected to serve as written procedure cards. These cards carry a +3 modifier bonus and should be spread out across the top row so that the Defenders can differentiate them from the other six Procedure cards, as shown in Figure 2.

Scenario Creation

The IM then draws a card from each of the attack categories to develop the incident scenario. In this example, we will describe an incident based upon the following attack cards: Bring Your Own (Exploited) Device, Internal Password Spray, New User Added, and Gmail, Tumblr, Salesforce, Twitter as C2. We will reveal each attack card as they are detected by the Defenders throughout our example.

Turn One

To begin play, the IM will vaguely describe the cards to give the Defenders a rough idea of what kind of incident they might be facing. In this example, the IM might say, "Our intrusion detection system just alerted us to rapid login attempts. It appears to have been focused on one of our devices, but now the attempts seem to be targeting several devices across our network." The Defenders would then select a Procedure card that they believe would best address the incident.

Since the Defenders want to keep the intrusion from spreading further, they elect to play the Isolation card, which has the +3 point modifier. The Defenders then roll an eight, which results in a total of 11 points after the modifier has been added. Since the roll is greater than ten, the IM now checks the Detection section of each attack

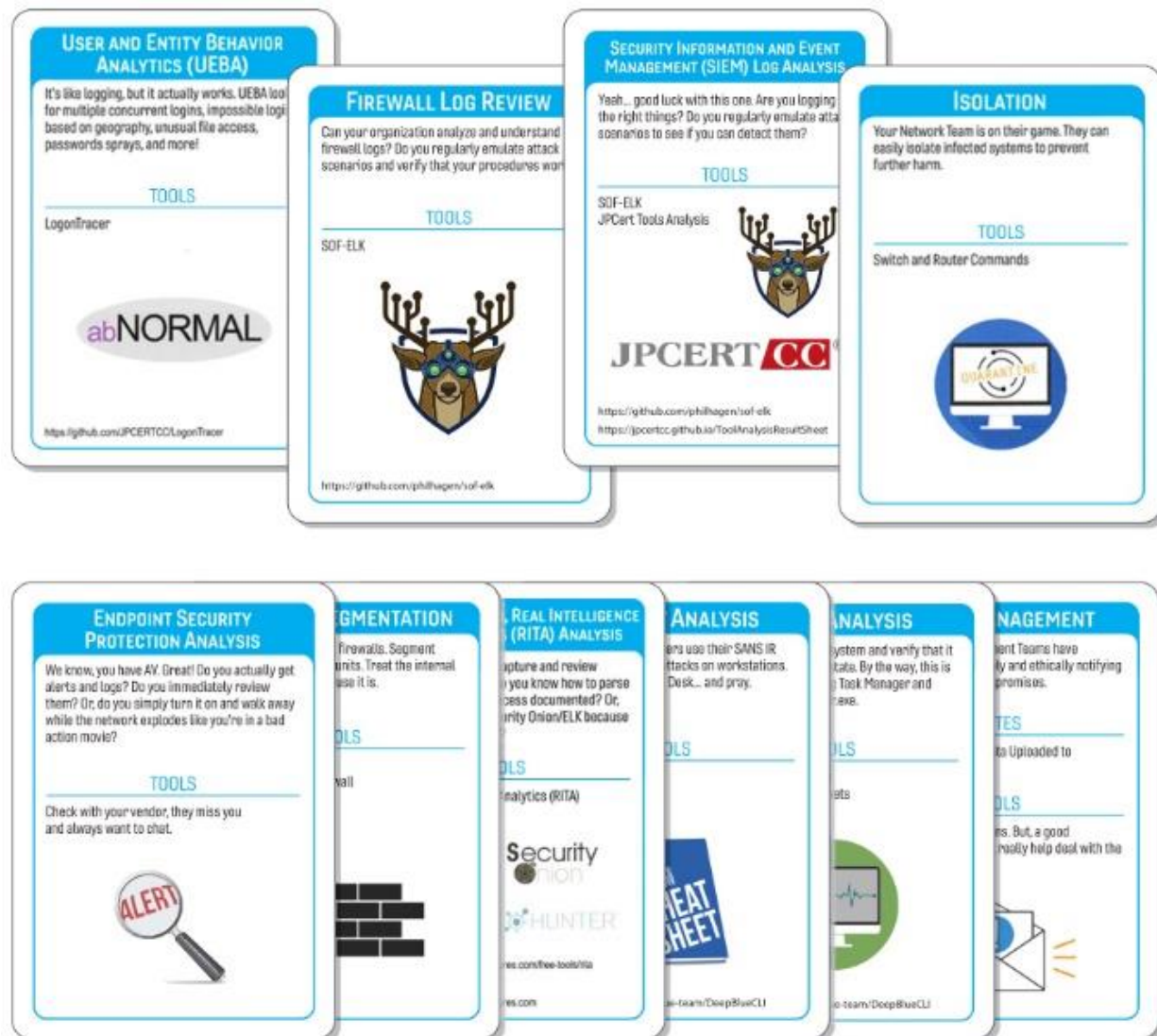


Figure 2: Procedure Cards

card to see if the Isolation procedure defeats any of the attacks. In this case, it does not, so the turn is unsuccessful. The IM can always add some humor by coming up with a reason for why the procedure did not work, such as, "Despite our objections, the CEO doesn't want you to 'waste your time' with isolation since he believes the devices already shouldn't have been able to communicate with one another."

Turn Two

The Defenders respond by selecting the Endpoint Analysis card and roll a 14. Since the roll was greater than ten and the Endpoint Analysis card detects the New User Added attack card, it would be revealed to the Defenders (see Figure 3). The Endpoint Analysis card can also be replayed during another roll. For this turn, the IM could

explain how the Persistence aspect of the incident was defeated by saying, "Your quick decision to analyze each endpoint resulted in the discovery of an unauthorized account on a file server."

Turn Three

For their third turn, the Defenders select the Server Analysis card and roll a 6, which is not large enough to reveal whether the card would have been effective. The IM might describe this outcome by saying, "No one ever established a baseline for this server, so we cannot tell if anything else has been changed." Therefore, the Defenders do not learn anything meaningful from this turn. Note, the Defenders cannot replay the Server Analysis card until at least turn seven.

Turn Four

The Defenders then select the User and Entity Behavior Analytics (UEBA) procedure card for their fourth turn and roll a 16, which results in a total roll value of 19 due to the modifier. The UEBA card successfully detects the Internal Password Spray attack card (see Figure 4). Since this turn was effective, the Defenders can replay the UEBA card during another turn.

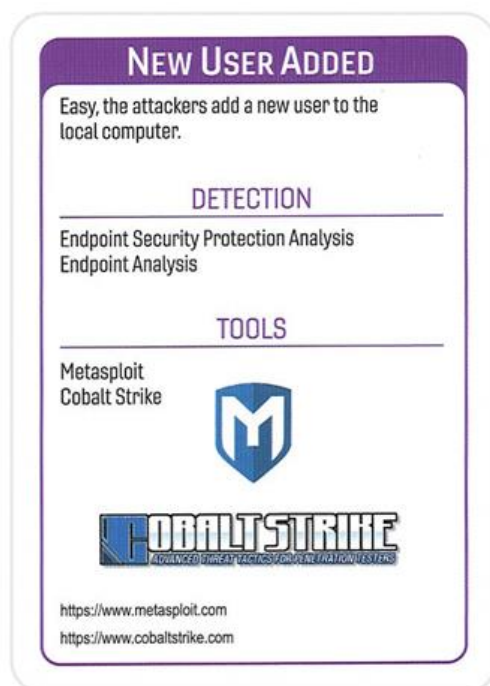


Figure 3: New User Added Attack Card

The IM could describe the outcome of this turn as, "We now know how the attackers gained access to the server. They launched the password spray from one of our workstations in the marketing department. Apparently, an employee was still using a password that was compromised in 2019. Although we are making good progress, we are unsure how the attackers gained access to our internal network."

Turn Five

For their fifth turn, the Defenders elect to play the modified Firewall Log Review card and roll a 4, for a total of 7. Since the procedure is ineffective, the Firewall Log Review card cannot be replayed until turn nine. The IM could describe this result as, "Unfortunately, it looks like our firewall logs were only retaining the last 48 hours of activity. It looks like the unauthorized user was added to the server a week ago, so we're still in the dark."

The IM might consider sharing more information about the Initial Compromise card to help them

select their next card. For example, the IM could say, "After quickly surveying our IT help desk staff, we found out that an employee asked for help connecting their personal device to the corporate network a couple weeks ago."



Figure 4: Internal Password Spray Attack Card



Figure 5: BYOD Attack Card

Turn Six

The Defenders select the NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis card for their sixth turn and roll a 12. Even though this card is effective against both of the remaining attack cards, the IM elects to reveal the BYOD card (Figure 5) to increase the difficulty. The Gmail, Tumblr, Salesforce, Twitter as C2 card (Figure 6) can only be detected by RITA, whereas BYOD can also be detected by the Firewall Log Review card.

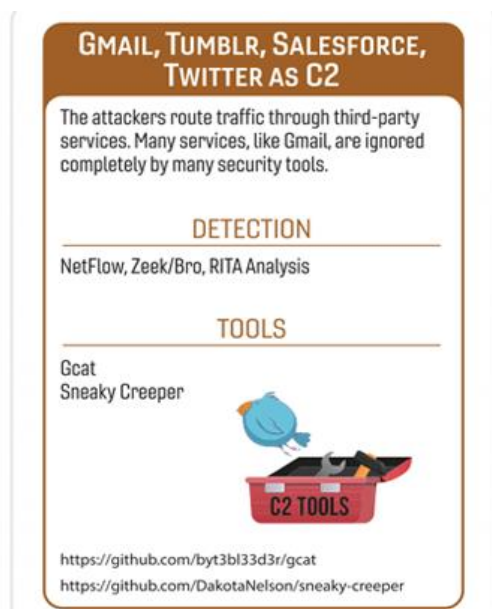


Figure 6: Gmail, Tumblr, Salesforce, Twitter as C2 Attack Card

Turn Seven

For their seventh turn, the Defenders decide to replay the RITA card. However, they only roll a 7 this time, which means it failed to detect the final attack card.

Turns 8, 9, and 10

Although the Defenders would still be able to play the remaining procedure cards, the RITA card is the only one that could detect the C2 & Exfil attack card. Therefore, the Defenders will ultimately lose the game since they were only able to successfully detect three of the four attack cards within ten turns.

5. IMPLEMENTATION

In this section, we describe how we employed *Backdoors & Breaches* into our courses and discuss the feedback we received from our students.

Audience

We piloted this exercise at both the graduate and undergraduate levels in the spring semester of 2021. We employed the game at the conclusion of a two-day module of an Executive Master of Business Administration program and at the end of the semester in two sections of a junior-level information security course. Students in the EMBA module had little to no prior experience with incident response, so the game simply provided a fun introduction to tabletop exercises. The undergraduate students had completed approximately 90% of a course tailored towards earning CompTIA's Security+ certification. Therefore, they managed to apply course content at a higher level as they worked through each incident response scenario.

Preparation

The instructor preselected attack cards to build multiple incident scenarios prior to each class meeting. The instructor also randomly selected four Procedure cards that would have a +3 bonus modifier for each scenario. Since the course was delivered using a hybrid manner (both in-class and remote) due to the COVID-19 pandemic, the Procedure cards were scanned and uploaded to the course learning management system so that students would be able to clearly view the options available during each scenario.

Implementation

In our pilot, the instructor served as the IM and all students played the defender role together. There were eight students in the EMBA module and 16 students in each section of the information security course, resulting in a total of 40 students. After the instructor provided an initial description of the scenario, students were encouraged to discuss the incident amongst themselves prior to agreeing on a Procedure card to play. The first ten-turn round of the game for each section took approximately 25 minutes to play, but subsequent rounds were typically completed in 15-20 minutes. We provide the estimated time to complete each stage of the exercise in Table 1 below.

Stage	Time	Total
Instructions	3 minutes	3:00
Scenario	2 minutes	5:00
Each turn	2 minutes	25:00

Table 1: Time Estimate for a Single Round

6. RESULTS

The exercise proved to be highly effective in introducing and reinforcing cybersecurity topics

to students with limited cybersecurity experience, as well as developing deeper critical thinking skills. Therefore, we believe that this exercise is appropriate for a diverse range of student backgrounds. For example, *Backdoors & Breaches* could also be played in introductory information systems courses to expose students in other majors to cybersecurity issues.

Reception

After completing three rounds of *Backdoors & Breaches*, we asked the 32 students in the undergraduate course to provide their thoughts on the exercise by answering a short survey. We received 21 responses (65.6% response rate). We summarize their feedback in this section, but also provide their responses in Appendix C.

First, we asked students what they enjoyed about the exercise. The most common theme was that they enjoyed how challenging the game was, while also allowing for multiple solutions. Others commented on how comprehensive the incidents were and how well they mimicked real-world scenarios. Several students also recognized how important effective teamwork is to successful incident response.

Second, we asked them to explain how playing *Backdoors & Breaches* helped them relate to the course material. Many students felt that the exercise forced them to think critically and better understand how to apply various security tools

and concepts to respond effectively, which is consistent with the “learn while playing” benefits of gamification. Even though the exercise was a low-stakes card game, several noted that they felt playing *Backdoors & Breaches* replicated the high-stress, time-sensitive, and unpredictable nature of incident response. Others stated that they felt playing the game better prepared them to respond to future incidents.

In our final question, we asked students to share how the exercise helped them realize the value of conducting tabletop exercises. While many further reiterated points made in their responses to the first two questions, several new themes emerged. Many enjoyed how playing *Backdoors & Breaches* provided a nice change of pace when compared to traditional lectures and lab activities. Some felt that participating in a tabletop exercise helped them better connect to the course content, whereas one mentioned that they are considering conducting an exercise at their current workplace.

7. FURTHER GAME DEVELOPMENT

In addition to the release of the expansion pack, further development of *Backdoors & Breaches* has occurred since we conducted our exercise. In this section, we describe an online and competitive version of the game.

Online Version

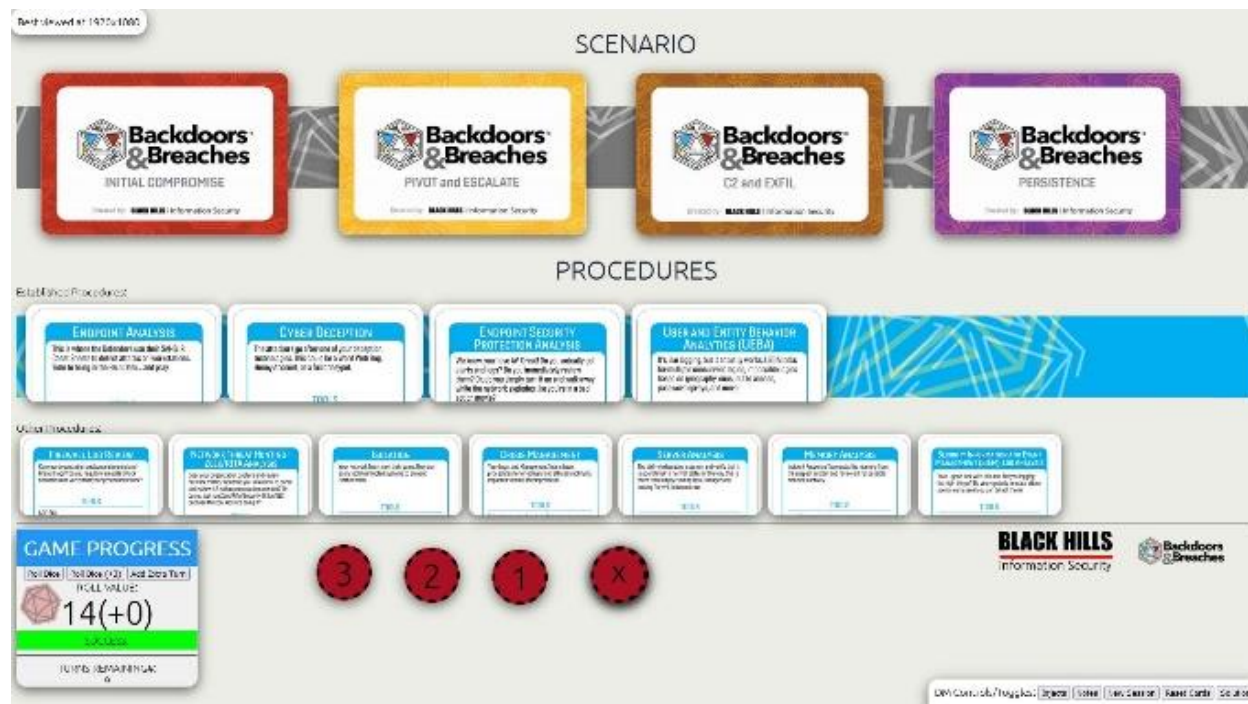


Figure 7: B&B Shuffle (Phung, 2021)

To make *Backdoors & Breaches* more accessible during the COVID-19 pandemic, Richard Phung (2021) published *B&B Shuffle*, an open-source version of *Backdoors & Breaches*. *B&B Shuffle* consists of an optimized interactive dashboard that simulates all the necessary functionality of the traditional game, including the ability to select either the core or expansion decks. Eventually, *B&B Shuffle* was officially released online by Black Hills (<https://play.backdoorsandbreaches.com/>), as shown in Figure 7.

Using *B&B Shuffle* would have greatly simplified our exercise delivery, especially when teaching in a hybrid environment. First, although the cost is minimal, using the online version would not have required purchasing any playing decks. Second, *B&B Shuffle* provides a far more polished way to display the game to students. That said, we recommend that incident masters practice developing scenarios prior to adopting the *B&B Shuffle* approach since the current version does not allow you to manually select attack cards.

Competitive Version

Black Hills Information Security & Active Countermeasures (2021) also developed a two-player, competitive version of the game with modified rules, as shown in Figure 8. Provided that enough playing decks have been purchased, instructors could consider extending our exercise by having students compete against one another.

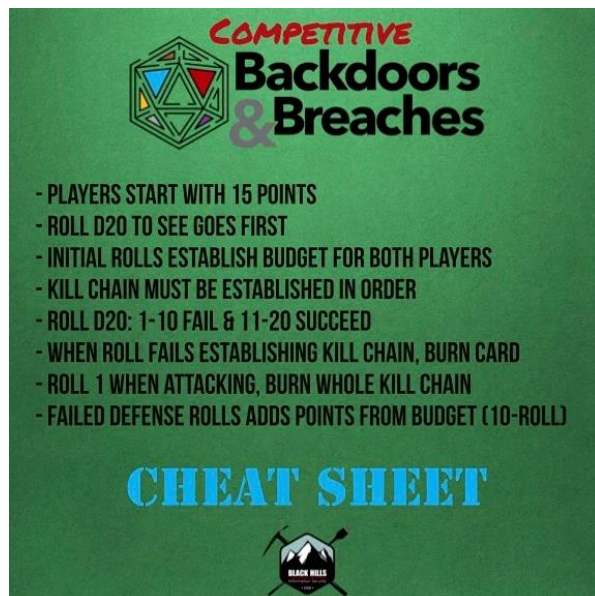


Figure 8: Rules for Competitive Version

Black Hills Information Security & Active Countermeasures (2021) also published a couple high-resolution playmat designs to enhance the

competitive version. We provide an example in Figure 9. Although the playmats can be printed at a vendor of the instructor's choosing, Black Hills recommends ordering them from Inked Gaming (<https://inkedgaming.com>).

8. RECOMMENDATIONS

After piloting *Backdoors & Breaches* in various class settings, we would like to provide several recommendations to help instructors adopt it in their courses. First, we recommend playing at least one complete round with the entire class serving as Defenders to introduce them to the mechanics of the game.



Figure 9: Competitive Playmat

Second, we encourage instructors to be generous in guiding the Defenders through the first couple of rounds. Once the class has demonstrated that they understand how to play, the IM can withhold more information and begin using Inject cards to increase unpredictability.

Third, we also encourage instructors to allow students to facilitate their own games in smaller groups. A single deck allows for up to six games to be played simultaneously, each with a completely different scenario, since there are at least six cards in each attack category. However, a more economical approach would be for students to create scenarios using *B&B Shuffle*, the online version.

9. FUTURE RESEARCH

Our motivation for this research project was to simply assess the mechanics of B&B to ensure that it was suitable for an academic environment. Now that we have determined that B&B can be a valuable addition to existing courses, we intend to further study the game's efficacy through more rigorous methodology. For example, we plan to conduct an experiment that compares student learning under the traditional lecture approach to a method that also integrates B&B. This study would allow for a more quantitative analysis.

10. CONCLUSION

In this paper, we have demonstrated how *Backdoors & Breaches* can be employed to teach students the value of conducting tabletop exercises and to prepare them for incident response scenarios. Given the critical importance of business continuity and the multi-functional representation on incident response teams, we encourage instructors to consider implementing the game in information systems courses at all levels and disciplines, not just those that focus on cybersecurity. Doing so would not only enhance the education experience for students, but also prepare them to participate in incident response activities throughout their careers.






11. ACKNOWLEDGEMENTS

We appreciate Black Hills Information Security and Active Countermeasures for granting us permission to reproduce the playing cards and associated resources for this article. We must also thank them for developing such an enjoyable and effective game.

12. REFERENCES

- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, 3(6), 1–19. 10.1002/spy2.126
- Black Hills Information Security. (2019). *How to Play Backdoors & Breaches, Incident Response Card Game by Black Hills Infosec*. youtube.com/watch?v=TAiJVrOzWMw
- Black Hills Information Security, & Active Countermeasures. (2021). *Backdoors & Breaches*. blackhillsinfosec.com/projects/backdoorsandbreaches/
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, 800(61), 1–147.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, 59, 102334. 10.1016/j.ijinfomgt.2021.102334
- Phung, R. (2021). *B-B-Shuffle*. https://github.com/p3hndrx/B-B-Shuffle
- Puchkov, O., Subach, I., Zhylin, A., & Tsyganok, V. (2021). Criteria for classification of cyber-training and analysis of organizational and technical platforms for their conduct. *CEUR Workshop Proceedings*, 2833, 37–47.
- Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, 57(3), 779–800. 10.1080/00207543.2018.1483586
- Spearfish General Store. (2021). *Backdoors & Breaches, Incident Response Card Game*. spearfish-general-store.myshopify.com/collections/backdoors-breaches-incident-response-card-game
- Straub, J. (2020). Assessment of cybersecurity competition teams as experiential education exercises. *ASEE Annual Conference and Exposition, Conference Proceedings, 2020-June*. 10.18260/1-2--34187
- White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: Testing an organization's ability to prevent, detect, and respond to cyber security events. *Proceedings of the Hawaii International Conference on System Sciences*, 37(C), 2635–2644. 10.1109/hicss.2004.1265411
- Wilson, B. (2000). Business continuity planning: a necessity in the new e-commerce era. *Disaster Recovery Journal*, 13(4), 24–26.

Appendix A – Example Cards

Initial Compromise	Pivot & Escalate	Persistence
<p>BRING YOUR OWN (EXPLOITED) DEVICE</p> <p>Your organization allows users to bring in their own devices. Or, another way to put it, they bring in their own exploited devices. The attackers use these devices to compromise your organization.</p> <p>DETECTION</p> <p>Firewall Log Review NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>The completely asinine belief that somehow allowing people to bring their own devices in is a worthy cost savings.</p> <p>https://www.blackhillsinfosec.com/pentesting-dropbox-on-steroids</p>	<p>INTERNAL PASSWORD SPRAY</p> <p>The attackers start a password spray against the rest of the organization from a compromised system.</p> <p>DETECTION</p> <p>User and Entity Behavior Analytics SIEM Log Analysis</p> <p>TOOLS</p> <p>Domain Password Spray</p>  <p>https://github.com/dathack/DomainPasswordSpray https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack</p>	<p>NEW USER ADDED</p> <p>Easy, the attackers add a new user to the local computer.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Metasploit Cobalt Strike</p>  <p>https://www.metasploit.com https://www.cobaltstrike.com</p>
<p>C2 & Exfil</p> <p>EMAIL, TUMBLR, SALESFORCE, TWITTER AS C2</p> <p>The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Gcat Sneaky Creeper</p>  <p>https://github.com/byt3bl33d3r/gcat https://github.com/DakotaNelson/sneaky-creeper</p>	<p>ENDPOINT SECURITY PROTECTION ANALYSIS</p> <p>We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?</p> <p>TOOLS</p> <p>Check with your vendor; they miss you and always want to chat.</p> 	<p>LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT</p> <p>Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."</p> <p>NOTES</p> <p>They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p> 

Appendix B – Example Exercise Turns



Use this chart to keep track of turns, rolls, and notes.

BHIS encourages your team to revisit what they learn during the game to evaluate what they may need to adjust in their organization.

Perhaps your team will realize they should write down more of their procedures or add completely new procedures.

Turn	Roll	Notes
1	11	Played the Isolation card, but it was ineffective.
2	14	Successfully played the Endpoint Analysis card, revealing the New User Added card.
3	6	Played the Server Analysis card, but the roll was too low.
4	19	Successfully played the UEBA card, which detected the Internal Password Spray card.
5	7	Played the Firewall Log Review card, but the roll was too low.
6	12	Successfully played the RITA card, so the incident master revealed the BOYD card.
7	7	Replayed the RITA card, but failed to defeat the C2 and Exfil card due to a low roll.
8		
9		
10		

Created by: **BLACK HILLS** | Information Security

www.backdoorsandbreaches.com

Appendix C – Student Comments

What did you enjoy about the exercise?
I liked how it made me take everything we know about the situation and cards into account instead of just shooting at whatever I was looking at.
I liked the skill needed and the real-world equivalencies that it introduced. The teamwork and debate were super interesting too.
It was a new and interesting way to see how an attack occurs and how hard it is to prevent the attack once it has occurred.
Fun approach to learning about security concepts.
I liked how it used everything that we have learned thus far in the class. I also liked how it stressed me out a little, it forced me to try and think of what to do on the spot.
The difficulty of the process. Trying to understand the scenario, then think about what it would take to solve it was challenging and forced us to really think about what it would take to get a resolution.
It was a creative way to practice stuff.
That there could be multiple answers to different scenarios.
I liked how it let us try multiple strategies for a given scenario.
It makes you think through every scenario
It was interesting and took the pressure off learning each individual way to know how to solve a problem and instead just throwing stuff to see what works.
It was a nice change of pace from our typical class exercises.
I thought it was enjoyable thinking through what solutions would be most effective and what would be most important.
I enjoyed the "real life" aspect of the dice roll and taking away certain cards because they may not have worked in real life. Also, just figuring out the other options that would work.
I enjoyed being able to practice situations that could happen and figuring out how to solve them.
I liked how it made me think about which incidents would work against what scenarios and it gave me an extensive thought procedure when thinking about these real-world events.
It was definitely a unique exercise; I've never done something like this before in any of my classes. I enjoy the hands-on nature of the stuff we do in this class.
I enjoyed that the exercise encouraged some collaboration and allowed multiple people to share their ideas.
I enjoyed simulating somewhat of an incident response scenario and deciding what the best mode of attack was in real-time.
I really enjoy the interactiveness of this exercise.
Even though I did not know much to begin with, it was interesting to see how many classmates were so knowledgeable on the subject. I enjoyed watching them collaborate.

How did the exercise enhance your understanding of security concepts?
It made me think about what each card said specifically.
I liked how it highlighted the stressfulness and timeliness of such a compromise and how it showed how random different instructions could be.
This helped me understand how there is no clear-cut response to an attack every time and that the responders will need to try a variety of methods to stop an attack.
I read over the cards to try and apply one of them to the given situation. My understanding of the concepts is still not all there but the exercise did help.
It forced me to think about how to use the security tools I have learned about in a real-world setting, and more specifically made me think about what concepts would (and would not) apply to a real-world situation.
At first blush, it kind of scrambled my thinking. By the third exercise, it started to make more sense to me what steps might need to be taken to get to the end of the process. Trying to keep straight how things might fit together for a solution and the importance of the tools you have available is what stood out to me. This also made me realize there is so much more to the security side than you realize.
It gave me an idea of how to deal with specific situations, and how to figure out what to do during a breach.
That a lot of the scenarios can do the same thing, but some are just better to use in certain situations.
It showed me multiple routes to solve a scenario and demonstrated how uncontrollable events could hamper progress.
It helps you think about what tools or practices to use in specific scenarios
It put concepts into practice in a simulated random environment in a fun way.
The game had us think about what each scenario was doing and which tools had a chance to work.
It helped me remember some of the different crisis response methods and network monitoring methods.
Especially when pairing it with the die rolls, it enhanced my security concepts because typically if one method does not work, another one will. Obviously, there are some scenarios where only one method worked.
I learned how to think about and solve security breaches.
It made me think in a procedural way about how we can use our defense mechanisms in order to stop or prevent attackers from escalating their attacks.
Going through realistic scenarios helps me understand the issues better. I'm someone who learns by doing things, rather than just reading out of a book.
I found that the exercise helped me understand some of the use cases and the security techniques we have discussed.
It introduced me to some concepts such as written procedures and pivot and escalate methods.
I enjoyed the exercise making us think about the various skills and how they interact with other skills.
It really showed me just how difficult cybersecurity can be in the real world. It was difficult for us, and everyone was going back and forth. I can only imagine how difficult it is in the real world.

