From Incident Response to Incident Response Management (IRMA)

Lillian Røstad

Lillian.Rostad (a) sintef.no

Norwegian Centre for Information Security (SIS)

SIS

7/23/2004

www.norsis.no

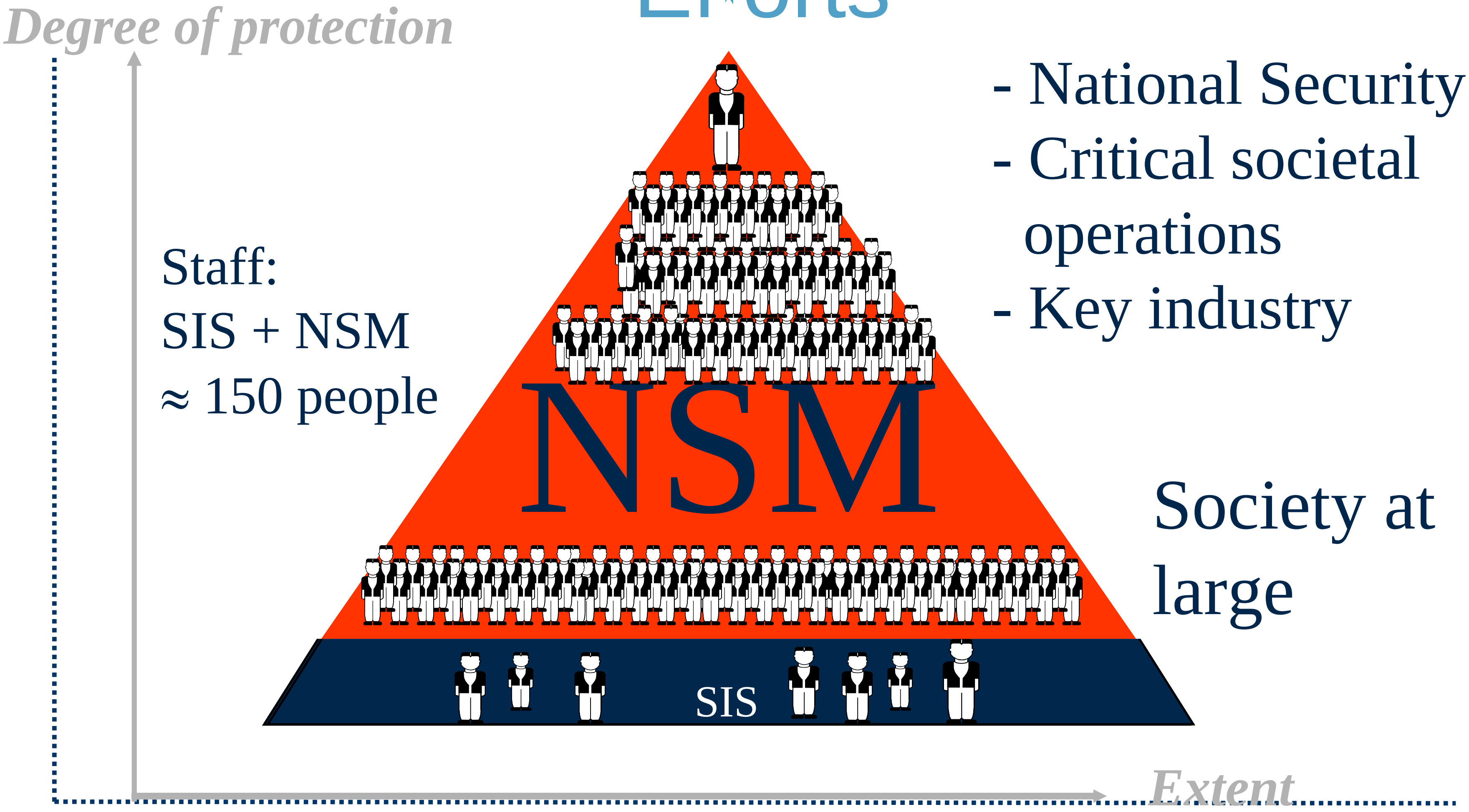
Presentation outline

- About SIS
- IR: technical aspects
- IR: organisational and cultural aspects
- From IR to IRMA

Main Objectives of the Centre

- To survey the threats towards information and communication technology (ICT) systems in Norwegian society
- Spread security knowledge and expertise about threats and their countermeasures
- Network with organisations providing similar services in other countries
- In *trial period* not responsible for security and preparedness in emergency situations

SIS Complements Existing Efforts



Degree of protection

Staff:
SIS + NSM
≈ 150 people

NSM

SIS

- National Security
- Critical societal operations
- Key industry

Society at large

Extent

SIS’ Long-term objective

The objective of the centre long-term is to be responsible for the national co-ordination of tasks within incident response, warning, response for threats or attacks, and exchange of experience

Contact Point

www.norsis.no

Incident response: technical aspects

- *Incident response (IR)* is the process of handling a computer security related incident involving infrastructure and data.
- Traditionally, incident response has been about putting out the fire and returning all systems to normal operation – the ultimate goal being to minimise downtime, loss of business and economical consequences.
- IR “state-of-the-art” mainly focuses on technical aspects

Incident response – technical and organisational aspects

- Human related factors are often found to be the weakest link.
- An optimal incident response planning methodology needs to include the human aspects as well as the technical.
- The possible employment of new countermeasures or adjustment of existing defences after an incident will often necessitate adjustments in the management and employee attitudes and procedures (e.g. skill development, cultural changes and increased awareness) as well as appropriate technical changes.

