

Awareness, Behaviour and Policy

from a senior management view

John Lindström, PhD

john.lindstrom@ltu.se

LuSec 2010, 19-Feb-2010

Agenda

- Information security
- Awareness
- Behaviour
- Policy

- Discussion on relations...

Information security?

→ Information + IS + IT

- CIA is just the beginning... (Stamp, 2005)
- Changes affecting the business and risk management have expanded the view of confidentiality to give ways for new laws and rules on privacy (Wylder, 2004)
- Security seen from a business executive's perspective need additional components as cost effectiveness and ease of use, approaching from a risk management standpoint (Wylder, 2004)
- Dhillon (2007) sees CIA as principles like responsibility and accountability, and means that information security "*needs to become a more fundamental function of the corporation for solid and widely accepted measures and practices for information systems security to take hold*"

ISO/IEC (1996) suggested definition: **CIA + auditability/accountability, authenticity and reliability**

Awareness (of information security)?

- Often senior managements lack awareness of information security, and information security competes for attention with other topics that more visibly contributes to objectives and short term results.
- It is necessary to enhance the awareness of information security among all employees. The key to success is to raise the level of awareness and understanding of the senior management (Kajava et al, 2004)

Problems

- Not much accumulated research (Siponen, 2001), but deemed as a very important research topic (McClean, 1992; Spurling, 1995; Thomson and von Solms, 1998; Straub and Welke, 1998; Siponen, 2000).
- No (or very few) tested awareness models that are established
- Awareness needed before training/practice to achieve learning and/or change in behaviour (Thomson and von Solms, 1998 and 2006)

Behaviour?

- Dhillon (2007) means that the key to interpreting structures of responsibility is an ability to understand the underlying patterns of behaviour.
- Also important according to Dhillon and Backhouse (1996) is to understand the behaviour of stakeholders and where communication breaks down as this renders security problems.

Problems

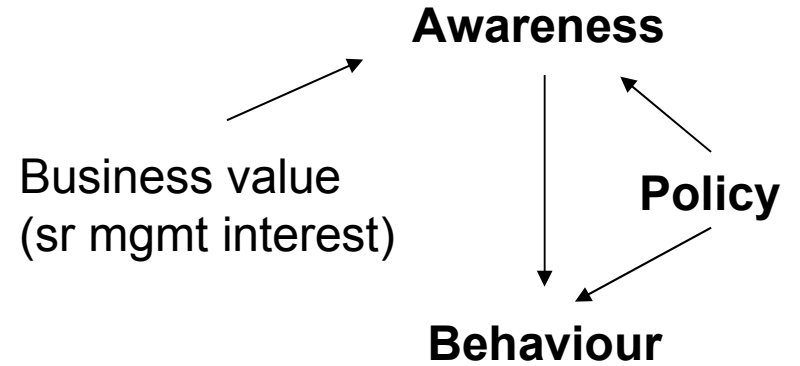
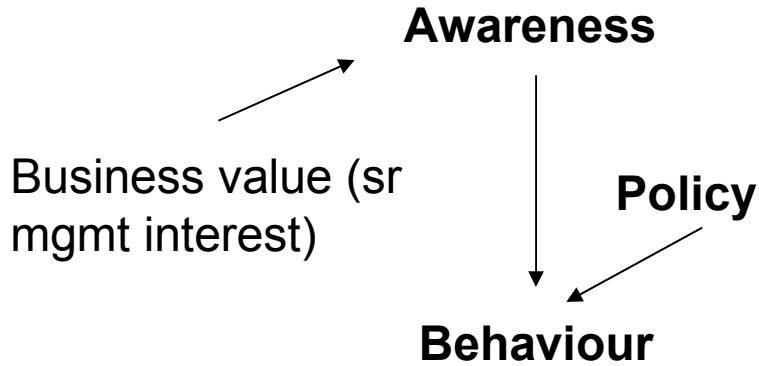
- Can the insight that formal information systems security dimensions, responsibility/authority structures, understanding behaviour, where communications breaks down create an interest among senior managements to take ownership for information security?
- Role-models – senior management – important? What happens otherwise?

Information security policy?

- Rules – informal and formal ones. Need to work together (Kolkowska, 2005)
- Informal rules, or values, start to develop from the inception of an organization and continue to develop during the life-cycle of the organization (Hofstede, 1990)
- The formal rules, or policies, are decided rules that are grouped together in policies for different areas. The purpose is to guide the members of an organization on how to behave internally as well as externally while acting on behalf of the organization.
- A more specific purpose, from a senior management view, is to protect an organization and its assets
- The security should originate from the policy (Whitman and Mattord, 2005)

Problems

- Acceptance – rules followed? Role-models?
- Need to develop a security culture → "glue" (Dhillon, 2007)



?

