



Information Security Awareness and Behaviour

Per Oscarson
Technology Nexus Security
Stockholm, Sweden

Per Oscarson

- Management consultant at Nexus
 - Director for the "Information Security School" for professionals
 - The method "Secure behaviour"
- Former university lecturer at Örebro University, Sweden (1996-2004)
- On-going doctoral thesis at Linköping University, Sweden: *Actual and Perceived Information Systems Security*

What is the problem?

Recent surveys show clearly that shortcomings in human behaviour lay behind the majority of incident costs, and

Awareness raising is the greatest information security challenge for in the future

For example:

- 2004 CSI/FBI Survey
- Ernst & Young Global Information Security Survey, 2004
- Information Security Culture, Information Security Forum (ISF), 2000
- Meta Group
- Krisberedskapsmyndigheten "Preparedness for malicious code", 2005

However...

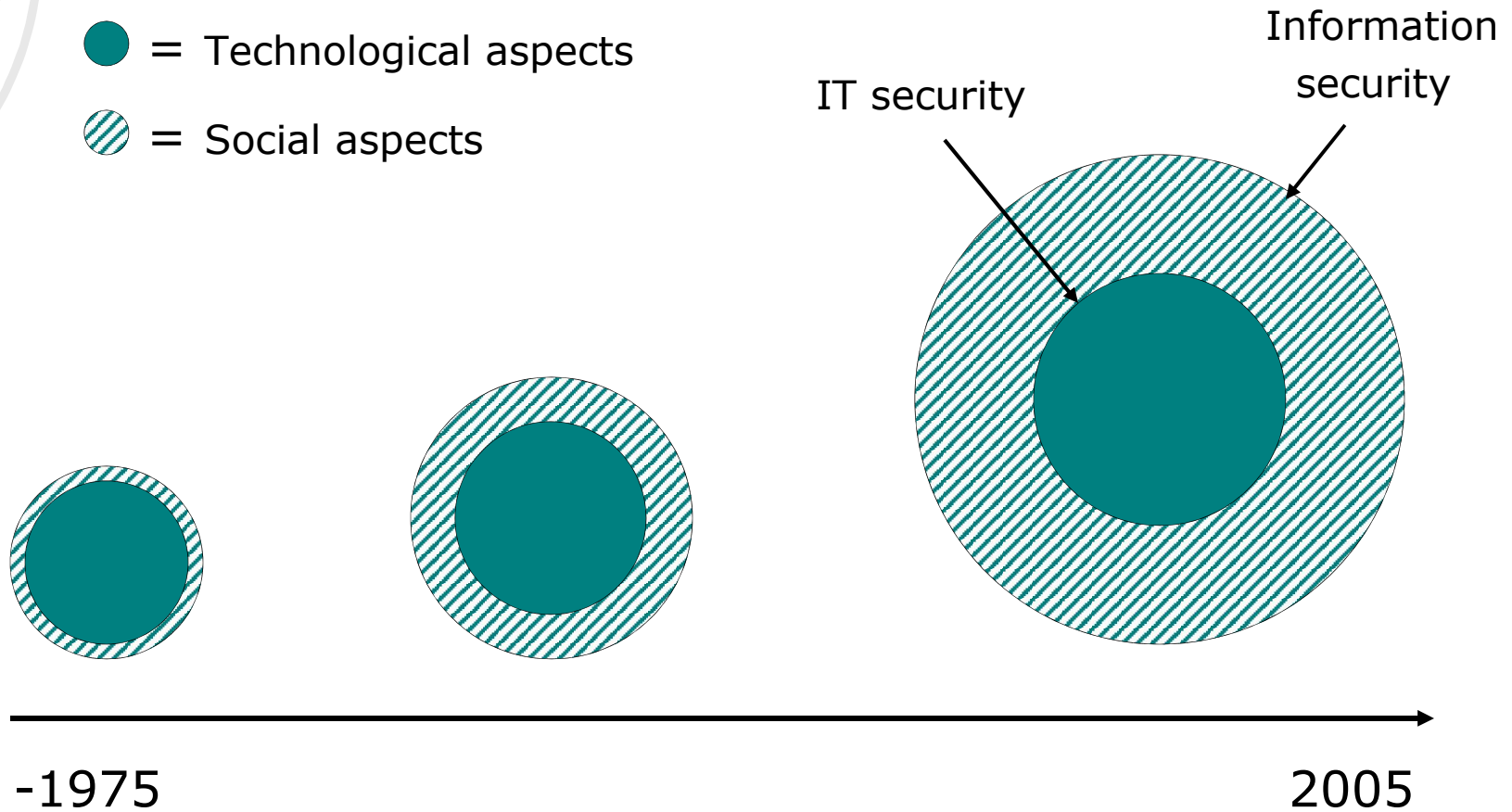
Investments in this area is not in line with its impact

