

A Prototype for assessing information security awareness

Agenda

- 1 Introduction**
- 2 Background**
- 3 Methodology**
- 4 Application**
- 5 Conclusion**

1 Introduction

2 Background

3 Methodology

4 Application

5 Conclusion

Introduction

- For Information Security (protecting confidentiality, integrity and availability of information) every member needs an Awareness/Understanding for information security (dynamic process)
 - Implementation of awareness programs
 - Creation of an security positive environment (culture)
- Measurement of the awareness program effectiveness
 - business and management process level
 - Technical level business and management process level

1 Introduction

2 Background

3 Methodology

4 Application

5 Conclusion

Key Facts About the Partnership Company

- African global producer with 25 operations in 11 countries and a gold production of over 6 million ounces annually
- The company has one of the largest reserves and resources in the world and employs more than 62,500 workers
- For an organization of this size and complexity, it is very difficult to manage the information risk

Main Goals

- Raise awareness of potential risks and ensure that the risk is managed
- Based on awareness, computer users should follow existing policies and procedures when using information technology

Six Golden Rules

- Keep passwords and personal identification numbers (PINs) secret
- Use e-mail and the Internet with care
- Be careful when using mobile equipment
- Report incidents like viruses, thefts and losses
- The last and most important point is the awareness and that all actions have consequences

Implementation

- The program was rolled out to all computer users, not all employees
- All participants received videos and brochures
- Various internal marketing campaigns in different languages like target group-specific posters in business units, articles in the company magazine or intranet
- The purchased toolkit contains a basic measurement tool based on multiple choice questions which the awareness of the computer users can be measured

Agenda

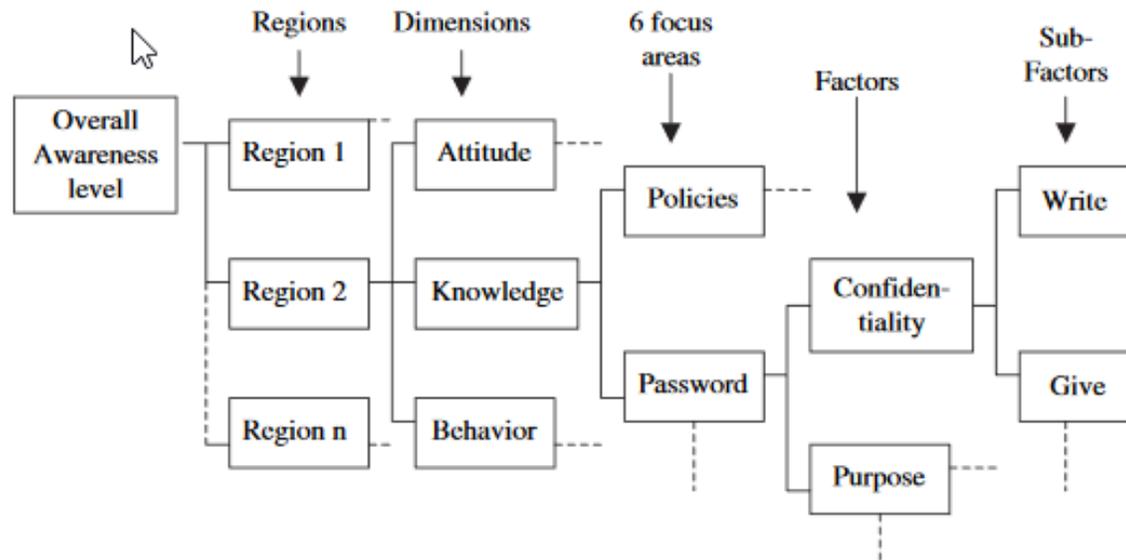
1 Introduction

2 Background

3 Methodology

4 Application

5 Conclusion



■ Top-Down

- Basis: social psychology
- Procedure (visualized in value tree):
 - List different regions
 - Every region is divided into 3 dimensions (based on social psychology)
 - Dimensions are subdivided into focus areas including several factors

Example question to test *knowledge*:

Internet access on the company's systems is a corporate resource and should be used for business purposes only **1. True 2. False 3. Do not know**

Example question to test *attitude*:

Mobile equipment is usually covered with existing insurance cover and there is no special need to include them in security policies **1. True 2. False 3. Do not know**

Example question to test *behaviour*:

I am aware that you should never give your password to somebody else – however, my work is of such a nature that I do give my password from time to time to a colleague (only to those that I trust!) **1. True 2. False**

- **Bottom-up:**

$$V(a) = \sum_{i=1}^n v_i(a)w_i$$

- Basis: pairwise comparison, formula
- Prioritization and definition of weighting of factors
 - 35 questions were defined
 - calculation bottom-up

- **Advantages:**

- Detailed measurements at different levels
 - Efficient launch of measures
- Changes in awareness can be measured
 - Ability to react

Agenda

- 1** Introduction
- 2** Background
- 3** Methodology
- 4** Application
- 5** Conclusion

Application

- the prototype tool was applied to the Australian regional office of the company discussed in Section 2
- The choice of region:
 - based on a management request
 - the environment (staff, infrastructure, etc.) was reasonably stable
 - staff complement was small enough to get feedback and input

- Step 1:
 - determine what to measure
 - a value tree was constructed -> 44 aspects were identified that could be measured to cover the knowledge, attitude and behaviour dimensions with the associated six focus areas in each dimension

- Step 2:
 - a simple questionnaire to capture the information required
 - to provided valuable input and helped to refine the questionnaire, different tests were performed
 - ensure that a model was developed which complies with the principles of sustainability, ease of use and scientifically sound

- Step 3:
 - calculate the importance weights based on input from all relevant managers
- Step 4:
 - questionnaire results and importance weights were processed in a spreadsheet application

one example of a graph showing the overall awareness level:

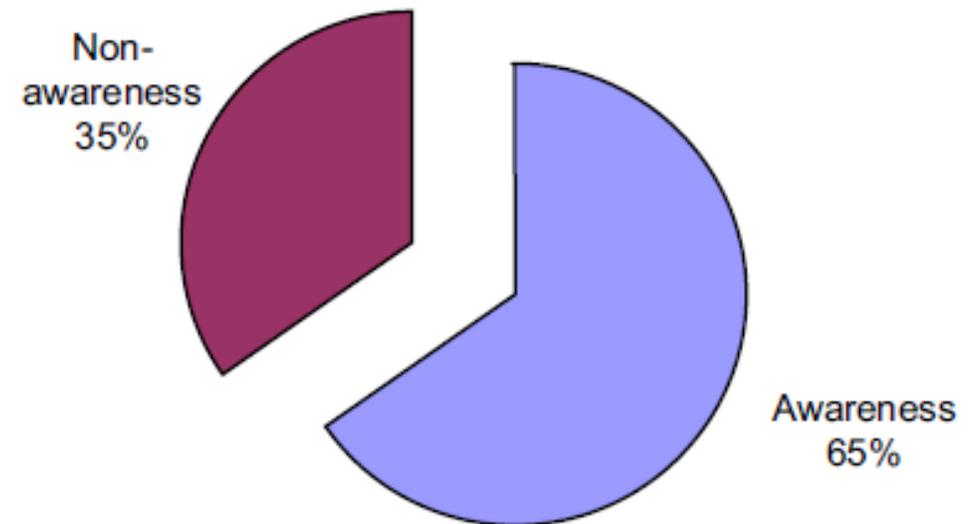


Fig. 3 – Overall awareness level.

