Overview

Nancy R. Mead
Anne Kohnke

April 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 1.0. The case study collection is not comprehensive but represents the start of a case study library in support of CyBOK. Such a library would allow faculty to select suitable case study for specific CyBOK areas of interest, 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 more case studies than would have been possible otherwise on this small short-term project.

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 are needed.

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.

Acknowledgements

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

Roderick Chapman, Protean Code
Shamal Faily, Bournemouth University
Nancy Mead, Carnegie Mellon University (ret)
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 this project:

Anne Kohnke, University of Detroit Mercy
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 Case Study Name

ACME Water Case Study

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
  - 2.5. Risk Governance
    - 2.5.2. The Human Factor and Risk Communication
- 4. Human Factors
  - 4.3. Human Error

Exercise 2: Risk & Trust

I. Human, Organisational & Regulatory Aspects
- 2. Risk Management & Governance
  - 2.6. Risk Assessment and Management Principles
    - 2.6.2. Elements of Risk

IV. Software Platform Security
- 16. Secure Software Lifecycle
  - 16.2. Prescriptive Secure Software Lifecycle Processes
    - 16.2.1. Secure Software Lifecycle Processes
      - 16.2.1.2. Touchpoints

Exercise 3: Personas

I. Human, Organisational & Regulatory Aspects
- 4. Human Factors
  - 4.2 Usable Security - The Basics
    - 4.2.1. Fitting the task to the human

Exercise 4: Requirements

I. Human, Organisational & Regulatory Aspects
- 4. Human Factors
  - 4.2 Usable Security - The Basics
    - 4.2.1. Fitting the task to the human

Exercise 5: User Interfaces

I. Human, Organisational & Regulatory Aspects
- 4. Human Factors
  - 4.2 Usable Security - The Basics
    - 4.2.1. Fitting the task to the human
      - 4.2.1.3. Interaction Context

Exercise 6: Architecture

IV. Software Platform Security
- 16. Secure Software Lifecycle
  - 16.2. Prescriptive Secure Software Lifecycle Processes
    - 16.2.1. Secure Software Lifecycle Processes
      - 16.2.1.2. Touchpoints

Exercise 7: Authentication

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

2.6. Risk Assessment and Management Principles
2.6.2. Elements of Risk
III. Systems Security
13. Authentication, Authorisation & Accountability
13.5. Authentication
13.5.2. User Authentication
13.5.2.2. Biometrics for Authentication

Exercise 8: Authorisation

III. Systems Security
13. Authentication, Authorisation & Accountability
13.3. Authorisation
13.3.1. Access Control
13.3.1.1. Core Concepts
13.3.1.3. Role-based Access Control

Exercise 9: SEAT & Privacy

I. Human, Organisational & Regulatory Aspects
4. Human Factors
4.4. Cyber Security Awareness and Education
5. Privacy & Online Rights
5.5. Privacy Engineering
IV. Software Platform Security
16. Secure Software Lifecycle
16.2. Prescriptive Secure Software Lifecycle Processes
16.2.1. Secure Software Lifecycle Processes
16.2.1.2. Touchpoints

Exercise 10: Economics & Entrepreneurship

I. Human, Organisational & Regulatory Aspects
4. Human Factors
4.2. Usable Security - The Basics
4.2.1. Fitting the task to the human
4.2.1.2. Goals and tasks

Aircraft Service Application Case Study

IV. Software Platform Security
16. Secure Software Lifecycle
16.2.1 Secure Software Lifecycle Processes
16.2.1.2 Touchpoints

Archetypal Users—Personae non Gratae (PnGs) Case Study

I. Human, Organisational & Regulatory Aspects
2. Risk Management and Governance
2.6 Risk Assessment and Management Principles
2.6.2 Elements of Risk
2.6.3 Risk Assessment and Management Methods

Driver Assistance System Safety & Security Case Study

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

III. Systems Security
- 12. Distributed Systems Security

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

V. Infrastructure Security
- 18. Hardware Security
- 19. Cyber-Physical Systems Security

Drone Swarm Case Study

IV. Software Platform Security
- 16. Secure Software Lifecycle
  - 16.2.1 Secure Software Lifecycle Processes
    - 16.2.1.2 Touchpoints

