Improving Information Security Management: an Australian Universities case study.

ISI
Information Security Institute

QUT isi Information Security Institute

Topics

1. Overview
2. Information Security Management Issues
3. Security Practitioner's Management Model
4. Conclusion

ISI
Information Security Institute

QUT isi Information Security Institute

Overview

ISI
Information Security Institute

QUT isi Information Security Institute

Overview

- The design of a model which integrates and shows the relationship between:
  - Organisational context
  - Behavioural aspects
  - Functional management
  - Practical use (to security practitioners)

ISI
Information Security Institute

QUT isi Information Security Institute

The University Environment

- Diverse and often conflicting goals:
  - Corporate mandates
  - Provision of education
  - Cultural and pedagogical pursuits of academic:
    - Teaching
    - Learning
    - Research

ISI
Information Security Institute

QUT isi Information Security Institute

Literature Overview

- Not much on security management in universities
- Focus on:
  - Senior management ~ effective corporate governance
  - approaches to operation security management
  - policy frameworks and content
  - awareness of security, cultural compliance to security
- In many cases security is not prioritised in line with its accepted importance

ISI
Information Security Institute

QUT isi Information Security Institute

Methodology

- **Data generation:**
  - **Survey (35 open, closed questions) with 100% participation from all AVC Australian universities**
  - **Researcher's role as Information Security Manager at Southern Cross University**
- **Gathered data:**
  - **Synthesised into the Security Practitioner's Management Model**

ISI
Information Security Institute

QUT isi Information Security Institute

- Overview
- Information Security Management Issues
- Security Practitioner's Management Model
- Conclusion

Information Security Management Issues

ISI
Information Security Institute

QUT isi Information Security Institute

Issues

- What is the current status of information security management?
- What are the key issues surrounding information security management?
- How could information security management be improved?

ISI
Information Security Institute

QUT isi Information Security Institute

Senior Management Involvement

➢ Key issues

- **Institutions that maintain strong reporting and communication to senior management have a clear advantage in terms of resourcing and support.**
- **Only approximately one third of institutions maintain reporting yet suffer resource and support issues.**

➢ How to improve?

- **Improve structure of approach to include reporting and ensure security is aligned to business as corporate governance issues over assets and reputation.**

ISI
Information Security Institute

QUT isi Information Security Institute

Security Management Approach

➢ Key issues

- Various standards in use.
- Difficulties in how to implement approach.
- Lack of structured, coordinated approach.

➢ How to improve?

- Adopt a coordinated, structured enterprise approach.
- Incorporate organisational requirements within Security Manager's model.

ISI
Information Security Institute

QUT isi Information Security Institute

Security Policy

➢ Key issues

- Policy development and implementation effectiveness varies widely.
- Policy considered to fundamentally underpin security.
- Issues with policy monitoring and enforcement.

➢ How to improve?

- Look to international standards.
- Adoption policy 'abstraction and refinement'.
- Increase awareness on policy.

ISI
Information Security Institute

QUT isi Information Security Institute

Security Awareness

➢ Key issues

- Security awareness lacking resulting in users constructing their own reality of security risks.
- Security awareness raising not prioritised due to resourcing.

➢ How to improve?

- Adopt strategic, targeted continuous awareness program.
- Model on 'framework and content' as NIST recommends.
- Integrate behavioral theory where appropriate.

ISI
Information Security Institute

QUT isi Information Security Institute

Security Compliance

➢ Key issues

- Emerging regulatory drivers.
- Difficulties in measuring security effectiveness due to intangibility.
- Point based solutions emerging.

➢ How to improve?

- Seek organisational compliance from a cultural perspective via security management model.
- Seek balancing factors including technology based policy enforcement.