but

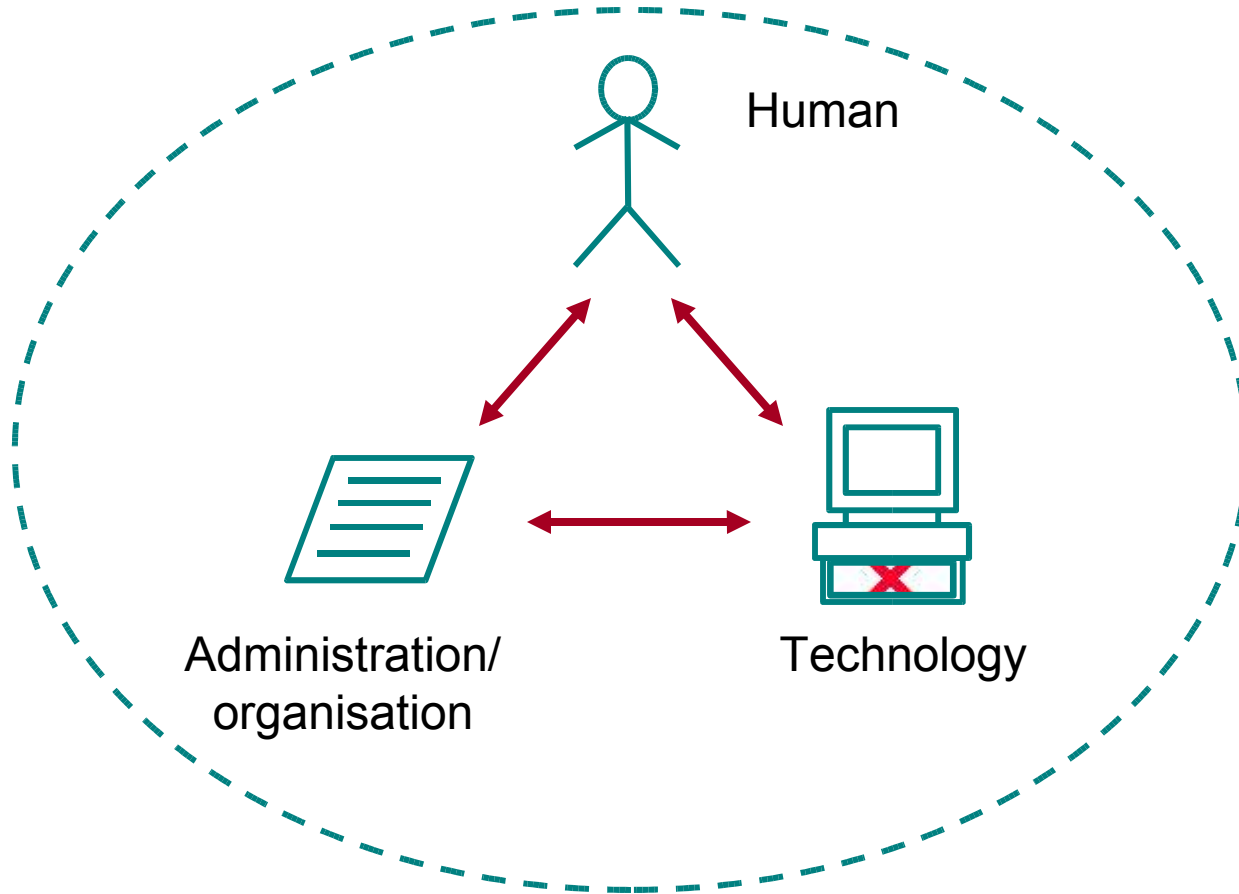
There is an increasing awareness that awareness is important...