FAA ERAM Outage Case Study

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

IV. Software Platform Security
- 14. Software Security
  - 14.1, Categories of Vulnerabilities
    - 14.1.1, Memory Management Vulnerabilities
  - 14.2, Prevention of Vulnerabilities
    - 14.2.1, Memory Management Vulnerabilities
  - 14.3, Detection of Vulnerabilities
    - 14.3.2, Dynamic Detection

GPS Spoofing of UAV Case Study

I. Human, Organisational & Regulatory Aspects
- 2 Risk Management and Governance
  - 2.1 Secure Software Lifecycle Processes

Heartland Payment System Breach Case Study

II. Attacks and Defences
- 7. Adversarial Behavior
  - 7.2 The Elements of Malicious Operation
  - 7.3 Models to Understand Malicious Operations
- 8. Security Operations & Incident Management
  - 8.2 Monitor: data sources
  - 8.5 Execute: Mitigation and countermeasures

III. Systems Security

11. Operating Systems and Virtualization
    11.1 Attacker model
13. Authentication, Authorisation, & Accountability (AAA)
    13.5 Authentication

Mt. Gox Bitcoin Theft Case Study

II. Attacks and Defences
    6. Malware & Attack Technologies
        6.1, A Taxonomy of Malware
        6.2, Malicious Activities by Malware
    7. Adversarial Behavior
    8. Security Operations & Incident Management
    9. Forensics
        9.1, Definitions and Conceptual Models
            9.1.3, Conceptual Models
                9.1.3.1, Cognitive Task Model
III. Systems Security
    10. Cryptography
    13. Authentication, Authorisation, & Accountability (AAA)

National Grid SAP Adoption Case Study

I. Human, Organisational & Regulatory Aspects
    2. Risk Management and Governance
        2.6 Risk Assessment and Management Principles
        2.7 Business Continuity: Incident Response and Recovery Planning
IV. Software Platform Security
    16. Secure Software Lifecycle
        16.2 Prescriptive Secure Software Lifecycle Processes
            16.2.1 Secure Software Lifecycle Processes
            16.2.2 Comparing the Secure Software Lifecycle Models
        16.3 Adaptations of the Secure Software Lifecycle
            16.3.6 Ecommerce/Payment Card Industry
        16.4 Assessing the Secure Software Lifecycle
            16.4.1 SAMM
        16.5 Adopting a Secure Software Lifecycle

Organization Risk Management: The Widget Company Case Study

I. Human, Organisational & Regulatory Aspects
    2. Risk Management and Governance
        2.6 Risk Assessment and Management Principles

Secure Acquisition Case Study 1: Project Initiation

IV. Software Platform Security
    16. Secure Software Lifecycle
        16.2.1 Secure Software Lifecycle Processes
            16.2.1.1 Microsoft Security Development Lifecycle (SDL)

Secure Acquisition Case Study 2: Acquisition/SCRM Project Risk Analysis

IV. Software Platform Security
16. Secure Software Lifecycle
16.2.1 Secure Software Lifecycle Processes
16.2.1.1 Microsoft Security Development Lifecycle (SDL)

Secure Acquisition Case Study 3: Adequacy of Acquisition Practice

IV. Software Platform Security
16. Secure Software Lifecycle
16.2.1 Secure Software Lifecycle Processes
16.2.1.1 Microsoft Security Development Lifecycle (SDL)

Secure Acquisition Case Study 4: Supplier Capability Evaluation

IV. Software Platform Security
16. Secure Software Lifecycle
16.2.1 Secure Software Lifecycle Processes
16.2.1.1 Microsoft Security Development Lifecycle (SDL)

SQUARE Case Study

IV. Software Platform Security
16. Secure Software Lifecycle
16.2.1 Secure Software Lifecycle Processes
16.2.1.1 Microsoft Security Development Lifecycle
16.2.1.1 (2) Define Security Requirements

Tokeneer ID Station Project Case Study

IV. Software Platform Security
16. Secure Software Lifecycle
16.2 Prescriptive Secure Software Lifecycle Processes
16.2.1 Secure Software Lifecycle Processes

Using Malware Analysis to Improve Security Requirements Case Study

II. Attacks and Defences
6. Malware & Attack Technologies
6.3 Malware Analysis
6.3.1 Analysis Techniques
IV. Software Platform Security
16. Secure Software Lifecycle
16.2 Prescriptive Secure Software Lifecycle Processes
16.2.1 Secure Software Lifecycle Processes
16.2.1.1 Microsoft Security Development Lifecycle
16.2.1.1 (2) Define Security Requirements