ISI
Information Security Institute

QUT isi Information Security Institute

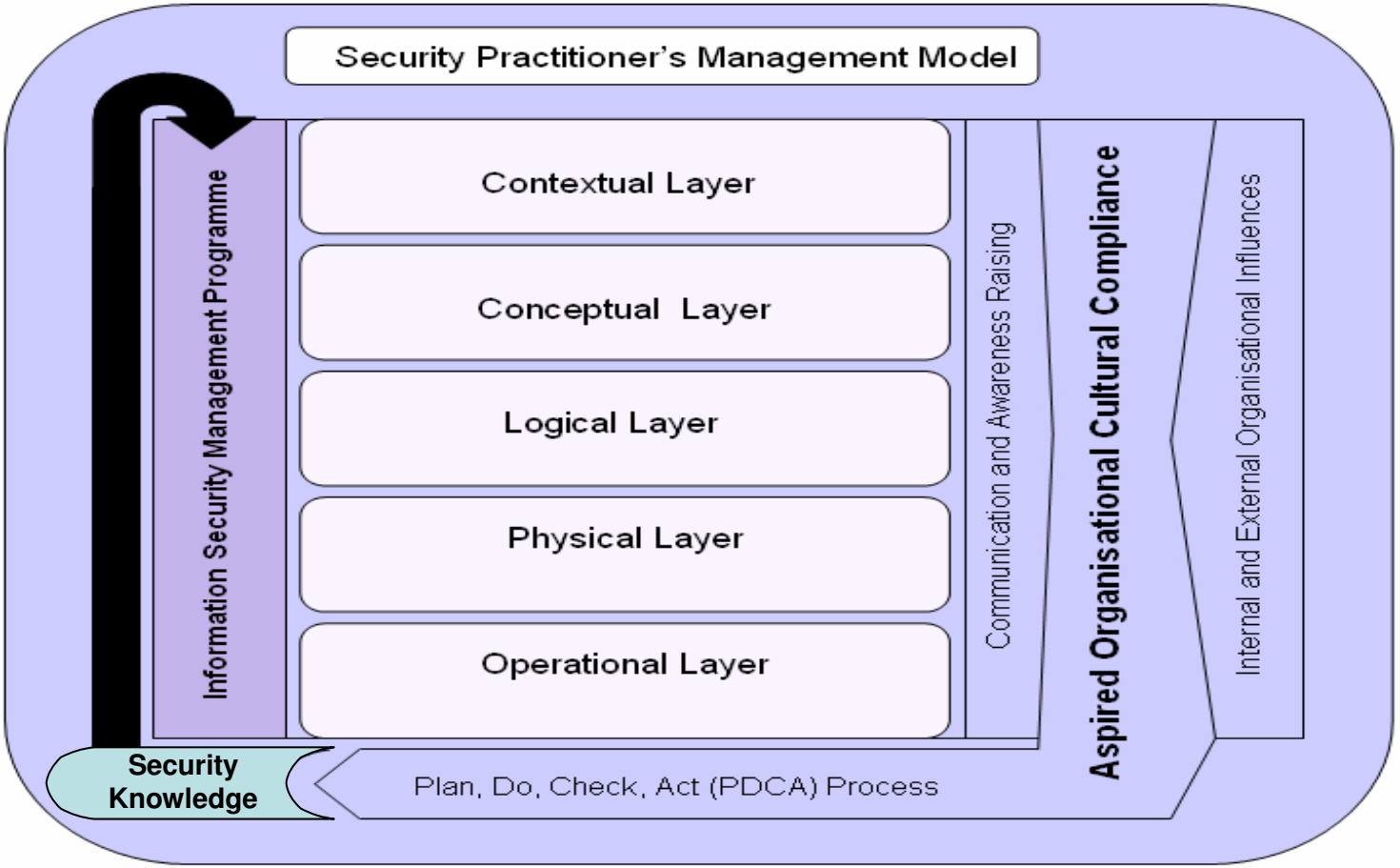
- Overview
- Information Security Management Issues
- Security Practitioner's Management Model
- Conclusion

Security Practitioner's Management Model

ISI
Information Security Institute

QUT isi Information Security Institute

Security Practitioner's Management Model



ISI
Information Security Institute

QUT isi Information Security Institute

A Systemic Approach

- **Operational level goal:**
  - **To enable security practitioners to apply the management of information security in a structured and cohesive manner**
- **Organisational level goal:**
  - **To increase the transparency and effectiveness of the information security process towards organisational goals**

ISI
Information Security Institute

QUT isi Information Security Institute

The Use of Standards in the Model

- **Any information security management standards can be incorporated into the model.**
- **Hybrid best-practices can be incorporated into the model.**
- **Enables consistency with business risk management and control framework.**

ISI
Information Security Institute

QUT isi Information Security Institute

Process Flow through the Model

1. Feed in security practitioner's knowledge.
2. Channel knowledge through contextual, conceptual, logical, physical, operational layers.
3. Encourages cultural compliance.
4. Which feeds back to 1.

ISI
Information Security Institute

QUT isi Information Security Institute

Communication and Awareness

- **Motivation of people through:**
  - **Active participation**
  - **Persuasive communication**
- **Technology Acceptance Model (TAM)**
- **Learned behaviour**
- **Recognition**

ISI
Information Security Institute

QUT isi Information Security Institute

Validation

- Strong applied research component
- Qualitative research model
- Real-world phenomena methodology
- Thematic data analysis technique:
  - triangulation of observations, participation, literature reviews and the survey instrument
  - inductive model for illuminating processes

ISI
Information Security Institute

QUT isi Information Security Institute

Conclusion

ISI
Information Security Institute

QUT isi Information Security Institute

Conclusion

- Universities are an important foundation of society
- Security Practitioner's Management Model encourages:
  - Transparent, accountable data processes
  - Balance between civil liberties and state-based control (i.e. security and privacy)
  - Acceptance of knowledge-gathering role of security practitioner
  - Raised awareness and compliance of all staff

ISI
Information Security Institute

QUT isi Information Security Institute

Thank you!

- Dr. Lauren May (Principle Supervisor)
- Dr. Kavoos Mohannak (Associate Supervisor)
- Dr. Nev Meyers (Associate Supervisor)

Q&A