Information security – not only technological aspects

- = Technological aspects
- ◌ = Social aspects

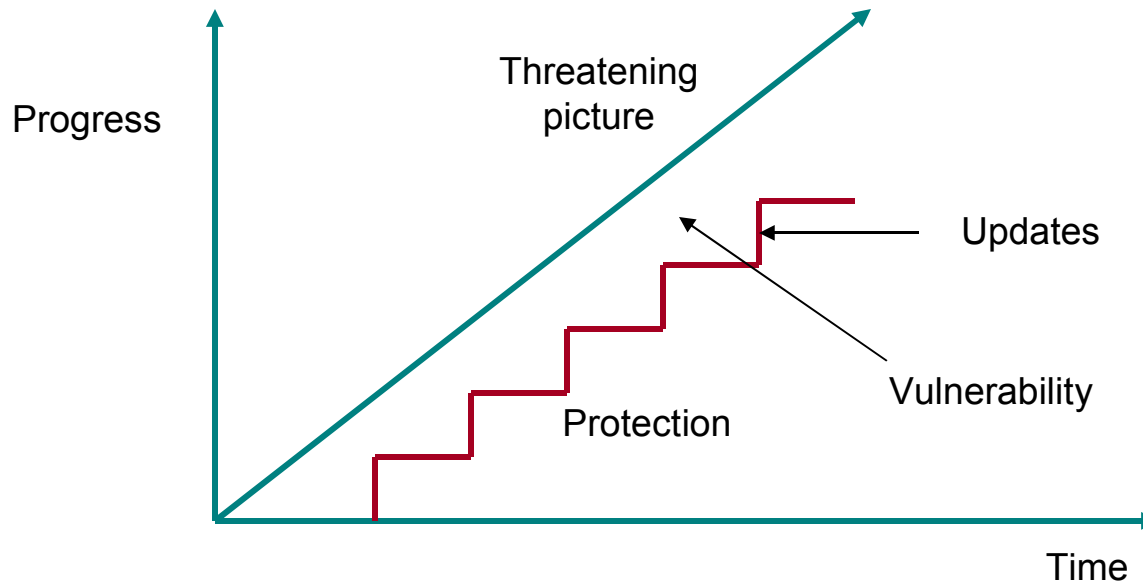