How did completing the exercise help you realize the value in conducting tabletop exercises?

It showed me it is possible to practice without setting up a test environment.

I already knew the value of tabletop exercises, but it is really well put together and I think it's pretty interesting.

Completing this exercise helped show a simplified version of what we have been learning about all year. This helped me grasp the terms and dangers of attacks while giving me a fun game to play with my peers.

It was a nice change from what we have been typically doing all semester, so I guess the variety was some of the value in this exercise.

As we proceeded through the three scenarios, I felt as though I was to better identify which card to use, or at least understand why a card would/wouldn't be used.

It's kind of like the fire drill in school. Hopefully, you never have to do it for real but practicing it might make the actual event work as expected. We did these types of scenarios at my old company before I came here, but that was in the late 90's so some of the threats we have today were not even thought of yet or in their infancy. Doing this today makes me want to do some of this type of stuff just for my own unit on a smaller scale maybe. What to do if you get that phishing email, or you see something that doesn't look right. Being ready for a disaster before it happens can only be a good thing.

This exercise just makes you think more about how it all goes together.

It boosts teamwork and teaches multiple topics at the same time, bettering my understanding of the material.

It can be more engaging than a lecture.

It's basically like practicing for the real thing in terms of concepts rather than execution but still helps.

The real world is unpredictable, sometimes the right tool just doesn't work.

It was interactive, which is often more memorable than lectures.

I feel like completing this exercise gave me a better understanding of incident response and how to act when an incident does arise and what other options there are for it.

Tabletop exercises are effective in building problem-solving skills and getting used to the unpredictability of cybersecurity.

I think it is a great way to become acclimated to the procedures that must be taken when an alert or hint comes in. I think it sets up the general mindset in order to prepare for the unexpected by running through scenarios before the real thing happens, which is very valuable.

Similar to above, actually *doing* things in classes instead of just hypothetical situations and examples reinforces material and helps it stick. Not just for this exercise, but there have been a few times where I've applied the CompTIA labs to my internship, so I thoroughly enjoy the way this class is set up.

Matching up security methods with attacks helped show how some of those methods can be used in a more obvious way than in lectures or labs.

It helped me realize the value as it emphasizes the importance of preparation in any cybersecurity breach. Covering single points of failure, responsibilities, chain of command, and executive leadership are crucial in determining the best course of action in the event of an actual attack.

Tabletop exercises allow for a hands-on application besides the traditional methods of education. I really like these alternative exercises.

Again, it showed me how hard it can be to prevent cyber security crimes.

Going Beyond Considering the Use of Competency-based Education for Designing a Cybersecurity Curriculum

Fred L. Strickland
fred.strickland@maine.edu
College of Arts and Sciences
University of Maine at Presque Isle
Presque Isle Maine 04769, United States

Abstract

The National Security Agency (NSA) uses Knowledge Units (KUs) as a way to cover important topics. An institution would document how its courses mapped to the KUs. If an institution covered certain KUs and met other requirements, then it would be designated as a Center of Academic Excellence (CAE). Reviewers found it hard to determine if an institution was fully covering the KUs. Periodically, the NSA's stakeholders (such as the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the National Institute of Standards and Technology, National Initiative on Cybersecurity Education, the National Science Foundation, the Department of Defense Office of the Chief Information Officer, and US Cyber Command) would review the CAE program. About 2020, they decided that major changes were needed. The 2021 guidance now requires that a KU's learning outcomes and topics to be in one course instead of being in two or more courses. Achieving CAE was changed to being a two-step process. An institution needed to complete the Program of Study step. Then it would need to complete additional requirements before receiving the CAE designation. New applicants and current CAE holders would need to comply with these changes. In 2019, ABET published cybersecurity accreditation criteria. In 2020, the ACM published *Computing Curricula 2020*, which focused on competency-based learning. This paper covers how our university is working to comply with the NSA and with the ABET by using the Competency-Based Education approach.

Keywords: Curricula, Competency-Based Education (CBE), National Centers of Academic Excellence (NCAE), Knowledge Units (KUs)

1. INTRODUCTION

With input from outsiders, the University of Maine at Presque Isle (UMPI) cybersecurity program was created. The first class started in Fall 2019. Right away, we realized that 2 of the 13 computing (COS) courses were not true academic courses and more courses were needed and that changes were needed. We wanted to obtain the National Security Agency's (NSA's) designation as a Center of Academic Excellence in Cybersecurity and to obtain ABET accreditation. Since we had a new program, we were free to make major changes. So we wanted to follow the best educational approach, which appeared to be

competency-based education (CBE). A paper presented at EDSIGCON 2021 (Strickland, 2021) reported on our efforts to determine what courses should be added and to shift from knowledge-based learning to competency-based learning. This journal article will review the high points of that paper and provide additional information.

Credentialing

Subject to state-level approval, any institution could create a cybersecurity program. The program could be housed in the Information Technology unit or in the Computer Science unit or in the Business unit. An institution may seek program credentialing from the NSA's National Centers of Academic Excellence (NCAE) in

Cybersecurity program office. The Computing Accreditation Commission (CAC) of the ABET (2022) looks at programs that have a computing viewpoint.

For these agencies, credentialing means that a program meets certain requirements and covers certain learning outcomes (LOs). ABET looks directly or indirectly at programs globally and has accredited 23 cybersecurity programs. The NSA looks at programs in the United States (US) and its possessions and has approved 357 cybersecurity programs.

Program Building Approaches

Most approaches take LOs as a given. In the previous paper (Strickland, 2021), two major approaches were mentioned. The first explored model is what I called the "Japanese approach" (Kim and Beuran, 2018, October 26-28) and it was used to create a cybersecurity academic program. The second approach is the City University of New York (n.d.) ADDIE (Analysis, Design, Development, Implementation, and Evaluation) instructional design process model for building any type of course.

In a survey of the literature, the previous paper (Strickland, 2021) found that many practitioners took the LOs as a given. In *The Theory and Practice of Online Learning* (Anderson, 2008c), most authors (Ally, 2008; Anderson, 2008b, 2008d; Conrad, 2008; Fahy, 2008; Kanuka, 2008; Kondra, Huber, Michalczyk, & Woudtra, 2008; and Parker, 2008) started with the premise that LOs are a given. Davis, Little, & Stewart (2008) did note that LOs needed to be "based upon a good understanding of an institution's or company's core business and values." The authors deviated when they wrote about the need to address the "student market and the needs of the curriculum." The authors did not consider using input from credentialing authorities nor from hiring companies.

Hutchison, Tin, and Cao (2008) pointed out that there is a need to evaluate LOs. Anderson (2008a) was on the same track when he noted that there is a need to assess LOs. However, no details were provided to explain what is needed to be done for evaluating or for assessing the LOs.

Caplan and Graham (2008) wrote about the ideal course development team. The subject matter expert is to "ensure that the content of the online course is an appropriate alternative to the lecture content normally given in a traditional course." The instructional designer needed to write

"statements of learning outcomes." But the authors did not mention the source for these LOs.

Parker (2008) came closer to the matter of defining LOs when she wrote:

Another tension emanates from the fact that the bulk of what is delivered in the online environment consists of discrete training modules directed to particular job skills or competencies. While there seems to be slippage between what is articulated in the realm of learning outcomes (the skills we expect graduates to demonstrate) and our expectations around the values associated with the liberal arts, it is fair to say that higher education aims should be broader than the goals of the corporate training sector.

Parker did not answer the question about the sources of those LOs.

What is presented in conferences, in workshops, and in other venues is similar to the presentation at the 3rd Annual Texas A&M Assessment Conference where Osters and Tiu (n.d.) stated that "a measurable learning outcome" is about

- Student learning behaviors
- Appropriate assessment methods
- Specific student performance criteria / criteria for success

All these sources failed to address the topic of using standards or authorities for creating course LOs. Instead, they implied or stated that the instructor is the one responsible for defining the knowledge and the skills that students should be mastering in a course. In practice, the instructor may follow what a textbook contains. And textbooks may be organized around the author's own LO list or around a defined "Body of Knowledge" area or around something else.

A noteworthy exception is Clark, Stoker, and Vetter (2019). They wrote about their experience

for seeking the CAE in Cyber Defense Education (CAE-CDE) designation in 2018. They wrote about the CAE-CDE changes from 2017 to 2018 and the required additional work. They addressed LOs. Their paper was insightful, but the numerous changes made to the CAE-CDE process has rendered some of their insights as obsolete.

2. COMPETENCY BASED EDUCATION (CBE)

In the previous paper (Strickland, 2021), the second section provided background information on CBE. Information was provided from the Competency-Based Education Network website (n.d.) about how this helped “students [to] acquire and [to] demonstrate their knowledge and skills by engaging in learning exercises, activities[,] and experiences that align with clearly defined programmatic outcomes.” And Levine and Patrick (2019) wrote that CBE is driven to “transform [the] educational system so all students can and will learn through full engagement and support and through authentic, rigorous learning experiences inside and outside the classroom.”

The rest of the second section went into greater detail on the philosophy and provided information on how different agencies are implementing CBE. Retained for this paper is the information about UMPI, an abridged presentation on the NCAE program, and the credentialing agencies.

UMPI Embracing CBE

UMPI has fully embraced CBE for its on-line degrees (YourPace) and has the Center for Teaching and Learning (CTL) for helping instructors to design courses to use CBE.

YourPace takes advantage of a person’s previous knowledge and experiences. Courses are organized as modules called “Learning Outcomes.” The person demonstrates mastery of the module’s content. Then moves to the next module. Hence, the name of “YourPace.”

The CTL has many resources such as instructional designers, a professional development lending library, workshops, and so on. The Curriculum Coordinator works with instructors for crafting their courses along CBE lines.

The National Security Agency’s (NSA) National Centers of Academic Excellence (NCAE) Program

There are three designations:

- CAE in Cyber Defense Education (CAE-CDE)
- CAE in Research (CAE-R)

- CAE in Cyber Operations (CAE-CO)

Information on all these can be found at <https://www.nsa.gov/resources/student-educators/centers-academic-excellence/>

The major component is the knowledge unit (KU) requirement. A KU has LOs and required topics. There are 3 foundational KUs that all programs must have. There are 5 core KUs. The remaining KUs are based on what is the mission of the program. Table 1 summarizes the NSA’s (2020) KU requirements.

Academic Level	Foundational KUs	Objective Driven KUs	Program Choice KUs
Associates	Required 3	5 Technical core OR 5 Non-technical core	3
Bachelors			14
Masters	Required 3 or evidence from another program		7 plus a thesis
Doctoral			3 plus a dissertation

Table 1: Knowledge Unit Requirements

The most recent change is dated January 2022 (Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG), 2022). This codified all the draft changes into a final authoritative document. New applicants and renewing programs must comply with these requirements.

The two largest changes are that an academic course needs to contain all of an individual KU’s LOs and required topics and that achieving the CAE is a two-step process. The first step is the Program of Study (PoS) and the second step is the CAE-CDE Designation.

For the PoS step, an institution must show its curriculum path and must show that students are enrolled and are successfully completing the curriculum path. And the students must be receiving some type of recognition for the effort. In short, the PoS addressed the curriculum, the student related information, the faculty profiles and their qualifications, and the continuous improvement efforts.

The course listing must be designed to support the Program-Level LOs. The courses listed for the PoS step must be all required courses. Elective courses are not considered. The PoS must be published on the institution’s website.

For the NSA to validate a PoS, the program must have been in existence for at least three years and at least one class (minimum of three

students) has completed or graduated from the program. No changes may be made during this period. If any changes are made, then the “clock” is reset.

The reviewers would be asking for information on the following items:

- How the program aligns with the National Initiative for Cybersecurity Education (NICE) Framework
- Syllabi for all courses with a KU alignment.
- Identify courses with applied labs and the instructions for those labs.
- Program-Level LOs
- Mapping of the Program-Level LOs to courses.
- Documentation for the assessment indicators for each Program-Level LOs.
- How the KUs align to the PoS.
- Identify which courses support which KU.
- Listing of course LOs for each KU aligned course.
- The academic year when each KU aligned course was last offered.
- Enrollment figures for the last three years.
- At least three redacted student transcripts from within the past three years.
- Documentation that recognizes the students’ completion of the program.
- Samples of students’ work.
- Documentation of students’ participation in extracurricular activities.
- Faculty information
- Proof of continuous improvement

Program-Level LOs must be identified and on the program’s web page. The self-study must document the KUs and the alignment of the KUs to the relevant courses. The new approach means that it is better to fully align a KU to a course than to spread pieces of a KU across two or more courses.

An institution could have several PoS offerings. If a PoS has been reviewed and validated by the NSA, then that fact could be used as a marketing point.

The institution must have a validated PoS before working on the CAE-CD Designation step. The institution needs to have the following items:

- Evidence of an institutional cybersecurity posture and plan. Someone designed as the official for overseeing implementation of a plan for protecting the institution’s critical information and systems.
- The established of a physical or virtual cybersecurity center.

- The institution must affirm their commitment to the CAE-C Core Values and Guiding Principles.
- Proof that the program will continue.
- Professional development opportunities.
- Other degree programs must include some cybersecurity elements.
- Outreach beyond the home institution’s campus.
- Transfer of credit agreements.

For the CAE-C Post-Designation Reporting Requirements, an institution must submit an annual report, must continue to improve, must continue to meet the CAE-CD Designation requirements, and must attend various meetings. Due to space limitations and the scope of this paper, those details will not be covered here.

The Association for Computing Machinery (ACM) and IEEE Computer Society (IEEE-CS) Support of CBE.

While the NSA “will rely upon the institutional accreditation [from a regional agency] for sufficiency of program construction and maintenance” (Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG), 2022), there are other agencies that look at the rigor of the actual academic program.

The ACM has published documents pertaining to curricula recommendations. These have tended to be knowledge-based. Recently the ACM and the IEEECS with input from others published *Computing Curricula 2020* (2020). This report is a major shift from knowledge-based learning to competency-based learning. The change was necessitated as the knowledge-based learning paradigm had not been sufficient to prepare ready-to-work graduates. Too many universities produce computing graduates that are intellectually smart, but have difficulties functioning in a workplace setting.

The report stated that knowledge is only one part of a competency. “... the idea of competency as the foundational idea on which to base academic program design permits a stronger alignment between the product of an education and the needs of professional practice in the workplace.”

The report provided a framework for creating competencies [Competency = [Knowledge + Skills + Dispositions] in Task].

- Knowledge: The factual understanding of computing concepts. This is the “know-what” dimension.

- **Skills:** The capability of applying knowledge to complete a task. This is the “know-how” dimension.
- **Dispositions:** The socio-emotional skills, behaviors, and attitudes that address the desire to carry out tasks and the sensitivity to know when and how to engage in those tasks. This is the “know-why” dimension.
- **Task:** The “construct that frames the skilled application of knowledge and makes dispositions concrete.”

Using a competency model for defining a computing curriculum produces benefits for the many constituencies. A list of competencies can come from many stakeholders. (For example, UMPI is an institution that serves small businesses and agricultural interests. There is an advisory board that communicates the needs of the major constituencies.)

A competency statement describes an area. Then it has a list of required competencies with the needed knowledge and skills. The disposition is presented in the context of activities such as presenting to a group, producing useful procedures, or monitoring activities in a work unit.

3. CAE IN NEW ENGLAND AND IN MAINE

See the previous document (Strickland, 2021) for this information.

4. CHANGING UMPI’S CYBERSECURITY PROGRAM

As noted in the introduction, the UMPI cybersecurity program needed to be revised. The NSA’s CAE-CD requirements were not being fully addressed. The current program could prepare graduates to serve in any arena, but the graduates could not claim that they had graduated from an NSA approved program.

If UMPI wanted the CAE-CD designation, then the program would need to be changed in order to comply with the current CAE-CD requirements. The planned changes would make it distinctive by being a technical offering that would enable a person to wear additional “hats” (a technology manager, an IT worker, database manager, and a software programmer). This would support many of the UMPI’s constituencies that are composed of small businesses, small government agencies, and similar entities. As UMPI is located

in an agricultural area, the person would learn about supply chain security first-hand.

The UMPI distinctiveness would be based on having:

- A CBE approach.
- A solid program that would obtain the PoS the first time out.
- And obtain the CAE-CD soon thereafter.
- Program accreditation. A typical person may not understand the value of a program being a holder of the PoS or of the CAE-CD, but he or she would understand accreditation.
 - Of the 22 accredited cybersecurity programs in the US, the closest ones to Maine are located in Maryland.
- A think-outside-of-the-box approach by offering something to schoolteachers.

5. UMPI AND THE NSA’S KUs

The NSA requires bachelor’s programs to have at least 22 KUs as defined in Table 1. UMPI would comply by having the following KUs covered by these UMPI courses:

- 3 Cybersecurity Foundational KUs
 - **ISC** IT Systems Components in UMPI COS 210 IT System Components
 - **CSF** Cybersecurity Foundations in UMPI COS 2ddCybersecurity Foundations and Principles
 - **CSP** Cybersecurity Principles in UMPI COS 2dd Cybersecurity Foundations and Principles
- 5 Technical Core KUs
 - **BSP** Basic Scripting and Programming in UMPI COS 110 Programming Fundamentals
 - **BNW** Basic Networking in UMPI COS 240 Network Concepts
 - **BCY** Basic Cryptography in UMPI COS 2ad Basic Cryptography
 - **OSC** Operating Systems Concepts in UMPI COS 310 Operating Systems
 - **NDF** Network Defense in UMPI COS 440 Network Security Administration and Defenses
- 14 Program Choice KUs
 - **DST** Data Structures in UMPI COS 120 Introduction to Data Structures
 - **ALG** Algorithms in UMPI COS 230 Algorithm Theory and Development
 - **DVF** Device Forensics in UMPI COS 232 Device and Digital Forensics
 - **DFS** Digital Forensics in UMPI COS 232 Device and Digital Forensics

- **FAC** Forensic Accounting in UMPI BUS/COS 2bb Forensic Accounting
- **SCS** Supply Chain Security in UMPI COS 2ii Supply Chain Security
- **CPM** Cybersecurity Planning and Management in UMPI COS 2ae Cybersecurity Planning and Management
- **IDS** Intrusion Detection/Prevention Systems in UMPI COS 340 Intrusion Detection and Prevention Systems
- **DMS** Database Management Systems in UMPI COS 350 Databases and Database Management Systems
- **DAT** Databases in UMPI COS 350 Databases and Database Management Systems
- **CCR** Cyber Crime in UMPI COS 410 Cyber Crime and Cyber Threats
- **CTH** Cyber Threats in UMPI COS 410 Cyber Crime and Cyber Threats
- **PLE** Policy, Legal, Ethics, and Compliance in UMPI COS 485 Cybersecurity Policy, Legal, Ethics, and Compliance
- **FPM** Fraud Prevention and Management in UMPI COS 4ee Fraud Prevention and Management

Since UMPI's niche is small businesses and small government entities, our graduates would need additional skills. Many of the Choice KUs would enable a graduate to be a knowledgeable business staffer, to be an IT person, to be a database manager, and to be a programmer.

6. UMPI AND PROGRAM ACCREDITATION

UMPI has both computer science and cybersecurity programs. The CAC of the ABET considers accreditation based on the program's name. If the name contains the phrase "computer science," then it must satisfy the computer science program requirements. If the name contains the word "cybersecurity," then it must satisfy the cybersecurity program requirements. Both program requirements have the same five program LOs. Both have a requirement for discrete mathematics. (This paper will not explore the UMPI computer science programs.)

Cybersecurity programs must have at least 45 semester credit hours of computing or cybersecurity courses and 6 semester credit hours of mathematics (discrete mathematics and statistics). Cybersecurity programs do not have a lab-based science requirement. In addition, the criteria for accrediting computing programs are updated every cycle.

The CAC of the ABET uses the curriculum guidance as provided by certain agencies.

The ACM and the IEEE CS formed the Joint Task Force on Computing Curricula. The final document was published in 2013 as *Computer Science Curricula 2013* (The Joint Task Force on Computing Curricula, 2013).

A few years later, these two entities along with participation from the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) formed the Joint Task Force on Cybersecurity Education. The final document was published in 2017 as *Cybersecurity Curricula 2017* (Joint Task Force on Cybersecurity Education, 2017).

To obtain program accreditation, the UMPI cybersecurity program must draw from these resources.

7. DISCUSSION: UMPI AND THE CBE APPROACH FOR DESIGNING THE CYBERSECURITY PROGRAM

We looked at the LOs from the NSA, from the CAC of the ABET, from the ACM curriculum guidance documents, and from other entities. Once a list was created for a course, then the course would be structured to address each LO.

To track the LOs, these are numbered with the course code and a sequence number as in "COS 110) 1." In the narrative, the source document is cited. This was done so that upon a course review, the reviewer could check to see if the source document has changed. The following shows a sample of LOs for UMPI COS 110 Programming Fundamentals course from four sources:

- COS 110) 1. Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks). [BSP 1]
- COS 110) 5. Analyze and explain the behavior of simple programs involving the fundamental programming constructs variables, expressions, assignments, I/O, control constructs, functions, parameter passing, and recursion. [Assessment] [SDF/FPC 1]
- COS 110) 14. Trace the execution of a variety of code segments and write summaries of their computations. [Assessment] [SDF/DM 1]

- COS 110) 17. Model the way programs store and manipulate data by using numbers or other symbols to represent information. [1A-AP-09]

Since we are pulling from several authorities for LOs, a particular concept may appear in two or more sources. We would assign the same course LO code to these. We would retain the duplicates in order to show that we are addressing the LOs from all authorities.

With a firm LO list, then we would find resources that would support each course LO. We have used resources from research papers, from conference papers, from Open Education Resources materials and from high quality websites.

Each class session or module would start with a listing of the LOs to be covered. The students know what would be covered. The instructors know what needs to be covered. Any adjunct or substitute instructor would know what needed to be taught. One or more assignments would be given with the purpose of reinforcing the LOs. The final assessment could be an academic exam or a project.

In many disciplines, there is a progression from familiarity to expert and this is done over several courses. Since a program designer needs to select 14 out of the 60 KUs available, the NSA has designed the KUs to be independent and the knowledge to understand a concept is included. This approach has been used in many of the UMPI COS courses.

8. DISCUSSION: THE NEXT STEP

The previous paper (Strickland, 2021) provided information on what we wished to do and what we needed to do.

Since the NSA and the CAC of the ABET are still using knowledge-based LOs, these will be recorded. The UMS Academic Program Planning and Assessment Policy (APPA) process uses the word "competencies." From the context, it appears this could be a synonym for LOs.

As course syllabus documents are created, the appropriate subset of the LOs will be listed. A new section will be added that will document the associated skills and dispositions. The calendar contains the assignments, and this will be revised to document the supporting tasks.

The next step is to take the knowledge-based LOs and render into an official University of Maine

System approved package. The steps for doing this are documented in *Academic Program Planning and Assessment Policy Manual* (University of Maine at Presque Isle, 2021 October 26).

The APPA guidance stated that proficiency areas are to be documented in a spreadsheet. The reviewers will be able to see how the program competencies align with the corresponding program courses, program proficiencies, and competency priority levels.

In order to capture the tracking requirements of the various agencies, the following columns are used:

- The program competencies. One column for each one.
- Degree Program (CYB, COS, or Both).
- Course Learning Outcome code (i.g., COS 110) 1).
- Competencies (Free text narrative.)
- OPR (Office of Primary Responsibility: ACM, NSA, CSTA).
- Source Document
- Reference Code (How to find the actual text in the source document.)
- Competency Priority Level (See codes below).
- Competency Levels (Cognitive) (See codes below.)
- Competency Levels (Physical) (See codes below.)
- Bloom Taxonomy or ACM Word
- A column for each course. (Use the cognitive competency letter codes from below.)

The competency priority levels will be documented. The codes are:

- 0 = immaterial for all
- 1 = immaterial for most
- 2 = material for some
- 3 = material for most
- 4 = material for all
- 5 = critical for some
- 6 = critical for most
- 7 = critical for all

Cognitive competency (letters) and physical competency (digits) are documented. The codes are:

- A = Awareness/Define
- B = Situational Identification
- C = Universal Application

- D = Compare, Contrast appropriate alternatives, synthesize
- E = Create, innovate, Invent
- H = Historical Context/Origins
- 1 = Perform with Guidance
- 2 = Perform partly without guidance
- 3 = Perform and problem solve
- 4 = Perform with innovation

The last column before the actual course details contains the Bloom Taxonomy.

Table 2 is an extract. This is for a networking concept course. The extract shows some of the NSA's Basic Networking KU LOs, the ACM's cybersecurity LOs, and the ACM's computer science LOs.

A state education department may not require such a detailed document. The NSA does require a document that maps the program-level LOs to each course in the program. Table 3 is an extract for the BS in Cybersecurity. An institution has some freedom in designing the lay-out of the information.

The APPA package will include additional documents such as course sequencing, individual course documentation, and program documentation.

9. CONCLUSION

Taking a CBE approach for designing a degree program and each course in that program is labor intensive. It requires reviewing and reworking the weak areas. This is necessary if an institution wishes to teach the important concepts and avoid assigning busy work tasks.

We are still creating new courses and it may take teaching and revising a course a few times, before we get it exactly the way it should be. When this is done, then a student would have the option of testing out of a module or out of an entire course.

For years, the ACM and the IEEE have emphasized knowledge-based learning. Now they are shifting to competency-based learning (ACM & IEEE, 2020). The two organizations plan to revise all of the curriculum documents to reflect a CBE approach. In the meantime, a website (<https://www.cc2020.net/>) will be launched that will have resources such as work-in-progress CBE courses. (At this writing, the website has not been launched.)

This will be an on-going process. It may take time to get all of the pieces working.

Established programs may discover that their NSA designation will be revoked. Reviewing our efforts may help them to fix their programs. New programs may be able to avoid numerous missteps by reviewing our efforts.

10. ACKNOWLEDGEMENTS

I wish to acknowledge the insights provided by Jason Johnston, the CTL, fellow professors, and CSTA Maine. This paper was influenced by attendees to the session where I presented the first paper and by the journal reviewers.

11. REFERENCES

- ABET. (2015). ABET Constitution. <https://www.abet.org/wp-content/uploads/2020/02/Ratified-ABET-Constitution-2015-Public.pdf>
- ABET. (2022). "Criteria for Accrediting Computing Programs, 2022 – 2023." <https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2022-2023/>
- ACM & IEEE. (2020). *Computing Curricula 2020: Paradigms for Global Computing Education*. <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf>
- Ally, M. (2008). Foundations of educational theory for online learning. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 15-44). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Anderson, T. (2008a). Social software to support distance education learners. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 221-241). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Anderson, T. (2008b). Teaching in an online learning context. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 343-365). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Anderson, T. (Ed.). (2008c). *The Theory and Practice of Online Learning* (2nd ed.). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

- anuales_u/99z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Anderson, T. (2008d). Towards a theory of online learning. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 45-74). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG). (2022) *National Centers of Academic Excellence in Cybersecurity CAE 2022 Designation Requirements and Application Process For CAE-Cyber Defense (CAE-CD)*. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-proposed-cae-cd_designation_requirements.pdf
- Caplan, D. & Graham, R. (2008). The development online courses. In T. Anderson (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 245-263). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- City University of New York. (n.d.). "Course Design & Development Tutorial." <https://spscoursedesign.commonscs.cuny.edu/introduction-to-design-and-development/>
- Clark, U., Stoker, G., & Vetter, R. (2019). Looking ahead to CAE-CD program changes. In *2019 Proceedings of the EDSIG Conference*. Information Systems and Academic Professionals. <http://proc.iscap.info/2019/pdf/4920.pdf>
- Competency-Based Education Network. (n.d.). "What is competency-Based Education?" <https://www.cbenetwork.org/competency-based-education/>
- Computer Science Teachers Association. (2017). *CSTA K-12 Computer Science Standards, Revised 2017*. <http://www.csteachers.org/standards>
- Computer Science Teachers Association. (2020). *Standards for Computer Science Teachers*. <https://csteachers.org/page/standards-for-cs-teachers>
- Conrad, D. (2008). Situating prior learning assessment and recognition (PLAR) in an online learning environment. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 75-90). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Davis, A., Little P., & Stewart, B. (2008). Developing an infrastructure for online learning. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 121-142). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Fahy, P. (2008). Characteristics of interactive online learning media. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 167-199). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Hutchison, M., Tin, T., & Cao Y. (2008). "In-your-pocket" and "on-the-fly:" Meeting the needs of today's new generation of online learners with mobile learning technology. In T. Anderson (Ed.), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 201-219). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- The Joint Task Force on Computing Curricula. (2013, December 20). *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf
- Joint Task Force on Cybersecurity Education. (2017, December 31). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>
- Kanuka, H. (2008). Understanding e-learning technologies-in-practice through philosophies-n-practice. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 91-118). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Kim, E., & Beuran R. (2018, October 26-28). On designing a cybersecurity education program for higher education [Paper presentation]. 2018 10th International Conference on Education Technology and Computers, Tokyo,

- Japan.
https://www.jaist.ac.jp/~razvan/publications/designing_cybersecurity_program.pdf
- Kondra, A. Z., Huber, C., Michalczyk, K., & Woudtra, A. (2008). Call centres in distance education. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 367-395). AU Press.
https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Levine E., & Patrick S. (2019). *What is competency-based education? An updated definition*. Vienna, VA: Aurora Institute
- National Security Agency. (2020). *2020 Knowledge Units*.
https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf
- Osters, S., & Tiu, F. S. (n.d.). Writing Measurable Learning Outcomes."
<https://www.gavilan.edu/research/spd/Writing-Measurable-Learning-Outcomes.pdf>
- Parker, N. (2008). The quality dilemma in online education revisited. In T. Anderson, T (Ed), *The Theory and Practice of Online Learning* (2nd ed.). (pp. 305-340). AU Press.
https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf
- Strickland, F. (2021). Using competency-based education to design a cybersecurity curriculum. In EDSIGCON Proceedings 2021.
<https://proc.iscap.info/2021/pdf/5532.pdf>
- University of Maine at Presque Isle. (2021, October 26). *Academic Program Planning & Assessment Policy Manual*.

