Overview

Nancy R. Mead
Anne Kohnke
Bastian Tenbergen

December 2021

Table of Contents

Overview

The objective of the CyBOK Case Study project was to identify a collection of case studies that were related to CyBOK for classroom use by faculty. Each case study is mapped to relevant topic areas in CyBOK 1.1. Although the case study collection includes at least one case study in each CyBOK area, it is not comprehensive. However, faculty can select at least one case study for each CyBOK area, and thus reduce the level of effort that faculty would otherwise spend researching the topic area, developing their own cases studies, identifying suitable references and so on. Since the Case Study project leveraged prior research and classroom work, we were able to identify many case studies.

Cross-references between the case studies and the CyBOK topic areas appear two different ways. For each case study, there is a mapping to relevant CyBOK areas in this Overview document, and for the relevant CyBOK areas, there is a mapping to case study names. These mappings appear only in this Overview document and not in the individual case study documents, so that when CyBOK is modified in the future, only this document needs to be revisited for currency rather than the individual case study documents. It also provides an indication of CyBOK areas where additional case studies would be useful.

Within the case studies themselves, to the extent possible, the authors indicated: 1) Whether the case study was suitable as a classroom example, assignment, or lengthy project, and whether it was more suitable for an individual student activity vs a team activity. 2) Provided example student instructions and instructor notes, and 3) Provided a list of references. 4) For those case studies where example solutions existed, these were provided, although in some cases there is no single perfect solution. 5) Each case study also contains a copyright statement that is specific to that case study.

A companion document to the set of case studies is a report on classroom usage, including both objective and subjective results to illustrate their benefit to students.

Acknowledgements

We would like to acknowledge the following individuals who generously identified or provided case study documents for this project.

Anne Kohnke, University of Detroit Mercy
Roderick Chapman, Protean Code
James Early, State University of New York at Oswego
Shamal Faily, Bournemouth University
Christopher Harris, University of Northern Colorado
Nancy Mead, Carnegie Mellon University (ret)
Randy Odendahl, State University of New York at Oswego (ret)
Andrii Paziuk, DAI Ukraine
Nafees Qamar, Governors State University
Dan Shoemaker, University of Detroit Mercy
Bastian Tenbergen, State University of New York at Oswego
Carol Woody, Carnegie Mellon University

Advisory Committee

The following individuals worked in the capacity of an Advisory Board for the initial version of this project, in order to ensure it was on a firm footing:

Dan Shoemaker, University of Detroit Mercy
Bastian Tenbergen, State University of New York at Oswego
Carol Woody, Carnegie Mellon University

CyBOK Topic Area(s) Cross-references Sorted by CyBOK Topic

The table below relates the CyBOK Knowledge Areas to the case studies that are applicable to them. The version number in the rightmost column reflects the CyBOK version for which the respective case study was created, however we believe each case study is suitable for any version.

Cat.	Knowledge Area	Case Study Mapping	CyBOK version
Human, Organizational and Regulatory Aspects	Risk Management & Governance	ACME Water	1.0
		Archetypal Users – Personae non Gratae	1.0
		FAA ERAM Outage	1.0
		GPS Spoofing of UAV	1.0
		National Cybersecurity Governance	1.1
		National Grid SAP Adoption	1.0
		Organization Risk Management: The Widget Company	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Secure LAN	1.1
	Law & Regulation	National Cybersecurity Governance	1.0
		Ransomware	1.1
	Human Factors	ACME Water	1.0
		FAA ERAM Outage	1.0
	Privacy & Online Rights	ACME Water	1.0
		Driver Assistance System Safety & Security	1.0
		Penetration Test	1.1
		Role Based Access Control	1.1
Attacks and Defences	Malware & Attack Technologies	Deciphering	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Using Malware Analysis to Improve Security Reqs	1.1
		Wireshark	1.1
	Adversarial Behaviours	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
	Security Operations & Incident Management	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		National Cybersecurity Governance	1.1
		Penetration Test	1.1
		Ransomware	1.1
	Forensics	Mt. Gox Bitcoin Theft	1.0
		Wireshark	1.1

