Information security culture:
A management perspective

Background - Why is it necessary?

- organizations need information systems to survive and prosper

  → need to protect their information assets.

- the processes needed to protect these assets are dependent on: human cooperated behavior

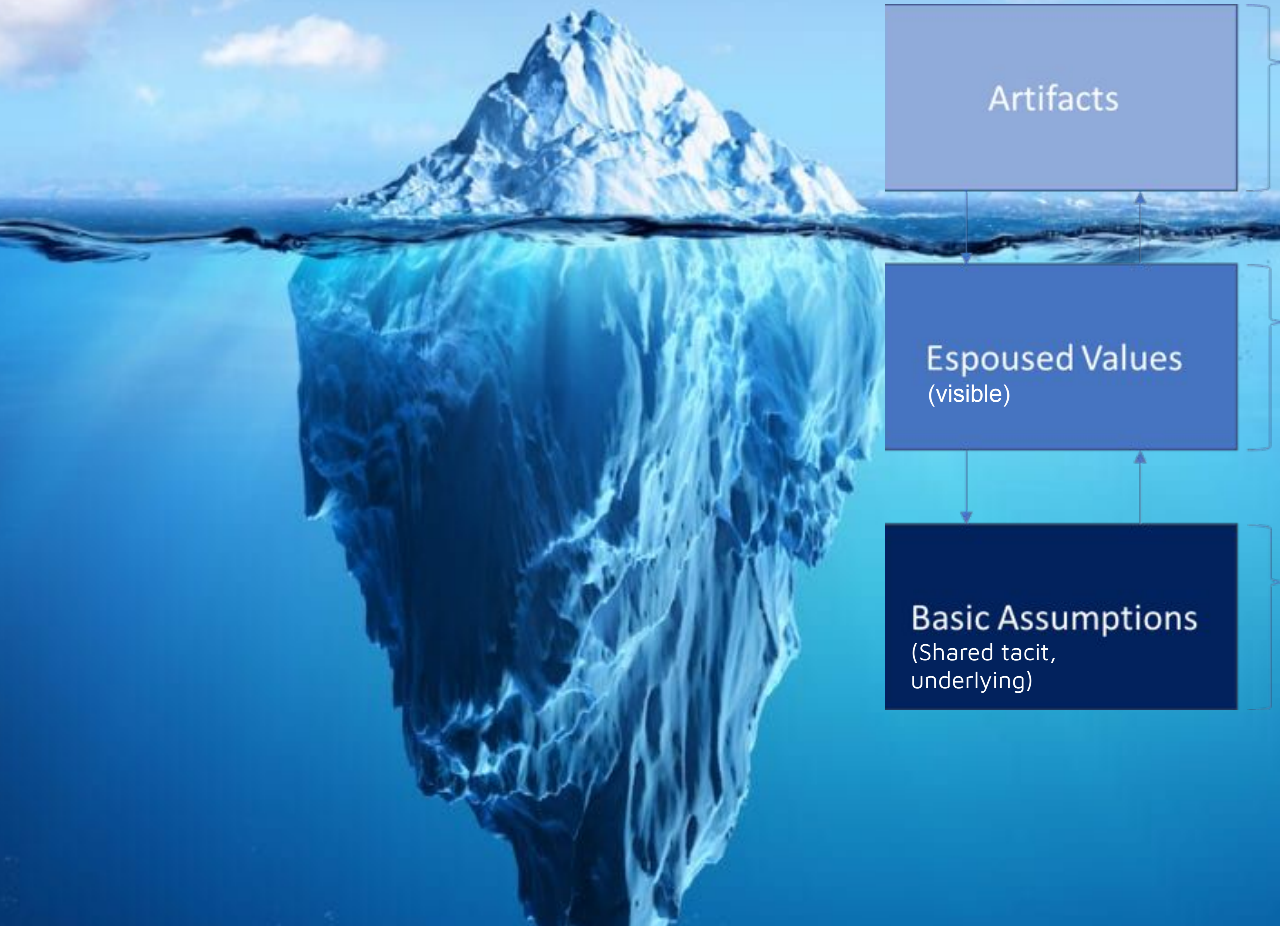
  → greatest threat to information security (no adequate level of user cooperation, knowledge)