Appendix

	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	CYB3 and COS	CYB4 and COS4	CYB5 and COS5	CYB6 and COS6		Degree Program	CLO Code	Competencies (Learning Outcomes)	OPR	Source Document	Reference Code	Competency Priority Level	Competency Levels (Cognitive)	Competency Levels (Physical)	Bloom Taxonomy or ACM Word
1															
2															
3															
4															
5															
6				C		BOTH	COS 240) 4	4. Use a network monitoring tools to observe the flow of packets (e.g., WireShark).	NSA	BNW	BNW4	4 A		1	3
7				C		BOTH	COS 240) 5	5. Perform network mapping (enumeration and identification of network components) (e.g., Nmap).	NSA	BNW	BNW5	4 A		1	1
8				C		BOTH	COS 240) 6	6. Describe common network vulnerabilities.	NSA	BNW	BNW6	4 A		1	1
9				C		BOTH	COS 240) 7	4.4e. Describe the components and interfaces of a networking standard provided.	ACM	CSEC2017	CSEC2017-4.4e	4 A		1	1
10				C		BOTH	COS 240) 8	4.4q. Describe an attack on a specified node in a TCP/IP network given the description of a vulnerability.	ACM	CSEC2017	CSEC2017-4.4q	4 A		1	1
11				C		BOTH	COS 240) 9	4.4r. Explain why transmission attacks can often be viewed as connection attacks on network components (physical or software).	ACM	CSEC2017	CSEC2017-4.4r	4 A		1	2
12				C		BOTH	COS 240) 10	AR/IC 4. Compare common network organizations, such as ethernet/bus, ring, switched vs. routed.	ACM	CSC2013	CSC2013-AR/IC-4	4 A		1	Familiarity
13				C		BOTH	COS 240) 11	NC/I 1. Articulate the organization of the Internet.	ACM	CSC2013	CSC2013-NC/I-1	4 A		1	Familiarity
14				C		BOTH	COS 240) 12	NC/I 2. List and define the appropriate network terminology.	ACM	CSC2013	CSC2013-NC/I-2	4 A		1	Familiarity
15				C		BOTH	COS 240) 13	NC/I 3. Describe the layered structure of a typical networked architecture.	ACM	CSC2013	CSC2013-NC/I-3	4 A		1	Familiarity
16				C		BOTH	COS 240) 14	NC/I 4. Identify the different types of complexity in a network (edges, core,	ACM	CSC2013	CSC2013-NC/I-4	4 A		1	Familiarity

Table 2: Extract from the "Program Inventory"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Program-Level Learning Outcomes Curriculum Map and Plan																	
2	Program Name: BS in Cybersecurity																	
3	Updated: 2021.12.31																	
4																		
5	Program Level Learning Outcomes:																	
6	CYB 1	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.	COS/BUS 2bb	COS/BUS 2a	COS 101	COS 110	COS 120	COS 200	COS 205	COS 210	COS 220	COS 230	COS 232	COS 235	COS 240	COS 250	COS 255	COS 2
7	CYB 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.	0	0	0	C	0	#N/A	#N/A	C	#N/A	C	0	#N/A	0	#N/A	#N/A	#N/A
8	CYB 3	Communicate effectively in a variety of professional contexts.	C	0	0	C	C	#N/A	#N/A	0	#N/A	C	0	#N/A	C	#N/A	#N/A	#N/A
9	CYB 4	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	C	0	0	0	0	#N/A	#N/A	0	#N/A		0	#N/A	0	#N/A	#N/A	#N/A
10	CYB 5	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	0	0	0	0	0	#N/A	#N/A	0	#N/A		0	#N/A	0	#N/A	#N/A	#N/A
11	CYB 6	Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]	C	C	0	0	0	#N/A	#N/A	C	#N/A	C		#N/A	C	#N/A	#N/A	#N/A
12	CS 6	Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]	0	0	A	C	C	#N/A	#N/A	0	#N/A	C	0	#N/A	C	#N/A	#N/A	#N/A
13	CYB 7	Solve mathematical problems with discrete mathematics and statistics and apply these in a computing environment.						#N/A	#N/A	0	#N/A	C	0	#N/A	C	#N/A	#N/A	#N/A
14			-19	-20	-21	-22	-23	-24	-25	-26	-27	-28	-29	-30	-31	-32	-33	
15	Legend																	
16	Awareness/Define																	
17	Situational Identification																	
18	Universal Application																	
19	Compare, Contrast Appropriate Alternatives, Synthesize																	
20	Create, Innovate, Invent																	
21	Historical Context/Origins																	

Table 3: Extract from the "Curriculum Map and Plan" – BS in Cybersecurity

Preparation for a Cybersecurity Apprenticeship Program (PCAP)

Jonathan Lancelot
lancelotj@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Grace Smith
gls4018@uncw.edu

Chris Nichols
cmn9093@uncw.edu

Ulku Clark
clarku@uncw.edu

Ron Vetter
vetterr@uncw.edu

William Wetherill
wetherillw@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

Despite the coronavirus disease 2019 (COVID-19) job market disruption, demand for cybersecurity professionals remains high, with 460,000+ online job listings for U.S. cybersecurity-related positions posted from April 2020 through March 2021 (Cybersecurity Supply/Demand Heat Map, 2021). A key effort to generate the talent needed to fill the current shortage involves cybersecurity apprenticeships. While apprenticeships can be win-win-win for employers, students, and schools, there are challenges in getting to that state. Ensuring students have foundational knowledge makes the process easier for employers and leads to more successful apprenticeship programs. This article considers key employer concerns about apprenticeships and describes how a preparation program can satisfy many of them.

Keywords: Cybersecurity, Apprenticeship, Pre-apprenticeship, Certifications, OJT, RIT, RTI

1. INTRODUCTION

Cybersecurity is a demanding field that requires new methods of organization building and skills acquisition. All organizations face the challenge of continuously defending computer networks from attack while periodically dealing with cyber-skilled staff shortages and budget limitations. The International Information System Security Certification Consortium ((ISC)²) reports that the global cybersecurity workforce gap stands at ~3.1 million ((ISC)², 2020), which is a reduction from the gap reported in 2019 but nonetheless still sizeable. According to Cyber Seek, the national cybersecurity workforce shortage (as of April 2022) is close to 600,000 (www.cyberseek.org). As has been noted in many places for several years now, the field of cybersecurity needs actionable and concrete ways to manage the skills gap. A Forbes article from a few years ago captured the prevailing sentiment well:

Security work is either not getting done or is being done by people who lack the background or aptitude. [...] Security teams are either understaffed or under-skilled and are falling further behind while our adversaries are getting more automated, more mature and more sophisticated in their search for high-value soft targets. (Lloyd, 2017, para. 2)

While organizations are struggling to find needed cybersecurity talent, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reports (FBI, 2021) that cybercrime continues to rise with internet crime complaints up year-over-year nearly 70% in 2020 to a new high of 791,790 (Figure 1).

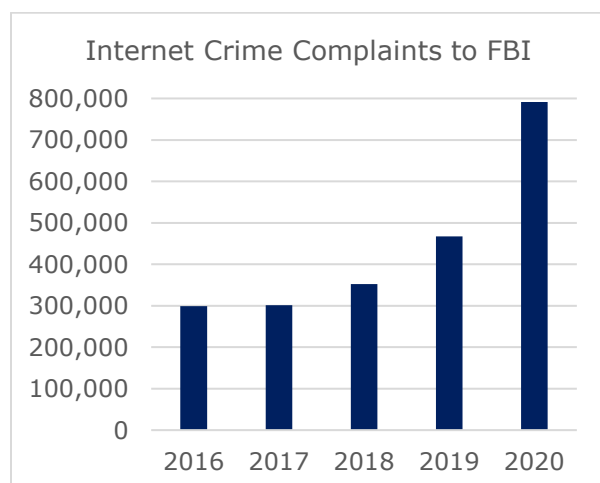


Figure 1: By year, 2016-2020, number of internet crime complaints to the FBI's IC3

An old chicken-egg problem faced by many new entrants to the job market is the issue of experience. Organizations prefer employees with previous work experience, while new job market entrants need work in order to gain experience (Champlain College Online, 2021).

The latest ISACA (formerly Information Systems Audit and Control Association) State of Cybersecurity report (2021) based on survey results from 3,659 cybersecurity professional respondents indicates that 55% of organizations have unfilled cybersecurity positions, that only 28% of hiring managers believe half or more cybersecurity job applicants are well-qualified, and that prior hands-on cybersecurity experience is, by far, the most important factor in determining if a cybersecurity candidate is qualified. Figure 2 displays results for the question: "How important is each of the following factors in determining if a cybersecurity candidate is qualified?". This finding seems to align with the observation that nearly 88% of cybersecurity job postings require at least 3 years of experience (Burning Glass Technologies, 2019).

Given the requirements for building and maintaining a competent cybersecurity apparatus, many organizations struggle to determine how to find the best talent available in the market, while on the other side of the job search continuum, candidates are typically confused by a somewhat hazy recruiting process and are unclear about the knowledge, skills, and abilities (KSAs) needed to fill an entry-level position. One method of bridging the skills gap is via apprenticeship programs.

Apprenticeships have the potential to provide a win-win-win arrangement for employers, students, and schools (Stoker et al., 2021). However, getting to the point where all three win and feel like they are winning can be a challenge. Apprenticeship sponsors often have concerns that include program cost, apprentice commitment, apprentice qualifications, etc. In this paper, we discuss how many of the problems perceived by employers can be mitigated with programs that support student obtainment of industry certifications, and we provide some practical suggestions for sustaining such programs.

2. APPRENTICESHIP REVIEW

Overview and Current Apprenticeship Data

The apprenticeship model of hands-on learning supervised by an expert has existed throughout human history and across all cultures (Douglas, 1921). Ancient sources like Hammurabi's Code

(rules 188 & 189) circa 1750 BC (King, 2008) make this clear with records of laws and norms governing the obligations of the apprentice and the mentor.

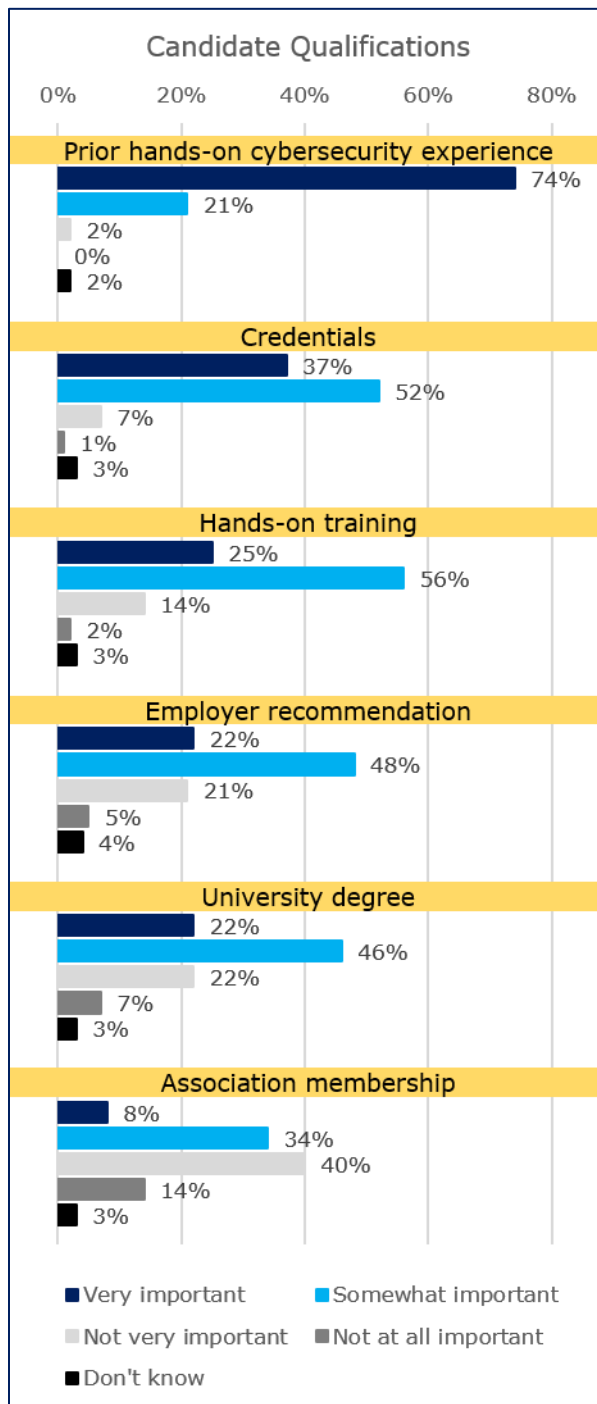


Figure 2: Results for: "How important is each of the following factors in determining if a cybersecurity candidate is qualified?" (ISACA, 2021)

For centuries, apprenticeships have provided a way to train people for crafts and trades but should also be understood as a complex social and economic system. Apprenticeships have always involved the exchange of training for labor. Skilled masters host apprentices in the workplace for an agreed period of time. (Frenette, 2015, p. 352)

In classic *everything old is new again* (Allen, 1974) fashion, there has been a sharp turn towards the tried-and-true ancient institution of apprenticeship beyond the trades and into leading-edge industries like cybersecurity (McCarthy, 2021). Compelled, in part, by the existing skills gap and the U.S. Bureau of Labor and Statistics (BLS) projected cybersecurity-related job growth of 31% through 2029 (BLS, 2021b), the U.S. Department of Labor (DoL) has been advocating the creation of new registered apprenticeship programs in areas outside of traditional craft and trade fields.

Using DoL-provided data (DoL, 2021b), Figure 3 shows via gray bars and the left-hand y-axis that active participation across all DoL-registered programs has been on the rise over the past five years, including during the heavily COVID-19-affected year of 2020. In addition to the increasing numbers of individual participants, there have been thousands of new apprenticeship programs registered each year during that same time frame as indicated by the dark line with markers and the right-hand y-axis.

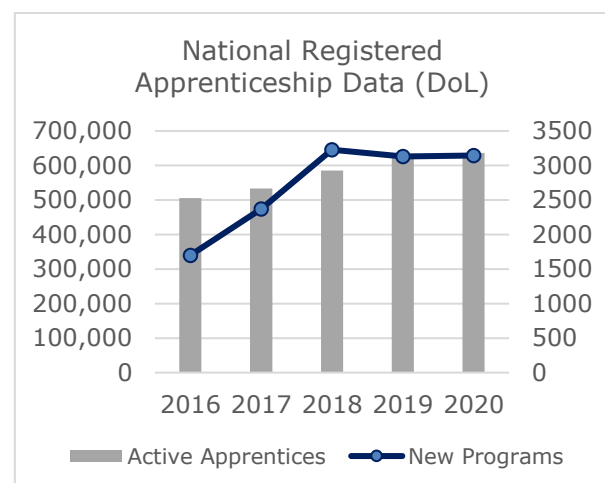


Figure 3: Dual-y-axis chart for years 2016-2020 showing number of active apprentices across all DoL registered programs (left axis) and number of new registered programs (right axis)

Among the DoL industry classifications are "Information" and "Professional, Scientific, and Technical Services" (PSTS), which are the ones most likely to be capturing programs related to cybersecurity. While currently both constitute quite a small number of apprentices compared to other industries (e.g., construction is 68% of all apprentices), both are experiencing above-average growth in recent years (Figure 4).

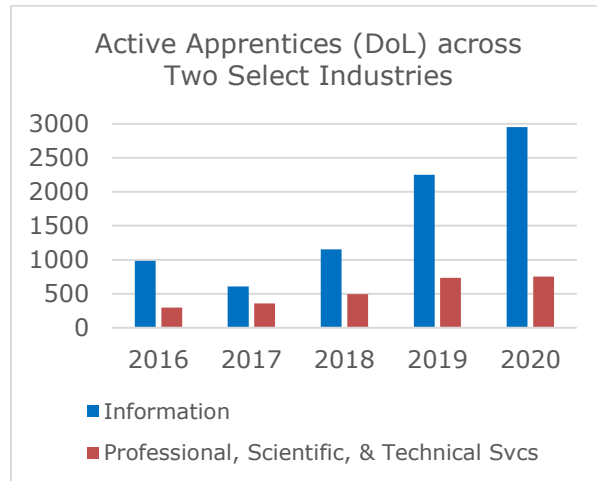


Figure 4: 2016-2020 yearly data for number of active apprentices in the information industry and the PSTS industry

Normalizing the active apprentice numbers to 2016 data, we see more clearly that the growth rate for Information and PSTS apprentices is markedly more robust than all programs generally (Figure 5).

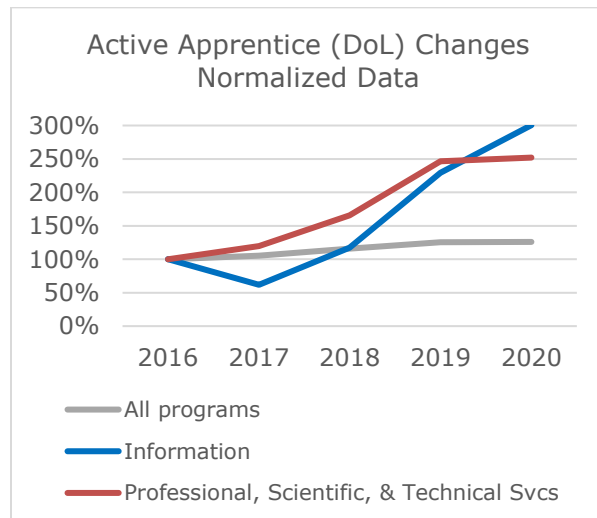


Figure 5: Percent change of active apprentices compared to 2016 base year across all industries, information industry, and PSTS industry.

While these growth rates are encouraging, the overall number of Information and PSTS apprenticeship programs still appears smaller than warranted given the volume of unfilled cybersecurity positions.

There were just 2,716 registered apprentices, 0.43% of the more than 630,000 overall, in cybersecurity occupations during 2020 (DoL, 2021a), while total cybersecurity job openings (464,420) plus the total employed cybersecurity workforce (956,314) (Cybersecurity Heat Map, 2021) represents 0.88% of the total labor force (161,086,000) (BLS, 2021a).

Employer Challenges

In spite of the growing enthusiasm for apprenticeship programs, many businesses remain hesitant or feel unable to start such programs. The reasons for this vary a bit from company to company, but we will focus on a group of reasons which seem likely to impact cybersecurity apprenticeship programs and explain how and why we believe they can potentially be mitigated.

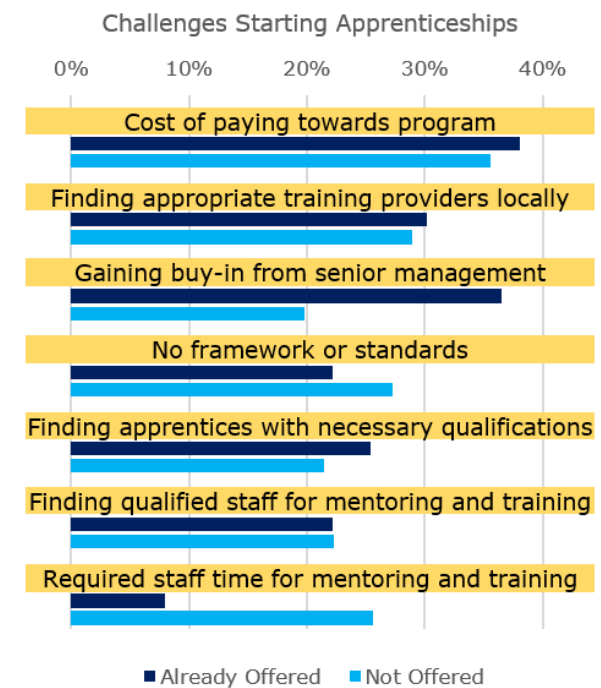


Figure 6: Top responses to the question: "What do you think the challenges are of introducing or embedding Higher Apprenticeships in your company?" (Mieschbuehler et al., 2015)

Investigating the challenges related to creating apprenticeships, Mieschbuehler et al. (2015)

surveyed organizations from across the 9 regions of England – 63 that currently had apprenticeship programs and 121 that did not. While actual results in other areas of the world would presumably differ, we make the simplifying assumption that the differences would not be significant.

In Figure 6, we show a portion of the results in response to the question: “*What do you think the challenges are of introducing or embedding Higher Apprenticeships in your company?*” (Higher is equivalent to undergraduate in this context.) We are showing the top half of responses as determined by adding the percentage of respondents from both groups.

Another survey of 947 sponsors of registered apprenticeship programs based in the U.S. done in 2007 presented a fixed list of potential drawbacks and requested that respondents indicate if each was a significant problem, a minor problem, or not a problem (Lerman et al., 2009). These results are presented in Figure 7.

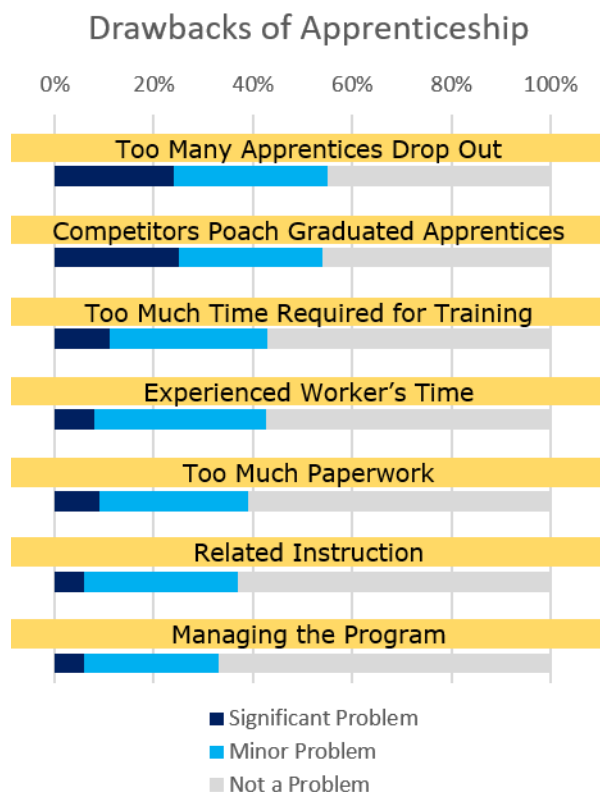


Figure 7: Apprenticeship sponsor views on specific drawbacks of apprenticeship programs (Lerman et al., 2009)

From these two lists, the challenges/drawbacks that we plan to address are:

- Cost of paying towards program
- Gaining buy-in from senior management
- Finding apprentices with necessary qualifications
- Required staff time for mentoring & training
- Too many apprentices drop out
- Too much time required for training
- Experienced workers' time
- Related instruction

In the rest of this paper, we outline some aspects of a program designed to help close this gap, and we explain how we believe it will help allay the challenges and drawbacks identified above.

3. READYING APPRENTICES

The challenges enumerated in the previous section motivate the development of a Preparation for Cybersecurity Apprenticeship Program (PCAP), which looks to close the distance between students seeking qualifications to be eligible for an apprenticeship program and the needs/expectations of the company sponsoring the apprenticeship.

The Question of Cost

While cost concerns are understandable and often uppermost in the minds of organization leaders, studies indicate that apprenticeship programs are usually win-win for firms and workers (Lerman, 2019; Reed et al., 2012). The stylized cost/benefit model of apprenticeship in Figure 8 depicts this idea.

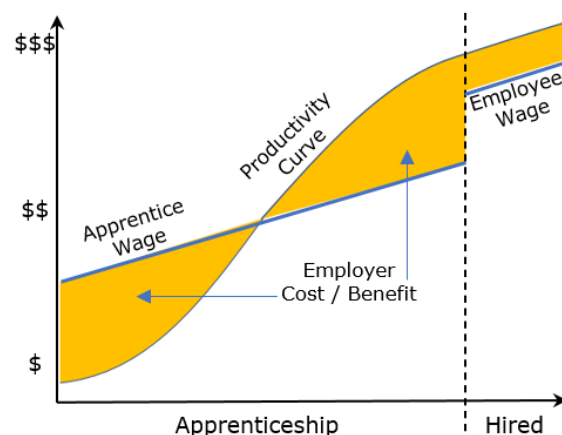


Figure 8: Stylized cost/benefit model of apprenticeship based on (Lerman, 2019) and (Gambin et al., 2010).

The model reflects that apprentices are paid a relatively low wage, but at a cost to the employer

above the benefit of the apprentice's initial productivity benefit. At some point during the apprenticeship, the productivity benefit overtakes the cost of the apprentice wage, and the employer recoups the initial up-front cost of bringing on the apprentice. Post apprenticeship, the worker is hired at a higher wage and operates at a productivity level above the wage cost to the employer. Later in the paper, we will present a modified version of this chart that shows how the initial employer costs can be reduced.

Apprentice Qualification Standards

The DoL's advocacy for the creation of cybersecurity apprenticeship programs is a key step towards satisfying the industry's requirement and/or desire that job candidates have prior hands-on cybersecurity experience. While this should help future cybersecurity job seekers, it raises the question of what kinds of KSAs cybersecurity apprentice candidates require to be attractive to organizations offering apprenticeships and to motivate other organizations to begin sponsoring apprenticeship programs.

Looking to a well-established apprenticeship program for some clues, we consider requirements for electrical apprentices. The apprenticeship system for electrical workers dates back to 1891 with national standards efforts dating to 1941 (IBEW, 2016). It seems reasonable to believe they have carefully considered the issue of apprentice pre-qualification. Currently, the Electrical Training Alliance (ETA) specifies basic standards to which local programs may have additional, geographic-specific requirements (ETA, 2021).

These basic standards are:

- Minimum age 18
- High school education
- One year of high school algebra
- Qualifying score on an aptitude test
- Drug free

Examples of additional requirements include (ITAP, 2019):

- Pass a color blindness test
- Provide a DMV printout
- Participate in an in-person interview

Through this brief examination of an industry with well-established apprenticeship programs, we can glean some useful hints regarding apprenticeship programs generally and what might make sense when crafting a pre-apprenticeship program for cybersecurity – we enumerate three. First, it will likely take some time to establish an industry-

wide consensus on basic requirements for cybersecurity apprentices. So, getting started locally with industry-informed ideas while remaining flexible to incorporate slowly shaping national standards is likely a reasonable approach.

Second, while apprenticeship might informally be thought of as a learning process that provides all required KSAs for a given trade or career field, it is clear that each program will have some baseline expectations of apprentices. Apprentice candidates who meet the required baseline will learn and develop job specific KSAs atop this base. Confirmation of this idea comes from the National Initiative for Cybersecurity Education (NICE) Working Group's Apprenticeship Subgroup (NICE, 2021) which has an active project that is investigating this issue and asking, among other things, "What is the preparation and training necessary for success in the On-the-Job Training (OJT) component of the registered apprenticeship?" (Clement, 2021, pg. 22).

The knowledge complement to OJT is often called related instructional training (RIT) or related technical instruction (RTI). The more RTI completed prior to an apprenticeship, the more quickly an apprentice can increase productivity.

Third, the more universally and easily understood the baseline standards, the better. For example, while it is hard to understand the difference between an unweighted grade point average (GPA) of 3.7 from one high school and a weighted GPA of 4.56 from another high school, it is much easier to understand the difference between having graduated high school and having dropped out or having taken one year of algebra compared to having no experience with algebra.

Industry Certification Benefits

The first step in preparing students for cybersecurity apprenticeship is, unsurprisingly, relevant coursework grounded in cybersecurity principles and a robust selection of courses that allows students to move toward their specialty and foster collaboration among students, faculty, and staff.

