

MANAGING INFORMATION SECURITY IN GROWING SMEs

Ilona Ilvonen
TUT



Background

Large amount of information security management literature written for large companies (e.g. Tipton & Krause 2004, Egan & Mather 2005, Whitman & Mattord 2003, Kairab 2005)

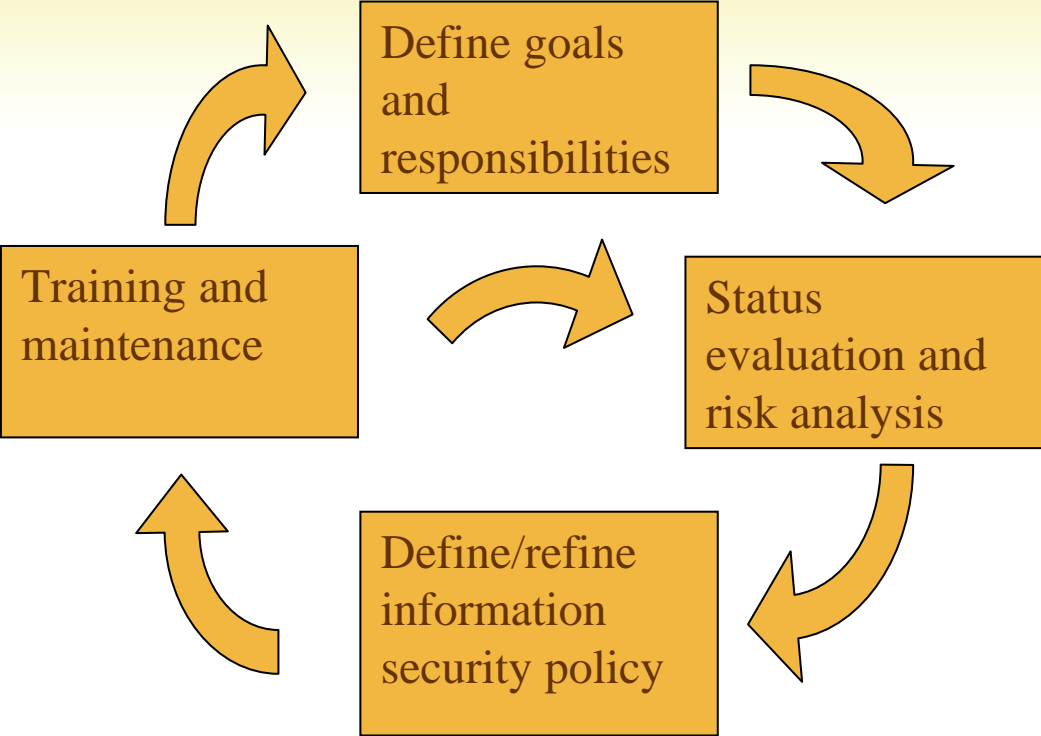
Small and middle enterprises have less resources, still the need for information security remains

Growth in all forms poses challenges to management

Management of information security is no exception



Framework for managing information security in SMEs



Source: Ilvonen 2006

Growth of small enterprises

Growth can be approached from different angles,
such as

Economic growth

Geographical growth

Organic growth

(e.g. by Penrose 1959)

This study focuses mainly in organic growth



Research methodology

10-15 small and middle size enterprises in Tampere region are interviewed over information security issues annually

The interviews are performed as an assignment on a master-level course

- Students perform the interviews
- Companies get reports and suggestions for improvement
- An overview of the reports is prepared by the course staff



Results from a study made in spring 2008

Middle size enterprises are more likely to have organized information security management

Small companies have not taken much effort in documenting policies or defining responsibilities

”When we become a company of 15/25/50 employees, we need to focus on information security management, now we are so small, that we can handle it without documentations”



Applying the management model to growth

Pay attention to training of new employees as well as the old ones

Training and maintenance

Define goals and responsibilities

Assign information security roles and responsibilities to new employees

Status evaluation and risk analysis

Define/refine information security policy

Emphasize on this regularly. How has the situation changed due to growth?

Documents need to be made, and updated/complemented when there is need



Paper for this conference

Introduce theoretical background for the management model

Introduce growth as a context for the model

Apply the management model to the context of growth

What growth models/theories would work best for this?



Plans for future work

A "then, when" –syndrome?

- Companies think that they don't need to focus on infosec management yet, but later
- At what point they must focus in infosec?

How to study this further

- Next round of interviews on January 2009
- How to find out the motivation to focus on information security management?

References

- Egan, M. Mather, T. 2005. "The executive guide to information security – threats, challenges and solutions". Indiana, Addison-Wesley. 268 p.
- Ilvonen, I. 2006. Tietoturvallisuus pirkanmaalaisissa tietointensiivisissä pk-yrityksissä. EBRC research reports 35.
- Kairab, S. 2005. "A Practical Guide to Security Assessments." Boca Raton, CRC Press. 498 p.
- Penrose, E. 1959. The Theory of the Growth of the Firm. (3rd ed. 1995) Oxford university press. 272 p.
- Tipton, H. Krause, M. (eds.) 2004. "Information security management handbook". 5th edition. Boca Raton, CRC Press. 2036 p.
- Whitman, M. E. Mattord, H. J. 2003. "Principles of information security". Canada, Course Technology. 532 p.

