Postgraduate Cybersecurity Education for Non-Specialist Professionals

James H Davenport

(University of Bath)

Tim French

What is this about?

- NOT Cybersecurity specialist education
- Rather fulfilling the general requirement that all computer professionals know something about cybersecurity
- Specifically, British Computer Society (BCS) accreditation requirements.
- “Knowledge and understanding of: Information security issues in relation to the design, development, and the use of information systems”.
- Context: currently online MSc courses (see paper https://ieeexplore.ieee.org/abstract/document/11016598 for details)

Topics taught (in our 8-week course)

1) Principles of Security
2) Cyber Security as a Risk and Associated Responses
3) Secret-key and Public-key Messaging
4) Cryptography in Practice
5) Identity, Awareness and Deception
6) What is Big Data and How Secure is it? SQL Injection.
7) Biometrics, 2FA and banking
8) The Weakest Link — Humans

What's not taught (in our 8-week course)

1) Forensics (mentioned, 4 ACPO principles, no details)
2) Cryptocurrency (mentioned in ransomware, no details)
3) Therefore no cryptocurrency forensics
4) Cloud security/ "Shared Responsibiity" (lack of time + devil is in the detail)
5) Dark Web (brief mention under ransomware and sale of stolen data; ethics/security issues with any practical work)

Assessment 1: Norsk Hydro/Travelex [30%]

1) Compare and contrast these exemplars of Ransomware. [20%]
2) Wider implications for Finablr (Travelex owner). [10%]
3) Find corresponding examples from last year, and discuss. [20%]
4) What risk does ransomware pose to your business. [20%]
5) Ask GenAI “Learning the lessons from ransomware attacks is vital. Draw up an idealised incident response timeline (expressed in hours/days before/after D day, the day the attack actually takes place), identifying the target’s actions and responses to a ransomware cyber attack upon a generic fintech (e.g. e-banking) provider. You should show adversarial actions too. The target doesn’t pay the ransom immediately.” [5%]
6) Comment on the answer [25%]

Assessment 2: Payment cards [70%]

A. Make a fake online purchase, submit HTML archive etc. [10%]
B. Individual report on purchase [35%]
    1. What sites do you go to, and which worry you [50%]
    2. Where does the card number go [20%]
    3. What effect would a DNS hack have on your transaction [20%]
    4. To what extent do you understand the HTML/JS/… [10%]
C. Group report: take these five, comment on them and rank them as candidate's for your company's new site [25%]

Conclusions

- Cybersecurity is as much about conveying a mindset as conveying facts, and this aspect is more difficult to explain and assess.
- It is possible to devise assessments that students are grateful for!
- Generative AI is a risk to assessment, but Cybersecurity can be less vulnerable than other parts of CS.