- key to managing human factors

  → establishment of organizational sub-culture “information security culture”

  →however, still existence of “trade offs”/”conflicts of interests” that need to be managed

Corporate culture (Schein)



Artifacts

Visible manifestation of organizational culture (i.e., organizational structures, processes and behavior patterns such as rites and rituals)

Espoused Values
(visible)

Formalized statements of organizational culture (organizational strategies, goals and philosophies)

Basic Assumptions
(Shared tacit, underlying)

Implied suppositions of organizational culture which are invisible and include unconscious beliefs, thoughts and feelings that are taken for granted

Information security culture

Artifacts

to perform information related tasks securely
How to perform: day-to-day in a secure way

Espoused Values

policy document adequately address to the organization’s security needs (needs to know what to include)

Basic Assumptions
(Shared tacit)

beliefs and values of employees: knowing why a specific control is needed, might play a vital role in ensuring compliance

Knowledge

Necessary underlying Information Security related Knowledge (What, How, and Why)

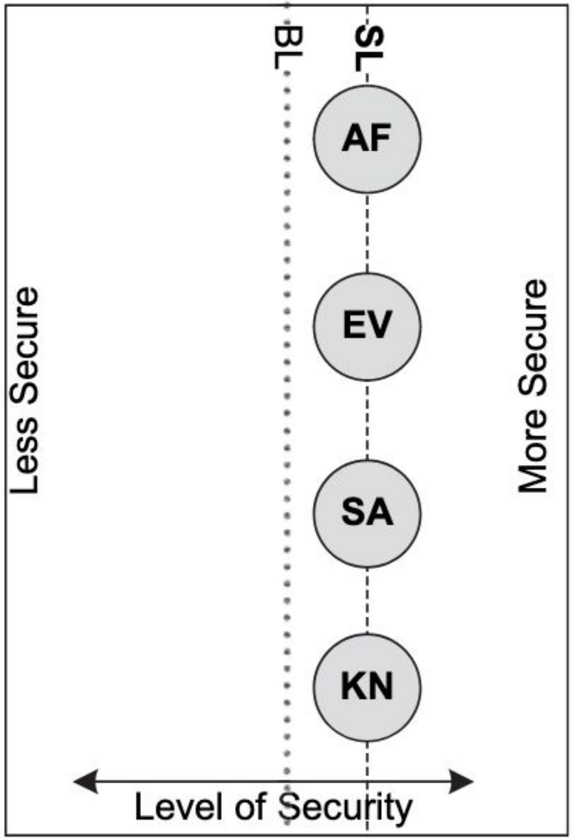
Awareness campaign → key element: to ensure

Basic elements and terminology of the conceptual framework

BL: Minimum Acceptable Baseline – This line indicates what would be an acceptable minimum security baseline

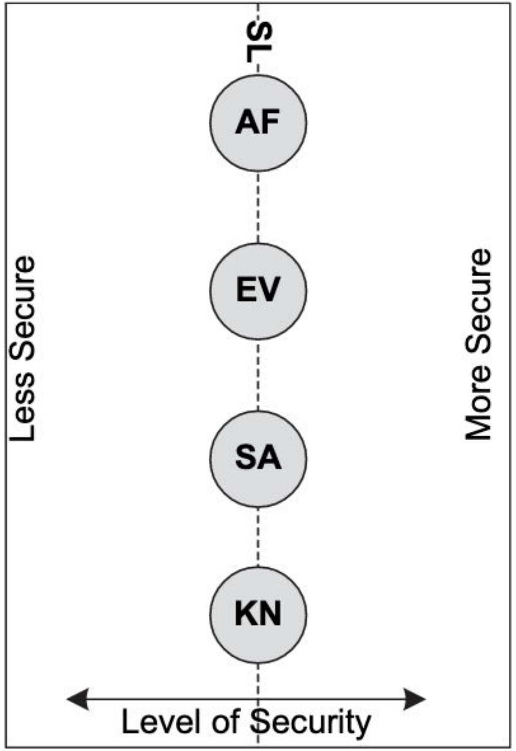
SL: Nett Security Level – This line indicates the actual nett effect of the culture on the overall security effort -> the cumulative effect of the four underlying levels of the culture

