CRM Reading guide 2015

Examination questions are based on understanding

I) the content of lectures provided and

II) the topics discussed in the papers / videos.

The lists below indicate important concepts to focus on when reading / studying the literature. This does not mean that you can skip everything else. All of the papers is exam material unless explicitly stated otherwise.

Mandatory online video material

More materials may be added during the course.

- ComputerWeekly: Managing IT Risk: Trends in Global Information Security
  - Disrupting the killchain
  - Risk tolerance
  - Capability extension

- George Cybenko: The Future of Cyber Security Risk (you can skip the first 3 minutes)
  - How to measure progress?
  - Worst-case vs. specific attacker
  - Where to get the data?
  - Challenges to cyber security risk

Mandatory literature

  - FAIR risk concepts and control types
  - You don’t need to remember the calculation tables

- Several related definitions of cyberspace
- Differences between information security and cyber security
- 3-layer cyberspace model with key assets: cyber securities
- Meaning of the bowtiemodel
- Acceptable risk
- You can skip section 4.0


- Benefits of causal models; limitations of other risk assessment methods
- Terminology in causal models for risk
- Interpretation / semantics of causal models; correlation and causation


- The difference between probabilistic and adversarial risk models
- Assumptions in game theory
- Difference between equilibrium analysis and minimax analysis, and relation to assumptions
- You don't need to calculate equilibriums, or distinguish types of equilibriums


- The role of system models in risk analysis
- Considerations in determining weakest links and the link to risk concepts


- The role of attacker models in risk analysis
- Relevant properties in attacker / threat agent models and how they can be used in risk analysis
- Combining attacker models with system models
  o Assets, architecture graphs, and reachability
  o Possible paths and their likelihood
  o Link to attack trees

  o Types of metrics
  o Questions that can be answered with metrics
  o Relative and absolute metrics
  o Relation to qualitative approaches

  o Obviously the “key points”
  o Definition and calculation of ROSI
  o Quantifying exposure, mitigation and solution cost, and issues involved
  o Link to FAIR concepts

  o Approaches to justifying security investments and their limitations
  o Components of a typical security architecture
  o Metrics for the quality of components
  o The kinds of parameters that are used in investment models
  o The kinds of calculations that are used in investment models
  - Why there is a need for a new research paradigm proposed termed "Global Systems Science"
  - Examples of system instabilities and cascading effects
  - What global systems science challenges have been identified by Helbing

  - How Internet governance is defined illustrated by some example questions
  - The five global policy debates mentioned by DeNardis
  - The impact of privatization