The next step is a schematic for certifying candidates for an apprenticeship program tailored to target programs or employer requirements. If we re-visit the survey data provided in Figure 2 and re-organize it so that the "very important" and "somewhat important" response numbers are combined, we have the result in Figure 9.

This slightly different view of the data reveals that cybersecurity hiring managers consider industry credentials as the second most important indicator of a hire's qualification after previous hands-on cybersecurity experience. Industry certifications range from cybersecurity specific certifications such as the Security+ certification, the CYSA+ or the Certified Ethical Hacker certification, to certifications with more of a networking focus such as the CCNA, to the CISSP certification which is suitable for those with an ample knowledge of cyber security and a few years of industry experience.

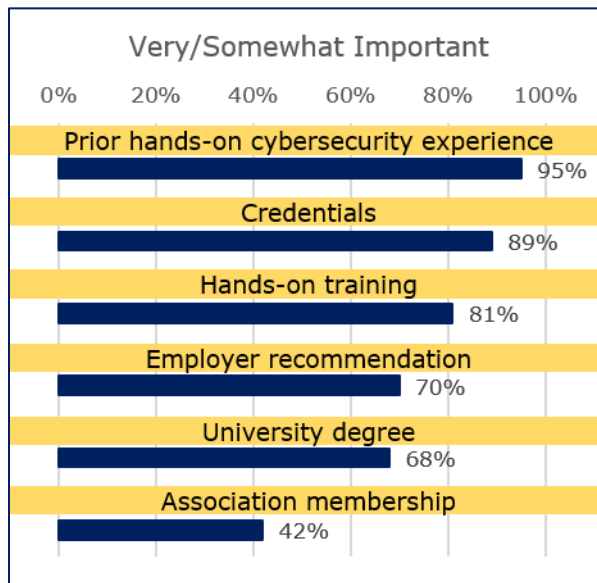


Figure 9: Combined results of “very” and “somewhat” important for the question: “How important is each of the following factors in determining if a cybersecurity candidate is qualified?” (ISACA, 2021).

While standardized tests have many detractors, they have the advantage over alternative methods of evaluation of presenting a common standard that permits straightforward comparison (Wainer, 2006). Industry certification exams have the additional advantage that the knowledge being tested is field-specific, and presumably more directly applicable to the evaluation of a potential employee's job qualifications.

Looking back at the list of eight employer challenges and drawbacks from the end of section two, we see how industry certifications can serve as a key to easing these concerns. First, we reconsider the question of cost. We modify Figure 8 by adding four components: a dotted-dashed curve indicating the remaining RTI an apprentice would be expected to learn, a second y-axis on

the right corresponding to the remaining RTI curve, a vertical dotted line labeled Certification Advantage, and a shaded area of Employer Cost that indicates the Employer Cost Savings as a result of the industry standard certification knowledge with which the apprentice arrives.

The idea expressed in Figure 10 is that as industry certifications are primarily concerned with industry-specific knowledge, an apprentice possessing a certification will (likely) join the apprenticeship program with necessary foundational knowledge and have less remaining RTI than an apprentice without the same certification. This means the apprentice will be further along the productivity curve and cost the employer less up-front.

The increased amount of knowledge and decreased remaining RTI will presumably have a direct net positive effect on five of the other challenges & drawbacks:

- Finding apprentices with necessary qualifications
- Required staff time for mentoring & training
- Too much time required for training
- Experienced worker's time
- Related instruction

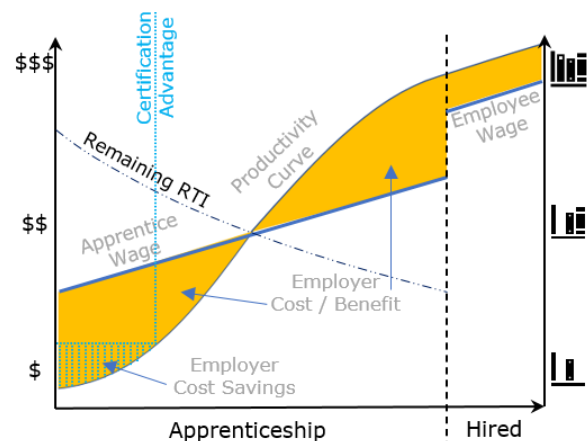


Figure 10: Stylized cost/benefit model of apprenticeship with added “Remaining RTI” curve, corresponding right-side y-axis, “Certification Advantage” line, and “Employer Cost Savings” shading.

As certifications are likely to be outside of regular curriculum requirements, attaining one likely demonstrates a firmer commitment to the cybersecurity path and, we believe, will potentially lead to fewer dropouts. The last challenge – gaining buy-in from senior management – should be reduced as a second-order effect of the risk reduction related to the

other challenges/drawbacks. For example, per Figure 10, the up-front employer cost as well as required staff time for training and mentoring would be reduced.

4. DISCUSSION

Given this reality, we have begun to more directly and aggressively encourage students to sit for industry certification exams after successfully completing certain classes. The example we will discuss is the Computing Technology Industry Association (CompTIA) Security+ exam. While our efforts to unite course objectives related to attainment of a university degree with certification exam preparation are not unique (Ngo-Ye & Choi, 2016; Al-Rawi & Lansari, 2008; White, 2006), we do have some pragmatic advice that we have not found elsewhere in the literature.

A significant component of a PCAP program is funding for students to sit for the certification exams. Certification exam prices are not generally considered cheap by students. The CompTIA currently retails their Security+ exam, for example, for \$370 (CompTIA, 2021b) and offers it to academic partners for \$240 (CompTIA, 2021a). Students new to industry certification exams also seem to find them intimidating, regardless of the level of preparation. Beyond providing them with knowledge, preparation and encouragement, support in the form of exam fee assistance can help them overcome their reluctance to attempt the exam. Of course, providing financial assistance shifts the financial risk burden to the funds provider and raises concerns that students will not prepare as vigorously as when their personal funds are at risk.

In an effort to balance these concerns, we have piloted two arrangements that seem to work well for the different types of students interested in taking an exam. One arrangement is full reimbursement for passed exams. Students pay for their exam, take it, and, if they pass, submit for reimbursement from our cybersecurity center. There are some administrative challenges with this arrangement that need to be worked out with the finance department, but this option is very low risk to both the well-prepared student and the fee provider.

The second arrangement is a simple cost share regardless of the outcome. Students pay \$60 and our cybersecurity center pays \$180. This alternative works well for those students who are well-prepared, but just seem to lack confidence

that they know “enough.” There is potentially more risk involved for the majority fee payer in this case as some students may not see \$60 as much of a burden and decide to take an exam without sufficient preparation. While this is not our common experience (i.e., for most students \$60 represents real skin-in-the-game and prepare diligently for the exam) this risk can be offset by requiring students to take a pretest before agreeing to pay the \$180.

While creating these two arrangements to achieve a high student pass rate is important for showing program value, the challenge to find funds remains non-trivial. We have been able to meet this challenge with both deliberate and ad-hoc approaches.

Our deliberate method involved enlisting the support of our advisory board. We pitched the ideas outlined above and found they were enthusiastic about supporting students in such a tangible and risk-balanced way both on a personal level and as representatives of their respective companies. A number of our advisory board members have hired our students as apprentices for their programs. During the apprentice selection process, the companies utilized the faculty feedback, and were very pleased with the apprentices hired. The majority of the apprentices that went through the local apprenticeship programs have become full-time employees upon graduation. The success of the prior placements has been an incentive for local apprenticeship programs to sponsor even better qualified incoming apprentices. This appears to be a sustainable method for raising exam fees going forward.

Once we had this overall idea in mind, it also became easier to spot ad-hoc opportunities to secure funds for student exam fees. Two examples we encountered were unallocated year-end money from national-level programs and a portion of facilities and administrative (F&A) funds that trickled back to the college and department levels from awarded grants.

5. REFLECTION AND RECOMMENDATIONS

Our university Information Technology Security Department started an apprenticeship program last year, and the apprentices were selected based on their prior academic performance, and their performance in a pilot cybersecurity recruitment program our university participated in. We found that the apprentices completing the pilot recruitment program were focused, well-prepared, and dedicated. When the pilot program

was completed, in an attempt to keep the quality of the recruited apprentices high, we designed the PCAP program.

Universities that have apprenticeship programs where students are selected based on university works and achievements are highly selective internal to the university; the quality of candidates is high given the abundance of RIT within the academic environment. Information security teams who are staffers at the university would guide apprentices through OJT and competency building.

Within our institutional program, apprentices demonstrate their ability to adapt and apply their RIT to the OJT, complemented by one-on-one instruction through mentorship. After a brief period of one-on-one instruction, group instruction is the next step, yet not before making sure that each apprentice is on the same page regarding information, access to tools, and methods of investigation. Once group instruction is in progress, team-building and communication take place to gain real-world experiences and independence due to confidence-building exercises.

Measuring the competency and knowledge base of the apprentices is the next step before we establish the next step towards program completion and career services. The establishment of a rubric to develop metrics on what the apprentices learned and certifying their capacity for critical thinking and information processing is an achievable goal. Establishing metrics for evaluating apprentices will give employers a holistic perspective on the individual candidate's capabilities and skills.

Significant advancements in the candidates' skills have been observed throughout the first few months of the apprentices working hands-on. The apprentices have demonstrated a degree of independence and trust comparable to an entry-level employee with a reasonable amount of hands-on experience. Success feeds upon itself; therefore, employers are likely to fund programs that yield candidates of the highest caliber. The main factor in accomplishing success is the student's exposure to RIT in the classroom and support preparation for certification exams.

A pre-apprenticeship program sets out to create a standard model for training and designed to bridge two problems: preparing students for entering the field through apprenticeship and bely the employer's fear of hiring apprentices that lack drive, dedication, experience, and

knowledge. Suppose employers are informed, satisfied, and eager to employ candidates. This could lead to other apprenticeships forming to the same standard across the board to meet this demand for those who have gained experience through apprenticeship programs.

6. CONCLUSION & FUTURE WORK

Initiatives to create cybersecurity apprenticeships to help close the gap created by negative unemployment in the cybersecurity industry have exposed another gap – between the skills of the available student talent pool and the expectations of organizations willing to offer apprenticeships. In this paper, we examined eight of the key challenges and drawbacks expressed by organizations that are sponsoring or considering sponsoring apprenticeships. We explained how a preparation for cybersecurity apprenticeship program (PCAP) anchored by industry certification attainment would diminish those eight concerns. Because of the cost challenges associated with taking certification exams, we also provided some practical suggestions for making the program sustainable.

In future inquiries into this topic, we plan to deconstruct the “why” behind the employers' concerns. Given the national security implications of negative unemployment in the cybersecurity industry and the increase of cybercriminal activity within the United States, it is critical for employers and universities to recognize the impacts of organizational stagnation. As well, the results in Figures 2 and 9 indicate that employers' view of the importance to a cybersecurity career of a university degree is rather dim. It raises the question of whether universities can keep up with the demands and innovations within the field of cybersecurity. The industry certifications are valued highly by recruiters for entry-level analyst positions and hands-on experience is the number one criterion for selection into a cybersecurity job (Figure 9). “The prediction is there will be a variety of entrants moving into the higher education space, offering valuable credentials and providing the skills needed to launch professionally” (Weinberg, 2020). Given this challenge to the traditional liberal arts university model, the higher education should adapt to the current environment in cybersecurity and the tech industry as a whole.

As our PCAP and in-house apprenticeship programs mature, we will evaluate them together, along with partnering company programs, for sustainability and viability moving forward. Solutions in funding, budgets, and

marketing will be explored and scrutinized for long-term planning. The development of metrics and rubrics will be critical in overall analysis and data acquisition, which would yield a holistic view of the programs progress and results.

7. REFERENCES

- Allen, P. (1974). Everything Old is New Again. <https://www.songfacts.com/facts/peter-allen/everything-old-is-new-again>
- Al-Rawi, A., & Lansari, A. (2008, June). Integrating the Security+ exam objectives into information technology curricula. In 2008 Annual Conference & Exposition (pp. 13-768). <https://peer.asee.org/integrating-the-security-exam-objectives-into-information-technology-curricula.pdf>
- Burning Glass Technologies. (2019, June). Recruiting Watchers for the Virtual Walls; The State of Cybersecurity Hiring. https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf
- Champlain College Online. (2021). The Cybersecurity Skills Gap & Barriers to Entry [Report]. <https://online.champlain.edu/sites/online/files/2021-10/Adult%20Viewpoint%202021%20Survey-Champlain%20College%20Online-Final.pdf>
- Clement, K. (2021, May 27). DRAFT Comparative Analysis Cybersecurity Education Models Project white paper.
- Computing Technology Industry Association (CompTIA). (2021a). CompTIA ACAD Security+ (Exam SY0-501) Voucher. <https://academic-store.comptia.org/comptia-acad-security-plus-exam-voucher/p/ACADCompTIAS>
- Computing Technology Industry Association (CompTIA). (2021b). Exam prices. <https://www.comptia.org/testing/exam-vouchers/exam-prices#security>
- Cybersecurity Supply/Demand Heat Map. (2021, March). CyberSeek Project Web site. <https://www.cyberseek.org/heatmap.html>
- Douglas, P.H. (1921). American Apprenticeship and Industrial Education [Google Books version]. <https://books.google.com/books?id=uQIwYkwa4cwC&dq=apprenticeship&lr&g=PA209>
- Electrical Training Alliance (ETA). (2021). Apprenticeship Training. <https://electricaltrainingalliance.org/training/apprenticeshipTraining>
- Federal Bureau of Investigation (FBI). (2021, March). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Frenette, A. (2015). From apprenticeship to internship: The social and legal antecedents of the intern economy. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, 13(2), 351-360. <https://www.triple-c.at/index.php/tripleC/article/view/625>
- Gambin, L., Hasluck, C., & Hogarth, T. (2010). Recouping the costs of apprenticeship training: employer case study evidence from England. *Empirical research in vocational education and training*, 2(2), 127-146. <https://ervet-journal.springeropen.com/track/pdf/10.1007/BF03546492.pdf>
- Independent Training & Apprenticeship Program (ITAP). (2019, October 11). Electrician Apprenticeship – How to Become an Electrician. <https://itap.edu/electrician-apprenticeship-how-to-become-an-electrician/>
- International Brotherhood of Electrical Workers (IBEW). (2016, July). History & Structure, Celebrating 125 Years of IBEW Excellence. <http://www.ibew.org/Portals/31/documents/Form%20169%20-%20History%20and%20Structure.pdf>
- International Information System Security Certification Consortium (ISC)2. (2020, November). Cybersecurity Professionals Stand Up to a Pandemic. Cybersecurity Workforce Study 2020. <https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B>
- ISACA. (2021). State of Cybersecurity 2021. Part 1: Global Update on Workforce Efforts, Resources and Budgets. <https://www.isaca.org/go/state-of-cybersecurity-2021>
- King, L. W. (Trans.). (2008). The Code of Hammurabi. Lillian Goldman Law Library, Yale Law School, Avalon Project Web site. <https://avalon.law.yale.edu/ancient/hamfra-me.asp>
- Lerman, R. (2019). Do firms benefit from apprenticeship investments? IZA World of Labor. <https://wol.iza.org/articles/do-firms-benefit-from-apprenticeship-investments/long>

- Lerman, R., Eyster, L., & Chambers, K. (2009). The Benefits and Challenges of Registered Apprenticeship: The Sponsors' Perspective. Urban Institute (NJ1). <https://files.eric.ed.gov/fulltext/ED508268.pdf>
- Lloyd, M. (2017, September 8). Negative Unemployment: That Giant Sucking Sound In Security. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2017/03/21/negative-unemployment-that-giant-sucking-sound-in-security/?sh=60d2b07c7206>
- McCarthy, M. A. (2021). 19. Past as Prologue: Apprenticeship and the Future of Work. In *The Great Skills Gap* (pp. 184-193). Stanford University Press. <https://www.degruyter.com/document/doi/10.1515/9781503628076-027/html>
- Mieschbuehler, R., Hooley, T., & Neary, S. (2015). Employers' Experience of Higher Apprenticeships: Benefits and Barriers. Derby and Melton Mowbray: International Centre for Guidance Studies, University of Derby and Pera Training. <https://derby.openrepository.com/handle/10545/576935>
- National Initiative for Cybersecurity Education (NICE). (2021). Apprenticeships in Cybersecurity Community of Interest. <https://www.nist.gov/itl/applied-cybersecurity/nice/about/community-coordinating-council/apprenticeships-cybersecurity>
- Ngo-Ye, T. L., & Choi, J. (2016). PREPARING STUDENTS FOR SECURITY CERTIFICATION: AN EXPLORATORY EXPERIMENT. *Issues in Information Systems*, 17(3). https://iacis.org/iis/2016/3_iis_2016_59-69.pdf
- Reed, D., Liu, A. Y. H., Kleinman, R., Mastri, A., Reed, D., Sattar, S., & Ziegler, J. (2012). An effectiveness assessment and cost-benefit analysis of registered apprenticeship in 10 states (No. 1b5795d01e8a42239b3c98dcc1e1161a). Mathematica Policy Research. https://wdr.doleta.gov/research/FullText_Documents/ETAOP_2012_10.pdf
- Stoker, G., Clark, U., Vanajakumari, M., & Wetherill, W. (2021). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. *Information Systems Education Journal*, 19(2), 2. <http://isedj.org/2021-19/n2/ISEDJv19n2p35.pdf>
- U.S. Bureau of Labor Statistics (BLS). (2020, September). Employment by major industry sector. <https://www.bls.gov/emp/tables/employment-by-major-industry-sector.htm>
- U.S. Bureau of Labor Statistics (BLS). (2021, July). Table A-1. Employment status of the civilian population by sex and age. <https://www.bls.gov/news.release/empsit.t01.htm>
- U.S. Bureau of Labor Statistics (BLS). (2021, April). Occupational Outlook Handbook; Information Security Analysts. <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
- U.S. Department of Labor (DoL). (2021a). Cybersecurity. <https://www.apprenticeship.gov/apprenticeship-industries/cybersecurity>
- U.S. Department of Labor (DoL). (2021b). Data and Statistics: Registered Apprenticeship National Results Fiscal Year 2020. <https://www.dol.gov/agencies/eta/apprenticeship/about/statistics/2020>
- Wainer, H. (2006). Book Review: Defending Standardized Testing. *Journal of Educational Measurement* 43(1), 77-84. <https://www.jstor.org/stable/pdf/20461810.pdf>
- Weinberg, A. (2020, September 13). Google just changed the higher education game. Colleges and universities should be paying attention. *Business Insider*. <https://www.businessinsider.com/google-careers-certificate-program-changed-game-universities-should-pay-attention-2020-9>
- White, G. L. (2006). Vendor/industry certifications and a college degree: A proposed concentration for network infrastructure. *Information Systems Education Journal*, 4(48), 07. [http://isedj.org/4/48/ISEDJ.4\(48\).White.pdf](http://isedj.org/4/48/ISEDJ.4(48).White.pdf)

Teaching Case

Rubber Duckies in the Wild: Proof of Concept Lab for USB Pen Testing Tool

Anthony Serapiglia
Saint Vincent College, Latrobe, PA, 15650
Anthony.Serapiglia@stvincent.edu

Abstract

Ethical Hacking has matured into a widely accepted and necessary part of the cybersecurity world. Actively probing and testing the defenses of a network or business system is essential to maintaining CIA benchmarks of Confidentiality, Integrity, and Availability. Penetration testing has evolved into a special subset of the industry. Companies and organizations of all sizes and across a range of industries rely on pen testers to proactively identify weakness in cyber-defenses before a real attack effects real damage. One of the primary objectives of penetration testers is the creation of a remote access shell into a system. A common method of achieving this is through the use of "rubber ducky" USB devices that, when inserted into a computing device, initiates an active session from inside a network to allow remote access to the pen tester. This teaching case provides background and instructions on incorporating a proof-of-concept rubber ducky build into an undergraduate cybersecurity course.

Keywords: Penetration Testing, Ethical Hacking, Cybersecurity, Rubber Ducky, White Hat Hacking

1. INTRODUCTION

NIST Special Publication 800-115 begins to define penetration testing (pen test) as "...security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network" (NIST, 2008).

Pen tests differ from standard vulnerability scanning. The end goal of the scanning is simply the identification of weak spots such as missing patches or outdated software versions. The final product is a report that may or may not be actionable. Pen testing goes further. As part of a thorough pen test, an attempt is made to exploit the vulnerabilities identified in scanning. This extra step is crucial to identifying the difference between theoretical vulnerabilities and ones that can be actively exploited. This allows a more precise classification of priorities in remediation. It also helps to get the attention of "C-Suite" or managerial decision makers who may not understand the urgency of the situation.

A good pen test should be performed by actors outside of the organization being tested. Thus, the testers do not subconsciously bring inside information to the table when executing their attacks. Very few people in an organization should know that a pen test is being performed. This helps to ensure that tests are performed under normal working conditions and that defenses have not been artificially raised for the occasion only to be dropped later.

Full pen tests encompass entire systems. This includes systems that are both inside an organization and possibly hosted elsewhere. Many times, a pen test will also include a test of physical security and surrounding systems, policies, and procedures. It has been a common theme of many organizations that much effort is placed on technical perimeter defenses for internet connected systems, but internal controls allowing for physical access to devices and networks remain a soft underbelly ripe for attack.

Critical to any pen test operation is that a set of ground rules be agreed upon by both parties prior to the test. Boundaries and scope of work must

be declared. An emergency contact(s) must be in place in case anything would stray from the accepted field of play or if, as part of the response to a potential 'breach of security' event, personnel of the target company engage law enforcement. Someone must be available to notify those involved to stand down and that the test is an authorized exercise.

A case in Dallas County, Iowa in September of 2019 resulted in two employees of cybersecurity firm Coalfire Labs being arrested. While testing security at the county courthouse, the two performed a physical pen test, attempting to gain physical access to the courthouse. They had been engaged by Iowa's State Court Administration and had a written statement, or "get out of jail free card" with them, but the local sheriff proceeded to arrest both for felony third-degree burglary charges. They were released after a night in jail and posting \$100,000 in bond. Charges were later reduced to misdemeanor trespassing. It was nearly a year until the charges were dropped after an education campaign and widespread publicity generated by the larger ethical hacking and cybersecurity community (Krebs, 2020; Osborne, 2020). Of the contributing factors in the misunderstanding, two stand out. First, the terms of the pen test agreement clearly stated that no doors should be forced open. The pen testers stated that they had entered through an unlocked front door. The Sheriff disagreed. Second, the contacts on the "get out of jail free" card were not able to be reached for verification at 12:30 in the morning to verify that the two were in fact cybersecurity contractors (Goodin, 2019).

2. RUBBER DUCKY

One of the many characteristics of an ethical hacker/pen tester is the ability to be creative and to become a "maker". After all, the evolution of the term hacker in the modern sense begins with a model train club at MIT (Levy, 1984) and grew through communities, "...who enjoy exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary (Yagoda, 2014).

An essential step in the maturation of a hacker is the ability to create their own tools. A hacker who is able to create and craft their own tools is one who recognizes the situation at hand, the environment and variables, and applies problem solving techniques to develop a solution that can cross from a virtual world of the theoretical and into the physical world of action.

This is an area where practice can move from rote recipe to an evolving art. Not every attempt is guaranteed success. There may be some false starts. There will be troubleshooting and debugging. There may be frustration. There is value in frustration. Once a solution is achieved and a task accomplished, the greater the frustration the greater the reward.

A primary objective of penetration testers is the creation of a remote access shell from within the system. A common method of achieving this is through the use of "rubber ducky" USB devices that when inserted into computing services activate an active session from inside a network to allow remote access to the pen tester.

A USB rubber ducky is most commonly a keystroke injection tool disguised as a generic flash drive. Computers recognize it as a regular keyboard and automatically accept its pre-programmed keystroke payloads at over 1000 words per minute (Hak5, 2021).

The first rubber ducky hacking devices were drop keys, USB sticks that had been preprogrammed to deliver a payload when inserted into a computer. These devices were left in open spaces to be picked up by unsuspecting people, many of whom would plug them into a computer either to attempt to find the owner or for personal use. Many users still commonly log in and perform their daily functions on their computers utilizing an account with administrative privileges (Krebs, 2006; Burnette, 2020). This often allows executables to run without any further prompting or warning messages to the user. Rubber ducky drop keys essentially functioned as a message in a bottle floating randomly on the sea, with the difference being that the researcher did not have to rely on the finder to actively send a message back. Executing a program to phone home happened automatically.

As a pen tester, a more precise and direct targeting is both possible and expected. Gaining physical entry into a building, organization, or just an individual in a public space such as a coffee shop can allow a pen tester sufficient access to discretely insert a USB device and gain access to a computer. Heightened awareness and popularity of the directed use of a rubber ducky for hacking purposes was reached after being featured in the television series *Mr. Robot* in 2016. Commercial pre-programmed rubber ducky devices are readily available and retail for price of \$50. The material cost of the hardware to develop a rubber ducky can come in below \$3 per unit. In many of the use cases, these devices become

expendable and are not recaptured, making a compelling case for the DIY route.

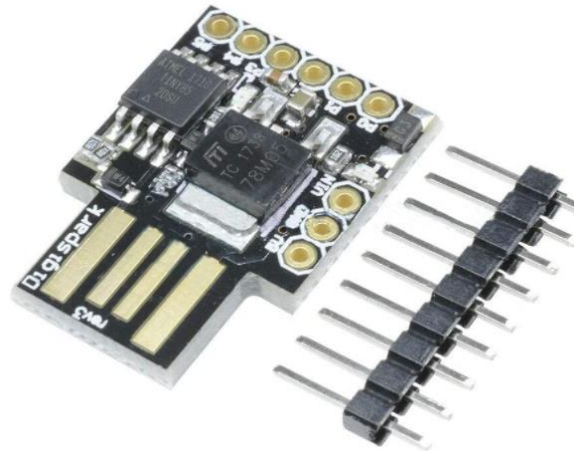


Figure 1: ATTINY85 controller

At the core of a rubber ducky is a programmable controller chip with a USB connector. This assignment will assume a common Digispark ATTINY85 for Arduino General Micro USB Development Board. In July of 2021, 5-piece packs of ATTINY85 controllers could be purchased for \$13.99 (<https://www.amazon.com/AITRIP-Digispark-Kickstarter-ATTINY85-Development/dp/B08HYHPTX2/>).

3. ASSIGNMENT

Task

Create a droppable USB Rubber Ducky that when inserted into a Windows computer will create a text file on the user's desktop named "pwned.txt" and containing the text "Hello World – You have been pwned."

Ingredients

- Arduino IDE found at: (<https://www.arduino.cc/en/software>)
The Arduino development environment is free, open source, and available on Linux, Mac, and windows platforms.
- ATTiny85 (Digispark) USB Controller Board (generally available for purchase for approximately \$3 or less per unit)
- Digispark driver (if necessary) can be found at:
<https://github.com/digistump/DigistumpArduino/releases>

Getting Started

This exercise proceeds in the following order: setup of the development environment,

programming of the device, testing the device, and deployment of the device.

Environment Setup

Follow instructions for Arduino IDE installation based on your operating system.

Post-installation, the IDE will need to be updated with a specific board manager for the ATTINY85. go to File -> Preferences. Next to "Additional Board Manager URLs:" enter: http://digistump.com/package_digistump_index.json

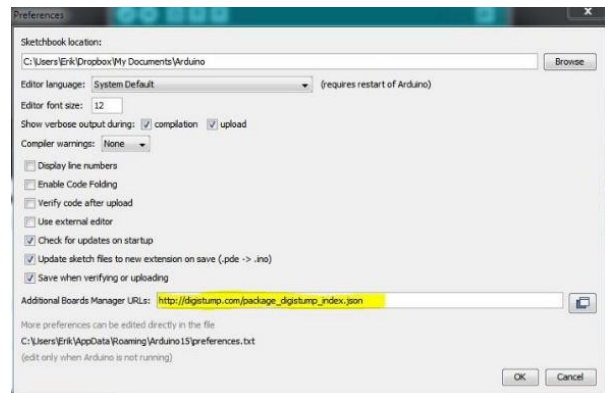


Figure 2: Preference setting to add board manager in Arduino IDE

Once the URL is added, go to Tools > Board "Arduino Uno" > Boards Manager. In the textbox at the top, type Digispark and install the Digistump AVR Boards board manager. If necessary, install Digispark device drivers.

Programming

A basic build of a beginner rubber ducky will program the ATTINY chip to be recognized as an HID (Human Interface device) when inserted, acting as a keyboard delivering keystroke input at up to 1000 words per minute.

Given the nature of the device, many possibilities exist for payload options. The ATTiny85 chip supports C, but is Arduino-compatible. Utilizing the Digispark board manager in the Arduino IDE opens a full range of natural language commands. DuckyScript was developed by Hak5 as a scripting language for their proprietary products. A community of developers have contributed many preconfigured scripts available through quick search efforts. Free online services such as the digiQuack DuckyScript convertor are also available to make these scripts usable in the Arduino environment (<https://cedarctic.github.io/digiQuack/>).