SL > BL more secure
SL = BL neutral
SL < BL less secure



AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

Interpreting the conceptual framework

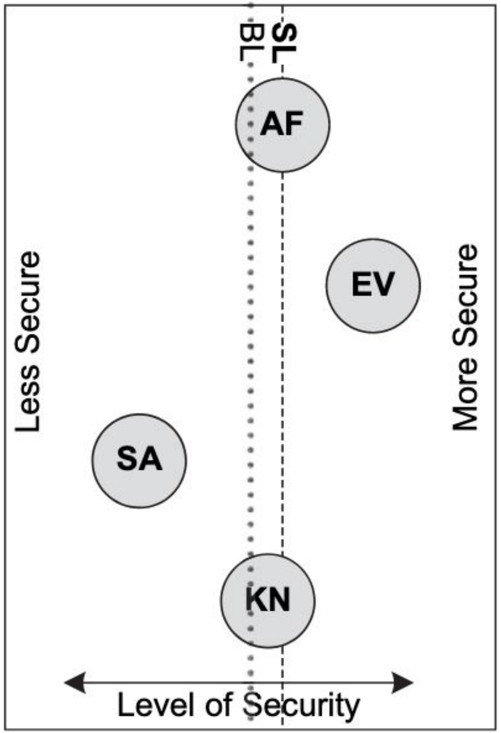


AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

‘‘Neutral’’ and Stable

- desirability of the various levels of culture is ‘‘neutral’’, or average
- various levels will neither negate nor reinforce the effects of other levels on the overall security
- such a culture would thus be predictable and stable

Interpreting the conceptual framework

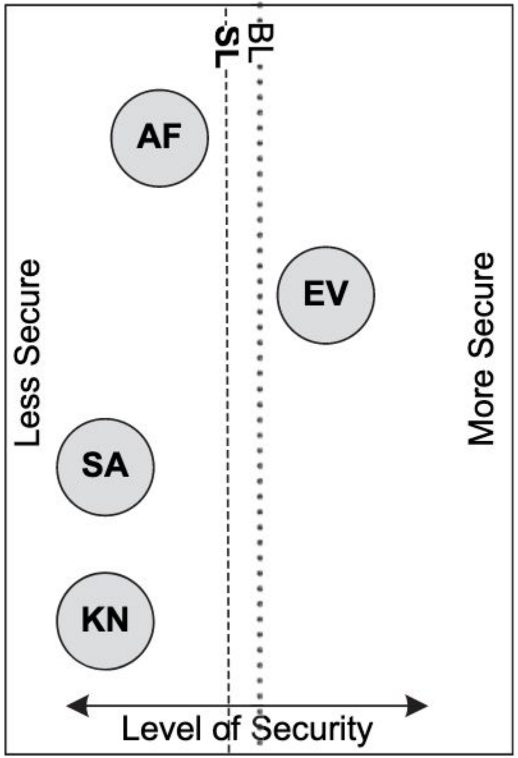


Secure and ``Mostly Stable’’

- the espoused values and the shared tacit assumptions in this culture are of sufficient strength to meet the minimum acceptable baseline standard
- In this culture, the employees do not have the requisite level of information security related knowledge
  -> *policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lacks the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lacking amongst the responsible employees*
- It is thus possible for the measurable artifacts to fall short of the minimum acceptable baseline
- This misalignment between the various levels also means that it would be difficult to predict the exact relative strength of the overall security level

AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

Interpreting the conceptual framework

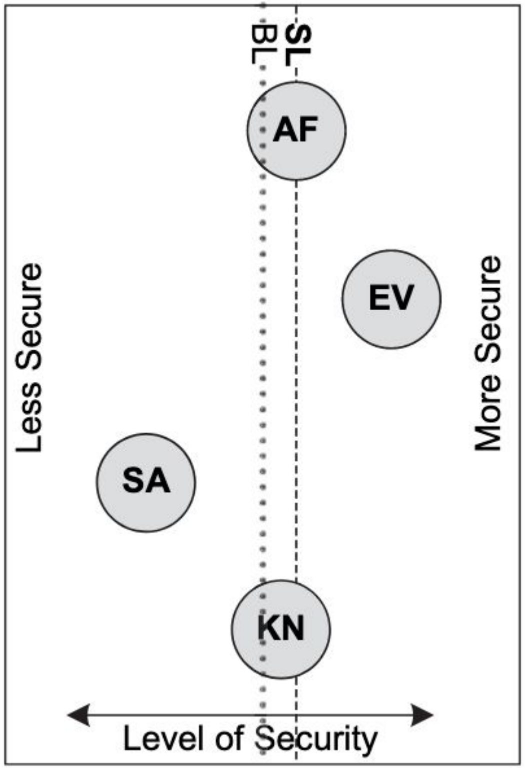


Insecure and Unstable

- The various levels contributing to the culture are not aligned
- nett effects of the culture might be unpredictable, due to the opposing forces at play in this culture
- The espoused values are very desirable, but the users lack the requisite knowledge and do not have the desired beliefs and values, resulting in a measurable artifact level that is not secure
- be very difficult to predict the nett security level of this culture
- Such a culture would not be a desirable culture. In order to make this culture more desirable it would be necessary to address both the lack of knowledge and the underlying shared tacit assumptions of the employees

AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

Interpreting the conceptual framework

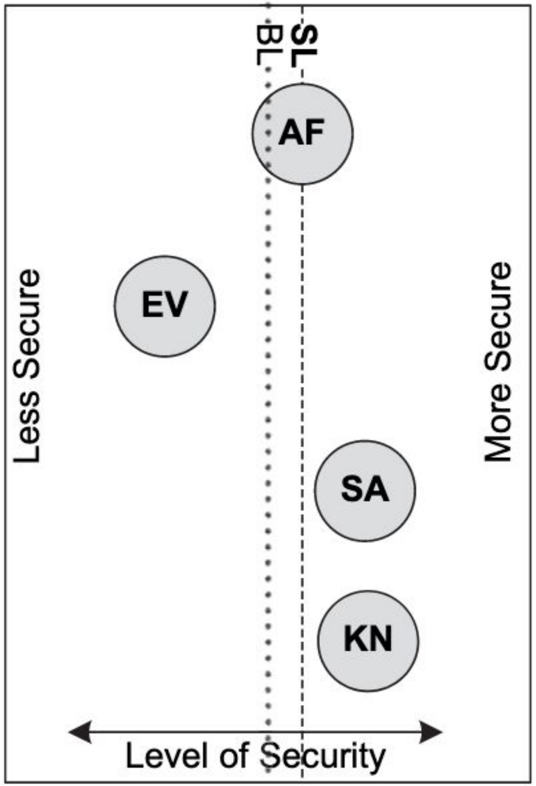


AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

Secure and Unstable

- The various levels contributing to the culture are not aligned. The espoused values are desirable, and the users have adequate knowledge
- resulting in an overall culture that is more secure than the minimum acceptable baseline
- this culture should be considered not desirable, because its effects cannot always be predicted -> It might be possible for the users to behave insecurely with regards to a specific security control because the specific control conflicts with their beliefs
- If employees can be convinced of the importance of their respective roles and responsibilities towards the organization’s information security the culture should start to align itself

Interpreting the conceptual framework



AF: Artifacts; EV:Espoused Values; SA:Shared tacit Assumptions; KN:Knowledge

Secure and Unstable

- various levels contributing to the culture are not aligned. In this case the figure models the scenario where the organization is small and all staff are skilled IT professionals who have both the requisite knowledge levels and the personal belief systems that enable secure behavior.
- there are little or no espoused values
- not a desirable culture -> without adequate security policies (espoused values) in place,there can be no guarantees of desirable behavior.
- appointment of additional staff members who might lack the underlying security knowledge can easily move the observable artifacts in this model back towards the less secure side
- espoused values will never align themselves without active intervention.

Additional Information

- above examples only reflect a few possible scenarios
- the ‘‘perfect security culture’’ = is completely inelastic (one where all four underlying levels are stronger than the minimum acceptable baseline and perfectly aligned relative to each other)
- model is abstract and not quantifiable