Information security requires a holistic view

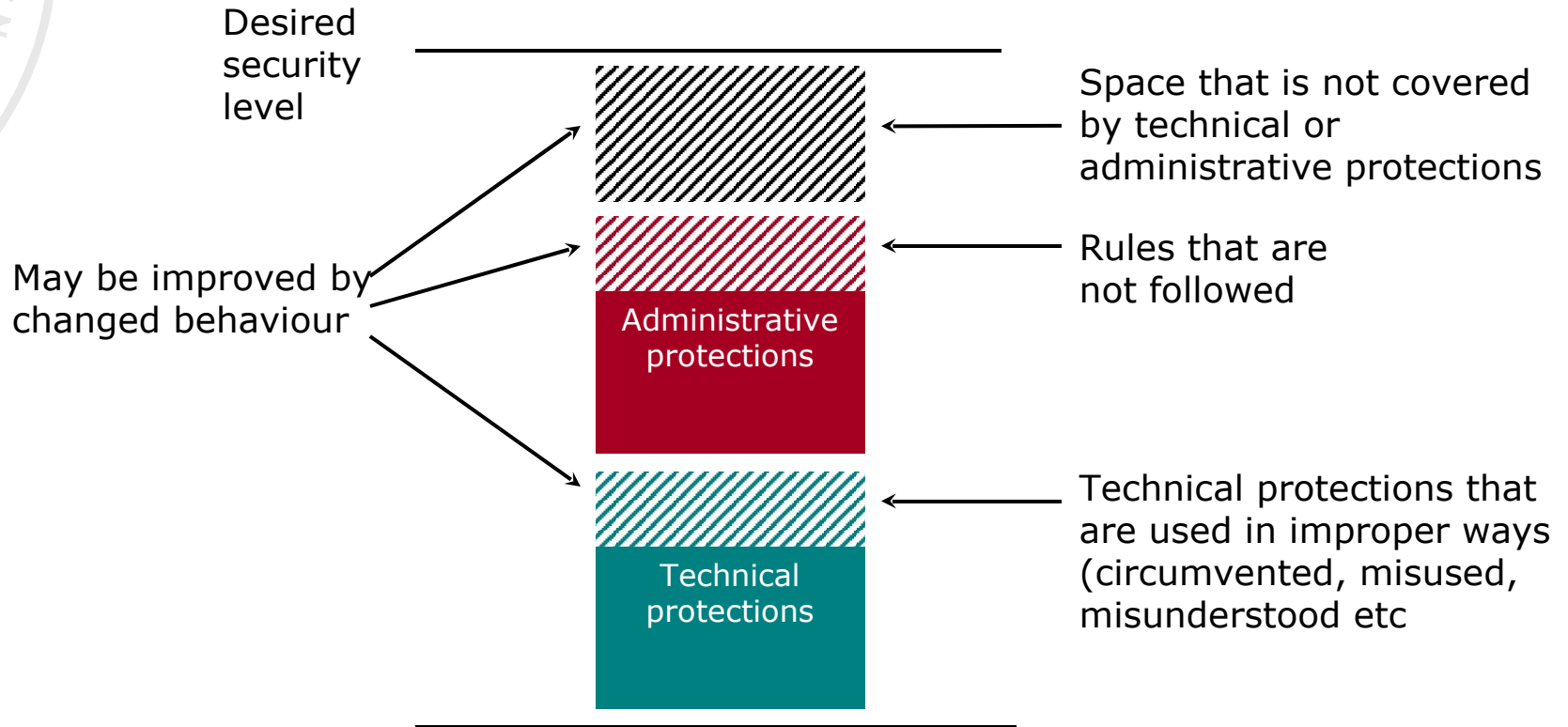


Security is not stronger than the weakest link!

