Handed out 26/1/2025.
Answers presented 2/2/2026

Problem Class 1 (Security Engineering 25/26)

Risks & Threat Actors (Lecture 1 & 2)

1. Cyber insurance claims data reveals business email compromise/funds transfer fraud, ransomware and data breaches are the riskiest cyber incidents (see Lecture 1). To what extent do the findings in the FBI's IC3 report align with the cyber insurance claims.
2. All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems. So why is installing the latest software updates still good security advice for most people despite this?
3. Why did ransomware evolve from automated software targeting individuals with fixed demands to targeting companies and opening up negotiations?
4. Recall Ross Anderson's 4-way classification of the threat actor ecosystem (crooks, spooks, geeks and the swamp). Are there actors who fall into multiple categories? Any threat actors who don't fall into any of these?
5. What are some similarities and differences between bug bounty programs and ransomware payments?

Security Policies & Banking Security (Lecture 3 & 4)

6. Was the IC's move to multi-level security for intelligence stored in computer systems more successful in protecting information than the equivalent physical system? what kind of security violations are possible despite MAC?
7. Why is the concept of "trusted computing" particularly important in power metering situations? How are the associated security assumptions supported by periodic physical inspections of the meter?
8. Why is the optimal amount of card not present fraud non-zero? Who benefits from the current liability regime for card not present fraud, and who shoulders the cost?
9. Many banking apps now use on-device biometrics (like finger prints) to authenticate users. How could a criminal log into the victim's account using the only using the criminal's finger print? (There are at least 2 examples, with varying digress of likelihood)
10. Historically, joint bank accounts required a signature from both account owners on both cheques and bank transfer requests. What are the barriers to adopting a similar separation of duties in online banking? Which cybercrimes would this help prevent?

Handed out 26/1/2025.
Answers presented 2/2/2026

Economics & Psychology (Lecture 5 & 6)

11. Microsoft issued patches for 1,246 Common Vulnerabilities and Exposures (CVEs) across its products in 2025. What economic ideas help explain why individuals and businesses continue to use Microsoft products?
12. Antivirus software is sometimes considered a "market for lemons". To what extent is this true, and is it down to hidden information, hidden action, or both?
13. Provide an example of a cyber attack technique that exploits each of: (1) skill-based behaviour; (2) rule-based behaviour; and (3) knowledge based-behaviour. Can you think of an example that exploits multiple?
14. Imagine that you are designing a spear-phishing attack designed to scam Edinburgh students out of money. How would you do it, who (or what) would you impersonate, how would you extract the money, and could you use Prospect Theory to increase your chances? Are there any other social-psychology tricks that might help?