A basic script to complete the task of message creation for this assignment can be completed in less than 20 lines of code. Be creative. Experiment. Test and debug.

Testing and Deployment

As with any project related to penetration testing and ethical hacking, testing should be performed in a restricted and secured lab environment. Deployment of this device should only be done under instructor guidance, or under contract with explicit boundaries stated.

4. CONCLUSION

Becoming a pen tester requires a full spectrum of knowledge and skills inside and outside of technology. The after-action reports of pen testers can read like movie scripts. It is an exciting and thrilling area of cybersecurity that is unlike any other. One of the features that sets pen testing apart from other areas of cybersecurity is the crossover into the real world. Full pen testing often encompasses in-person physical exploitation of work environments. Field work is unpredictable, and success depends on flexibility, adaptability, and a full set of tools.

The USB Rubber Ducky has taken many forms recently; from experiments on seeding an environment with innocuous flash drives to see if one is randomly picked up to phone home, to Swiss Army knives full of exploitable packages deployed with precision by a pen tester in person. Most use cases for a ducky involve leaving it behind, with a low percentage chance of recovery.

It has been a legacy of many professions that one of the signs of an apprentice maturing into a master is the ability to create their own tools. This step forward shows that the neophyte understands the greater depth of their environment, the specific task or problem to be solved as well as the exact tool necessary to solve it. It also shows the command of the resources available to them in the creation of a suitable tool for the task.

Including labs that require beginning cybersecurity students to create their own tools helps to foster this progress in them. It synthesizes the various and multiple technologies together. It provides a springboard to further creative projects that bring the individual building blocks together after experiencing the initial success in building a foundational platform for direct use in real world exploitation.

5. REFERENCES

- Burnette, M. (2020, January 23). Why You Should Not Use an Admin Account. Retrieved May 21, 2021, from <https://www.lbmc.com/blog/why-you-should-not-use-an-admin-account/>
- Goodin, D. (2019, November 13). How a turf war and a botched contract landed 2 pentesters in Iowa jail. Retrieved February 9, 2021, from <https://arstechnica.com/information-technology/2019/11/how-a-turf-war-and-a-botched-contract-landed-2-pentesters-in-iowa-jail/>
- Hak5, LLC. (n.d.). USB RUBBER DUCKY. Retrieved April 21, 2021, from <https://docs.hak5.org/hc/en-us/categories/360000982554-USB-Rubber-Ducky>
- Krebs, B. (2006, April 18). Windows Users: Drop Your Rights. Retrieved July 11, 2021, from http://voices.washingtonpost.com/securityfix/2006/04/windows_users_drop_your_rights.html
- Krebs, B. (2020, January 31). Iowa Prosecutors Drop Charges Against Men Hired to Test Their Security. Retrieved June 12, 2021, from <https://krebsonsecurity.com/2020/01/iowa-prosecutors-drop-charges-against-men-hired-to-test-their-security/>
- Levy, S. (2014, November 21). The Tech Model Railroad Club. Retrieved March 3, 2021, from <https://www.wired.com/2014/11/the-tech-model-railroad-club/>
- Osborne, C. (2020, February 03). Charges dropped against Coalfire security team who broke into courthouse during pen test. Retrieved June 12, 2021, from <https://www.zdnet.com/article/charges-dropped-against-penetration-testers-who-broke-into-courthouse/>
- Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (September, 2008). Technical Guide to Information Security Testing and Assessment, NIST Computer Security Resource Center Special Publications 800-115. Retrieved February 16, 2021, from [Technical guide to information security testing and assessment \(nist.gov\)](https://nvd.nist.gov/technical-guides/information-security-testing-and-assessment)
- Yagoda, B. (2014, March 06). A Short History of "Hack". Retrieved March 3, 2021, from <https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack>

An IoT Based New Platform for Teaching Web Application Security

Zhouzhou Li
zli2@semo.edu

Ethan Chou
echou1s@semo.edu

Charles McAllister
cdmcallister@semo.edu

The Department of Computer Science
Southeast Missouri State University
Cape Girardeau, MO 63701, U.S.

Abstract

Web application security is a core issue that must be addressed in cybersecurity degree programs to adequately prepare students for leadership in industry. To teach a "Web Application Security" course, a good exercise platform that can cover the context of Web application is crucial to the learning outcomes. Unfortunately, existing platforms cannot satisfy both cost and efficiency requirements. In this paper, a cost-effective and easy-to-use full-stack Web application platform, ESP32-CAM, is introduced to the course, which is an Internet of Things device with a built-in face recognition Web App. Our major contribution in this paper includes the thoughtful design of an exercise series around the platform, which can provide more hands-on practice in the class, strengthen students' practical skills, and further inspire the students' learning interests on a matured technique such as Web applications. Furthermore, through this platform students can explore the cutting-edge technologies in their class projects or capstone project, e.g., "transfer learning" to extend the face recognition to emotion recognition or generative adversarial network to fool the Artificial Intelligence model, which will greatly involve students in academic research.

Keywords: Web Application Security, Internet of Things, Artificial Intelligence, Reverse Engineering, Penetration Testing, Secure Software Development.

1. INTRODUCTION

According to International Telecommunication Union (Buyannemekh & Chen, 2021), by 2019, 53.6% of the world population had stable Internet access and enjoyed the wealth of information. With the Internet, a user who has no technical or engineering background can solve some technical challenges by using his/her World Wide Web (WWW, or just Web) browser to search the Internet for hints or answers. The Web is a critical

application for the Internet. Due to its core role played on the Internet, Web application's security is naturally a significant issue that needs to be addressed in the industry and in academic establishments.

In current usage, the Web becomes a de facto standard for Internet. Other Internet applications (such as email, instant messaging, interactive game, file transfer, cloud storage, etc.) either build themselves upon Web or provide their Web

version of solutions. Figure 1 shows the context of Web application, where it depends on the lower-level Internet protocols and supports other Internet applications. Every component in this figure can potentially impact the security. Therefore, the Web Application Security should cover all.

Unfortunately, considering both cost and efficiency, it is difficult to find a suitable platform providing full-stack protocols for students to exercise during course study. The major concerns include:

- Only opening the (Web) application layer for Cybersecurity students to attack. No details for the implementation of the lower layers. Not to mention their vulnerabilities.
- Only provide an over simplified Web layer for Cybersecurity students to attack. Seemingly not a real system.
- Not free if the user wants to experience the advanced functionalities.

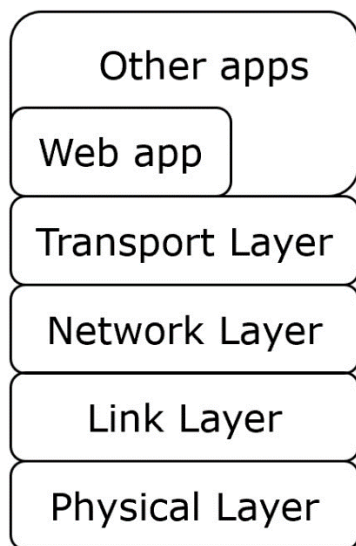


Figure 1: The Context of Web App Security

A good platform for students to practice Web application security but limiting the impact to the real networks need to be well designed.

The remainder of this paper is organized as follows. In the 'Literature Review' section, we review the current courseware or labs designed for teaching Web App Security. In the 'Background' section, the Internet of Things (IoT) device-based face recognition Web platform will be introduced, and its advantages will be explained. In the 'Teaching Objectives' section, the teaching goals of the Web App Security course will be discussed. Then, a list of exercises to

support the teaching goal through the platform will be provided. In section 'Student Feedback', students' feedback proved the ESP32-CAM a good platform for learning 'Web App Security' will be given. With the 'Outcomes' section providing quantitative evaluation on the learning effect. A summary of what areas can be improved, as well as a conclusion of discussion will be provided in "Conclusions and Future Work" section.

2. LITERATURE REVIEW

Currently, the most popular platform for teaching Web App Security is Virtual Machine (Chen & Tao, 2011; Schweitzer & Bolang, 2009; Chen et al., 2010; Liegle & Meso, 2005), though in (Yu et al., 2006), the authors still tried using the traditional high-performance Cyber Defender Lab. The advantage of using a VM platform is obvious: cost-effective. In (Oh et al., 2020), a Raspberry Pi 3 based platform was proposed, which also had the cost advantage (cost was about \$234) but provided a real platform to the students. A corresponding survey was conducted in a course. The result showed that most students prefer the real-world Web applications for them to attack and defend; they are tired of practicing in a virtual environment.

A Raspberry Pi can be treated as a minicomputer. Most IoT devices are even smaller and less expensive. The insight here is, if we can move the Web App Security teaching platform to a IoT device, we may achieve further cost-saving.

Fortunately, we found one. And its performance is even better.

3. BACKGROUND

ESP32-CAM (Fig .2) is an IoT hardware-based Web App providing quick, accurate and cost-effective "Face Recognition". A typical use case/scenario is given below:

- New users should enroll their face image to the Web App first. A unique ID is then assigned to that face. After that, the face image is saved in the system and the user cannot access it anymore.
- The security department places the ESP32-CAM hardware to the gate/door they want to implement access control by face recognition.
- A user stands in front of the ESP32-CAM hardware. The Web App analyzes the input, i.e., the face image, to generate landmarks for that face and search the image database for matched face. If found, access privilege

will be given to the user; if not, access will be denied.



Figure 2: ESP32-CAM Board (Front & Back Views)

The cost of the ESP32-CAM hardware is about \$8.00. Considering the peripheral cable and bridge device, the overall cost of one set of exercise hardware is just about \$15.00.

And the Web App is ready, within 1 minute, a user can deploy it. Furthermore, it can cold start in 10 seconds, which is much faster than all the known platforms. Not to mention that it is 100% open-source. The instructor doesn't need to verify the potential Intellectual Property issue. And it is easy to maintain and expand, after all, only 4 source files need to be maintained with two of them are header files.

Besides the reasonable price and good performance, another attractive feature this Web App can provide is the integration of IoT and Artificial Intelligence (AI) technologies.

Internet of Things

IoT is an emerging technology. Though many students have shown their interests in IoT, a course about IoT fundamentals is often still only offered as a course elective in degree programs. If exercises in this Web App Security course can be provided by using an IoT device, then state-of-the-art and valuable content can be added to this old-technique course. It is not necessary for students to take a full IoT course to touch on the embedded hardware as well as wireless communication.

This IoT hardware-based platform is also good for students to conduct edge computing research, which is a hot subarea of cloud computing, by focusing on customized computing to provide prompt responses and accurate results. The AI model integrated in ESP32-CAM was trained by a dataset with different faces. Its generality was already verified. However, when it is applied to a

specific face, its recognition accuracy and speed are not perfect, i.e., there is room for new research to improve. In one of the capstone projects, one student group realized the sensitivity of the ESP32-CAM AI model somehow was impacted by personal face features.

Artificial Intelligence

As aforementioned, an AI model is integrated in the ESP32-CAM Web application (Zhang, Zhang, and Qiao, 2016). This generation of AI is an emerging technology, which is based on supervised and unsupervised machine learning. And face recognition belongs to the supervised learning. Most CS/ECE departments already offered Machine Learning/AI courses. Consequently, this course for Web App Security can offer hands-on opportunities for students to comprehensively utilize what they have learned from the ML/AI courses. Due to the interactive character of this AI model, students showed their great interests to the face recognition application.

This AI-integrated platform is also good for students to conduct transfer learning research, which does not change the existing AI model, but builds the new learning framework on top of the existing model. For example, enhance the face recognition to emotion recognition.

Furthermore, with the prevalence of AI models, model-based attacks emerge, which makes the traditional code-based countermeasures outdated. Students will get a chance to learn the newest research in data poisoning, data manipulation, and Generative Adversarial Network.

4. TEACHING OBJECTIVES

After completing this course, students will be able to:

1. Understand HTML and front-end code.
2. Describe the components of a Web App.
3. Deploy a Web App to a specific device.
4. Conduct preliminary reverse engineering & re-engineering.
5. Understand the Software Maturity Model with concentration on Security.
6. Describe different vulnerabilities and their root causes.
7. Conduct pen-testing or attacking by code review, auto vulnerability scanning, and fuzz testing.
8. Describe functional and non-functional requirements and their relationships to security requirements.
9. Conduct threat modeling.

10. Follow secure coding standards to write and review code.
11. Describe the function of a certificate. Apply certificates in Web Apps.
12. Apply Public Key Cryptography in Web Apps.
13. Describe the data impact to Web App Security.

These objectives are the result of decomposing the high-level outcomes of this course into small technical areas and integrating practical skills/tools into these areas. The high-level outcomes source from the NSA CAE-CDE designation requirements.

5. EXERCISES

An attempt to fully utilize the proposed platform was made by designing a variety of exercises for students to experience the different aspects of the Web Application Security. In total, 15 independent exercises were prepared, but together, can provide a systematic layout.

1. The first two exercises are related to user experience – before attacking or defending a Web App, the students will need to get familiar with it.
2. The next six exercises cover how to attack a Web App and fundamental skills and tools. Among them, four exercises are related to finding the vulnerabilities of the Web App by studying the code. Followed are auto vulnerability scanning & fuzz testing exercises.
3. After the students understand how to attack a Web App, countermeasures (defending skills and tools) can be introduced. Four exercises related to Secure Software Development Life Cycle and one exercise related to symmetric encryption are provided in this part to students.
4. The next two exercises address the non-code vulnerabilities caused by AI models.

A corresponding optional project was designed to respond to the requests from a few of students, who would like to do correlated research in this Web App Security course, an independent study, or in their capstone course.

As a summary, here is the list of hardware, Integrated Development Environment (IDE), and software used in the exercises:

Hardware:

- a ESP32-CAM IoT board (including a mini camera)
- a FTDI Mini USB to TTL Serial converter
- a mini-USB cable
- accessories (glasses, hat, makeup, etc.)
- selfies.

IDE:

- Arduino IDE with the ESP32 add-on.

Software:

- HxD Hex Editor
- Gunzip
- Cscope
- Vi
- Wireshark
- OWASP ZAP
- Microsoft STRIDE
- gcc

Figure 3: Resources Used in Exercises

Deploy the face recognition Web application to an ESP32-CAM IoT board

Students will need to learn how to **deploy** a Web application to an IoT device.

1. The application code is ready in Arduino IDE after installing the appropriate ESP32 board's add-on.
2. Students need to connect the ESP32-CAM board to a host (where Arduino IDE is running), then cross-compile the code in Arduino and download the executable from the host to the board.
3. After reset, the board is up with the face recognition Web application ready.
4. Access a pre-defined URL to reach the application's control panel, where a user can enroll a face and see if the board can recognize it later when the same face appears in front of the camera of the ESP32-CAM board.

This is a team project with 4 or 5 members in the team. Exercise hardware includes an ESP32-CAM board, an FTDI Mini USB to TTL Serial converter, and a mini-USB cable.

For most of the students, this is the first time they touch an IoT device or an embedded system. Students are curious and worried. A clear instruction manual can help them quickly accomplish this exercise so that they will build their confidence on learning a new technique/skill/method.

Through this exercise, students can explore fundamentals of IoT development and application

deployment, and they can identify the basic components of a Web application, which could be deployed on any hardware. They have learned Web application development concepts in their freshman or sophomore year but deploying a Web application to independent physical hardware is the first time for most of them.

Furthermore, this is a good chance for students to experience IoT in a Web App Security course.

Fool the AI model

The AI model integrated to the Web application can provide quick and accurate face recognition. However, it cannot guarantee 100% correctness. This exercise encourages the students to stably reproduce false positive and false negative situations, which will inspire the students to think about the deeper logic in the AI model though it appears a black box so far. This is a very whimsical yet important exercise, and how creative students are can be observed. Some students tried making funny faces to cause false negative cases. Others tried wearing glasses, hats, or even a fake beard to fool the AI model, like a fashion show. Creatively, some students directly used a printed photo and successfully made the Web application believe this is the enrolled person. Students can sample the problem the AI model has, but do not know why. Having the question not directly answered here will keep students' curiosity piqued until later they are asked to get hints from the papers about Data Manipulation, Data Poisoning, and Generative Adversarial Networks. This is a good chance for students to experience AI in a Web App Security course.

Reverse Engineering

Reverse engineering is an important practical skill that can be used in attacking a system or pen-testing. Through reading and analyzing the source code or binary program, the attacker or tester can infer the original design ideas and architecture. In this designed exercise students will be asked to determine the design of the face recognition Web application from the published C code. Either the architecture or the pseudo code of the Web application should be submitted.

There will be several challenges for students to overcome. The first one is the library code, which was not published by the application developers. Only four C source files were published, but the most fundamental functions were provided by the libraries with (debugging) symbols stripped off. Students will need either read the assembly code (not recommended to them due to the difficulty

level) or perform a Google search for the source code of the libraries.

Re-engineering

The ESP32-CAM Web App provided a complicated control panel to configure the attached camera and the face recognition parameters. However, half of these parameters are too professional to be changed by most of the students. Therefore, simplifying the control panel can reduce the confusion and distraction on the face recognition application itself. Figure 4 shows the simplified version of the control panel, which is much simple.

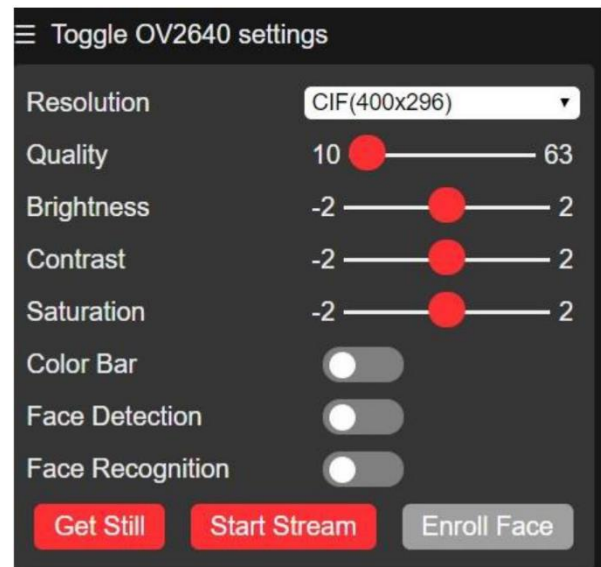


Figure 4: Simplified Control Panel of the Web App

To accomplish this exercise, students will need to overcome several small challenges:

1. Understand the original HTML code and identify the unnecessary elements on the HTML page. Because several elements have dependency relationships, before deleting one unnecessary element, students must first resolve its dependencies.
2. Because the original HTML page was compressed then saved in the ESP32-CAM flash, to replace it with the simplified page, students will need to know how to convert their HTML code to .gzip format.
3. Also, the compressed HTML page is saved as an array of hex bytes in ESP32-CAM. Students will need to convert the raw bytes of the .gzip file to a hex byte array. To complete this task, students must master one Hex Editor.

These are practical skills related to Web App Security.

Determine vulnerabilities of the Web App

Before taking this course, the students already had a solid foundation in Cybersecurity from earlier courses. Thus, it is easy for them to detect several vulnerabilities of the face recognition Web application. However, to provide full coverage, they will need to have a systematic view and comprehensively utilize their knowledge, skill, and inference capability. This exercise will provide a record of how many vulnerabilities they can find without further education. After they finish this course study, they can retry this exercise to identify what additional vulnerabilities they can find.

Fix the Buffer Overflow vulnerability demonstrated by a video

Buffer Overflow once was a top vulnerability. And the original code of the face recognition App suffered from this vulnerability. A recorded video can show how the attack vector "http://{IP}/control?var=framesize&val=512" could corrupt the face recognition Web application because the variable used to save the 'framesize' parameter is just an 8-bit integer. This attack vector was not determined through the auto vulnerability scan nor the reverse engineering because its URL is a hidden one. When a user changes a parameter through the control panel, the front-end code will generate a similar but hidden URL to update the parameter saved at the Web server. To expose the hidden URL, students will need to understand the front-end code (i.e., the HTML page), use Wireshark to capture the network traffic for analysis, or understand the back-end code.

At minimum, a student will need to master one of the following skills before they can find the Buffer Overflow vulnerability:

- Efficiently trace the front-end code in HTML and Java Script.
- Know how to filter network traffic by Wireshark and narrow down the packets of interest.
- Efficiently trace the back-end code in C and C++.

Unfortunately, it is not easy, but students will realize tools alone are not the most important factor in Web App Security. Both understanding the target's code and using automatic tools are crucial.

Auto Vulnerability Scanning & Fixing

There are many automatic scan tools for Web App vulnerabilities, which can greatly save the attacker or tester's effort during target vulnerability scanning. The Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP) (Wikipedia Contributors, 2021a) is a good one for Web App attacking or testing. Using it, students can scan the vulnerabilities of the face recognition Web App in an automatic style. Based on hints provided by the ZAP report, students will need to explore the back-end code for the best place to put the fix.

Fuzz Testing

Fuzz testing or Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program (Wikipedia Contributors, 2021b). Its purpose is to verify the reliability of the target, and it can verify the coverage of the implemented code. It is a good tool for Web App attacking or testing. In previous exercises, the 'control' hidden URL has been exposed. Thus, students can direct OWASP ZAP to feed a wide range of inputs to the face recognition Web App to see if some inputs can trigger exceptions to the App. Students should be able to experience automated testing and realize its efficiency.

Secure Software Development Life Cycle (SDLC)

To prevent vulnerabilities from being integrated into the Web App from scratch, the secure development process is crucial, which can monitor the quality of Web App development. And security is just one aspect of the product quality metrics. Thus, knowing the impacts from non-security requirement is also important. The goal of this exercise is to give the students a systematic view about the security. OWASP Software Assurance Maturity Model (SAMM) allows teams and developers to assess, formulate, and implement strategies for better security which can be easily integrated into an existing organizational Software Development Life Cycle (SDLC). This is especially important when students run/join software companies in the future.

Students are expected to read the OWASP SAMM Quick Start Guide (Wen, 2017).

Secure Software Design

Producing secure software requires conducting secure practices as early in the SDLC as possible. Design is the next phase after the customer requirement analysis. At this phase, platform, environment, constraints, components, and their

relationships as well as interactions are decided. Integrating security consideration at this phase can greatly reduce software vulnerabilities. Therefore, it can avoid the most cost for finding and fixing the vulnerabilities in downstream. In this exercise, students will need to analyze the security requirements of the Web App, then propose an architecture (update) and detail the interactions between the components in the architecture. Both sunny-day and rainy-day scenarios should be performed to exclude potential vulnerabilities.

Sequence diagrams that focus on different aspects of security should be submitted as the result of Secure Software Design.

Threat Modeling

Threat modeling is a powerful tool, which can be used to determine the attack surface of the Web App. It is useful for

- Ensuring the design complements the security objectives.
- Making trade-offs and prioritizing efforts
- Reducing the risk of security issues during development and operation.

In this exercise, students will try Microsoft's threat modeling framework, STRIDE (Spoofing, Tampering, Repudiation, Information, DoS, Elevation of privilege) to determine the attack surface of their Web App.

Best Coding Practice

Best coding practice is a kind of accumulation of experience from existing events. Though it cannot defeat all attacking attempts, it can fix most severe vulnerabilities and mitigate the attacking consequence. Students are expected to go through a check list (i.e., OWASP Secure Coding Practices Quick Reference Guide (Lala, Kumar, & Subbulakshmi, 2021)) to review and evaluate the overall security of their code.

Asymmetric Cryptography

To protect the confidentiality of the Web traffic, encryption should be conducted. Usually, asymmetric cryptography is used to generate public and private keys for symmetric key and signature distribution. The core part of the asymmetric cryptography is the difficult mathematic problem, such as the big integer factoring problem.

A Fermat Sieve-based 64-bit C program was given to students to demonstrate the big integer factoring algorithm as well as the time consumption. Because the program cannot

handle numbers larger than 64 bits, the students are expected to port the logic to a Python program, which can handle larger numbers.

Data Manipulation & Poisoning

During training, machine learning algorithms search for the most accessible pattern that correlates pixels to labels. But when a common yet trivial pattern is given a higher weight, a noise or a small piece of polluted data could cause the wrong judgement of the trained AI model. Students will need to read two articles to realize and understand the non-code impact to Web App Security:

1. The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey (Ibitoye et al., 2019).
2. Adversarial machine learning (Vorobeychik & Kantarcioglu, 2018).

Generative Adversarial Network

Generative modeling discovers and learns the patterns in input data in such a way that the model can be used to generate new examples that plausibly could have been drawn from the original dataset. In a GAN, two sub-models (the generator model for new examples and the discriminator model for classification) are trained together adversarial, until the discriminator model is fooled about half the time, meaning the generator model is generating plausible examples. Students will need to read one article to realize and understand the GANs' impact to Web App Security: Generative Adversarial Networks (GAN) A Gentle Introduction (Wang, 2017).

Capstone Projects or Research Directions

Based on the compact ESP32-CAM IoT hardware and the integrated face recognition AI model, there are three capstone projects, or three research directions suggested for students who want to try different things beyond this course study.

- **Transfer Learning** (Wikipedia Contributors, 2021c) – the AI model will generate five landmarks (points) for each input/face image. The face recognition Web App will compare enrolled one with the current input/face image to evaluate their similarity by calculating a correlation coefficient between the landmarks. If the landmarks are used as the starting point for further emotion recognition, the function of the Web App is enhanced while leaving the integrated AI model intact. Emotional information is a supplement to the face information, which will enhance the security when they are used in

access control and authentication/authorization scenarios.

- **Edge Computing** (Wikipedia Contributors, 2021d) – the face recognition AI model was trained by public datasets. However, different people have different facial features. When this AI model is deployed in a specific target environment, its application context may be limited to a small group of people. Then, one thing perhaps may be enhanced: customize the AI model for the target environment to provide quicker and more accurate response. This direction belongs to the scope of Edge Computing.
- **Data Manipulation, Data Poisoning, & GAN** (Chen et al., 2017; Ledig et al, 2017) – Examples have been seen that adding some trivial noise to the input image can mislead the AI model. Due to the black-box character of the AI model, these are hard to explain. Moreover, the traditional countermeasures for code-based vulnerabilities cannot be reused for the model-based (or data-based) vulnerabilities. Evaluating the impact and finding a solution is a good project topic or research direction.

6. STUDENT FEEDBACK

In Spring 2021, one of the authors delivered this proposed platform-based courseware to 37 senior Cybersecurity undergraduate students in the CY410 Web App Security online course. CY410 is a major core course. Its prerequisites include "Python Programming", "Java Programming", "Introduction to Cybersecurity", "Web Development", "Data Protocol Security", and "Information Security in System Administration". At the end of the semester, 59% students provided their feedbacks to CY410. Overall, the feedbacks are positive, and the average 'grade' the students gave to the instructor was 4.55 (the program's average was 4.27 and the school's average was 4.29). The students also realized the depth of this course because of so many tricky hands-on exercises. Though they never admitted it. What the students complained most was they couldn't get enough hardware for the team projects. Only one set of devices were given to a project team. Due to the COVID-19 pandemic, projects or teamwork is not sufficiently organized. Each team member individually wanted to use the hardware. Therefore, assigning a set of equipment to each student rather than each project team may further improve their feedbacks.

7. OUTCOMES

Table 1 (in the Appendix) shows the learning outcomes corresponding to the teaching objectives in section 3.

8. CONCLUSIONS AND FUTURE WORK

The ESP32-CAM IoT and AI platform provides rich features from almost every aspect for students to experience Web App Security and attracts students to touch the cutting-edge research in IoT, Edge Computing, and Transfer Learning. Totally it can support more than 16 corresponding hands-on exercises. In the future, we plan to connect database to this platform or implement a 'little' DB in it. A prototyping has been done. We will provide more details in our future paper. Furthermore, at a cost of \$15/student, this IoT platform provides a cost-effective solution for teaching Web App Security, which is the lowest-cost platform so far to our best knowledge. This means the instructors can offer sufficient hardware to the students. The teaching effect showed students gave very positive feedback to the new teaching/exercise platform. We expect further improvement in the student feedback (currently 4.55) when we equip every student with one set of the device.