Systems Security	Cryptography	Deciphering	1.1
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
	Operating Systems & Virtualisation Security	Deciphering	1.0
		Heartland Payment System Breach	1.0
		Penetration Test	1.1
		Secure LAN	1.1
	Distributed System Security	Driver Assistance System Safety & Security	1.0
		Secure LAN	1.1
		Wireshark	1.1
	Formal Methods for Security	Deciphering	1.1
		Tokeneer ID Station Project	1.0
	Authentication, Authorisation & Accountability	ACME Water	1.0
		Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Role Based Access Control	1.1
		Secure LAN	1.1
Software Platform Security	Software Security	Driver Assistance System Safety & Security	1.0
		FAA ERAM Outage	1.0
		Penetration Test	1.1
	Web & Mobile Security	Driver Assistance System Safety & Security	1.0
		Role Based Access Control	1.1
		Secure LAN	1.1
	Secure Software Lifecycle	ACME Water	1.0
		Aircraft Service Application	1.0
		Drone Swarm	1.0
		National Grid SAP Adoption	1.0
		Secure Acquisition	1.0
		SQUARE	1.0
		Tokeneer ID Station Project	1.0
		Using Malware Analysis to Improve Security Reqs	1.1
Infrastructure Security	Applied Cryptography	Deciphering	1.1
		Penetration Test	1.1
	Network Security	Role Based Access Control	1.1
		Secure LAN	1.1
		Wireshark	1.1
	Hardware Security	Driver Assistance System Safety & Security	1.0
	Cyber-Physical Sys Security	Driver Assistance System Safety & Security	1.0
	Physical Layer & Telecommunications	Penetration Test	1.1
		Secure LAN	1.1
		Wireshark	1.1

CyBOK Topic Area(s) Cross-references Sorted by Case Study Name

This section relates the case studies to their respective CyBOK Knowledge Areas. The version number from Table 1 is indicated in parentheses.

ACME Water Case Study (since CyBOK 1.0)

This case study has 10 separate exercises that span the following CyBOK topic areas:

Exercise 1: Introduction & Human Error
- I. Human, Organisational & Regulatory Aspects
  - 2. Risk Management & Governance.
  - 4. Human Factors

Exercise 2: Risk & Trust
- I. Human, Organisational & Regulatory Aspects
  - 2. Risk Management & Governance
- IV. Software Platform Security
  - 17. Secure Software Lifecycle

Exercise 3: Personas
- I. Human, Organisational & Regulatory Aspects
  - 4. Human Factors

Exercise 4: Requirements
- I. Human, Organisational & Regulatory Aspects
  - 4. Human Factors

Exercise 5: User Interfaces
- I. Human, Organisational & Regulatory Aspects
  - 4. Human Factors

Exercise 6: Architecture
- IV. Software Platform Security
  - 17. Secure Software Lifecycle

Exercise 7: Authentication
- I. Human, Organisational & Regulatory Aspects
  - 2. Risk Management & Governance
- III. Systems Security
  - 14. Authentication, Authorisation & Accountability

Exercise 8: Authorisation
- III. Systems Security
  - 14. Authentication, Authorisation & Accountability

Exercise 9: SEAT & Privacy
- I. Human, Organisational & Regulatory Aspects
  - 4. Human Factors
  - 5. Privacy & Online Rights
- IV. Software Platform Security
  - 17. Secure Software Lifecycle

Exercise 10: Economics & Entrepreneurship
- I. Human, Organisational & Regulatory Aspects
  - 4. Human Factors

Aircraft Service Application Case Study (since CyBOK 1.0)

IV. Software Platform Security

17. Secure Software Lifecycle

Archetypal Users—Personae non Gratae (PnGs) Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects

2. Risk Management and Governance

Deciphering Case Study (since CyBOK 1.1)

II. Attacks & Defences

6. Malware & Attack Technologies

III. Systems Security

10. Cryptography

11. Operating Systems & Virtualisation

13. Formal Methods for Security

V. Infrastructure Security

18. Applied Cryptography

Driver Assistance System Safety & Security Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects

5. Privacy & Online Rights

III. Systems Security

12. Distributed Systems Security

IV. Software Platform Security

15. Software Security

16. Web & Mobile Security

V. Infrastructure Security

20. Hardware Security

21. Cyber-Physical Systems Security

Drone Swarm Case Study (since CyBOK 1.0)

