# Developing a 1st and Second year Cybersecurity Seminar

Chris Kreider – Christopher Newport University



# Overview

- Problem Background
- Problem Solution
  - Structure
  - Key Topics
- Discussion/Recommendations
- Conclusions
- References

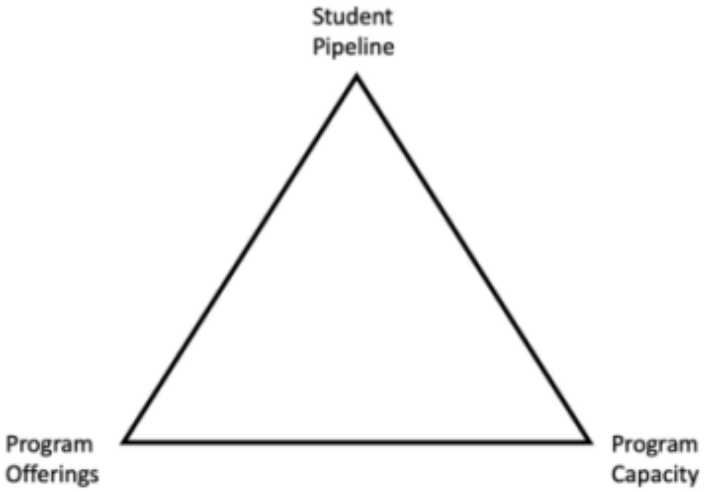


Problem Background



# Problem Background

- The Cybersecurity Jobs Gap
  - Estimated 3 million unmet cybersecurity staffing positions worldwide (Goupil Et Al. 2022)
  - Working towards solving these problems requires generating more skilled graduates/professionals
    - This requires a “student pipeline” (Kreider and Almalag 2019)



# Problem Background

- Kreider & Almalag (2019) Define the student pipeline problem as "Assuming a set of comprehensive educational programs, and infinite resources with which educational institutions could use to implement, would there be enough students willing and capable to engage in such programs?"
- Wei et al (2016) specifically identify 3 potential student focused sources of entrants into cybersecurity programs including:
  - high school students,
  - two-year college students,
  - university students from other majors
- The "university students from other majors" can be a two way street as well, with students
- Another source of students came from competitions (Pusey et al., 2016)



# Problem Background

- The student pipeline can have entrants with different background and expectations
  - True New Entrants – A new student planning on attending college, interested in studying cybersecurity with no prior background
  - Continuing Entrants – A new student planning on attending college, with non-trivial prior experience in cybersecurity (e.g. already have security+)
  - ”Curious” Entrants – existing students who may have heard from various sources that cybersecurity might be interesting and a good fit for them.
- Failure to provide a route through the pipeline may result in loss of students.



# Problem Background

- The Challenge – How can we provide a pipeline into the cybersecurity major for the various sources of entrants When
  - Some entrants may have no idea what cybersecurity entails
  - While others are excited to start studying
  - Many students will not take cybersecurity classes until 2nd semester, 2nd year or later



Problem Solution



# Solution

- Solution was to develop a mixed level cross listed 1st and 2nd year cybersecurity course
- To minimize credit impact, kept at a 1 credit course.
- Designed for and advertised/registered for by
  - Incoming freshman interested in cybersecurity
  - Second year cybersecurity students who have not yet met pre-requisite for full major specific courses
  - Adjacent majors (CS, IS, EENG, CENG) who may be curious what the cybersecurity major is about



# Solution

- Course design introduced several pedagocial challenges
  - How to engage purely “new” students interested
    - No common background or experience to engage in discussion
  - How to provide challenge/excitement for students with prior experience
  - How to provide contrast to other majors
- Used research on student sources to help gudie and structure the course



# Solution

- The seminar class was designed along an opening leture series (2 weeks),
- Followed by 3 modules (over 12 weeks)
  - Current Events in Cybersecurity
  - Cybersecurity Tools
  - Cybersecurity in Context
- Wrapping up the semester with a capture the flag or other similar competition (final week and final exams)



# Opening Lecture Series

- Provide a common foundation for the class to prepare presentations and engage in discussion
  - CIAs
  - Level of Impact
- Provide background on types of cybersecurity actors/teams
  - White hat, blat hat, red team, blue team
- Provided guidance on the path through to being a cybersecurity professional
  - Details on the broad topics that one may focus on in cybersecurity (framed from highly technical to highly human)
  - Details on the specific path at our university (highlight majors, areas of emphasis and minors)
  - Details on types of careers and career advise for future cybersecurity professionals



