CyBOK

The Cyber Security Body Of Knowledge

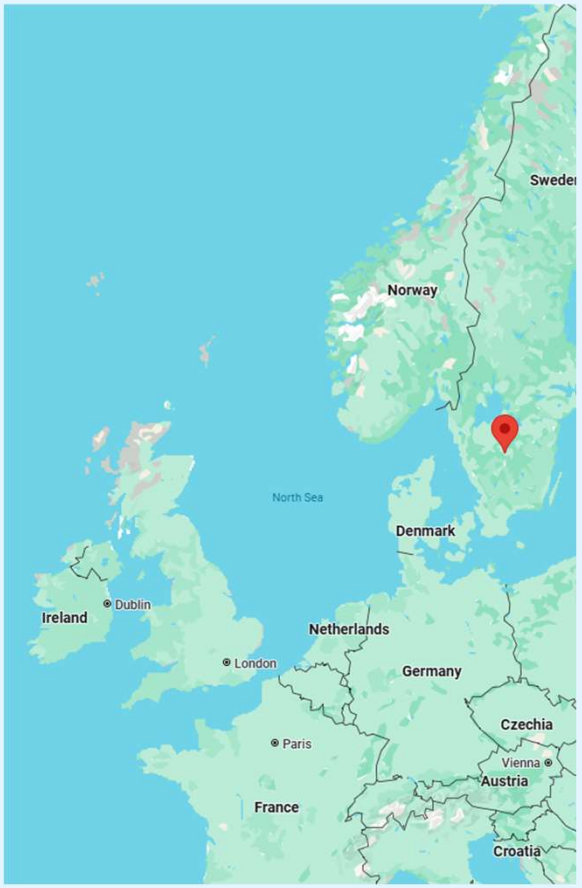
Developing first-cycle university course curriculum based on CyBOK

Joakim Kävrestad, Jönköping University, Sweden

contact@cybok.org
www.cybok.org

About me

- Assistant professor in Computer science
- Jönköping University
- Background as forensic examiner
- Glory Glory Man United!



About the project

- Use of CyBOK in a first-cycle university course
- Course is called cybersecurity
  - Pentesting
  - Incident response
  - Digital forensics
- Approx 40 2nd year students with network engineering background
- Goals:
  - Develop curriculum and education resources
  - Integrate with other resources (Both CyBOK and other)

About the project

Course part	Core knowledge areas	Existing material to utilize	New material to develop
Penetration testing	Adversarial Behaviours & Malware and Attack Technologies	Open source CyBOK practical challenges and learning resources[1]	Three lectures
Incident management and response	Security operations and Incident Management	Open source CyBOK practical challenges and learning resources	Three lectures Tabletop incident response lab
Cybercrime and digital forensics	Forensics	Developing and testing a memory analysis workshop[2]	Three lectures Secondary storage analysis lab

Pedagogical ideas

- Learn by doing
  - Labs, lots of labs
  - Equip students to solve problems
- (Modularity)
  - All modules used as one course
  - They can also be used as smaller individual modules
- Liberating structures
  - “easy-to-learn microstructures that enhance relational coordination and trust. They quickly foster lively participation in groups”
  - Simple structures that, in this case, foster discussions and peer-learning
  - I used one called 1-2-4-all

https://www.liberatingstructures.com/1-1-2-4-all/

1-2-(4-all)

- Everyone take 1 minute to write down (or think of) core ideas of questions about what I just presented.
- Then, take another minute to compare notes with a peer
- Then, take another mi… …of four
- Finally, lets see if w… …are some reflections with everyone

We usually only do the first two, because I talk too much

https://www.liberatingstructures.com/1-1-2-4-all/

Course description - Pentesting

- CyBOK Knowledge Areas:
  - Malware and Attack Technologies
  - Adversarial Behaviours
- Lectures:
  - Penetration testing – Introduction and methods
  - Penetration testing - Tools and tricks
  - Penetration testing – Research and state of the art

- Suggested labs:
  - Using SecGen (Open source CyBOK practical challenges and learning resources)
    - Introduction to Linux and security
    - Introducing web security
    - Authentication lab
  - Using TryHackMe
    - CompTIA pentest+
    - Jr Penetration tester

Course description – Incident mgmt…..

- CyBOK Knowledge Areas:
  - Security Operations and Incident Management
- Lectures:
  - Incident mgmt. and response – Introduction and methods
  - Incident mgmt. and response - Tools and tricks
  - Incident mgmt. and response– Research and state of the art

- Suggested labs:
  - Using SecGen (Open source CyBOK practical challenges and learning resources)
    - Backups lab
    - Live analysis lab
    - SIEM and ELK Stack lab
  - Using TryHackMe
    - SOC Level 1
  - Tabletop
    - A TTX developed within the project which allows students to experience an incident response process

Course description – forensics

- CyBOK Knowledge Areas:
  - Forensics
- Lectures:
  - Digital forensics
  - Memory analysis
  - Incident mgmt. and response– Research and state of the art

- Suggested labs:
  - Malware analysis lab from "Developing and testing a memory analysis workshop"
  - Deadbox analysis lab developed within the project

- Additional literature:
  - Kävrestad, J., Birath, M., & Clarke, N. (2024). *Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-031-53649-6

Student evaluation (1-7, 22/41 responses)

Statement	Mean
The course was well structured	5.5
The course had a good mix of different activities (Combination of theory and practice)	**6.3**
The course challenged me to analyse ideas and concepts	5.8
The course content was relevant for my education	6.5
The literature was relevant to the course content and objectives	**6.0**
My perception of the course was (1= Not satisfied, 7=Very satisfied)	5.8

Student evaluation CyBOK focus

Question	
Wha was your overall perception of the course	The responses highlight the mix of practice and theory as fun and engaging. Some students asked for more practical's while some felt that they were too difficult. This can be expected in a relatively large group of students and suggests a reasonable level.
How would you describe CyBOK?	The idea with the question was to see if the students perceived CyBOK as something else than the literature and the response shows that several students used CyBOK resources other than the mandatory literature. Several responses describe CyBOK as a good source of knowledge for many different security topics.
What is your overall perception of CyBOK?	Most of the responses include a simple "good". While no negative comments are given, one student states that there is a lack of practical examples. Three students specifically describe CyBOK as easy to read and engaging. I summary, the results suggest that CyBOK is a good option as course literature in general.
What are the best aspects of CyBOK?	This question was only responded to by a few students, and they mention a free resource as positive. Two students also describe CyBOK as easy to read and follow.

Future plans

- Ongoing development of materials, of course
  - To be posted on GitHub

- Evaluation of the use of large open educational resources
  - I am using CyBOK in several courses of different difficulty and mode
  - Interesting to see:
    - How CyBOK sparks interest in security topics
    - How and if students get interested in other topics than the topics covered by course literature
  - Not applying for CyBOK funding, but I'll do it anyway
  - Plan to publish at some conference, probably HAISA2025
  - Happy to report to the CyBOK community ☺

That’s it!

- Questions?

- Happy to connect and discuss
  - LinkedIn
  - Joakim.kavrestad@ju.se
  - Some pub after the event