University of BRISTOL

CyBOK

Project: Case Studies in Support of Cyber Security Body of Knowledge

Nancy R. Mead, SEI Fellow, CMU (ret)
nrmcmu@gmail.com

bristol.ac.uk

Case Study Project Description

- Research and collect educational case studies in CyBOK areas, structure them into a standard format, identify the original sources, and ensure there are clear usage (copyright) permissions for educational purposes. Each case study is cross-referenced to CyBOK 1.0 area(s).

- 18 case studies along with an overview document were provided and are available from the CyBOK website.

- Case studies were contributed by a team of faculty experts and other volunteers in the community

Case Study Standard Format

- ***Background.*** Brief overview of the real-world and/or fictional example at hand and provides sufficient context to frame the problem space. This section makes references to externally available resources, if applicable, or suggests further reading.

- ***Case Study Overview.*** Describes the learning activities to be carried out on the basis of the information given in "Background" to meet CyBOK learning outcomes.

- ***Student Instructions.*** Concrete work assignments for students with sufficient detail to understand what is expected but with enough leeway to allow the learner to explore the problem space. This section may be subdivided into multiple tasks or provide partial solutions to get started.

- ***Instructor Notes.*** Pedagogical strategies on how to apply the case study. For example, this may entail ways to tailor one case example for group vs. individual project assignments or exam questions, or solution templates.

- ***Example Solution.*** Example solution (if available), key grading criteria, success factors, or caveats depending on the case study at hand.

- ***References.*** References to external resources and/or further reading.

Case Study Overview - 1

CyBOK

ACME Water	Provide a secure operating environment for SCADA, Telemetry and Control Systems associated with assets owned and operated by ACME.
Aircraft Service Application	Develop the requirements for a secure aircraft service management application to replace a legacy system with hand-held device support.
Archetypal Users: Personae non Gratae	Support malicious user identification and assessment by developing personas of unwanted, possibly nefarious users and derive security requirements pertaining thereto.
Driver Assistance System Safety & Security	Use a real-world owner's manual for a car to "reverse engineer" the requirements specification with special focus on safety and security requirements.
Drone Swarm	Conduct threat modeling with secure cards for deliveries with search & rescue drones.
FAA ERAM Outage	Model the strategic importance of Federal Aviation Administration's EnRoute Automation Modernization project and find flaws in its software testing and cybersecurity plan. Conduct risk & threat analysis.
GPS Spoofing of UAV	Review real-world incident reports to investigate necessary design changes to path a security vulnerability that allowed attackers to hijack a military Unmanned Aerial Vehicle.
Heartland Payment System Breach	Investigate and re-create the anatomy of an SQL injection attack and develop possible countermeasures to avoid risks.
Mt. Gox Bitcoin Theft	Review popular science articles on the famous Bitcoin theft to discover procedural, organizational, and technological flaws in the Mt. Gox cryptocurrency trading system and derive ideas how to avoid them.

Case Study Overview - 2

National Grid SAP Adoption	Review popular science articles on a secure acquisition project discover procedural, organizational, and technological flaws that lead to project failure and avenues to avoid them.
Organizational Risk Management: The Widget Company	Investigate the organizational structure of a fictive company against organizational risks. Develop a mitigation and protection strategy.
Secure Acquisition (Case Studies 1-4)	Four case studies centered around adopting off-the-shelf components for a development project in a secure way.
SQUARE	Elicit and document security requirements for a software development project that expands existing infra-structure of a mission-critical system in a subsidiary of a fictitious company.
Tokeneer ID Station Project	Conduct a compliance and cost-effectiveness analysis of a development project for a top-secret level governmental development project.
Using Malware Analysis to Improve Security Requirements	Suggest a process model to conduct malware analysis and derive misuse cases to identify vulnerabilities in a software development lifecycle.

Mapping of Case Studies to CyBOK 1.0

Category	Knowledge Area	Case Study Mapping
Human, Organizational & Regulatory Aspects	Risk Management & Governance	ACME Water Arch. Users Personae non Gratae FAA ERAM UAV GPS Spoofing Nat. Grid SAP Adoption Widget Company
	Law & Regulation	
	Human Factors	ACME Water FAA ERAM
	Privacy & Online Rights	Driver Asst. Sys.
Attacks & Defences	Malware & Attack Technologies	Mt. Gox Theft Malware Analysis for Security Req'ts
	Adversarial Behaviour	Heartland Breach Mt. Gox Theft
	Security Operations & Incident Mgmt	Heartland Breach Mt. Gox Theft
	Forensics	Mt. Gox Theft

Mapping of Case Studies to CyBOK 1.0

Category	Knowledge Area	Case Study Mapping
Systems Security	Cryptography	Mt. Gox Theft
	Operating Systems & Virtualisation	Heartland Breach Mt. Gox Theft
	Distributed Sys. Sec.	Driver Asst. Sys.
	Authentication, Authorisation & Accountability	ACME Water Heartland Breach
Software Platform Security	Software Security	Driver Asst. Sys. FAA ERAM
	Web & Mobile Security	Driver Asst. Sys.
	Secure Software Lifecycle	ACME Water Aircraft Serv. App. Drone Swarm Nat. Grid SAP Secure Acquisition SQUARE Tokeneer ID Station Malware Analysis for Security Req'ts
Infrastr. Security	Network Security	
	Hardware Security	Driver Asst. Sys.
	Cyber-Physical Systems Security	Driver Asst. Sys.
	Physical Layer & Telecommunications	