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

I. Human, Organisational & Regulatory Aspects

2. Risk Management & Governance

FAA ERAM Outage Case Study

2.1 Secure Software Lifecycle Processes

GPS Spoofing of UAV Case Study

2.5. Risk Governance

2.5.2. The Human Factor and Risk Communication

ACME Water Case Study, Exercise 1: Introduction & Human Error

2.6. Risk Assessment and Management Principles

National Grid SAP Adoption Case Study
Organization Risk Management: The Widget Company Case Study

2.6.2. Elements of Risk

ACME Water Case Study, Exercise 2: Risk & Trust
ACME Water Case Study, Exercise 7: Authentication
Archetypal Users—Personae non Gratae (PnGs) Case Study

2.6.3 Risk Assessment and Management Methods

Archetypal Users—Personae non Gratae (PnGs) Case Study

2.7 Business Continuity: Incident Response and Recovery Planning

National Grid SAP Adoption Case Study

4. Human Factors

FAA ERAM Outage Case Study

4.2 Usable Security - The Basics

4.2.1. Fitting the task to the human

ACME Water Case Study, Exercise 3: Personas
ACME Water Case Study, Exercise 4: Requirements

4.2.1.2. Goals and Tasks

ACME Water Case Study, Exercise 10: Economics & Entrepreneurship

4.2.1.3. Interaction Context

ACME Water Case Study, Exercise 5: User Interfaces

4.3. Human Error

ACME Water Case Study, Exercise 1: Introduction & Human Error

4.4. Cyber Security Awareness and Education

ACME Water Case Study, Exercise 9: SEAT & Privacy

5. Privacy & Online Rights

Driver Assistance System Safety & Security Case Study

5.5. Privacy Engineering

ACME Water Case Study, Exercise 9: SEAT & Privacy

II. Attacks and Defences

6. Malware & Attack Technologies

6.1 A Taxonomy of Malware

Mt. Gox Bitcoin Theft Case Study

6.2 Malicious Activities by Malware

Mt. Gox Bitcoin Theft Case Study

6.3 Malware Analysis

6.3.1 Analysis Techniques

Using Malware Analysis to Improve Security Requirements Case Study

7. Adversarial Behavior

Mt. Gox Bitcoin Theft Case Study

7.2 The Elements of Malicious Operation

Heartland Payment System Breach Case Study

7.3 Models to Understand Malicious Operations

Heartland Payment System Breach Case Study

8. Security Operations & Incident Management

Mt. Gox Bitcoin Theft Case Study

8.2 Monitor: data sources

Heartland Payment System Breach Case Study

8.5 Execute: Mitigation and countermeasures

Heartland Payment System Breach Case Study

14.2 Prevention of Vulnerabilities

14.2.1 Memory Management Vulnerabilities

FAA ERAM Outage Case Study

14.3 Detection of Vulnerabilities

14.3.2 Dynamic Detection

FAA ERAM Outage Case Study

15. Web & Mobile Security

Driver Assistance System Safety & Security Case Study

16. Secure Software Lifecycle

16.2. Prescriptive Secure Software Lifecycle Processes

16.2.1. Secure Software Lifecycle Processes

Tokeneer ID Station Project Case Study

16.2.1.1 Microsoft Security Development Lifecycle (SDL)

Secure Acquisition Case Study 1: Project Initiation
Secure Acquisition Case Study 2: Acquisition/SCRM Project Risk Analysis
Secure Acquisition Case Study 3: Adequacy of Acquisition Practice
Secure Acquisition Case Study 4: Supplier Capability Evaluation

16.2.1.1 (2) Define Security Requirements

SQUARE Case Study
Using Malware Analysis to Improve Security Requirements Case Study

16.2.1.2. Touchpoints

ACME Water Case Study, Exercise 2: Risk & Trust
ACME Water Case Study, Exercise 6: Architecture
ACME Water Case Study, Exercise 9: SEAT & Privacy
Aircraft Service Application Case Study
Drone Swarm Case Study
National Grid SAP Adoption Case Study

16.2.2 Comparing the Secure Software Lifecycle Models

National Grid SAP Adoption Case Study

16.3 Adaptations of the Secure Software Lifecycle

16.3.6 Ecommerce/Payment Card Industry

National Grid SAP Adoption Case Study

16.4 Assessing the Secure Software Lifecycle

16.4.1 SAMM

National Grid SAP Adoption Case Study