Reality or Nightmare?

Fearless Frameworks for Information Security

David Simpson
CQR
Outline

► An introduction
► Security Frameworks
► The challenges
► The benefits
► The why’s of disturbed sleep – don’ts
► Ways of getting better rest
► Case Studies
► Summary and questions
Introduction

➤ Environment
- Changing business landscape
- Speed of change
- Blurring of traditional control boundaries
- Introduction of new technologies
- “Reach” of IT
Security Frameworks

Need

- A “managed” way of looking at risk
- Structure
- Clarity around responsibilities
- Ways of adapting to changes to conditions
What is a Framework

- Structured way of managing risk
- Multi-faceted approach to information security
- Collection of artefacts and behaviours
- Can be formal or informal
ISMS vs ISMF

- Information Security Management Systems (ISMS)
- Information Security Management Framework (ISMF)
- Mix and match – no real boundaries
What is an ISMF

- Provides overall structure (high level)
- Defines a number of different elements
- Defines an overall governance landscape
- Can include references to an ISMS
What is an ISMS

► Generally:
  – Formal management system to identify and manage risk
  – Defines clear structure and processes to ensure this happens
  – Made up of a number of sub-processes

► Can be based on formal standards
What is an ISMS

- Comprises:
  - Policies
  - Standards
  - Procedures and work instructions
  - Metrics
  - Technologies and tools
  - People and behaviours
What is an ISMS

► Objectives:
  – Secure the organisation’s critical (business) information assets
  – Against defined and unknown threats
► In a manageable and systematic manner
► Continuous improvement
The Challenges

► Complicated and specialised area
► No perceived business benefit
► Deemed too expensive
► Looks too hard
► Don’t know where to start
The Benefits

► Creates a platform to ensure improvements in security
► Provides assurance to
  – Internal management
  – External stakeholders
► Satisfies legal, regulatory and contractual requirements
The Benefits

► Focusses investment in information security
► Increased satisfaction amongst some staff
► Improves the “security culture”
Sleepless Nights

► What can go wrong:
  – No management commitment
  – Too ambitious
    – scope / timeframe
  – Lack of clarity around focus of the framework/system
  – Try to be “everything to everyone”
Sleepless Nights

► What can go wrong:
  – No buy-in from the “troops”
  – Loss of focus over implementation journey
  – After implementation “project” people think the job is done
Addressing the Issues

► Ensure management commitment exists
► Remain clear about scope
► Make sure that the processes are practical
► Documents and procedures should reflect organisational culture
Addressing the Issues

► Keep it simple
► Don’t try to be perfect
► Over-engineering is the cause of many failures
► Educate / involve people along the path
Case Studies

- SaaS Provider - ISMF
- Telco – ISMS
- Data Centre – ISMS
- IT Services Company - ISMS
Case Study - SaaS

► Providing software-as-a-service

► Need – internally recognised need to improve security

► Approach
  – Develop a set of guidance documents
  – Educate staff and implement ongoing program
Case Study - Telco

► Need – Customer demands for ISO 27001 certification

► Approach
  – Define and implement an ISMS

► Challenges
  – Scope
  – Commitment
Case Study – Data Centre

► Need – Customer demand for ISO 27001 certification

► Approach
  – Define and implement an ISMS

► Challenges
  – Scope - multiple data centres
  – Time – short time frame for implementation
Case Study – Services

► Need – deliver security services (“walk the walk”)

► Approach
  – Define and implement an ISMS across whole of business

► Challenges
  – Investment
  – Integration into normal business
Summary and Questions

► ISMF / ISMS - either or both
► Make sure you have management commitment
► Involve interested parties in the journey
► Keep it simple – no need for perfect
Questions

david.simpson@cqr.com

www.cqr.com

Follow us on Twitter @CQR