Hallett, J. (2019). *So, Tell Me What You Know, What You Really Really Know: Identifying the Knowledge Gaps of Future Security Information Worker*. Abstract from The 5th Workshop on Security Information Workers, Santa Clara, CA, United States. https://wsiw2019.sec.uni-hannover.de/

So, Tell Me What You Know, What You Really Really Know
Identifying the Knowledge Gaps of Future Security Information Workers

Joseph Hallett
University of Bristol
joseph.hallett@bristol.ac.uk

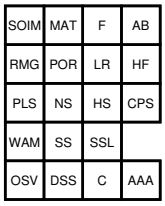
Awais Rashid
University of Bristol
awais.rashid@bristol.ac.uk

1 Introduction

Cyber security degrees are producing the future security information workers; but are they preparing them adequately? What are the knowledge gaps of these future security information workers? To better understand what these students learn from a cyber security degree, we are running a longitudinal study of cyber security Masters students at 7 different universities. We invite students to complete a survey designed to capture what they know about cyber security at the start of their degrees, and will ask them to complete the survey again at the end of their degrees. Hallett et al. showed that many Masters-level curricular frameworks poorly cover many low-level engineering topics [3], but is it because these topics are already known by students, or are key aspects of cyber security being overlooked? We report preliminary results from 51 students who completed the survey on entering their programs, capturing what they *think they know* starting their degree.

2 Survey Design

We aim to measure the breadth of students' cyber security knowledge. Unlike the work of Parekh et al. [4], we do not attempt to discover what students' cyber security concepts are but instead understand the gaps in their knowledge as they themselves perceive them. We base our survey on the Cyber Security Body of Knowledge (CyBOK): a broad foundation for cyber security that codifies existing literature, research, and standards developed in collaboration with industry and academia [5]. For each of CyBOK's 19 knowledge areas (KAs) (Figure 1) we ask if the student has *any* knowledge about the KA, and if so ask them to rate their knowledge of 3–6 sub-topics on a 5-point Likert scale. The survey is offered to students in the first week of their studies by the 7 participating universities in an opening lecture. We also capture limited demographic data about the student's level of education and experience coming into the degree, and their email address in order to link responses at the end of their program.



SOIM Security Operations and Incident Management **MAT** Malware and Attack Technology **F** Forensics **AB** Adversarial Behaviors **RMG** Risk Management and Governance **POR** Privacy and Online Rights **LR** Law and Regulation **HF** Human Factors **PLS** Physical Layer and Telecommunications Security **NS** Network Security **HS** Hardware Security **CPS** Cyber-Physical Systems **WAM** Web and Mobile **SS** Software Security **SSL** Secure Software Lifecycle **OSV** Operating Systems and Virtualization **DSS** Distributed Systems Security **C** Cryptography **AAA** Authentication, Authorization, Accountability

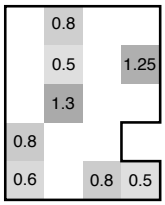


Figure 1: CyBOK KAs and *median* levels of reported self knowledge in each KA, based on the average of score of multiple questions asked on a 5-point Likert scale, where levels of knowledge range from: *0. none*, *1. a little bit*, *2. a moderate amount*, *3. a lot*, and *4. a great deal*.

3 Initial Results

Students reported, on average, knowing *something about*, 8.9 KAs, though with much variation ($\sigma = 5.0$). Broken down by KA, most students only reliably claimed to know a little bit about *Network Security* and the *Human Factors* KAs (score $\geq$ 1), with passing familiarity with a further 6 (score $>$ 0). 23 (45%) of students reported having industrial experience, but the rest claimed none.

Most reported knowing little about the KAs related to oft-advertised security jobs, such as SOIM, forensics and pentesting (Malware and Attack Technology), as well as low-level engineering topics such as cyber physical systems, hardware security, and the secure software lifecycle. If, as Hallett et al. suggest [3], these topics do not get taught, and that students don't know them coming into their degrees then the shortage of workers with these skills will persist [1, 2]. When the full survey completes, we will have more evidence as to what cyber security knowledge they gained over their degrees. This will start to provide further evidence if cyber security degrees are missing key topics and what needs to be done to address knowledge gaps of future security information workers.

References

[1] Lorrie Faith Cranor and Norman Sadeh. A shortage of privacy engineers. *IEEE Security & Privacy*, 11(2):77–79, 2013.

[2] Peter J Denning and Edward E Gordon. A technician shortage. *Communications of the ACM*, 58(3):28–30, 2015.

[3] Joseph Hallett, Robert Larson, and Awais Rashid. Mirror, mirror on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. In *USENIX Workshop on Advances in Security Education*, 2018.

[4] Geet Parekh, David DeLatte, Geoffrey L Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T Sherman. Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education*, 61(1):11–20, 2017.

[5] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. Scoping the Cyber Security Body of Knowledge. *IEEE Security & Privacy*, 2018.