IV. Software Platform Security

17. Secure Software Lifecycle

FAA ERAM Outage Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects

2 Risk Management and Governance

4 Human Factors

IV. Software Platform Security

15. Software Security

GPS Spoofing of UAV Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects
- 2 Risk Management and Governance

Heartland Payment System Breach Case Study (since CyBOK 1.0)

II. Attacks and Defences
- 7. Adversarial Behavior
- 8. Security Operations & Incident Management

III. Systems Security
- 11. Operating Systems and Virtualization
- 14. Authentication, Authorisation, & Accountability (AAA)

Mt. Gox Bitcoin Theft Case Study (since CyBOK 1.0)

II. Attacks and Defences
- 6. Malware & Attack Technologies
- 7. Adversarial Behavior
- 8. Security Operations & Incident Management
- 9. Forensics

III. Systems Security
- 10. Cryptography
- 14. Authentication, Authorisation, & Accountability (AAA)

National Cybersecurity Governance Case Study (since CyBOK 1.1)

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management & Governance
- 3. Law & Regulation

II. Attacks and Defences
- 8. Security Operations & Incident Management

National Grid SAP Adoption Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management and Governance

IV. Software Platform Security
- 17. Secure Software Lifecycle

Organization Risk Management: The Widget Company Case Study (since CyBOK 1.0)

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management and Governance

Penetration Test Case Study (since CyBOK 1.1)

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management & Governance
- 5. Privacy & Online Rights

II. Attacks & Defences
- 6. Malware & Attack Technologies

7. Adversarial Behaviour
8. Security Operations & Incident Management

III. Systems Security
10. Cryptography
11. Operating Systems & Virtualisation
14. Authentication, Authorisation, & Accountability

IV. Software Platform Security
15. Software Security

V. Infrastructure Security
18. Applied Cryptography
22. Physical Layer & Telecommunications

Ransomware Case Study (since CyBOK 1.1)

I. Human, Organisational & Regulatory Aspects
2. Risk Management & Governance
3. Law & Regulation

II. Attacks & Defences
6. Malware & Attack Technologies
7. Adversarial Behaviour
8. Security Operations & Incident Management

Role Based Access Control Case Study (since CyBOK 1.1)

I. Human, Organisational & Regulatory Aspects
5. Privacy & Online Rights

III. Systems Security
15. Authentication, Authorisation, & Accountability

IV. Software Platform Security
15. Web & Mobile Security

V. Infrastructure Security
19. Network Security

Secure Acquisition Case Study 1: Project Initiation (since CyBOK 1.0)

IV. Software Platform Security
17. Secure Software Lifecycle

Secure Acquisition Case Study 2: Acquisition/SCRM Project Risk Analysis (since CyBOK 1.0)

IV. Software Platform Security
17. Secure Software Lifecycle

Secure Acquisition Case Study 3: Adequacy of Acquisition Practice (since CyBOK 1.0)

IV. Software Platform Security
17. Secure Software Lifecycle

Secure Acquisition Case Study 4: Supplier Capability Evaluation (since CyBOK 1.0)

IV. Software Platform Security
- 17. Secure Software Lifecycle

Secure LAN Case Study (since CyBOK 1.1)

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management & Governance

III. Systems Security
- 11. Operating Systems & Virtualisation
- 12. Distributed Systems Security

IV. Software Platform Security
- 14. Software Security
- 15. Web & Mobile Security

V. Infrastructure Security
- 18. Network Security
- 22. Physical Layer & Telecommunications

SQUARE Case Study (since CyBOK 1.0)

IV. Software Platform Security
- 17. Secure Software Lifecycle

Tokeneer ID Station Project Case Study (since CyBOK 1.0)

III. Systems Security
- 13. Formal Methods for Security

IV. Software Platform Security
- 17. Secure Software Lifecycle

Using Malware Analysis to Improve Security Requirements Case Study (since CyBOK 1.1)

II. Attacks and Defences
- 6. Malware & Attack Technologies

IV. Software Platform Security
- 17. Secure Software Lifecycle

Wireshark Case Study (since CyBOK 1.1)

II. Attacks and Defences
- 6. Malware & Attack Technologies
- 9. Forensics

III. Systems Security
- 12. Distributed Systems Security

V. Infrastructure Security
- 19. Network Security
- 22. Physical Layer & Telecommunications