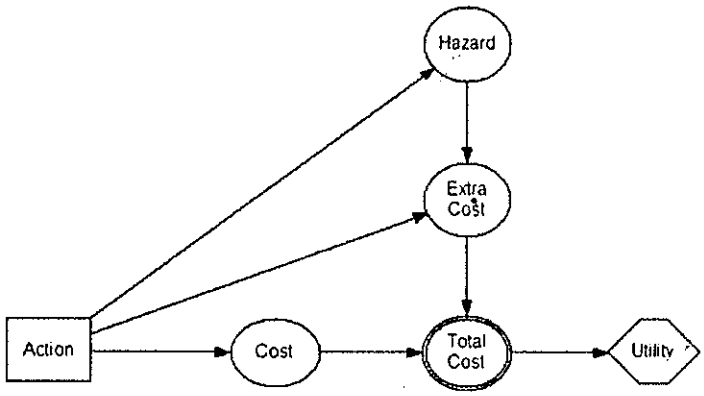
Cyber Risk Management resit exam, 25 January 2018, 9:00-11:00

TUDelft: SPM5442 UTwente: 201500026

Answer in ENGLISH. Start each numbered question (1-5) on a new page. 1-3 on sheet 1; 4-5 on sheet 2. *Min. 1 paragraph / max. 1 page per numbered question. Make sure that what you write is relevant to the question.*

1. In the ComputerWeekly video, the HP expert discussed ways to disrupt the killchain.
    a. Mention 2 best practices that according to the HP expert can contribute to disrupting the adversaries. Illustrate these in the context of disrupting the killchain of cybercriminals trying to steal credit card numbers from a webshop. (4 pts)
    b. Explain how properties of cyberspace and cyber governance change the crime risk landscape for shops compared to the physical environment. (3 pts)
    c. Explain how security policies can help in protecting a webshop against cyber threats. (3 pts)

2. An influence diagram is a causal model with two special node types: decision nodes, representing possible decisions of an actor (square), and utility nodes, representing the utility for an actor (diamond). This is an example of an influence diagram:



    a. Explain what decision can be made based on this diagram and how. Relate your explanation to risk and the FAIR framework. (5 pts)
    b. Explain how the difference between probabilistic and adversarial risk models could be represented in influence diagrams. (5 pts)

3. A company finds that the control strength of their authentication mechanisms is low, and therefore invests in password encryption, password policies, and two-factor authentication.
    a. Explain the relation between control strength and ROSI (return on security investment) using this example. Include how you define control strength (in FAIR) and ROSI. (10 pts)

4. Attacker profiles / threat agent models play a key role in some risk assessment methods.
    a. What is the key difference between using attacker skill and attacker motivation in risk analysis? Use the terms asset, vulnerability and utility in your answer. (5 pts)
    b. In addition to the Threat Agent Library, which 2 other types of libraries are needed in Threat Agent Risk Assessment, and how are they used in the risk assessment process? (5 pts)

5. In this course, different types of risk models and their application to cyber risks were discussed.
    a. Explain why the notion of reachability plays a key role in some cyber risk models. (4 pts)
    b. Compare the benefits and drawbacks of graphical vs. tabular notation w.r.t. comprehensibility of risk models. (6 pts)