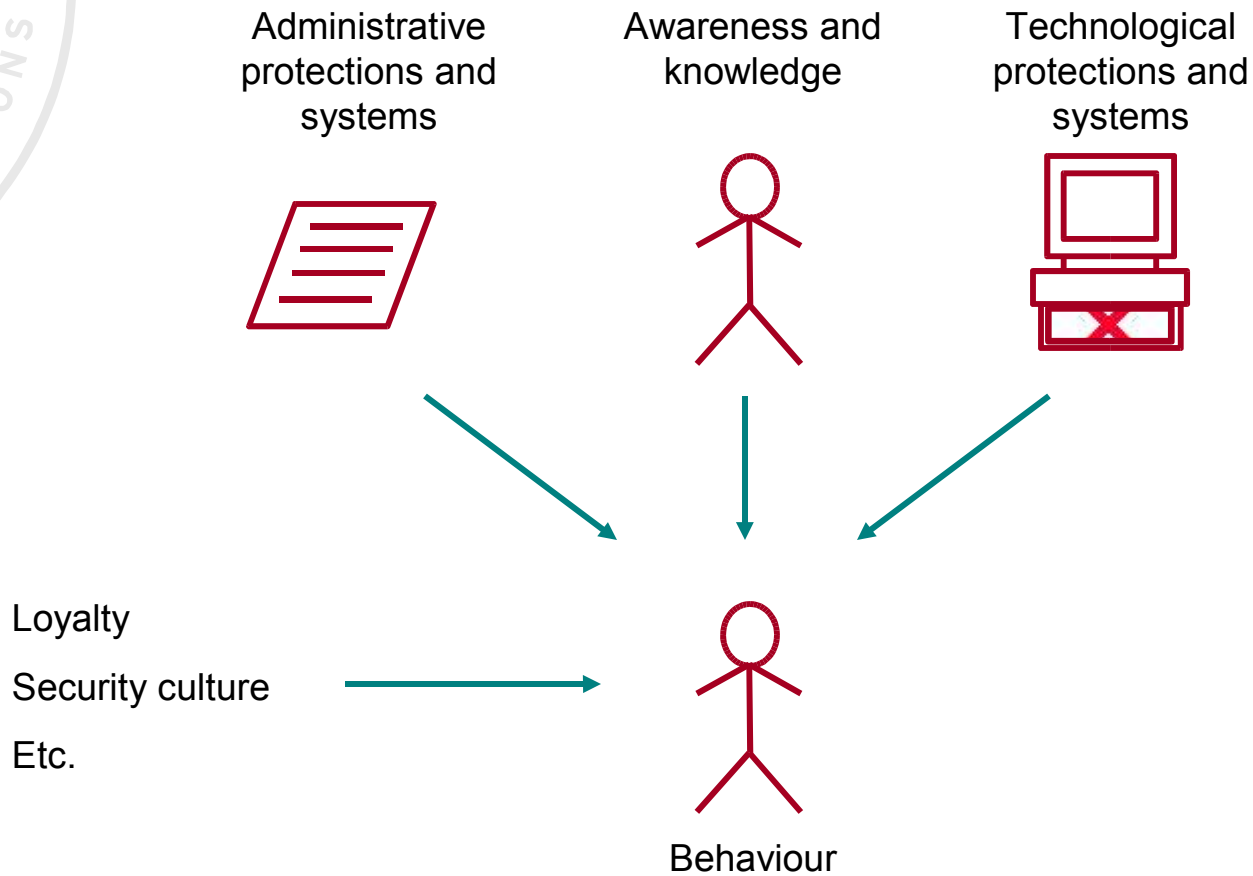
Awareness are dynamic – technology and policies are static



