

INFORMATION SECURITY: A STRATEGIC APPROACH

List of Figures.

Preface.

1. Introduction.

Strategy Overview.

Strategy and Information Technology.

Strategy and Information Security.

An Information Security Strategic Planning Methodology.

The Business Environment.

Information Value.

Risk.

The Strategic Planning Process.

The Technology Plan.

The Management Plan.

Theory and Practice.

2. Developing an Information Security Strategy.

Overview.

An Information Security Strategy Development Methodology.

Strategy Prerequisites.

Research Sources.

Preliminary Development.

Formal Project Introduction.

Fact Finding.

General Background Information.

Documentation Review.

Interviews.

Surveys.

Research Sources.

Analysis Methods.

Strengths, Weaknesses, Opportunities, and Threats.

Business Systems Planning.

Life-Cycle Methods.

Critical Success Factors.

Economic Analysis.

Risk Analysis.

Benchmarks and Best Practices.

Compliance Requirements.

Analysis Focus Areas.

Industry Environment.

Organizational Mission and Goals.

Executive Governance.

Management Systems and Controls.

Information Technology Management.

Information Technology Architecture.

Security Management.

Draft Plan Presentation.

Final Plan Presentation.

Options for Plan Development.

A Plan Outline.

Selling the Strategy.

Plan Maintenance.

The Security Assessment and the Security Strategy.

Strategy Implementation:

What is a Tactical Plan?

Converting Strategic goals to Tactical Plans.

Turning Tactical Planning Outcomes into Ongoing Operations.

Key Points.

BUY ONLINE AT: <http://www.27001.com/products/91>

Plan Outline.

3. The Technology Strategy.

Thinking About Technology.
Planning Technology Implementation.
Technology Forecasting.
Some Basic Advice.
Technology Life-Cycle Models.
Technology Solution Evaluation.
Role of Analysts.
Technology Strategy Components: The Security Strategy Technical Architecture.
Leveraging Existing Vendors.
Legacy Technology.
The Management Dimension.
Overall Technical Design.
The Logical Technology Architecture.
Specific Technical Components.
Servers.
Network Zones.
External Network Connections.
Desktop Systems.
Applications and DBMS.
Portable Computing Devices.
Telephone Systems.
Control Devices.
Intelligent Peripherals.
Facility Security Systems.
Security Management Systems.
Key Points.

4. The Management Strategy.

Control Systems.
Control Systems and the Information Security Strategy.
Governance.
Ensuring IT Governance.
IT Governance Models.
Current Issues in Governance.
Control Objectives for Information and Related Technology (CobiT).
IT Balanced Scorecard.
Governance in Information Security.
End-User Role.
An IT Management Model for Information Security.
Policies, Procedures, and Standards.
Assigning Information Security Responsibilities.
To Whom Should Information Security Report?
Executive Roles.
Organizational Interfaces.
Information Security Staff Structure.
Staffing and Funding Levels.
Managing Vendors.
Organizational Culture and Legitimacy.
Training and Awareness.
Key Points.

5. Case Studies.

Case Study 1 Singles Opportunity Services.
Background.
Developing the Strategic Plan.
Information Value Analysis.

Risk Analysis.
Technology Strategy.
Management Strategy.
Implementation.
Case Study 2 Rancho Nachos Mosquito Abatement District.
Background.
Developing the Strategic Plan.
Information Value Analysis.
Risk Analysis.
Technology Strategy.
Management Strategy.
Implementation.
Key Points.

6. Business and IT Strategy: Introduction.

Strategy and Systems of Management.
Business Strategy Models.
Boston Consulting Group Business Matrix.
Michael Porter Competitive Advantage.
Business Process Reengineering.
The Strategy of No Strategy.
IT Strategy.
Nolan/Gibson Stages of Growth.
Information Engineering.
Rockarts Critical Success Factors.
IBM Business System Planning (BSP).
So is IT really strategic?
IT Strategy and Information Security Strategy.
Key Points.

7. Information Economics.

Concepts of Information Protection.
Information Ownership.
From Ownership to Asset.
Information Economics and Information Security.
Basic Economic Principles.
Why is Information Economics Difficult?
Information Value Reducing Uncertainty.
Information Value Improved Business Processes.
Information Security Investment Economics.
The Economic Cost of Security Failures.
Future Directions in Information Economics.
Information Management Accounting Return on Investment.
Economic Models and Management Decision Making.
Information Protection or Information Stewardship?
Key Points.

8. Risk Analysis.

Compliance Versus Risk Approaches.
The Classic Risk Analysis Model.
Newer Risk Models.
Process-Oriented Risk Models.
Tree-Based Risk Models.
Organizational Risk Cultures.
Risk Averse, Risk Neutral, and Risk Taking Organizations.
Strategic Versus Tactical Risk Analysis.
When Compliance-based Models are Appropriate.
Risk Mitigation.
Key Points.
Notes and References.

Index.

BUY ONLINE AT: <http://www.27001.com/products/91>