TU Delft

Examination TPM

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

Course name:	**Cyber Risk Management**	**Course code:**	**SPM5440/5442**
Date:	**January 26, 2017**	**Time:**	**9:00 – 11:00**
Module manager:	**Wolter Pieters**		

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)*
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.

Final marking date:
(the maximum marking period is 15 working days)
February 16 (aim February 9)

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

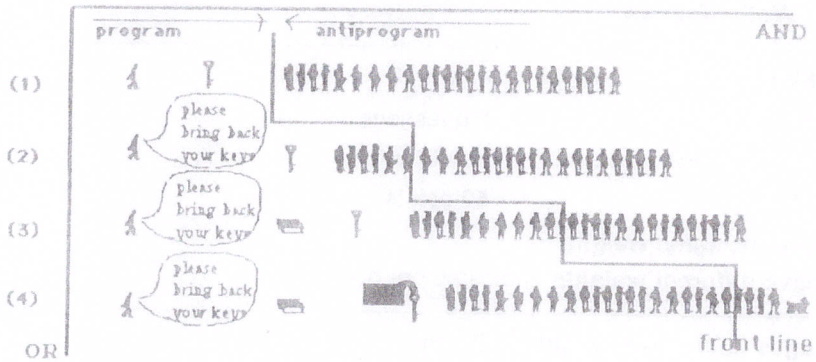
Examination TPM

Cyber Risk Management mid-term exam, 26 January 2017, 9:00-11:00

TUDelft: SPM5440 (4EC), SPM5442 (5EC) UTwente: 201500026 (5EC)

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. The following figure (Bruno Latour) is from the slides of lecture 3. Remember that the person on the left is a hotel manager, and those on the right are guests. The hotel manager tries several options to make the guests return their keys (request, sign, large object attached).



   a. Explain this figure in terms of risk concepts. Use the terms vulnerability, threat capability and control strength in your answer. (4 pts)
   b. Does this situation constitute probabilistic or adversarial risk? Why? (3 pts)
   c. Explain how security policies are represented in this figure. (3 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. Cavusoglu et al., in their paper "A Model for Evaluating IT Security Investments", discuss "quality parameters" of security solutions (firewalls and intrusion detection systems).
   a. Give 2 examples of parameters they use, and explain them. (4 pts)
   b. Explain how the quality parameters are used in evaluating security investment. (3 pts)
   c. How are quality parameters related to the notion of weakest link? (3 pts)

4. There are said to be 4 options for risk treatment: accept, reduce, transfer and avoid. A company expects 5 incidents each year, with an impact of EUR 10,000 each. They can buy equipment for EUR 40,000 that they believe will prevent 3 out of 5 of those for at least 3 years. Alternatively, they can buy full insurance against all incidents for EUR 15,000 per year.
   a. For each of the 4 general risk treatment options, explain how they would influence the FAIR risk factors. (4 pts)
   b. Calculate the 3-year return on security investment (ROSI) of the equipment. (4 pts)
   c. What would be your recommendation to the company and why? (2 pts)

5. Give 2 reasons (from the lectures on cyberspace and cyber governance) why the cyberspace domain makes cyber risk management harder compared to traditional risk management. Explain your answers (5 pts each).