9. REFERENCES

- Buyannemekh, B., & Chen, T. (2021). Digital governance in Mongolia and Taiwan: A gender perspective. Information Polity. IOS Press BV. <https://doi.org/10.3233/IP-219005>
- Chen, L., Tao, L., Li, X., & Lin, C. (2010). A tool for teaching web application security. In Proceedings of the 14th Colloquium for Information Systems Security Education (pp. 17-24).
- Chen, L. C., & Tao, L. (2011). Teaching web security using portable virtual labs. In Proceedings of the 2011 11th IEEE International Conference on Advanced Learning Technologies, ICALT 2011 (pp. 491-495). <https://doi.org/10.1109/ICALT.2011.153>
- Chen, X., Liu, C., Li, B., Lu, K., & Song, D. (2017). Targeted backdoor attacks on deep learning systems using data poisoning. arXiv preprint arXiv:1712.05526.
- Ibitoye, O., Abou-Khamis, R., Matrawy, A., & Shafiq, M. O. (2019). The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey. arXiv preprint arXiv:1911.02621

- Lala, S. K., Kumar, A., & Subbulakshmi, T. (2021). Secure web development using OWASP guidelines. In Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021 (pp. 323–332). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICICCS51141.2021.9432179>
- Ledig, C., Theis, L., Huszár, F., Caballero, J., Cunningham, A., Acosta, A., ... Shi, W. (2017). Photo-realistic single image super-resolution using a generative adversarial network. In Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017 (Vol. 2017-January, pp. 105–114). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/CVPR.2017.19>
- Liegle, J., & Meso, P. (2005). Evaluation of a virtual lab environment for teaching web-application development. In Proceedings of ISECON.
- Oh, S. K., Stickney, N., Hawthorne, D., & Matthews, S. J. (2020). Teaching Web-Attacks on a Raspberry Pi Cyber Range. In SIGITE 2020 - Proceedings of the 21st Annual Conference on Information Technology Education (pp. 324–329). Association for Computing Machinery, Inc. <https://doi.org/10.1145/3368308.3415364>
- Schweitzer, D., & Boleng, J. (2009). Designing web labs for teaching security concepts. *Journal of Computing Sciences in Colleges*, 25(2), 39–45.
- Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial machine learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, 12(3), 1–169.
- Wang, S. (2017). Generative Adversarial Networks (GAN) A Gentle Introduction. Tutorial on GAN in LIN395C: Research in Computational Linguistics.
- Wen, S. F. (2017, November). Software security in open source development: A systematic literature review. In 2017 21st conference of open innovations association (fruct) (pp. 364–373). IEEE.
- Wikipedia contributors. (2021a, May 9). OWASP ZAP. In Wikipedia, The Free Encyclopedia. Retrieved 01:10, April 18, 2022, from https://en.wikipedia.org/w/index.php?title=OWASP_ZAP&oldid=1022316463
- Wikipedia contributors. (2021b, May 21). Fuzzing. In Wikipedia, The Free Encyclopedia. Retrieved 01:11, April 18, 2022, from <https://en.wikipedia.org/w/index.php?title=Fuzzing&oldid=1024357049>
- Wikipedia contributors. (2021c, May 10). Transfer learning. In Wikipedia, The Free Encyclopedia. Retrieved 01:53, April 18, 2022, from https://en.wikipedia.org/w/index.php?title=Transfer_learning&oldid=1022394104
- Wikipedia contributors. (2021d, June 6). Edge computing. In Wikipedia, The Free Encyclopedia. Retrieved 01:55, April 18, 2022, from https://en.wikipedia.org/w/index.php?title=Edge_computing&oldid=1027237845
- Yu, H., Liao, W., Yuan, X., & Xu, J. (2006). Teaching a web security course to practice information assurance. *ACM SIGCSE Bulletin*, 38(1), 12–16. <https://doi.org/10.1145/1124706.1121348>
- Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. *IEEE Signal Processing Letters*, 23(10), 1499–1503. <https://doi.org/10.1109/LSP.2016.2603342>

Appendices and Annexures

Objective ID	Objective Description	Pass Rate (grade > 4/5)	Exercise(s)
1	Understand HTML and front-end code.	86.5%	Re-engineering
2	Describe the components of a Web App.	100%	Deploy App & Reverse Engineering
3	Deploy a Web App to a specific device.	100%	Deploy App
4	Conduct preliminary reverse engineering & re-engineering.	86.5%	Reverse Engineering & Re-engineering
5	Understand the Software Maturity Model with concentration on Security.	100%	Secure SDLC (Read OWASP SAMM)
6	Describe different vulnerabilities and their root causes.	89.2%	Determine vulnerabilities & Fix Buffer Overflow
7	Conduct pen-testing or attacking by code review, auto vulnerability scanning, and fuzz testing.	91.9%	Auto scanning & Fuzz testing
8	Describe functional and non-functional requirements and their relationships to security requirements.	97.3%	Secure software design
9	Conduct threat modeling.	81.1%	Threat Modeling
10	Follow secure coding standards to write and review code.	91.9%	Best Coding Practice
11	Describe the function of a certificate. Apply certificates in Web Apps.	N/A	N/A
12	Apply Public Key Cryptography in Web Apps.	Non-graded	Asymmetric Cryptography
13	Describe the data impact to Web App Security.	100%	Data manipulation & poisoning, and GAN papers

Table 1. Learning Outcomes

Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C)

Jeff Greer
greerj@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Ulku Clark
clarku@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

Inspired by the U.S. military's levels of warfare model, we suggest a three-level cybersecurity model around which to orient strata of understanding, expertise, and education in the cybersecurity domain. Informal observation of the current cybersecurity education landscape appears to reveal an imbalance among the levels. We introduce the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) to encourage greater balance. IVLE4C is a tool and conceptual learning model based on six interrelated knowledge domains which, when aggregated, define a modern digital enterprise and its cybersecurity posture. IVLE4C can be used to teach inter-functional and/or intra-functional skills. We contend that IVLE4C can provide three key benefits: improve cybersecurity pedagogy, enhance cross-enterprise training, and advance cybersecurity technology development.

Keywords: Cybersecurity, Education, Virtual Learning Environment, Model, Paradigm

1. INTRODUCTION AND MOTIVATION

Consider how someone unfamiliar with soccer might begin to learn the game. Shown a match, the game's objective becomes rapidly apparent – a large field with one net at each end, one ball, 11 players on each side, and lots of running and kicking of the ball. Game understanding emerges naturally, simply through observation. We might call this "learning from a top-down perspective." Note: we eschew "top-down/bottom-up learning" to avoid confusion with those terms as used in cognitive systems research (Sun & Zhang, 2004).

If that same person wishes to become proficient at playing soccer, they will need to spend time learning skills from the bottom up – dribbling,

passing, shooting, etc. Integrating their top-down understanding of the game, they will begin to see why their bottom-up-acquired skills are useful and when to employ them. As they watch and participate in matches, they will begin to make associations between in-game situations and the lower-level skills they need to further develop to become more successful.

Now, imagine trying to teach this same person the game of soccer by engaging solely in bottom-up learning activities and without revealing that the game is played 11-v-11 on a field 115 yards (105 meters) long for two 45-minute halves. How could they see the importance of training to kick a ball over 40 yards or understand the concept of offsides?

The idea of teaching someone soccer in this manner rightly seems absurd. Unfortunately, we believe this manner of teaching more closely reflects the present state of cybersecurity education than many are aware or might care to acknowledge. There is tremendous focus on technical cybersecurity skills and great computer network-centric awareness – and rightly so. However, opportunities for learning how cybersecurity fits into an organization’s larger picture and how it links with inter/national-level guidance appears lacking.

In this paper, we generalize a conceptual three-level framework of cybersecurity perspective derived from the U.S. military model of warfare. This framework provides a useful paradigm for thinking about varied cybersecurity perspectives, needed full spectrum cybersecurity expertise, and broad-range complementary approaches to cybersecurity education. The model helps identify a gap in current cybersecurity education efforts for which we introduce and describe the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) to facilitate advanced skill development (Von Glasersfeld & Steffe, 1991). (*We pronounce IVLE4C as “I will foresee” with slightly German-accented English*).

2. EDUCATION MODEL GAP IDENTIFICATION

The U.S. Army’s capstone operations manual, which endeavors to set forth fundamental doctrinal concepts, traces its roots back to Baron von Steuben’s 1779 Regulations for the Order and Discipline of the Troops of the United States. The manual undergoes periodic review and revision to reflect the evolving needs of the U.S. and the changing nature of warfare. With the 1982 revision, the conceptual three-level warfare model (Figure 1) was introduced to modern U.S. military theory (Department of the Army, 1982). The model has been accepted, refined, and now occupies a central position in the joint doctrine for all services – Army, Navy, Air Force, Marines, and Coast Guard (Joint Chiefs of Staff, 2017a).

This unifying model was important and useful to the armed forces and the U.S. because:

War is a national undertaking which must be coordinated from the highest levels of policymaking to the basic levels of execution. Strategic, operational, and tactical levels are the broad divisions of activity in preparing for and conducting war. While the principles of war are appropriate to all levels, applying them

involves a different perspective for each. (Department of the Army, 1982, p. 2-3)

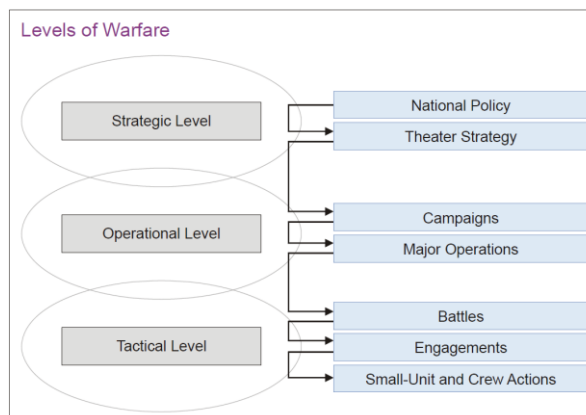


Figure 1: Levels of Warfare (Joint Chiefs of Staff, 2017a, Figure I-2)

This jointly-accepted, three-tier model provides a useful abstraction of warfare and offers a perspective that permits military units across the services and conducting various kinds of operations to speak a common language and act with unity of effort.

With modification, this model seems well suited for framing cybersecurity efforts at different strata and useful for thinking about how they tie together. Analogical and direct comparisons between war and cybersecurity have become common with journals and conferences devoted to or regularly featuring articles on cyberwarfare, including the International Conference on Cyber Conflict (NATO Cooperative Cyber Defence Center of Excellence, 2021), the Small Wars Journal (Small Wars Foundation, 2021), and the Cyber Defense Review (Army Cyber Institute, 2021). While levels of warfare are occasionally referenced, extending this model to cybersecurity education is, to our knowledge, new.

Luijff and Healey (2012) added a policy level on top of the three-level military model to construct a four-level “generalized tool for analysis” (p. 111) that “can be applied as an instrument to study the much broader context of organizational decision-making structures in government.” Raymond et al. (2014) referenced the three-level model when introducing the concept of key terrain at the four cyber planes: supervisory, cyber persona, logical, and physical (Raymond, et al., 2013). Schulze (2020) used the “three levels of warfare heuristic” (p. 184) to examine the utility of military cyber actions at each level.

In our derived model (Figure 2), we change the military-specific vocabulary to reflect the perspective from which cybersecurity efforts are being viewed: Government/Industry (GVI), Enterprise Leadership (EL), and Enterprise Employee (EE).

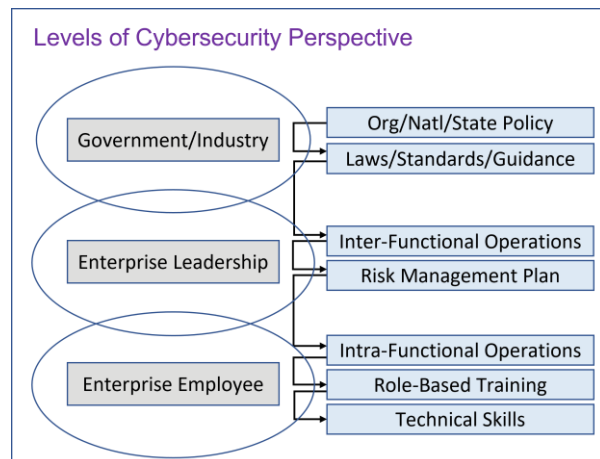


Figure 2: Cybersecurity Perspective Model

At the GVI level, political leaders issue directives, executive orders, etc. to set national/state policy, legislative bodies pass laws, and agencies/industry bodies provide guidance on best practices/standards. Enterprise leaders at the EL level, whether government or commercial, for or non-profit, public or private, create enterprise policies, procedures, and processes that support inter-functional operations and comply with and/or are influenced by laws, standards, and other guidance. The enterprise risk management plan is a key product generated at the EL level. Enterprise employees at the EE Level fill specific roles and acquire technical skills to conduct intra-functional operations and securely install, configure, and operate digital devices.

While reasonable people might prefer different words to describe the levels, we believe many will find the Cybersecurity Perspective three-level model as useful for thinking about cybersecurity as the military has found their model for thinking about warfare.

Key to the military model's enduring usefulness, and the version we adopt for cybersecurity, is that the boundaries are not rigidly defined, but rather provide a flexible linkage of efforts from top to bottom. Accepting this model as an acceptable way to view the cybersecurity domain, we then recognize that we have a need for experts at all three levels that are heavily versed at their respective tier, but that are also capable of contributing to the other tiers.

Continuing with the three-level paradigm, we propose the complementary model, *Required Cybersecurity Expertise* (Figure 3). When thinking about the various kinds of cybersecurity expertise needed across the spectrum, we identify policy, management, and technical expertise. We change the shapes representing these concepts to reflect the need for robust expertise among the levels. For example, cybersecurity technical expertise is broadly required across the entire EE level, but also required to a lesser extent at the EL and GVI levels. Cybersecurity policy expertise reflects an inverse image – broad requirement across the GVI level and more narrow need progressing down through the EL and EE levels. Cybersecurity management expertise of enterprise leaders and functional leaders is broadly required at the EL level and to a lesser extent both up and down to the GVI and EE levels respectively.

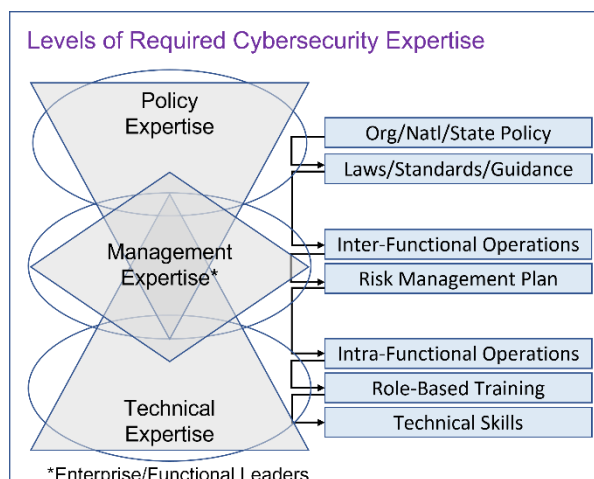


Figure 3: Required Cybersecurity Expertise

To create a stable of experts with the requisite expertise requires educational efforts across all levels; however, the current state of cybersecurity educational effort appears to have an imbalance that we believe is reflective of Figure 4 and that we will discuss in the next section. Figure 4 should be viewed as an abstract relative comparison. We are not suggesting that for every EE level workforce development course there should be one for EL and GVI development, but rather, that whereas it is plausible that current educational efforts are fully meeting EE level requirements, they are likely not meeting EL and GVI needs.

In this paper, we suggest that creating a conceptual learning environment will help grow and mature the cybersecurity pedagogy of the middle level – the EL view. It is at this level that

we will focus the paper starting in section 4. Just as the military's "operational level of warfare links the tactical employment of forces to national strategic objectives," (Joint Chiefs of Staff, 2017b, p. xi), we believe cybersecurity efforts at the EL level are vital for translating policy at the GVI level to actionable technical implementation at the EE level.

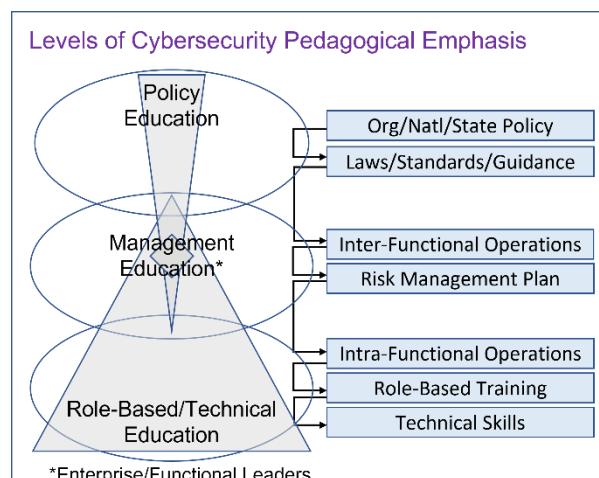


Figure 4: Current Levels of Cybersecurity Pedagogical Emphasis

3. CURRENT CYBERSECURITY EDUCATION LANDSCAPE

Traditional cyber ranges, by design, provide a computer network-centric viewpoint and focus on technical security. An early cyber range created to teach cybersecurity technical skills to college students is the IWAR laboratory (Schafer, Ragsdale, Surdu, & Carver, 2000). Created on premises at West Point, the isolated laboratory network fit into one classroom and consisted of machines built in the early-mid 1990s. This type of technically-focused cybersecurity learning environment proliferated rapidly – evolving and accelerating with the widespread adoption of virtual machines (VM) and web-based access.

Whether virtualizing a configurable network locally for computer science students (Du & Wang, 2008), providing non-engineering students exposure to hacking activities between two VMs on a laptop (Stoker et al., 2013), or hosting an open-source, publicly available, web-based learning [platform](#) on which anyone with interest can begin learning about cybersecurity (Kalyanam et al., 2020), technical-level cybersecurity educational innovations and opportunities abound. Outside of the physical and virtual classrooms, technical-level activity and competition-based cybersecurity events are

seemingly everywhere and include, among other things, capture the flags ([CTFs](#)), tournament-structured events like the National Collegiate Cyber Defense Competition ([CCDC](#)) initiated in 2004, and [CyberFIRE](#)-type cybersecurity investigation training events (Frost & Stoker, 2020) established in 2009. Technical cybersecurity education at the EE level is deep, wide, feature rich, and continues to expand.

At the other end of the perspective hierarchy, cybersecurity policy education opportunities providing a GVI-level perspective exist but are smaller in number and seem to cater to a select group. Often, the education is embedded in traditional policy-style courses designed to give future policy makers a level of cyberliteracy that will allow them to "understand a particular issue and synthesize the ramifications into other aspects of national security" (Kessler & Ramsay, 2013). Events supporting policy-level cybersecurity education also exist, the first perhaps taking place in 1996, titled "The Day After... in Cyberspace" (Anderson & Hearn, 1996). Since 2012, the Atlantic Council has hosted "Cyber 9/12 Strategy Challenge" [events](#) where students compete in "developing policy recommendations tackling a fictional cyber catastrophe" (Atlantic Council, n.d.).

A good indicator of the imbalance we perceive at the EL level may be found among the data on the CyberSeek cybersecurity supply/demand [heat map](#) (2021) webpage. A comparison of certification holders to job openings indicates that the entry-level Security+ certification is ~300% oversubscribed, while the Certified Information Systems Security Professional (CISSP) population would need to increase nearly 18% just to meet current demand. And, while there are some, e.g., Jacob et al (2018), who appear, like us, to recognize that current cybersecurity education efforts are overly weighted at the technical EE level and have voiced concern, we are unaware of an existing effort/system that captures the cybersecurity perspective of the EL level for the purposes of providing a virtual enterprise-level cybersecurity view. The lack of learning environment support to the EL level motivates our work on IVLE4C.

4. CONCEPTUAL LEARNING ENVIRONMENT

Traditional K-12 and post-secondary students do not typically have enterprise-level experience, so we propose to bring the enterprise into the classroom. We believe the primary value of IVLE4C will be in helping students lift and shift their view from the parts to the whole. With much

of the cybersecurity pedagogy focused on transactions among digital devices, students unsurprisingly tend to develop a head-down, computer network-centric view.

Motivating the Idea

Our guiding precept – coined Greer’s Truism – is that: *it is impossible to defend what cannot be visualized and described*. Therefore, it is essential to address the student enterprise knowledge gap before attempting to teach the means for assuring enterprise cybersecurity. Using IVLE4C will bring an EL perspective into the classroom, abstract away many of the technical details, and help students think about defending an enterprise rather than specific digital devices. Visualizing and describing an enterprise are challenging because of the operational scale, technical complexity, and geographic footprint involved. It is important to focus students on decision making for enterprise defense to achieve required cybersecurity objectives related to protection of assets and continuity of operations.

To help motivate and clarify this idea, consider the pervasive use of cloud-based services. Students contemplating threats & vulnerabilities to Amazon Web Services (AWS) might have only an abstract idea of AWS as virtual machines running “somewhere” out in the internet cloud. There is something about being able to see an actual AWS facility (Figure 5) that can make it feel real for students, capture their imagination, and expand their understanding of the enterprise that requires protecting.

Students need to see a modern digital enterprise from the viewpoint of an enterprise leader to properly understand enterprise cybersecurity. To our knowledge, there is no virtual learning user interface currently designed for this purpose.

In order to improve students’ understanding of and classroom experience with enterprise cybersecurity (the EL level in [Figure 2](#)), IVLE4C will create and integrate six different enterprise views into a single environment as outlined in [Appendix A](#) and enumerated here:

1. **Enterprise Operating Environment:** a 3D view of the world in which all enterprises operate.
2. **Enterprise Being Defended:** a geo-located view of one or more enterprise buildings being defended.
3. **Enterprise Digital Technology Stack:** a view of the digital technology (hardware, software, network communications, etc.) deployed in an enterprise's front office, back

office, production operations, and field for mission achievement.

4. **Enterprise Supply Chain:** a geo-located view of the enterprise/building’s supply chain that is purpose built for fulfillment of enterprise needs.
5. **Known Enterprise Threats & Vulnerabilities:** a web view of open-source intelligence needed for developing threat intelligence and identification of known vulnerabilities.
6. **Enterprise Risk Management Plan:** a risk register for capturing identified risks, their assessment, treatment, and selected security controls for enterprise defense.

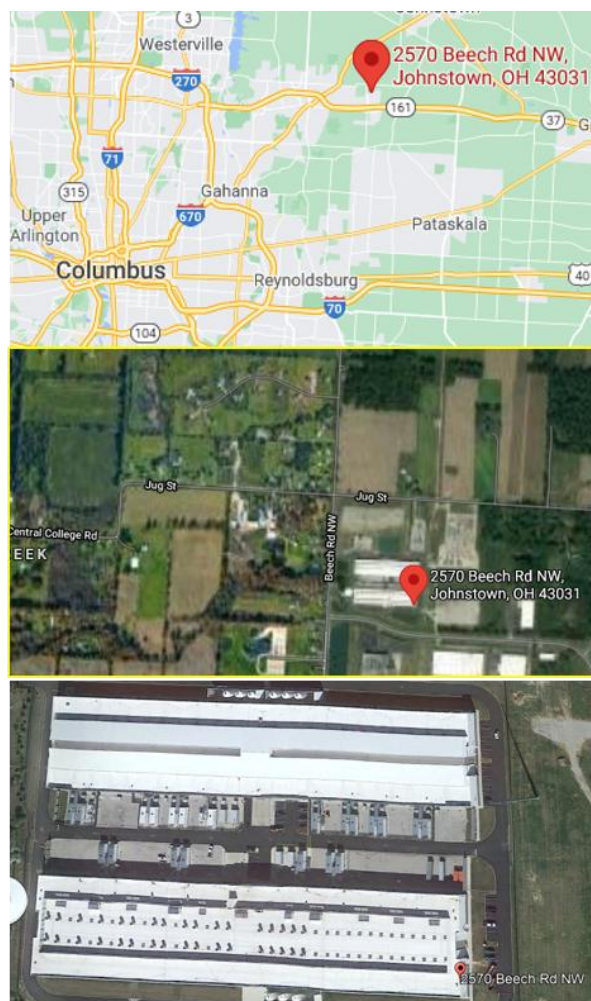


Figure 5: Three different-scale Google Maps views of the Johnstown, OH AWS facility (AWS facility, 2021)

Two-Level Conceptual Learning Model

Integrating all six enterprise views into a single virtual learning environment promotes conceptual learning at two levels. First, each individual view provides its own conceptual

learning opportunity for the topic matter contained within the view. For example, the notion of a digital technology stack, built for mission achievement, is an important cybersecurity topic in and of itself because students need to understand its architecture and inherent vulnerabilities. Second, the content in all six views is needed to create a conceptual learning opportunity for students at the enterprise or system level. There are relationships between the content in the discrete view topics that a student needs to understand before they can create a viable cybersecurity plan. For example, students need to develop an understanding of how cybersecurity controls are applied to an enterprise, its digital technology stack, and supply chain. Affording students with a two-level conceptual learning opportunity will accelerate their skill development and effectiveness. Further information on the views, their content, and use for creation of learning opportunities follows.

Learning Opportunities

Learning opportunities arise when all six views are integrated into a single virtual learning environment.

- Students will be able to see an actual image of a digital enterprise being defended and its operating environment versus imagining an abstract, nondescript enterprise.
- Students will better understand external versus internal threats once they draw a security demarcation boundary around the physical enterprise location(s).
- Students will develop better awareness of different digital technology stack designs based on enterprise type and strategy for mission achievement. Concepts like the Open Group's Architectural Development Method (ADM) will help students understand the functionality provided by digital technology in the context of enterprise requirements. Similarly, the Information Technology Infrastructure Library (ITIL) can be shown as a means for operating the digital technology stack for secure service delivery. Key to cybersecurity is the risk while using the digital technology stack which needs to be understood and treated.
- Students will be able to visualize an actual purpose-built supply chain that fulfills enterprise needs. Key is the number of suppliers and inter-action link types that exist between the enterprise being defended and its suppliers. This includes both traditional physical transport of goods and service technicians along with data transport over telecommunication circuits for remote

delivery of digital services. A supply chain represents a large and porous attack surface that is increasingly being exploited. Rendering the supply chain will promote student awareness of third-party supplier risk and the need for treating it.

- Students will become more effective in assuring cybersecurity once they learn how to assess a modern digital enterprise and its operating environment. It is common knowledge that there is no one-size-fits-all approach to cybersecurity for all enterprises. Tailoring the cybersecurity plan to the enterprise is promoted as a best practice. To do this, a student needs to have a baseline understanding of the enterprise being protected, its digital technology stack, and its supply chain. With this knowledge, it is then possible for a student to review open-source intelligence for identification of motivated threat actors and their attack tactics, techniques, and procedures (TTPs).
- Students need to become more effective in assuring enterprise cybersecurity. This can be accomplished by recording specific identified risks in a risk register. These risks can then be assessed and ranked based on probability of occurrence and enterprise impact. Each identified risk provides an opportunity for a student to determine an appropriate risk treatment using one of the seven options identified in ISO 31000 (ISO/IEC, 2019a). When deploying a physical, technical, legal contract, or policy security control, it is important for a student to link the security control to the enterprise being defended, its digital technology stack, or its supply chain. The cost of a cybersecurity risk management plan needs to be further assessed in terms of its cost and the risk appetite of enterprise leadership.

Creating Six Views Leads to a Seventh

The underlying data set, developed while creating the six views, is valuable and useful for creating a seventh view that is important for enterprise leadership and student learning. The seventh view is a near real time dashboard with descriptive statistics useful for better understanding and communicating about the enterprise and its cybersecurity plan. This information is essential for identifying enterprise leader control points for mission achievement and differentiation of normal versus abnormal operating conditions. An example of supply chain descriptive statistics includes the number of cyber suppliers in the supply chain. Of this number, it is important to know the number of trusted

suppliers. If a supplier is deemed to be trusted then what is the basis of trust, etc.

IVLE4C Architecture

IVLE4C is logically depicted in Figure 6. Think of it as a special variant or analog of a traditional computer aided design or engineering workstation. Instead of being used to design products or buildings, it will be used to design or document a digital enterprise and its cybersecurity risk management plan. Intended IVLE4C users are students, teachers, researchers, and working professionals. Users will input information required for decision making and resultant output will create the six views described above. The seventh view, with descriptive statistics, will automatically calculate as information is entered. Analysis of an enterprise being defended will be saved as a file instance for future review and use.

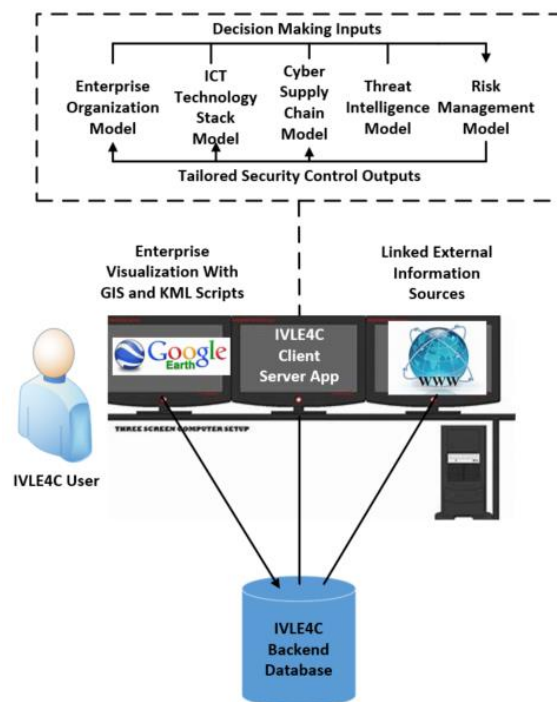


Figure 6: IVLE4C Logical Design

Expected Benefits

The expected benefits that will accrue to IVLE4C users include:

- Teachers will be able to create grade and class appropriate lessons using varying levels of input or description resulting in abstraction for delivery of key educational outcomes.
- As a client server web application, IVLE4C is extensible down to the student or working professional level as a VM session where they

can participate in hands-on learning experiences. Working to secure a named enterprise will result in a richer student learning experience.