# Current Events In Cybersecurity

- The first 4 weeks are dedicated to student presentations on current events
  - Cybersecurity is a field where new things happen nearly daily
  - Many seminal events in the field have occurred in the last 5-10 years
  - The widespread coverage of cyber events provides a variety of sources for students to explore at various levels of experience and interest
  - Gives students experience exploring, understanding and sharing information related to cybersecurity
- Conversations are focused around the CIAs and Level of Impact



# Hands on With Cybersecurity Tools

- The second 4 weeks, we introduce the cyberrange and Kali Linux
  - Cybersecurity is a major where getting hands on with the tools is an integral and exciting part of study
  - Students are given a list of tools in Kali linux, and they pick one
    - Depending on skill level, may perform live demo or may share a snippet of somebody else using it
  - Discussed in the context of CIA, and who/how it would be used (white/black, red/blue)



# Cybersecurity in Context

- Final 4 weeks of presentations focus on students understanding how cybersecurity events impact disciplines, individuals and organizations.
  - Students put themselves in the shoes of organizations or individuals that may have been hacked, and discuss how it would have impacted them, and what could have been done differently.
- At Virginia Cybereducation conference this year, keynote speaker highlighted a study of what employers were looking for
  - Technical skills were important, but (almost more so) soft/people skills were needed too
  - Speaker specifically used the word “empathy”



# Across All Modules

- Across all three modules, students gain
  - Experience researching and exploring cybersecurity events
  - An increased comfort and understanding of tools used un cybersecurity
  - Increased comfort preparing and presenting cybersecurity materials for general audience consumption
  - Increased knowledge of ”what it means” to go into cybersecurity



# Capture the Flag

- The final event is a capture the flag competition
- Students are given several weeks (overlapping with the last set of presentations) to participate in a jeopardy style capture the flag
- The final exam block is reserved for going over questions where they got stuck, and answering/demoing solutions as requested



# The 298 Variant

- The 198 (1st year) and 298 (2nd) year variants are identically structured, with additional expectations for the more advanced students including
  - First to present at the start of each module
  - A higher expectation for presentation quality and completeness
  - A live demo for the tools presentation (or one they pre-recorded – cannot use others videos)
  - Providing mentoring and review for 198 students as they prepare their presentations



Discussion/Recommendations



# Discussion

- So far, the class has been highly successful
- Class is scalable for smaller or larger size (once number of students exceeds presentation blocks available, then move to group presentation format)
- 4 weeks seems to be right amount of time for each module, reach “saturation”
  - Provides students useful context and understanding of “what” cybersecurity is



# Observations

- 1st Year student Challenges
  - Have sign-ups in class
  - Reminders at start of each week to post their topic
  - Open office hours for discussing topics
  - Offer to review presentations
- Handful of students from other majors find the class (1 credit status)
- Builds trust with the students (e.g. sharing problems)



# Recommendations

- What else should we cover in intro lecture series?
- What good resources are available for careers?
- What else can/should be passed on to them during this time?



Conclusions



# Conclusions

- Building a common foundation for discussing and understanding cybersecurity
  - Enables students from multiple pipeline sources to be engaged and challenged at skill appropriate levels
- Focusing on a wholistic view of cybersecurity highlights the importance of soft skills and technical skills



# Conclusions

- As I wrap up the semester I always remind my cyber students “you may be the most cybersecurity aware person in your family or community – you can help!”
- Future Work
  - Study on how this course sequence impacts student pipeline
    - Where students come from and end up
    - How this course played a role in that



References



# References


- Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022, July). Towards understanding the skill gap in cybersecurity. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1* (pp. 477-483).
- Kreider, Christopher and Almalag, Mohammad, "A Framework for Cybersecurity Gap Analysis in Higher Education" (2019). *SAIS 2019 Proceedings*. 6. https://aisel.aisnet.org/sais2019/
- Wei, W., Mann, A., Sha, K. and Yang, T. A. (2016) Design and Implementation of a Multi-Facet Hierarchical Cybersecurity Education Framework, IEEE Conference on Intelligence and Security Informatics, September 28 - 30, Tuscon, AZ, USA, 273-278.