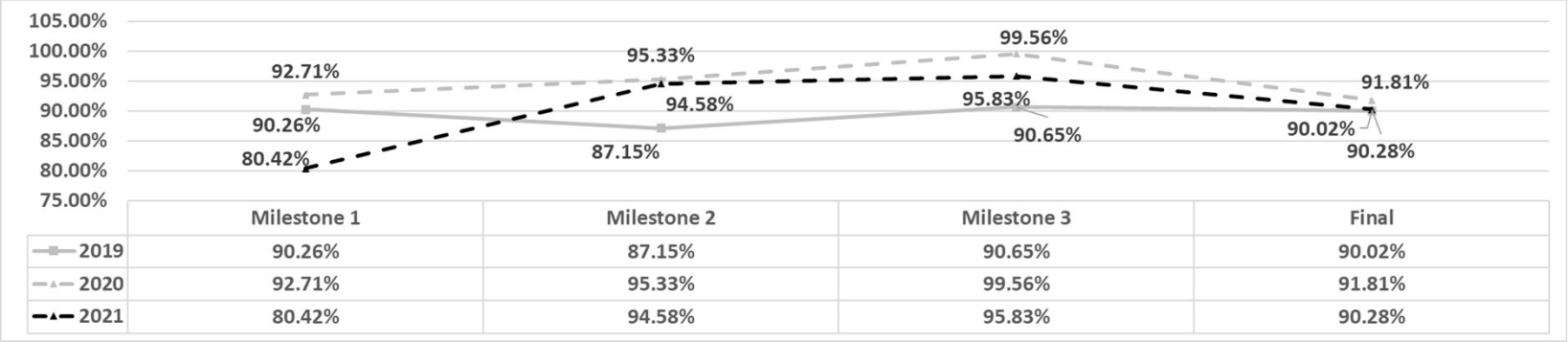
CyBOK 1.0 Coverage

- Case studies related to **84%** of the CyBOK knowledge areas
- Seven knowledge areas (36%) are addressed by a single case study .
- Nine knowledge areas (**47%**) are addressed by **at least two case studies**.
- “risk management & governance” and “secure lifecycle management” are addressed by six and eight case studies, respectively

Additional Related Accomplishments

- Refereed paper describing initial successes in classroom usage accepted at HICSS Conference Software Engineering Education Track, to be presented in January 2022
  - classroom results of one exemplary case study (Driver Assistance System)
  - demonstrated improved understanding by students

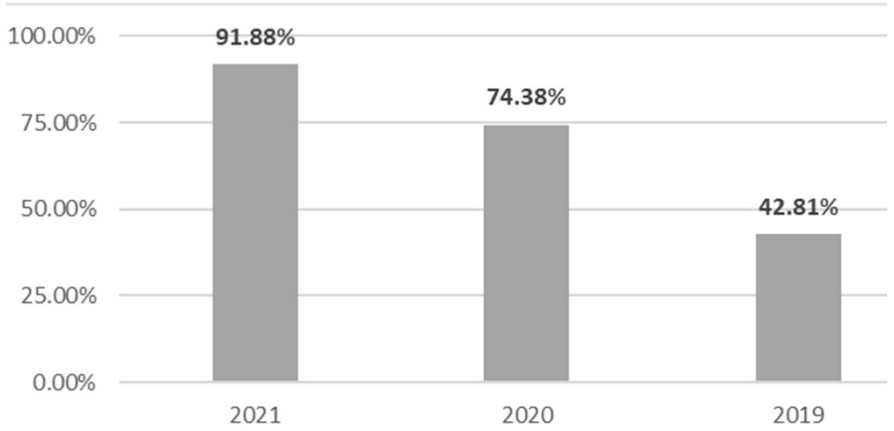
Case Study Efficacy



	Milestone 1	Milestone 2	Milestone 3	Final
2019	90.26%	87.15%	90.65%	90.02%
2020	92.71%	95.33%	99.56%	91.81%
2021	80.42%	94.58%	95.83%	90.28%

Project Milestone Scores, scores comparable to previous semesters, no significant differences.

Cumulative Exam Scores,
2021 >> 2019, p = 0.0318



Suggested Future Case Study Needs

- Expand case study library. Especially needed are case studies in "law & regulation", "network security", and "physical layer & telecommunications"
- Make updates to reflect CyBOK 1.1
  - Review existing case studies and align to CyBOK 1.1
  - Update case study mapping to reflect CyBOK 1.1
  - Review expanded/modified CyBOK areas to determine if more/different case studies are needed
  - Expand case study library to provide coverage in new areas: "Formal Methods for Cybersecurity" and "Applied Cryptography"
- Continue to collect objective and subjective feedback about the impact of CyBOK case study classroom usage

Additional Details

- Case Study Download: https://www.cybok.org/resources_developed_through_funded_projects/
- HICSS Paper: “Using Cybersecurity Body of Knowledge (CyBOK) Case Studies to Enhance Student Learning”, Authors: Anne Kohnke, Bastian Tenbergen, Nancy Mead
- Team Members: Nancy Mead, Rod Chapman, Shamal Faily, Anne Kohnke, Dan Shoemaker, Bastian Tenbergen, Carol Woody
- Contact info: Nancy Mead nrmcmu@gmail.com

bristol.ac.uk