The Road to Institutional Information Security Management

Peter Tinson

UCISA
In the beginning…
Why do it

• Cyber security became a hot topic
• Survey identified
  • Main risk was reputational damage
  • Main threat was accidental loss of data
  • Main asset at risk teaching-related and HR data
• “no simple answer to the challenge of developing effective IS”
• “clear risk of developing overly bureaucratic systems”
What it is

- Good, actionable advice on information security management:
  - Advice
  - Real-world exemplar materials
- Instructions on developing an Information Security Management System (ISMS) from where you are right now
- Designed for educational institutions - but usable by anyone
What it’s for

• Becoming ISO/IEC 27001 certified
• Showing good practice in information risk management (also known as cyber security)
• Reducing or controlling the risk of embarrassing or damaging information security incidents
Roadmap

**Stage 1 – Foundations**
- Understand the organisation
- Establish leadership and commitment
- Gain initial top management support
- Set policy/strategy
- Define roles and responsibilities

**Stage 2 – Planning, Assessment and Evaluation**
- Define scope of activity
- Define risk assessment methodology
- Assess risk and establish risk treatment plan
- Select controls
- Define necessary resources
- Deliver business case and review
- Define competencies

[§1] What is information security?
[§2] Information security governance
[§3] Relationships between drivers
[§8] Roles and competencies
[§13] Policies

[§4] Scoping
[§5] Risk assessment
[§6] Controls
[§7] Information management
[§8] Roles and competencies
[§9] Awareness raising
[§2] Information security governance
Roadmap (continued)

Stage 3 – Implementation, Support and Operation
- Establish operational support (resource, competencies, awareness etc.)
- Implement policies/controls and manage risk
- Address communication and awareness building
- Implement compliance checking vs regulations

Stage 4 – Performance, Evaluation and Improvement
- Measure and evaluate performance
- Respond effectively to incidents and when things go wrong
- Deliver continual improvement
- Implement iterative risk assessment

[§5] Risk assessment
[§6] Controls
[§8] Roles and competencies
[§9] Awareness raising
[§1] What is information security?

[§10] Measurement
[§11] When things go wrong: non-conformities and incidents
[§12] Continual improvement
[§5] Risk assessment
Stage 1 – Foundation

• Understand the organisational culture
• Identify organisational drivers
• Identify key points of control
• Establish how risk is managed
• Make initial contact with senior managers
  • Explain what the problem is
  • Provide outlines to them
• Get top level policy approved
Stage 2 – Planning, assessment and evaluation

- Develop an information risk management model
- This should be:
  - Congruent with existing risk management practices
  - Consistent with ISO 27001
  - Easy to explain
  - Sanity checked by those on the front line
  - Measurable
Stage 2 (continued)

- Identify key people and get them onside
- Promote it
- Present to the right people once the appetite is there
- Develop new/changed groups and functional areas
Stage 3 – Implementation, support and operation

- Programme/project management
- Generate actual KPIs
- Start new groups off strongly
- Use existing reporting lines
- Embed information risk management in standard operations
Stage 4 – Performance evaluation and improvement

• Audit – verify that controls are effective
• Learn from incidents
• Continual improvement
• Make this part of a GRC structure
Linking it all together

• Developing an ISM Tool
• Links the elements of the IS Management System
• Provides a repository for all things IS
Getting the message across

• Toolkit includes case studies on awareness raising (both from Cardiff)
• A number of institutions have carried out phishing exercises
• Information Security Awareness training
Information security awareness training
Working with other organisations

• Liaison with Jisc
  • use ISMT in training
  • developing (anti-)phishing service
• Promote with non-IT associations in the UK
• Promoted elsewhere – EDUCAUSE have recommended
• Happy for ISMT to be used…
Where we are in the UK
Conclusion

• It’s complicated – no silver bullet
• Set of tools to assist (developed by the community for the community)
• Toolkit recognised by Government agencies
• Happy to talk further…
  • Email: execsec@ucisa.ac.uk
  • Twitter: @pat3460
  • ISMT: www.ucisa.ac.uk/ismt
  • Information security awareness training: www.ucisa.ac.uk/infosectraining