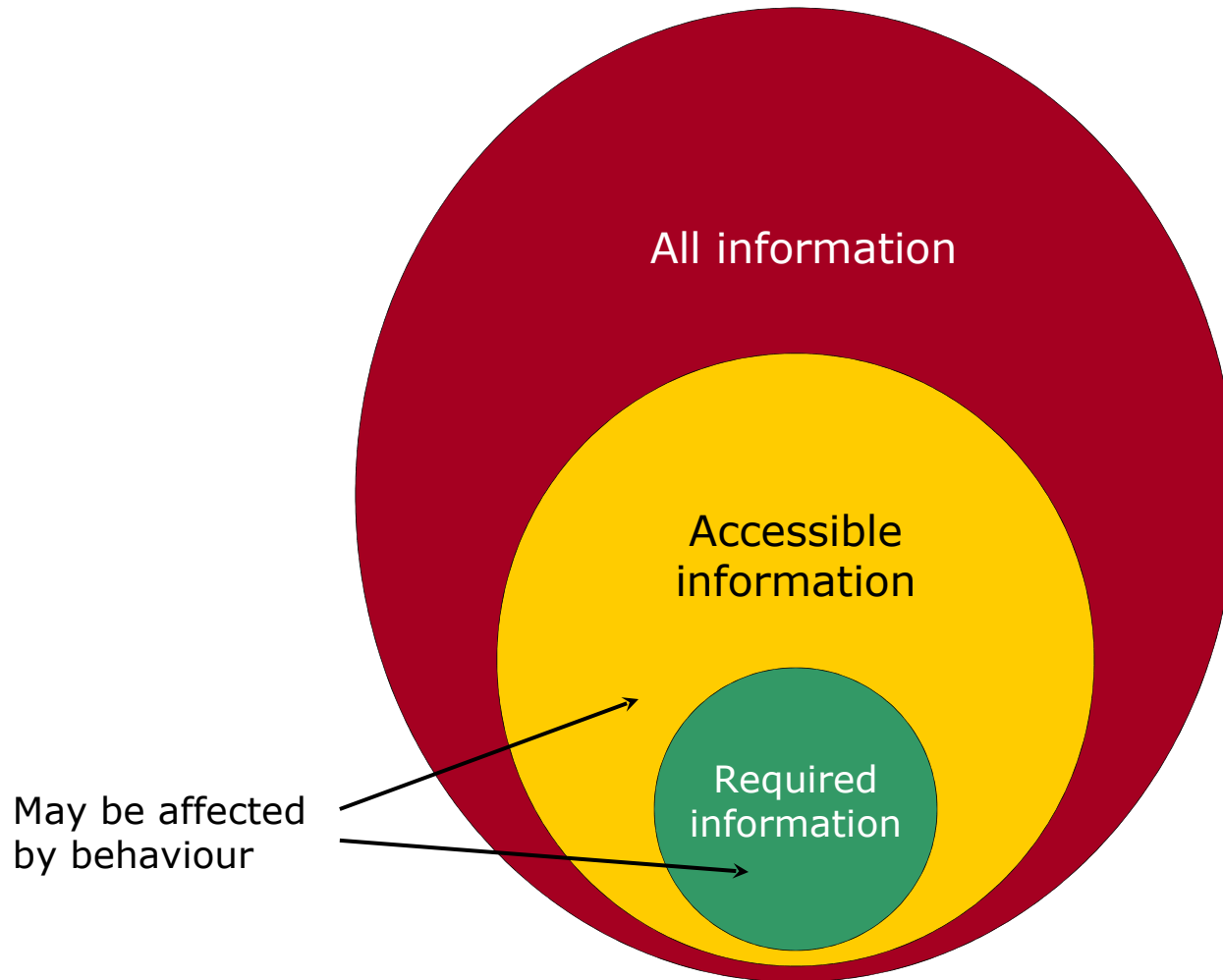
"Where" are the behaviour and awareness?



Factors that affect the behaviour



Required vs accessible information



The method *Secure Behaviour*



Phase 1

How is the current situation?
Which vulnerabilities?
Which measures will decrease or eliminate the vulnerabilities?

Phase 2

Which measures are economical rational to implement?

Phase 3

Implementation of measures
Evaluation

Categorisation of the target group

- Important – the message must be adjusted to the audience
 - To simple is boring
 - To advanced is neglected
- Temporary and outsourced staff is often forgotten!
 - *Consultants, trainees, students, cleaners, etc.*
- Top management and IT departments key groups
- Division may be done on several bases, e.g.:
 - Department, function etc.
 - Information systems
 - Current pre-knowledge

Activities for increasing the information security awareness

- Lectures and seminars
- Symbols, logotypes, mascots etc.
- Printed matters
 - Posters, folders, pens, mouse-pads etc.
- “The information security day”
- News letters
- Self studies
- Scenarios
- Participations in security work
- Information security ambassadors
- Competitions and awards
- ...