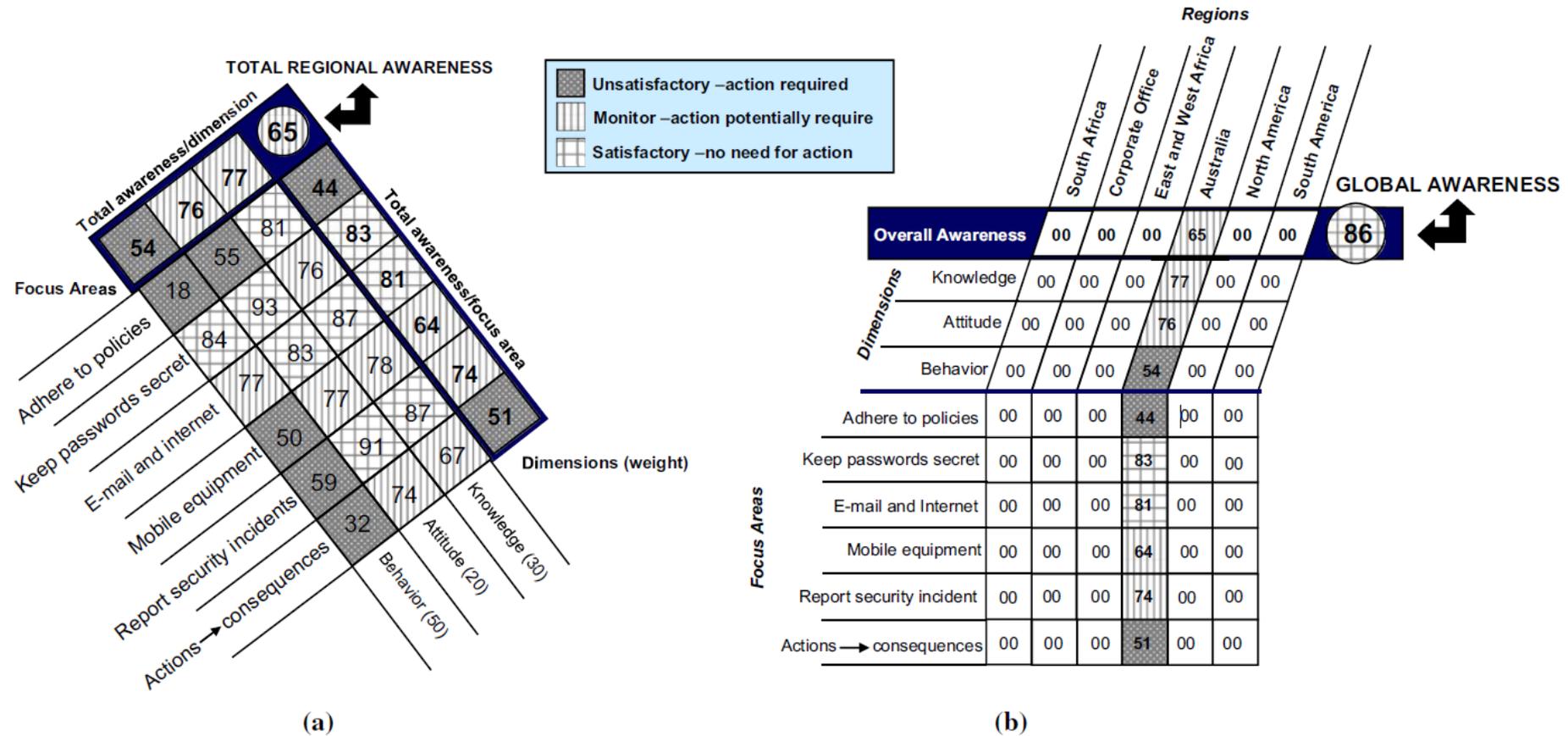


Fig. 4 – (a) Regional awareness map of Australia; (b) global awareness map.

- the issues that were identified during the development:
 - the model can only be successful if the “right” questions are asked to obtain correct data as input to the model
 - importance weightings should be obtained from relevant managers
 - the use of practical system data obtained from, for example, a system administrator should be considered
 - the tool should be automated

Agenda

- 1** Introduction
- 2** Background
- 3** Methodology
- 4** Application
- 5** Conclusion

Conclusion

- Need to integrate information security into corporate governance
- Importance of information security awareness measurement as Management task
- Importance of the structural implementation of the information security awareness program to ensure all employees understand their role in ensuring the security
- Helpful awareness measurement tool has been created within the study