From IR to IRMA

- *Incident Response Management (IRMA)*
  - *includes all aspects of appropriate incident response planning – technical, cultural, and organisational issues; from risk assessment, via immediate recovery to documentation and learning from the incident at all levels of an organisation.*

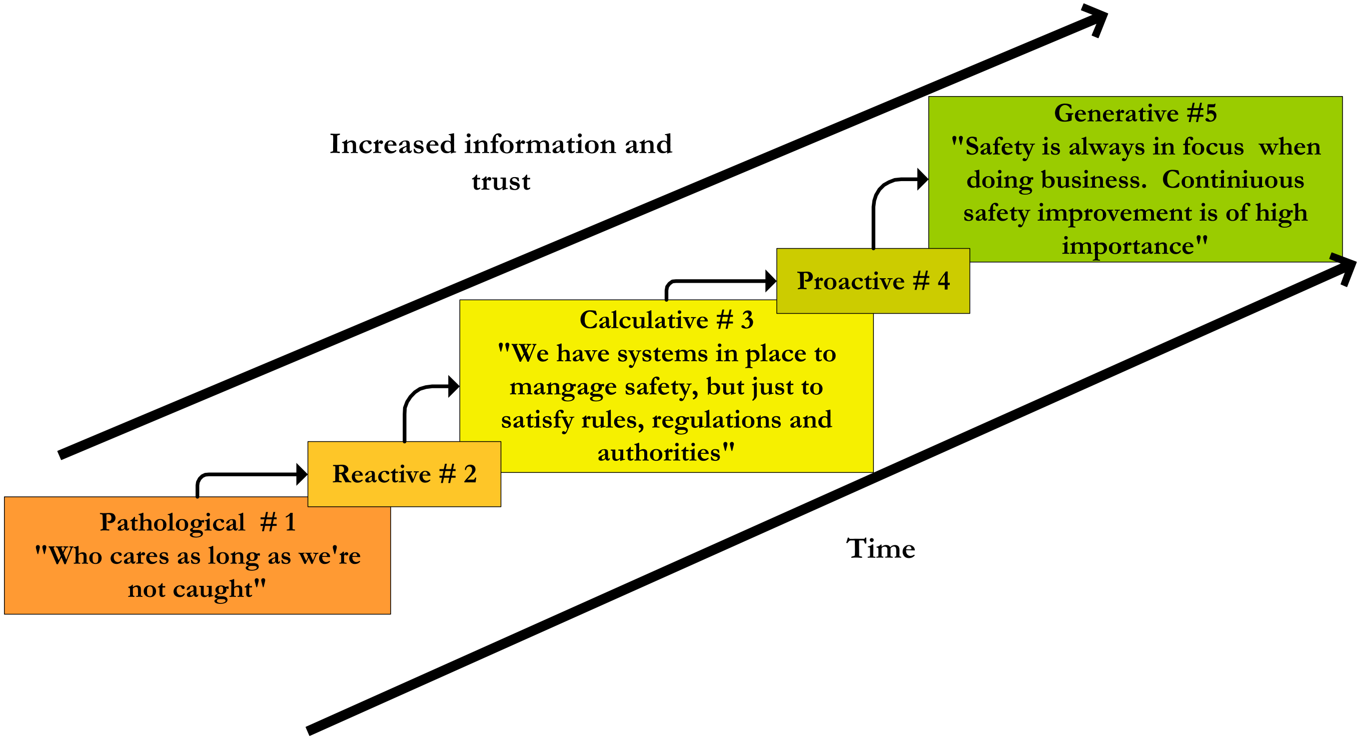
IRMA

- Introduces education and lessons learning as a vital part of incident response.
- It not only includes technical considerations, but also management and cultural issues.
- Risk management is a key factor in establishing a proper framework for incident response.

Learning from experience

- Organisations should try to maximise learning from an ICT security incident. Key questions to be addressed are:
  - How could this happen to us?
  - Why were we vulnerable?
  - How can we prevent this from happening again?
- To incorporate a suitable level of security one first needs to do a thorough risk assessment of the company and existing ICT infrastructure.

Safety culture



Increased information and trust
Generative #5
"Safety is always in focus when doing business. Continiuous safety improvement is of high importance"
Proactive # 4
Calculative # 3
"We have systems in place to mangage safety, but just to satisfy rules, regulations and authorities"
Reactive # 2
Pathological # 1
"Who cares as long as we're not caught"
Time

IRMA trials in the oil and gas sector

- It is of vital importance that CNI, such as an oil installation, is stable and maintainable.
- Safety culture must be seen in relation to incidents and the risk assessment and not as issue in it self. A major strength of an incident driven approach is that the safety issues, the organizational issues and the cultural issues could be discussed in relation to incidents that management and employees are familiar with.

Key lessons vs Proposed Methodology

- A holistic view of Safety culture (Safety culture is difficult)
- Interaction and involvement from the stakeholders
- Organisational learning with participation from key stakeholders

- Definition of Safety Culture includes all key components. (Good safety culture is exemplified.)
- Participation inside the company and across companies
- Establishing a methodology to achieve double loop organisational learning by changing “governing variables” as values, norms, procedures....