Cyber Risk Management mid-term exam, 1 October 2015, 15:45-17:45

TUDelft: SPM5440 (4EC), SPM5441 (5EC)
UTwente: 201500026 (5EC), 192195200 (6EC)

Start each numbered question (1-5) on a new page. Min. 1 paragraph / max. 1 page per numbered question. Make sure that what you write is relevant to the question.

1. It is often argued that cyber security requires adversarial risk assessment rather than probabilistic risk assessment.
    a. What is the difference between probabilistic and adversarial risk assessment in terms of the order in which you can estimate the key FAIR risk variables TEF, V, PLM? Explain your answer using the papers of Jones (FAIR) and Cox Jr. (game theory & risk analysis), and illustrate it with a small example (10 pts).

2. 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. Why do assumptions on attacker knowledge about the system / defenses matter for adversarial risk assessment? Explain your answer. (5 pts)

3. A company finds that humans are the weakest link in their organisation, and therefore invests in a security awareness campaign.

    a. Explain the relation between weakest links and ROSI (return on security investment) using this example. Use the FAIR terminology where appropriate (at least 2 terms from FAIR) and explain how you define ROSI. (10 pts)

4. In the lectures the causal models of Fenton and Neil were contrasted with attack (-defense) trees.
    a. Explain the difference between attack (-defense) trees and causal models. Use small examples for each to illustrate your answer. (10 pts)

5. In the ComputerWeekly video, the HP expert discussed ways to disrupt the killchain.
    a. Which types of controls would you choose to disrupt the killchain of cybercriminals trying to steal credit card numbers from a webshop? Discuss 2 types of controls and their relation to the threat agent attributes. (4 pts)
    b. How would you measure the effectiveness of these controls? (3 pts)
    c. How do properties of cyberspace and cyber governance change the crime risk landscape for shops compared to the physical environment? (3 pts)

TU Delft

Examination TPM

Delft University of Technology - Faculty of Technology, Policy and Management

Course name:	**Cyber Risk Management (/CSE)**	**Course code:**	**SPM5441 (/5440)**
Date:	**October 1, 2015**	**Time:**	**15:45 – 17:45**
Module manager:	**Jan van den Berg**		

Examination questions:

Number of open questions: **5** questions
Number of multiple choice questions: **0** questions
Max. number of points: **50** points

☐ **all questions have the same weight**
☒ **the questions have different weights** (indicated per question)

Total number of pages (incl. cover page): **2** pages

Use of tools and information sources:
During the examination, the use of any tools or information sources (this includes mobile phones, smartphones or any devices with similar functions) is strictly forbidden unless stated below.

Permitted tools and information sources:
☐ **books** ☐ **notes** ☐ **dictionaries** ☐ **readers** ☐ **formulae sheets**
☐ **calculator** ☐ **computer** ☐ **...**

Additional instructions: *(optional)*
N/A

Final marking date:
(the maximum marking period is 15 working days)
October 22 at the latest (aim October 15)

To be handed to the examiner or invigilator:
☒ Examination work with name and student number on each page.
☒ Examination documents

Any suspicion of fraud or any breach of the exam rules will be immediately reported to the Board of Examiners

For more information about fraud:
TU Delft Student portal> TPM> Rules and Guidelines