- Researchers will be able to comparatively analyze different enterprises in terms of their unique digital technology stacks, supply chains, and threat environments using a standard documented format.

5. DISCUSSION

With increasing frequency and impact, enterprises are being attacked and disrupted. In May 2021, President Biden issued an Executive Order on Improving the Nations Cybersecurity (Executive Order No. 14028, 2021). Shortly after signing the order, he called for greater private sector investment in cybersecurity. There is a limit to what government can do when partnering with privately owned enterprises. It is one thing to write an Executive Order and suggest greater private sector investment for cybersecurity; however, intelligent action is necessary along with continuity of effort to achieve enterprise cybersecurity and resilience.

An important question to consider is how IVLE4C can be used to promote enterprise cybersecurity. At a high-level there are three opportunities worthy of consideration and action. First, is the use of IVLE4C to help achieve the National Initiative for Cybersecurity Education (NICE) roadmap objectives. Second, is the use of IVLE4C to help working professionals implement the National Institute of Standards and Technology (NIST) cybersecurity frameworks along with others like the recent Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) requirements for defense industrial base (DIB) suppliers. Third, is use of core IVLE4C capabilities as an enabler for developing new digital and cybersecurity technology.

In 2008, the U.S. Government created NICE in response to a recognized need to expand the cybersecurity workforce and improve its effectiveness ("National Initiative for Cybersecurity Education," 2021). Over time, NICE needs to evolve if it is going to be maximally effective. The threatscape is constantly changing along with the application of new digital technology for enterprise mission achievement and changes in enterprise operating practices. With IVLE4C, NICE will be better able to expand the mission scope to include better enterprise leader development including both senior executive leaders and senior functional leaders who need to provide critical leadership for

enterprise cybersecurity. IVLE4C will facilitate team inter-action and skill development. K-12 and secondary students exposed to IVLE4C will develop an appreciation for the importance of cybersecurity, career opportunities, and the means for assuring enterprise cybersecurity. Early enterprise exposure will provide a broader learning context when a student is taking technical cybersecurity courses. This approach will promote greater skill development and help reduce the time for an enterprise employee to qualify for promotion into an enterprise-level leadership position.

In 2014, NIST released the Cybersecurity Framework (CSF) for enterprise use (NIST, 2020). While useful as a risk management framework, working professionals frequently comment on the framework's complexity and the resulting difficulty in implementing it. The same holds true for other cybersecurity frameworks and standards. The challenge then is how to simplify the complex for greater effectiveness. IVLE4C can play a key role in simplifying cybersecurity risk management frameworks. This includes both improved understanding and greater clarity in deployment. With IVLE4C it is possible to virtually architect and communicate a risk management and resiliency plan. Typically developed by a team of professionals working collaboratively in a conference room, having the ability to project the key views of IVLE4C in the conference room will help promote common understanding and better decision making. IVLE4C will be a repository which will document all assumptions, decisions, and actions. This is valuable information for computer incident response teams and development of after-action reports.

As a concrete example, consider the recent ransomware attack on Colonial Pipeline ("Colonial Pipeline," 2021) that shut down 5,550 miles of pipe and disrupted the daily delivery of ~100 million gallons of gasoline, diesel, and jet fuel to much of the east coast (Testimony of Joseph Blount, 2021). Though details are not yet fully known at the time of the writing of this article, Joseph Blount, Colonial's president and CEO, stated at a senate committee hearing that the current working theory is that the attackers exploited a legacy virtual private network (VPN) profile. We could imagine, given the history of DarkSide (Shakarian, 2021), that one of the avenues of exploitation might have involved the SonicWall VPN vulnerability, CVE-2021-20016. And, we might further imagine a technical-level discussion of this SQL-injection vulnerability that "allows a remote unauthenticated attacker to

perform SQL query [sic] to access username password and other session related information" (NIST, 2021).

Contrast that thought with the idea of discussing the attack in the context of IVLE4C with the ability to link to CEO testimony video, a pipeline map (Figure 7), Google Earth views of injection stations, delivery facilities, booster stations, etc.

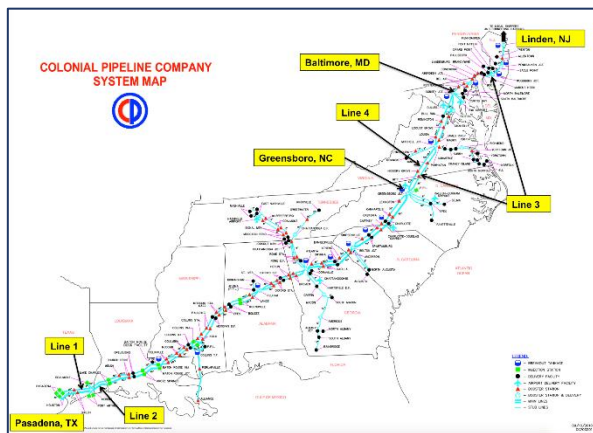


Figure 7: Colonial pipeline image (RBN Energy LLC, 2021)

Imagine IVLE4C users getting a deeper understanding of how business systems and operational systems interact and acquiring new insight into how errors and missteps at the EE level (software flaws, weak passwords, misconfigurations, clicking malicious links, opening dangerous e-mail attachments, etc.) can trigger a chain of events that disrupt the lives of tens of millions of people.

It is commonly acknowledged that early digital technology employed by enterprises was never designed for security. Over time, with successful cyber-attacks causing material damage, action was taken to create secure digital technology and operating environments for enterprise use. This trend is still ongoing and expected to carry forward into the future to address enterprise needs.

IVLE4C has a core capability that is needed for next generation cybersecurity technology. Its virtual enterprise model, views, and analytical data are essential for creating a state machine identifying normal and abnormal enterprise digital operations using AI. The notion of creating a secure digital operating environment is a top priority for an enterprise. Once the secure digital operating environment is established, applications can then be deployed to address enterprise needs. It is anticipated that intelligent

networks and smarter digital devices will communicate and interact with the state machine. IVLE4C will enable the cybersecurity focus to shift from the network or digital device to the enterprise being protected.

6. CONCLUSIONS & FUTURE WORK

In this paper, we introduce a paradigm, derived from the U.S. military three-level model for warfare, which is useful for thinking about cybersecurity understanding, expertise, and education. Analogical to the military's strategic, operational, and tactical levels of warfare, we designate three levels of cybersecurity perspective: Government/Industry (GVI), Enterprise Leadership (EL), and Enterprise Employee (EE) (Figure 2). Each level has different educational needs if government/industry leaders are going to effectively achieve policy objectives, enterprise leaders are going to assure enterprise security, and enterprise employees are going to securely employ systems and equipment (Figure 3).

To help close the education gaps identified above the technical level (Figure 4), we introduce IVLE4C, an Integrated Virtual Learning Environment for Cybersecurity Education. The IVLE4C creates a two-level conceptual learning opportunity the primary value of which will be to raise students' eyes and cybersecurity perspective from the parts of an enterprise to the whole.

IVLE4C development is ongoing. In parallel, research is being conducted on the use of IVLE4C for enterprise continuity planning as specified in ISO 22301 (ISO/IEC, 2019b). Continuity planning for resiliency runs parallel to cybersecurity and is essential for enterprise recovery as called for in the NIST Cybersecurity Framework. As IVLE4C becomes more fully developed, we anticipate that its use in a classroom environment for delivery of educational objectives will grow over time. Key will be IVLE4C's impact on the delivery of NICE K12 roadmap outcomes and cybersecurity pedagogy. Finally, as IVLE4C becomes more fully developed, exploratory work is planned for the development of a more secure enterprise and digital operating environment using new technical capabilities.

7. REFERENCES

- Anderson, R. H., & Hearn, A. C. (1996). An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After... in Cyberspace II". RAND CORP SANTA
- MONICA CA. <https://apps.dtic.mil/sti/pdfs/ADA319848.pdf>
- Army Cyber Institute. (2021). Cyber Defense Review. <https://cyberdefensereview.army.mil/About-CDR/>
- Atlantic Council (2021). Cyber 9/12 Strategy Challenge. <https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/>
- AWS facility. (2021). Google Maps. <https://goo.gl/maps/Q3g9K5RsYXJuRyzK7>
- Colonial Pipeline cyber attack. (2021). In Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack
- Cybersecurity Supply/Demand Heat Map. (2021, August). CyberSeek Project Web site. <https://www.cyberseek.org/heatmap.html>
- Department of the Army. (1982, August 20). Operations (FM 100-5). <https://cgsc.contentdm.oclc.org/digital/collection/p4013coll9/id/976/>
- Du, W., & Wang, R. (2008). SEED: A suite of instructional laboratories for computer security education. *Journal on Educational Resources in Computing (JERIC)*, 8(1), 1-24. <https://dl.acm.org/doi/pdf/10.1145/1348713.1348716>
- Exec. Order No 14028. (2021, May 12). Improving the Nation's Cybersecurity. <https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf>
- Frost, N. & Stoker, G. (2020). Novice Cybersecurity Students Encounter TracerFIRE: An Experience Report. In *Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 4901)*. <http://proc.iscap.info/2020/pdf/5337.pdf>
- International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 31010:2019 (2019a, June). Risk management - Risk assessment techniques. <https://www.iso.org/standard/72140.html>
- International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 22301:2019 (2019b, October). Security and resilience - Business continuity management systems - Requirements. <https://www.iso.org/standard/75106.html>

- Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T.A. (2018). Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors? Proceedings of the 16th International Conference on Scientific Computing (CSC'18). <https://par.nsf.gov/servlets/purl/10095246>
- Joint Chiefs of Staff. (2017a, July 12). Doctrine for the Armed Forces of the United States (JP 1). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf
- Joint Chiefs of Staff. (2017b, January 17). Joint Operations (JP 3-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_ch1.pdf
- Kalyanam, R., Yang, B., Willis, C., Lambert, M., & Kirkpatrick, C. (2020, October). CHEESE: Cyber Human Ecosystem of Engaged Security Education. In 2020 IEEE Frontiers in Education Conference (FIE) (pp. 1-7). IEEE. <https://aic-atlas.s3.eu-north-1.amazonaws.com/projects/e7299991-eb2b-4764-a849-4909e01fb07d/documents/THwopx8k3piBVcoXolb6jvstZa8bvlWHPspCJ59B.pdf>
- Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, 2, 35. <https://commons.erau.edu/cgi/viewcontent.cgi?article=1006&context=db-security-studies>
- Luijff, E. & Healey, J. (2012). Organisational Structures & Considerations. In *National Cybersecurity Framework Manual* (pp. 108-). Tallinn: NATO CCDCOE. https://www.researchgate.net/publication/261984614_Political_Aims_Policy_Methods
- National Initiative for Cybersecurity Education (NICE). (2021). In Wikipedia. https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education
- National Institute of Standards and Technology (NIST). (2021, February 4). CVE-2021-20016. <https://nvd.nist.gov/vuln/detail/CVE-2021-20016>
- National Institute of Standards and Technology (NIST). (2020, November 16). NICE Framework Resource Center History. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history>
- NATO Cooperative Cyber Defence Center of Excellence. (2021). International Conference on Cyber Conflict. <https://www.cycon.org/>
- Raymond, D., Conti, G., Cross, T., & Fanelli, R. (2013, June). A control measure framework to limit collateral damage and propagation of cyber weapons. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (pp. 1-16). IEEE. http://www.rumint.org/gregconti/publications/130324_CyCon_Malware_Full.pdf
- Raymond, D., Cross, T., Conti, G., & Nowatowski, M. (2014). Key terrain in cyberspace: Seeking the high ground. 2014 6th International Conference on Cyber Conflict (CyCon 2014), 287-300. http://www.rumint.org/gregconti/publications/Cyber_Key_Terrain_v14.pdf
- RBN Energy LLC. (2021). Colonial Pipeline Image. https://rbnenergy.com/sites/default/files/field/image/figure1_299.png
- Schafer, J., Ragsdale, D. J., Surdu, J. R., & Carver, C. A. (2000). The IWAR range: a laboratory for undergraduate information assurance education. <https://apps.dtic.mil/sti/pdfs/ADA408301.pdf>
- Schulze, M. (2020, May). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 183-197). IEEE. https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf
- Shakarian, P. (2021, May 24). Colonial Pipeline Breach: Vulnerabilities Used by DarkSide CYR3CON. <https://blog.cyr3con.ai/colonial-pipeline-breach-vulnerabilities-used-by-darkside>
- Small Wars Foundation. (2021). Small Wars Journal. <https://smallwarsjournal.com/>
- Stoker, G., Arnold, T., & Maxwell, P. (2013, October). Using virtual machines to improve learning and save resources in an introductory IT course. In Proceedings of the 14th annual ACM SIGITE conference on Information technology education (pp. 91-96). <https://dl.acm.org/doi/pdf/10.1145/2512276.2512287>
- Sun, R., & Zhang, X. (2004). Top-down versus bottom-up learning in cognitive skill acquisition. *Cognitive Systems Research*, 5(1), 63-89. <https://www.sciencedirect.com/science/article/pii/S1389041703000470>
- Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company, U.S. Senate Committee on Homeland Security and Governmental Affairs, 116th*

- Cong. (2021). <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf>
- Von Glasersfeld, E., & Steffe, L. P. (1991). Conceptual models in educational research and practice. *The Journal of Educational Thought (JET)/Revue de la Pensée Educative*, 91-103. https://www.jstor.org/stable/23767267?casa_token=k50ylvFfHwcAAAAA%3A2ntSGivNDgvk4i6F_IY4L5J3atM4gR4quf5tRnv6uZTD9RLCc9Mqz0OFCjmwdwHXowf5S0mht6qiHglPGH8cyIV-8yAizoh6zbzFml6tBp-f0Ooq3lin&seq=1&socuid=5c07442f-543a-4da1-afe1-8acf3007b596&socplat=email#metadata_info_tab_contents

Appendix A – Six Enterprise Leader (EL) Level Functional Views

(Alt + Left arrow to return to hyperlink location)

Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) Enterprise Leader (EL) Functional View Elements						
EL View- point	Enterprise Operating Environ- ment	Enterprise Being Defended	Enterprise Digital Technology Stack	Enterprise Supply Chain	Known Enterprise Threats & Vulnerabilities	Enterprise Risk Mgmt. Plan
Content Shown	3D Earth view	View of building located on the Earth's surface.	View of building ICT deployed for mission achievement.	View of supply chain vendors fulfilling enterprise needs.	View of motivated threat actors, potential attack vectors, & known vulnerabilities	View of identified risks, their assessment, treatment, and security control deployment

Teaching Case

Identity Attributes in Teaching Privacy

Yaprak Dalat Ward
ydalatward@fhsu.edu
Department of Advanced Education Programs
Fort Hays State University
Hays, KS 67601, USA

Li-Jen Lester
lys001@shsu.edu
Computer Science Department
Sam Houston State University
Huntsville, TX 77340, USA

Hook

Privacy and the *GREEN APPLE!*

Abstract

This case method presented an activity as the basis for teaching *Privacy* as part of the *Professionalism and Ethics* course of the Computer Science degree program at a state research university. The purpose of the activity was to help the students internalize the key facets of identity (*GREEN APPLE identity attributes*) as an essential starting point in teaching *Privacy*. Data collected during the activity by means of an online survey designed to capture the opinions of the students regarding identity attributes and reflections on these attributes served as a teaching and learning tool. In addition, the student progress was continually monitored by the faculty member observations and evaluations. As a result of this activity, the students were able to develop insights into identity attributes related to privacy issues; understand the language of privacy; develop more awareness of the fundamentals of diversity, equity, and inclusion; interpret the process of ethical decision-making; and acquire beneficial skills. In addition, this activity laid the groundwork for the students to interpret the privacy theories with ease.

Keywords: Diversity, Ethics, Equity, GREEN APPLE, Identity Attributes, Inclusion, Privacy, Professionalism

1. STARTING POINT OF THE ACTIVITY

As the digital landscape takes over our entire lives, computer science professionals face increasing levels of ethical dilemmas. Ethics, according to Nissenbaum (1998), "affects not only how we do things but how we think about them; it challenges some of the basic organizing concepts of moral and political philosophy such as property, privacy, the distribution of power, basic

liberties, and moral responsibility" (para. 2). To better prepare students for real-life issues of privacy from the perspectives of ethics, it is critical to offer meaningful learning which occurs when learning is active, constructive, intentional, authentic, and cooperative. One method is to use a teaching case in which students analyze, solve problems, and make decisions. According to Ellet (2007), students "give it meaning in relation to its key issues ... the goal is to come to conclusions

congruent with the reality of the case ... [and] communicate their thinking effectively" (p. 6).

In addition, teaching content by means of a case allows the students to work collaboratively and individually while engaging in dialogues involving a "stream of questions" and at times writing to "persuade the expert reader - all in a limited time" (Ellet, 2007, p. 5). Moreover, it is pivotal to use a real-life problem because it entails an "accurate causal analysis" of the problem (Ellet, p. 21); gaining insight; and being able to understand ethical decisions in real life.

This case (hereafter "activity") served as an essential starting point in teaching the unit *Privacy* as part of a required Computer Science course, *Professionalism and Ethics* (Lester, 2021). The objective of the course syllabus was "to examine the nature, need and value of well-formed ethical constructs within the digital forensics' profession" (Lester, p. 1). The method of teaching *Privacy*, particularly as it relates to the comprehension of *identity attributes* (Miller, 2021), cultural responsiveness, the fundamentals of diversity, equity, and inclusion (DEI), and being able to understand making ethical choices, had two purposes. First, this method met the internal program requirements regarding "developing ethical reasoning and/or ethical decision making" (Lester, 2021). In addition, the method complied with the Accreditation Board for Engineering and Technology (ABET) (2021) commitment to DEI: "ABET staff, volunteers and leadership are committed to the principles of diversity, equity, and inclusion through global leadership in STEM education, incorporating the highest standards of professional integrity, dignity, fairness, justice and respect for everyone" (para.1). Second, understanding the ethical implications of identity attributes allowed the students to have a social awareness, a cultural responsiveness, a solid foundation of DEI, and to be able to consider the consequential aspects of their actions when making decisions personally and professionally.

To teach this particular course, the faculty member (hereafter "instructor") developed an activity made up of five interrelated steps. The goal of the activity was to prepare the students to gain deep understanding of privacy. With this activity, the students would decipher the meaning of *identity attributes*; understand the essence of DEI; and "interrupt the fear that results in discriminatory attitudes and action" (Miller, 2021, p. 2) which would help students make more sense of ethical decision-making.

2. THE ACTIVITY PREPARATION

Prior to starting a case, explaining the "what" "why" and "how" to the students was fundamental as it provided more motivation and engagement, and eventually, leads to effective learning. The "what" "why" and "how" of this activity included three areas: 1) Types of case situations; 2) choice navigation and guidelines; and 3) learning theory and skills.

Types of Case Situations

It was essential to introduce the types of case situations including *Problems*, *Decisions*, *Evaluations* and *Rules* (Ellet, 2007) as it provided a framework for the students to "help organize their [sic] analysis" (Ellet, p. 20). This particular activity was categorized as a "problems" case, and involved understanding the notion of identity attributes, fundamentals of DEI, and ethical decision-making.

The instructor also explained that learning to understand, analyze real-life problems required to think deeply (Ellet, 2007) and be actively engaged. According to Marton and Säljö (1976) active engagement was about "*what* is learned, rather than *how much* is learned" (p. 4) and involved "deep-level processing" as opposed to "surface-level processing" (p. 4).

Due to the topic of the unit, the instructor also reminded the students that the activity was based on withholding judgement, exercising curiosity about the unfamiliar and differences and being able to adapt (Miller, 2021). In addition, this problem-case reiterated the importance of "diversity of identities" and "stepping away from euphemism...to get more specific and accurate in our goals, which can lead to more substantive and accurate conversations and strategies" (Bolger, 2020, para. 14).

Choice Navigation and Guidelines

Given that the activity required the students to "embark on the complex series of choices" (Duncan, Kim, & Soman, 2021, pp.100-101), leading to ethical decision-making, the students needed guidelines as iterated by Duncan et al., "one practical approach to help individuals navigate complex choice environments is to provide them with guidelines-in particular, a roadmap to help them make....decisions" (p. 97). The activity guidelines enabled the students to "convert a complex goal choice into concrete actions ... provide [sic] *vocabulary* to deal with a particular situation and a set of choice[s that are] ... *expert-driven*, meaning they come from a credible source" (p. 99).

Moreover, it was also essential to discuss the taxonomy of guidelines (*anchor*, *procedural*, and *informational guidelines*) so the students could start their learning with a solid foundation. The instructor explained that this activity would fall under *anchor guidelines* as the purpose of was to “motivate users to take action and get started” (Duncan et al., p. 101).

Furthermore, it was necessary to understand how real-world organizations functioned regarding “specific behavioral tendencies” (Duncan et al., 2021, p. 100) or behavioral change challenges, categorized as *compliance*, *switching*, *consumption* and *acceleration* because “most organizations were [sic] fundamentally in the business of behavioral change” (Soman, 2021, p. 4).

Learning Theory and Skills

For the students to make sense of their learnings, the instructor also provided an explanation of the different learning skills and theories (Knowles, 1977).

First, the explanations of “experiential,” “problem-solving,” and understanding of the “immediate value” (Knowles, 1977, p. 39) in the context of learning, provided the students with another layer of awareness.

Second, the students were able to understand their positionality using skill such as self-reflection, critical thinking, synthesis, data driven decision making, engaging in difficult dialogues (dialogic dialogues) and discussions, question formation, causal analysis, and being able to collaborate. As part of a scaffolding strategy in teaching (Bliss, Askew, & Macrae, 1996), these skills had been covered earlier in the course, making it easier for the students to anticipate the expected challenges in this particular unit, *Privacy*.

Third, given that the activity involved both individual and group work, it was important for the students to understand what individual and shared learning entailed: “Individual learning is tightly coupled with how the collectively created knowledge evolves. Individuals learn more if a shared understanding is created in the group” (Ley, Seitlinger, Dennerlein, Treasure-Jones, Santos, Lex, & Kowald, 2016, para. 3).

Fourth, referring to the previous unit learnings (*Ethics*, and *Intellectual Property*), the students were reminded that this activity required discussions and *deliberative dialogues* (Lester & Dalat Ward, 2019) on sensitive topics such as

identity attributes, cultural responsiveness, emotions, feelings, privacy issues. Therefore, they were asked to refrain from making assumptions and to work towards openness and information sharing. They were also asked to be actively engaged in these discussions and dialogues. According to Isaacs (1999) “we need both discussion and dialogue” (p. 45). While “*discussion* is about making a decision...*Dialogue* is about exploring the nature of choice...evoking insights, which is a way of reordering our knowledge-particularly the taken-for-granted assumptions that people bring to the table” (Isaacs, p. 45). Furthermore, “a dialogue not only raises the level of shared thinking, it [also] impacts how people act, and in particular, how they act together” (Isaacs, p. 22). Because such activities required deliberative dialogues, it was essential in guiding the students to better conduct themselves during difficult “learning conversations” (Stone, Patton, Heen, & Fisher, 1999, p. 16) as opposed to using these conversations to “deliver a message” (p. 16).

3. THE ACTIVITY

The required course, *Professionalism and Ethics* consisted of four units: *Ethics*, *Intellectual Property*, *Privacy*, and the *Internet of Things*. The unit, *Privacy*, followed the units *Ethics* and *Intellectual Property*.

The course was based on instructional scaffolding which allowed the students to understand the previous concepts used iteratively throughout the activity and to move progressively (Bliss, Askew, & Macrae, 1996).

Due to the Pandemic, the course enrollment included 25 undergraduate students as opposed to 50 students.

The activity prepared the students to gain deep insights into identity attributes, leading to better understanding the implications of privacy, fundamentals of DEI, and the process of ethical decision-making.

The role of the instructor was to provide guidance, direction, and explanation of the process, function as a facilitator to monitor and guide group discussions and serve as an observer and spectator.

This activity consisted of five interrelated steps: Step 1. Exploration: Dissecting a Privacy Problem; Step 2. Awareness: Diagnosing Identity Attributes; Step 3. Self-Reflection and Introspection: Recognizing Self; Step 4.

Connectivity: Thinking Together; and Step 5. Action: Understanding Ethical Decision-Making.

Allotted time for Steps 1, 3, 4 and 5 were 45 minutes and for Step 2 was 90 minutes. An additional 45 minutes was required for the post activity.

The summary of the steps is shown in Table 1. The detailed instructions for the steps are included in the appendices.

Steps	Short Description of Step Exercises
Step 1. Exploration: Dissecting a Privacy Problem (Time: 45 minutes)	In groups, using guiding questions, students evaluate privacy policies (see Appendix A).
Step 2. Awareness: Diagnosing Identity Attributes (Time: 90 minutes)	Instructor explains the attributes of the GREEN APPLE survey (see Appendix B). Students take the survey (see Appendix B). Instructor shares survey results and holds an informal discussion (see Appendix C).
Step 3. Self-Reflection and Introspection: Recognizing Self (Time: 45 minutes)	Based on their individual survey results, students reflect on their own identities, behavior choices (see Appendix D).
Step 4. Connectivity: Thinking Together (Time: 45 minutes)	Based on the survey results, in groups of 4-5, students engage in dialogues, discussions using guiding questions (see Appendix E). Then, students share their group outcomes.
Step 5. Action: Understanding Ethical Decision-Making (Time: 45 minutes)	Students create model privacy labels in groups and share their models (see Figure 1 and Figure 2, and Appendix F).

Table 1: Summary of the Activity

The Five Steps of the Activity

Step 1. Exploration: Dissecting a Privacy Problem. This step required the students to use "reasoning and evidence" (Ellet, 2007, p. 8) to explore and evaluate real-life texts and the language of such texts in relation to privacy issues.

Because a real-life proof was pivotal, the instructor shared three publicly available policies which came from the official sites of Apple, Google, and Microsoft (see Appendix A). The policies covered topics ranging from software,

application to apps and devices. The instructor also provided guiding questions (see Appendix A) for the students to be able to "take apart the language of the text to explore its critical assumptions" (Patton, 2015, p. 126).

Prior to evaluating the policies, the instructor prepared the students to act like qualitative researchers (see Appendix A) and decipher the texts using *linguistic inquiry* (Guest, MacQueen, & Namey, 2012, p. 51).

Acting like judges in groups of 4-5, each group explored the word choices and discussed the reasons for these choices, paying special attention to key-word-in-context (KWIC), as part of *thematic analysis* (Guest, MacQueen, & Namey, 2012).

The guiding questions allowed the students to carefully review, critique, and analyze as well as compare and confirm the outcomes of the statements and resulted in understanding what privacy meant in the real world. Connecting to real world problems better prepared the students to understand what was ethically good and bad; and right and wrong.

As a result of deciphering these policies, the students identified the following challenges: These policies were lengthy; they included legal terms making it difficult for laypeople to understand; and the personal data protection sections and options looked incomprehensible.

After having identified the problems related to the privacy policies as "a significant outcome...something important...but we don't know why" (Ellet, 2007, p. 21), the students were faced with making choices, decide, and evaluate "the worth, value, or effectiveness" (p. 23) of the appropriate criteria. Making choices would entail taking consumers into account and creating an ideal policy format made up of clear language.

Evaluating the quality of the authentic privacy policies of real businesses allowed the students to see what privacy meant in the real world.

Step 2. Awareness: Diagnosing Identity Attributes. This step required the students to first, take the GREEN APPLE (Miller, 2021) online survey (see Appendix B). Prior to taking the survey, it was essential for the students to understand the acronym, the history of the key facets of identity and what each attribute represented so they could understand what privacy entailed and how to select criteria for an ideal privacy language (see Appendix B). The

instructor referred to the book (Miller, 2021) and explained that GREEN APPLE was developed to build culturally responsive communities and included 10 attributes: "Gender Identity, Religion, Ethnicity and Race, Economic Class/Socioeconomic Status, Name/Family, Age, Place (Geography, National Territory), Perception of Belonging, Language, Exceptionality-Gifted or Challenged."

Once the students completed the survey, the instructor analyzed the data and shared the overall rankings (see Appendix C) in an informal discussion. The students also shared their reasons for selecting their rankings. The instructor observed that sharing the reasons in an informal manner allowed the students to recognize their positionality in relation to different identity attributes vis-a-vis privacy, and to become aware of the essence of DEI. Moreover, during these conversations, the instructor observed that the students felt more relaxed and prepared in respecting the privacy of others, and in were able to have difficult conversations in a culturally responsive community.

Step 3. Self-Reflection and Introspection: Recognizing Self. This step required the students to reflect on their own survey results by taking into consideration the three guiding questions provided by the instructor (see Appendix D).

