Problem Description

In recent years, an increasing number of ICT security incidents have been reported. Hence, organizations need to be prepared to handle incidents caused by both known and unknown vulnerabilities. Typical incidents include both general and single-purpose attacks caused by malware, in addition to minor errors with severe consequences. Several well-established standards and guidelines addressing incident management exist. Several factors are involved in determining how successfully organizations respond to ICT security incidents.

The main research question of this thesis is as follows:

- How do large organizations perform information security incident management in practice?

The main research question is further divided into sub-questions. A solid basis for discussing the main research question will be established by answering the following sub-questions:

- What plans and procedures for information security incident management are established in organizations?
- To what extent are existing standards/guidelines adopted in plans for information security incident management?
- How have previous information security incidents been handled in accordance with predetermined plans?

In order to answer the research questions information on incident management in various organizations as well as about actual incidents will be gathered. Experiences from a variety of incidents will be systematized and a study of incident handling processes will be performed.

Students:	Cathrine Hove and Marte Tårnes
Assignment given:	21. January, 2013
Supervisor:	Maria B. Line
Responsible professor:	Karin Bernsmed