Pedagogical advices

- Explain background and contexts
 - Not only *what* and *how*, but *why*
- Multiple senders
 - Some people have more confidence in top management than the local management and vice versa
- Multiple media – people adopt information in different ways
 - Reading, listening, watching etc.
- Doing is stronger than saying
 - People do as other people do, rather than what they are told to do!
 - Especially true when it comes to leaders, who must work as good examples
- Mix positive and negative mechanisms
 - Ex. Positive: Awards, encouragements, successful examples
 - Ex. Negative: Controls, penalties, negative examples

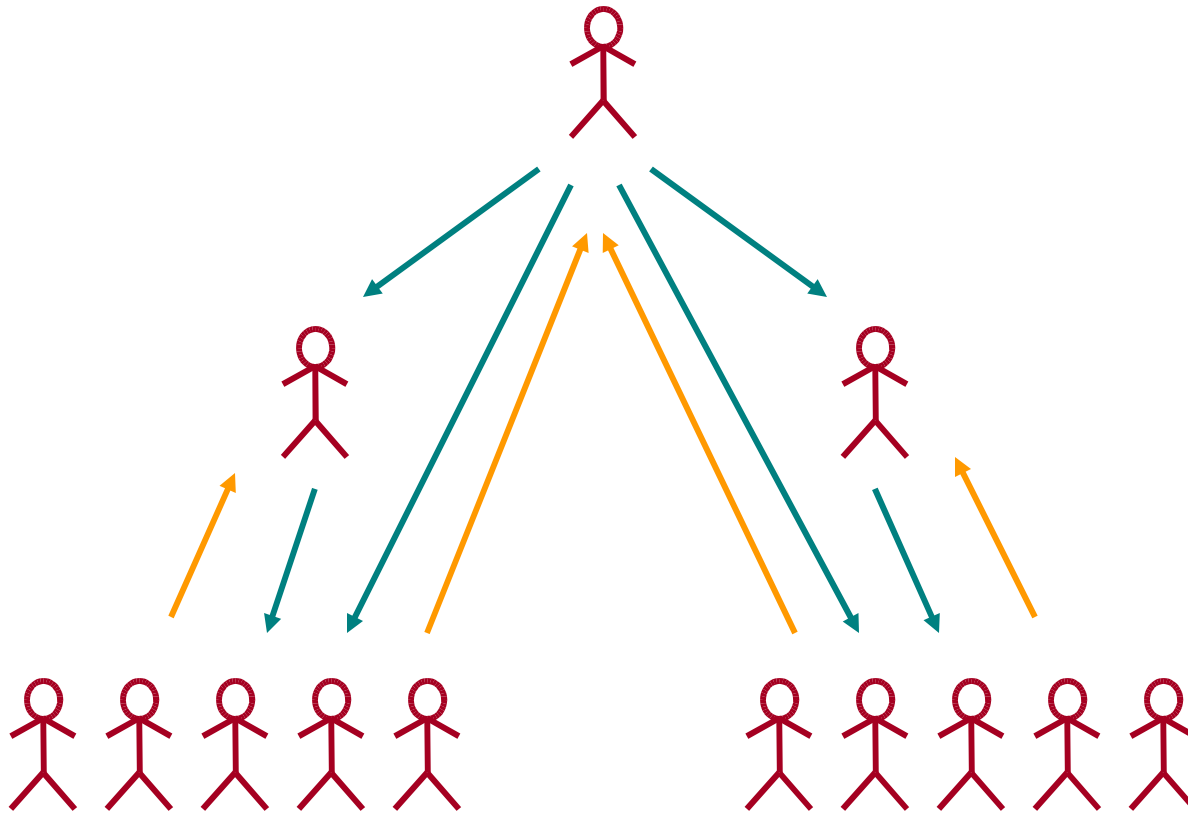
Contextual understanding



Commitment and motivation

- Education and information need resources – top management are the first who must be committed
- Focus on the business impact, i.e. not only *what and how*, but *why*
- Participation increases acceptance and commitment
- Commitment and motivation may be used as complement to formal and legal agreements

Not only top-down, but also bottom-up!



Questions?

Thank your for listening!

per.oscarson@nexus.se