First, the instructor shared the definition of the term *reflexivity* (Patton, 2015) and what self-reflection meant so students could make sense of this task (see Appendix D). One definition was: "A sense of self is a collection of schemata regarding one's abilities, traits and attitudes that guides our behaviours, choices and social interactions followed by the definition of *introspection*, which is believed to be a reflexive, metacognitive process, attending to or thinking about oneself or what is currently being experienced by oneself" (Overgaard, 2008, p. 4953). Another definition was: "The accuracy of one's sense of self will impact ability to function effectively in the world" (Johnston, Baxter, Wilder, Pipe, Heiserman, & Prigatano, 2002 p. 1808).

Then, the instructor invited the students to "consciously reflect on...sense of self....an important aspect of self-awareness" (Johnston, et al., p. 1808).

The self-reflection step served to bring awareness to each student regarding "respecting privacy of others" with an open mindset and demonstrated

that identity attributes were fundamental in understanding what the concept of privacy entailed, what the fundamentals of DEI were, and the process of ethical decision-making.

Step 4. Connectivity: Thinking Together. This step involved the students sharing their survey results which involved sensitive discussions and dialogues. The students used the five guiding questions provided by the instructor (see Appendix E).

The students first worked in groups of 4-5. To be able to engage in effective discussions, each group assigned roles to their group members as follows: Moderator, Note-taker, Timekeeper, and Collector of Materials. Then, the groups presented their outcomes and compared notes with others.

Due to the sensitive nature of the survey results, the instructor reminded the students to refrain from drawing conclusions that might not be accurate (Argyris, 1990). The students were also asked to be open and be encouraged to exercise curiosity when discussing their results. Given that the students had already been practicing deliberative dialogues during the first two units of the course, discussing their findings became a straightforward task. They knew how to withhold judgment.

These interactions led to understanding diverse identities and the importance of building and sustaining culturally responsive communities. By discussing their survey results, the students were able to reorder their thoughts and learn how to think together (Isaacs, 1999).

Step 5. Action: Understanding Ethical Decision-Making. As Step 5, following the intense discussions and dialogues, the students were ready to implement their learnings. The requirement was to develop a model privacy label using their learnings on identity attributes.

It was important for the students to be able to distinguish the identity attributes that needed protection regarding privacy. The instructor asked the students to reflect on the language of privacy (see Appendix F). Initially, the students were instructed to evaluate the U.S. Food and Drug Administration (2021) "nutrition facts label" (para. 1) as seen in Appendix F. They would be transferring the "nutrition facts label" to create a model privacy label.

Considering what was ethically right and wrong; and good and bad, working in groups, the students selected their *Internet of Things* device

to use in this exercise. They transferred the concept of a “nutrition facts label” to creating, a model privacy label (see examples in Figure 1 and Figure 2).

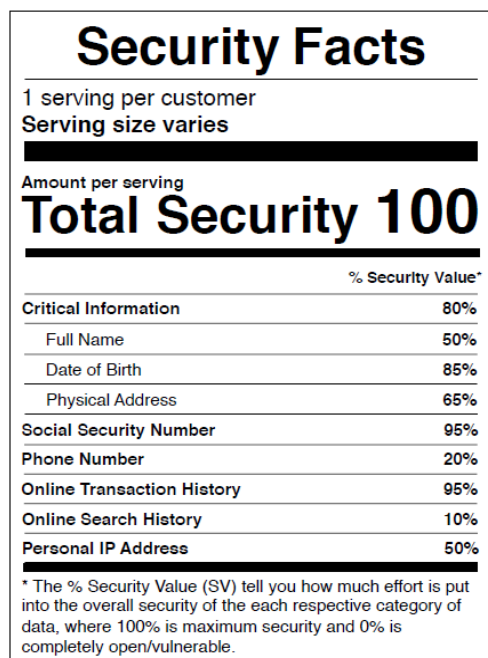


Figure 1: Privacy Label Example A

Then, they shared their model privacy labels with other groups and discussed the values of these labels. They shared their experiences regarding how they avoided ambiguous phrases to eliminate misunderstanding and misinterpretation. This step re-iterated the students’ learnings regarding how to interact with a diversified population, respect others’ privacy, and stay open-minded to accepting the cultural and demographic differences.

As a result, as observed by the instructor, the students were able to create model privacy labels with clear texts, leaving no place for ambiguity and/or misinterpretation.

4. INSIGHTS

The instructor noted the following insights as part of teaching *Privacy* by using this activity.

Instructor Observations and Evaluation. Throughout the activity, the instructor unobtrusively observed and evaluated the progress of the students through nonverbals, formal and informal interactions, “what does and doesn’t happen” (Patton, 2015, p. 383). The instructor made mental notes, transferring these notes into a notebook as “learning logs” (Patton,

2015, p. 375). These notes not only served to monitor the progress of the students but also as helped improve the course content.

Terms and Conditions of using our Medical Insurance Company Software

Note values are on a scale of 0%-100%. Percentage meaning varies, please be sure you understand what it means per section

PRIVACY 100% means you give up all of your privacy, 0% means you keep all of your privacy		
Personal Information	42%	100%
Name		100%
Age		100%
Biological Sex		100%
Email Address		100%
Payment Method		0%
Previous Insurance		100%
Social Security Number		100%
Copy of Drivers License		0%
Insurance Types		0%
Medical History		100%
Primary Doctor		0%
Estimated Yearly Income		0%
Location	0%	0%
Address		0%
IP Address		0%
INFORMATION SOLD		
IMPORTANT, ALL ITEMS LISTED HERE ARE 100% SOLD		
Information is sold to our sponsors listed below for the sole use of trying to provide you a more personalized and better health care experience. If you object to any of the following, DO NOT use our software.		
Insurance Policy		
Email address		
Name		
Age		
Biological Sex		
Medical History		
Social Security Number (note this is sold to insurance companies for them to prequalify you for insurance and NO other purpose)		
SECURITY		
ALL INFORMATION COLLECTED IS 100% SECURELY STORED, MAINTAINED, AND USED		
If any data breach occurs, you as a customer will be informed as to what the breach was, what we are doing to remedy it, and what information of yours may have been compromised		
Sponsored by: Insert a list of sponsors with the sponsors being ordered from Greatest support of our company to Least support of our company with each sponsor being separated by a comma		

Figure 2: Privacy Label Example B

The observations, particularly during the final step of the activity served as valuable feedback and revealed that the students were able to analyze and evaluate their learnings and demonstrate their understanding by means of creating successful privacy labels.

Probes and Guiding Questions. Step 1 (see Appendix A), Step 3 (see Appendix D) and Step 4 (see Appendix E) included *detail-oriented probes* and questions (Patton, 2015, p. 465) to guide the students to get a detailed picture of the activity and move forward in completing the tasks effectively. The instructor noted the way the students used these questions. Rather than a checklist, these probes and questions became “a menu of possibilities” (Patton, p. 382). They enabled the students to think critically, use their analytical and synthesis skills to manage the expected challenges.

The GREEN APPLE Survey and Survey Results. The goal of using the survey and the survey results as a teaching and learning tool was also pivotal. The online survey data provided a detailed picture of the student perceptions regarding identity attributes as it related to privacy. According to the results as indicated in

Table 2, the overall top three ranking attributes were as follows: The “**E**conomic Class/Socioeconomic Status” (one of the acronyms in GREEN) was the top ranked attribute followed by “**R**eligion” as the second, and “**P**lace (Geography, National Territory)” as the third. Sharing these rankings together with the reasons of rankings in an informal manner during Step 2 added the expected layer of awareness regarding privacy issues.

Item as the Top 3 Most Private Attribute	
Economic Class/Socioeconomic Status	83%
Religion	48%
Place (geography, national territory)	39%
Exceptionality - whether gifted or challenged	30%
Perception of Belonging	26%
Age	26%
Name/Family	22%
Ethnicity and Race	17%
Gender Identity	9%
Language (discourse community)	0%

Table 2: Green Apple Survey Results

In addition, these results served as the foundation for reflexivity during Step 3. Self-Reflection and Introspection: Recognizing Self. The self-reflection step added yet another layer of awareness encouraging self-evaluation with an open mindset. This step demonstrated that identity attributes were fundamental in grasping the concept of privacy, and the process of ethical decision-making.

Moreover, the survey results paved the way for difficult conversations as part of Step 4. Connectivity: Thinking Together. Sharing their individual responses and reflections openly showed that the students were able to have difficult conversations on sensitive topics.

Post-Activity Student Reflections. Finally, upon completing the entire activity, the instructor shared three graphs on how the students ranked the three GREEN APPLE attributes, **G**ender, **R**eligion, and **E**thnicity and Race as it related to DEI and privacy (see Appendix G). The students were asked to provide their reflections using a minimum of 60 words.

Based on these reflections, the common themes shared by the students were similar. The three following texts represent the overall perceptions of the students:

Student 1: “What I learned about attributes leading to understanding DEI by completing this

exercise was that not everyone has the same values about what should be private and what should not. I think that we should learn to accept each other's differences and not view another person differently because of it. In the work industry, you will never fully know what is “too private” of another person, so it is important to avoid asking them questions about these personal matters and above all, *respect them as a person.*”

Student 2: “I learned that all people, regardless of their abilities, disabilities, or health care needs, have the right to be respected and appreciated as valuable members of their communities.”

Student 3: “Our class's beliefs all differ, and certain information is not to be shared and should be kept private while other members may believe the complete opposite. This is the equality and inclusion aspect of the Green Apple exercise.”

Rather than a lengthy thematic analysis of the reflections, the instructor used *Wordle* (Viégas, Wattenberg, & Feinberg, 2009), a web-based tool for visualizing text (see Figure 3). The most commonly used words in the student reflections were shared with the class.

At an initial glance, the most used words included “People, Private, Ethnicity, Race, Gender, Religion.” The word “learned” was also noteworthy. This visualization helped the students see the whole picture and make more sense of the meaning of each attribute in the process of ethical decision-making.



Figure 3: Commonly Used Words in Student Reflections

5. CONCLUSIONS

This method of instruction promoted the understanding of identity attributes leading to the essentials of DEI and ethical decision-making. The perspective of the instructor was that 1) such cases can serve as a game changer, not only for

IT students, but for all students, preparing them for the constantly changing global economy and workforce. 2) Becoming more aware of the key facets of identity prepares students to better understand their moral obligations and the ethical implications of their actions whether in cyberspace or in face-to-face environments.

Teaching this activity and continually observing and evaluating the tasks, the instructor took notes on improving the course which included: 1) Add activities to emphasize the fundamentals of DEI in general. 2) Use a brainstorming and mind mapping session to identify familiar or common privacy attributes. 3) Provide more time on self-reflection and discussions on differences and similarities of identity attributes. 4) Hold a collaborative session on group reflection of learnings to further demonstrate the understanding of diverse identities. 5) Include a follow up session related to the implementation of learnings.

The authors would like to note that this paper shared the experiences of a particular group of students (N=25) at a time of the Pandemic. Under normal conditions, the class would have included an average of 50 students. With a smaller class size, it was easier for the students to share their learnings, discuss the topics. It was also easier for the instructor to deliver the content, manage the steps of the activity and observe and evaluate the student interactions and nonverbals.

To conclude, the authors would like to share one student's narrative which summarizes the value of the activity: "This exercise highlighted some key topics that some people may find uncomfortable to disclose and thus should be avoided to maintain a healthy work environment. Diversity is a good thing within people but should not be a factor in any decision. Making a decision from this would be unfair and impartial."

6. RECOMMENDATIONS

This paper presented an activity designed to teach *Privacy*. The goal of using data as a teaching tool provided the instructor with a "deep understanding of both the nature of learning and the conditions in which it is likely to flourish" (Bain, 2004, p. 84). Moreover, "because the methods work in helping students achieve, students develop faith in their instructors, and that trust becomes its own force" (Bain, p. 85).

To obtain more insight into student perceptions and student learnings, the authors recommend that additional textual and numerical data be collected by means of using instruments such as

in-depth student interviews, surveys, and/or focus group conversations.

The authors also recommend that an inductive analysis such as the applied thematic analysis (ATA) (Guest, MacQueen, & Namey, 2012) be conducted to have a more "descriptive and exploratory orientation" (Guest et al., p. 7).

7. REFERENCES

- ABET Accreditation (n.d.). Diversity, Equity & Inclusion. <https://www.abet.org/about-abet/diversity-equity-and-inclusion/>
- Argyris, C. (1990). *Overcoming organizational defenses: Facilitating organizational learning* (1st ed.). Pearson.
- Bain, K. (2004). *What the best college teachers do*. Harvard University Press.
- Bliss, J., Askew, M., & Macrae, S. (1996). Effective teaching and learning: Scaffolding revisited. *Oxford Review of Education*, 22(1), 37-61.
- Bolger, M. (2020, May 24). What's the difference between diversity, inclusion, and equity? General Assembly. <https://generalassemb.ly/blog/diversity-inclusion-equity-differences-in-meaning/>
- Dixon, N. M. (1999). *The organizational learning cycle: How we can learn collectively* (2nd ed.). Gower.
- Duncan, S., Kim, M., & Soman, D. (2021). A guide to guidelines. In D. Soman & C. Yeung (Eds.), *The behaviorally informed organization* (pp. 96-110). University of Toronto Press.
- Ellet, W. (2007). *The case study handbook: How to read, discuss, and write persuasively about cases*. Harvard Business School Press.
- Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Sage.
- Isaacs, W. (1999). *Dialogue: The art of thinking together*. Doubleday.
- Johnson, S. C., Baxter, L. C., Wilder, L. S., Pipe, J. G., Heiserman, J. E., & Prigatano, G. P. (2002). Neural correlates of self-reflection. *Brain: A Journal of Neurology*, 125(8), 1808-1814. <https://doi.org/10.1093/brain/awf181>
- Knowles, M. S. (1977). *The modern practice of adult education: Andragogy versus pedagogy* (8th ed.). Association Press.

- Lester, L. J. (2021). *COSC 4349: Professionalism and Ethics course syllabus*. Department of Computer Science, Sam Houston State University.
- Lester, L. J., & Dalat Ward, Y. (2019). Teaching professionalism and ethics in IT by deliberative dialogue. *Information Systems Education Journal*, 17(1), 4-17.
- Ley, T., Seitlinger, P., Dennerlein, S., Treasure-Jones, T., Santos, P., Lex, E., & Kowald, D. (2016). Individual and collective learning in collaborative knowledge building. *Learning Layers*. <http://results.learning-layers.eu/scenarios/individual-collective-learning/>
- Marton, F., & Säljö, R. (1976). On qualitative differences in learning: I. Outcome and process. *British Journal of Educational Psychology*, 46(1), 4-11. <https://doi.org/10.1111/j.20448279.1976.tb02980.x>
- Miller, D. L. (2021). *Honoring identities: Creating culturally responsive learning communities*. Rowman & Littlefield.
- Nissenbaum, H. (1998). *Information technology and ethics*. Routledge Encyclopedia of Philosophy. Taylor and Francis, <https://www.rep.routledge.com/articles/the-matic/information-technology-and-ethics/v-1>. doi:10.4324/9780415249126-L121-1
- Overgaard, M. (2008). *Scholarpedia*, 3(5). doi:10.4249/scholarpedia.4953
- Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage Publication, Inc.
- Soman, D. (2021). The science of using behavioral science. In D. Soman & C. Yeung (Eds.), *The behaviorally informed organization* (pp. 96-110). University of Toronto Press.
- Store, D., Patton, B., Heen, S., & Fisher, R. (1999). *Difficult conversations: How to discuss what matters most*. Penguin Books.
- The U.S. Food and Drug Administration (2021). How to Understand and Use the Nutrition Facts Label. <https://www.fda.gov/food/new-nutrition-facts-label/how-understand-and-use-nutrition-facts-label>
- Viégas, F. B., Wattenberg, M., & Feinberg, J. (2009). Participatory visualization with Wordle. http://hint.fm/papers/wordle_final2.pdf

Appendix A

Instructions for Step 1 (45 minutes)*

- **The instructor explains the task (10 minutes)**

Here are three publicly accessible privacy policies of three major companies including: 1) Apple, 2) Google, and 3) Microsoft. Please refer to the links.

Your task is to judge the worth and value of the meaning of these policies related to privacy (Guest, MacQueen, & Namey, 2012).

At this point before you go into your groups, let me present two qualitative research strategies which will be helpful in your "meaning-making process" (Patton, 2015, p. 3). Think of this as learning a beneficial skill which may be useful in your work.

These policies are considered texts. Take into consideration two strategies: 1) You can review the "key-word-in-context," or KWIC....like exploring and tagging text (Guest, MacQueen, & Namey, p. 51). You identify "a word as the locus for a theme or concept in a body of text without predefining the textual boundaries of the locus" (p. 51). 2) You can refer to "codebook development" (p. 52) which helps us sort the statements into categories, types, and relationships. The idea is to evaluate and interpret the meaning of these words, phrases and make sense.

- **The students work in groups of four or five**, using the following questions. They these policies apart, review the language, the word choices. **(30 minutes)**

1. Regarding your learnings, what meaning is conveyed in these three statements?
2. What are the specific elements which stand out?
3. Which words/phrases are clear? Why?
4. Which words/phrases are confusing? Why?
5. How would you change the parts or the statement which are confusing and why?

- **The groups share their "meaning-making process"** with class and compare notes. **(20 minutes)**

*** Instructor's Note:** Allocated time for each step is added to give the reviewer(s) an idea. Given the class size (N=25), and the nature of the tasks, timing worked well for this particular class. Understandably, the timing can be adjusted depending on the class size and the user.

Appendix B

Instructions for Step 2 (45 minutes)

- The Instructor explains the GREEN APPLE Acronym and Identity Attributes (20 minutes)**

Before you take the GREEN APPLE survey to rank the top five attributes related to privacy (based on your perceptions), let's review the acronym GREEN APPLE and each identity attribute including "Gender identity, Religion, Ethnicity and Race, Economic Class/Socioeconomic Status, Name/Family, Age, Place (Geography, National Territory), Perception of Belonging, Language, Exceptionality-Gifted or Challenged" (Miller, p. 3).

*** Instructor's note:** At this point, it is important to refer to the book (Miller, 2021) and talk about using Cultural Identity Literature (CIL) to bring awareness to differences as it relates to privacy.

Miller, D. L. (2021). *Honoring identities: Creating culturally responsive learning communities*. Rowman & Littlefield.

- The students take the GREEN APPLE Online Survey (25 minutes)**

Now you will take the GREEN APPLE online survey. Click on the following link to access the survey: XX. Rank your top 5 attributes (1 being the most important) related to privacy. Once you complete the survey, I will share the overall rankings with you so we can have a conversation on these rankings and your reasons for these ranking.

***The GREEN APPLE Survey Instructions:**

Below are the GREEN APPLE identity attributes: "Gender Identity, Religion, Ethnicity and Race, Economic Class/Socioeconomic Status, Name/Family, Age, Place (Geography, National territory), Perception of Belonging, Language, Exceptionality-Gifted or Challenged."

Rank your top five attributes (1 being the most important) related to privacy issues. Using the column "Reasons" (in a couple of sentences) provide your reasons for your ranking.

For confidentiality, the survey does not require your personal information.

GREEN APPLE Identity Attributes	Your Top Five Identity Attributes	Reasons
Gender Identity	1.	
Religion	2.	
Ethnicity and Race	3.	
Economic Class/Socioeconomic Status	4.	
Name/Family	5.	
Age		
Place		
Perception of Belonging		
Language		
Exceptionality-Gifted or Challenged		

***Note:** The instructor used Qualtrics for this survey.

Appendix C

Instructions for Step 2 (45 minutes)

- **The instructor shares the GREEN APPLE survey results (10 minutes)**

Below are your GREEN APPLE Survey results which display your selected rankings. Let's review your overall rankings and your reasons and have a conversation on and what the rankings reveal and how these attributes relate to privacy.

Student Priority Order Regarding Privacy from the GREEN APPLE Attributes	
Economic Class/Socioeconomic Status	83%
Religion	48%
Place (geography, national territory)	39%
Exceptionality - whether gifted or challenged	30%
Perception of Belonging	26%
Age	26%
Name/Family	22%
Ethnicity and Race	17%
Gender Identity	9%
Language (discourse community)	0%

- **The instructor starts an informal discussion sharing the survey results (35 minutes)**

* Instructor's note: It is important to refer to the book (Miller, 2021) and talk about the key facets of identity, cultural responsiveness, and demographics.

Miller, D. L. (2021). *Honoring identities: Creating culturally responsive learning communities*. Rowman & Littlefield.

Appendix D

Instructions for Step 3 (45 minutes)

- **The instructor explains reflexivity (10 minutes)**

Remember as part of Step 2, you took a survey and ranked the GREEN APPLE attributes from 1 to 10.

Now I invite you to “consciously reflect on...sense of self....an important aspect of self-awareness” (Johnston, et al., p. 1808) regarding “respecting privacy of others” with an open mindset. This will allow you to understand what the concept of privacy entails, and how to make ethical decisions.

For this step, I ask you to review your own survey results and become aware of your own voice and perspective. Use to following questions, analyze your responses: 1) How did you rank your attributes? 2) What does your top-ranked attributes reveal? 3) What shaped these views?

But before you go on, let’s review *Reflexivity* in detail, what it entails. First, according to Patton (2015): “Reflexivity is a critical self-exploration....it [sic] involves self-questioning and self-reflection...is to undertake an ongoing examination of what I know and how I know it” (p. 70).

Second, let’s consider two more definitions of self-reflection. What do you think of these definitions? One definition is “a sense of self is a collection of schemata regarding one’s abilities, traits and attitudes that guides our behaviours, choices and social interactions followed by the definition of *introspection*, which is believed to be a reflexive, metacognitive process, attending to or thinking about oneself or what is currently being experienced by oneself” (Overgaard, 2008) p. 4953). Another definition is: “The accuracy of one’s sense of self will impact ability to function effectively in the world” (Johnston, Baxter, Wilder, Pipe, Heiserman, & Prigatano (2002, p. 1808).

- **The students individually reflect on their own survey results (15 minutes)**
- **The whole class informally discusses their personal survey results and reflections (20 minutes)**

Appendix E

Instructions for Step 4 (45 minutes)

- **The Instructor explains the survey results, explains the task and the role of probes (10 minutes)**

Here are the overall results of our survey. Now that you discussed your individual results, you will have discussions and deliberative dialogues with your peers to discuss the overall findings of the survey. You will use the following five questions.

Remember you know how these discussions work. Given that you had already been practicing deliberative dialogues during the first two units of the course, discussing the survey results should be a straightforward task. You know how to withhold judgment. Please refrain from drawing conclusions that might not be accurate (Argyris, 1990). Please remain open. I also encourage you to exercise curiosity when discussing these results.

Let's review what these dialogues entail:

1. Share your input regarding why 83% of you considered the attribute "**Economic Class/Socioeconomic Status**" as the highest ranked GREEN APPLE attribute.
2. Share your input regarding why 48% of you considered the attribute "**Religion**" as the second highest ranked GREEN APPLE attribute.
3. Share your input regarding why 39% of you considered the attribute "**Place**" as the third ranked GREEN APPLE attributes.
4. Are your top three selected GREEN APPLE attributes aligned with your peers' GREEN APPLE attributes? If not, please share your views regarding why your top 3 selected attributes are important for you.
5. Taking into consideration your newly discovered awareness of privacy and diversity, equity, and inclusion, how would you use these GREEN APPLE rankings in your future career(s)?

- **Working in groups of 4-5 the students have discussions and dialogues (25 minutes)**

The instructor unobtrusively observes interactions, nonverbals, language of the students.

Reference for deliberative dialogues:

Lester, L. J., & Dalat Ward, Y. (2019). Teaching professionalism and ethics in IT by deliberative dialogue. *Information Systems Education Journal*, 17(1), 4-17.

- **The groups share their notes (10 minutes)**

Appendix F

Instructions for Step 5 (45 minutes)

- The instructor explains the task (5 minutes)**

Review the information on “nutrition facts-label” as presented on the U.S. Food and Drug Administration webpage <https://www.fda.gov/food/new-nutrition-facts-label/how-understand-and-use-nutrition-facts-label#NutritionFactsLabelVariations>. The example below shows a common nutrition label of pretzels.

Nutrition Facts			
3 servings per container			
Serving size 3 pretzels (28g)			
Calories	Per serving	Per container	
	110	330	
	<small>% DV*</small>	<small>% DV*</small>	
Total Fat	0.5g 1%	1.5g 3%	
Saturated Fat	0g 0%	0g 0%	
Trans Fat	0g	0g	
Cholesterol	0mg 0%	0mg 0%	
Sodium	400mg 17%	1200mg 52%	
Total Carb.	23g 8%	69g 24%	
Dietary Fiber	2g 7%	6g 21%	
Total Sugars	<1g	3g	
Incl. Added Sugars	0g 0%	0g 0%	
Protein	3g	9g	
Vitamin D	0mcg 0%	0mcg 0%	
Calcium	10mg 0%	30mg 2%	
Iron	1.2mg 6%	3.6mg 18%	
Potassium	90mg 0%	270mg 5%	

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

This exercise will help you develop a similar privacy label. As indicated in the U.S. government website “many consumers would like to know how to use this information more effectively and easily. The label-reading skills are intended to make it easier for you to use the Nutrition Facts labels to make quick, informed food decisions to help you choose a healthy diet” (para. 1).

Now you are ready select one of the *Internet of Things* to market your device by creating a privacy label such as a smart tv, robot, etc. You will focus on the GREEN APPLE identity attributes and design a model privacy label using the six variations listed below. It is critical to be aware of your consumers’ needs and to include the protection of identity attributes. Remember a quick scan of a “privacy label” reveals at least the following information.

- Product-specific information
 - Serving target
 - Benefits
 - Limitation
 - Facts Label Variations
 - Quick guide to percentage/value
- The students review the “nutrition facts label” and discuss it (10 minutes).**
 - The students work in groups to create a model privacy label and (20 minutes)**
 - The students share their model privacy with class (10 minutes)**

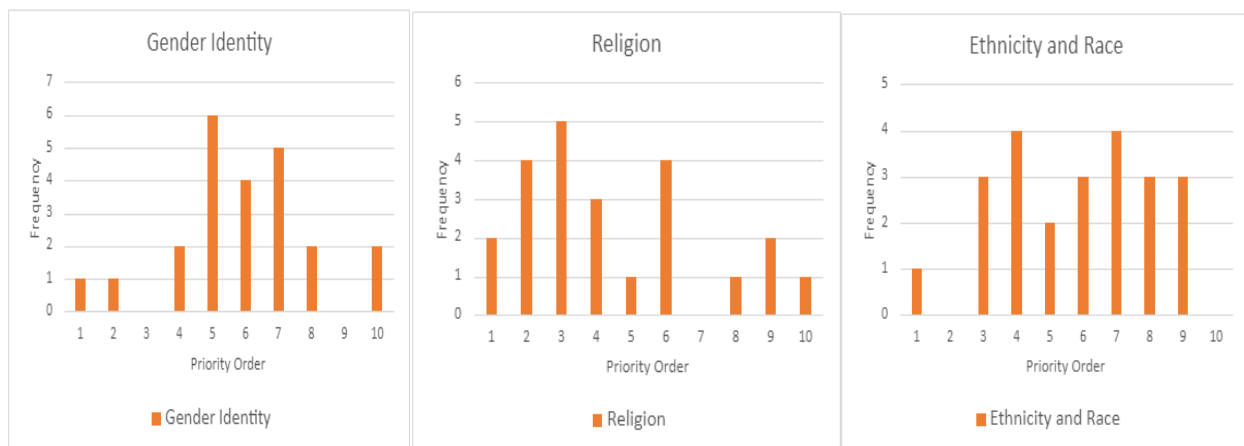
Appendix G

Instructions for the Post Activity Reflections (90 minutes)

The instructor explains the fundamentals of Diversity, Equity, and Inclusion (DEI) as it relates to privacy and the task (15 minutes)

The instructor talks about the fundamentals of Diversity, Equity, and Inclusion (DEI) and what it entails when it comes to identity attributes and privacy issues referring to the book (Miller, 2021) and goes onto explain that the three attributes of the acronym Green Apple, **G**ender, **R**eligion, **E**thnicity and Race, play an important role in our privacy issues and require our attention.

Here's your task: I developed the following three graphs showing how you ranked the attributes **G**ender, **R**eligion, **E**thnicity and Race regarding privacy. Now that you have the graphs, I would like you to provide your reflections describing what you think (a minimum of **60** words) about these three attributes, particularly as it relates to the fundamentals of Diversity, Equity, and Inclusion and privacy.



- **The students complete their reflections (20 minutes)**
- **The instructor uses the reflection data to create a Wordle or Word Cloud to display the most commonly used words (15 minutes)**
- **The instructor shares 1) the following Wordle, 2) discusses the implications with the students, and 3) wraps up the unit, *Privacy* (40 minutes)**

