

Organisation and Planning

Information Security

Dr Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 8

Interpersonal Roles

- Figurehead
- Leader
- Liaison

Learning Outcomes

After this week, students should

- Understand fundamental concepts of management
- Be able to use management concepts to plan effective and cost-efficient security measures
- Be familiar with different ways of organising a security organisation

Informational Roles

- Monitor
- Dissemination
- Spokesperson

Decisional Roles

- Entrepreneur
- Disturbance handler
- Resource allocator
- Negotiator

Different Layers of Management

Strategic Management Upper management do long-term planning. They define and evaluate organisation-wide, overall goals.

Functional Management Middle management is specialised for different functional areas of the organisation, such as finance, IT, (security?), estates, production, etc. Yet, functional managers have a long-term view, and work closely with upper management.

Operational Management Lower management is responsible for the day-to-day running of the business. Operational managers steer towards goals and targets set by higher-level managers, and manage the finer detail of the organisation.

Which layer is responsible for information security?

Strategic Management

- Security Planning
- Security Auditing and Certification
- Risk appetite
 - expensive, high-security service
 - low-cost service with some risk
- Strategic choices depends on customer base and target market

Senior Information Risk Owner (SIRO)

- Government requirement for all government departments
- Board-level individual responsible for information security across the department
- What's the purpose of this role?
- Raise security awareness to board-level
 - integrate security in board-level management
- Consistent risk management
 - one individual to decide on *acceptable risk*
- Liability and accountability?
 - someone to sack when it goes wrong?
 - or will the SIRO be able to pin the blame on someone else?
- Some departments have reached farther than others

Functional Management

- Risk management
- Risk-driven programme

Operational Management

- Implementations
 - fire walls
 - security software deployments
- Administration and Maintenance
 - software patches
 - monitoring
 - configuration
- Response to Incidents
 - Recovery
 - Reporting

Framework (from *Håndbok ...*)



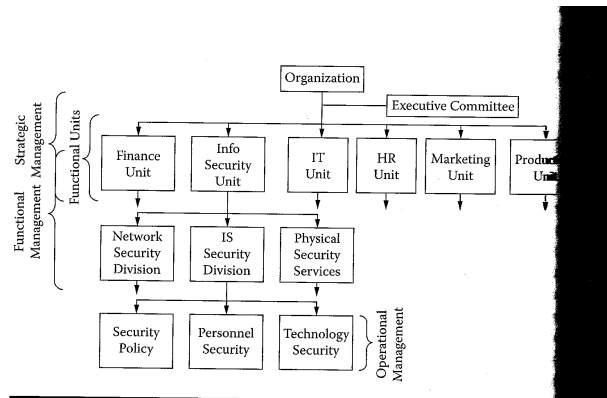
Placement of the Security Unit

- **Functional** Information Security Unit
- Information Security Subunit **under the IT unit**
- Matrix organisation with **orthogonal** Information Security Unit

What are the advantages and disadvantages?

Organisational Model

With Security Functional Unit (Raggad)



Organisational Model

Without Security Functional Unit (Raggad)

50 ■ Information Security Management: Concepts and Practice

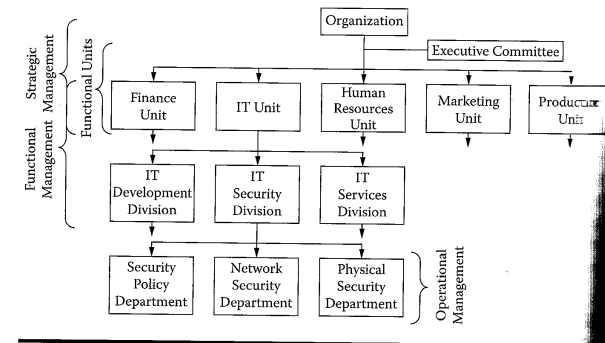


Figure 2.6 Organizational structure without a separate security unit.

Matrix organisation

- All functional units are responsible for security
 - within their area
- The security organisation oversees and co-ordinates
- Staff may have to report both
 - own functional or operational head
 - to a member of security staff liaising with their unit

Security in the Organisation

Do we need a functional unit for (Information) Security?

- Functional Unit Heads take part in Strategic Management
- With a Security Functional Unit
 - Security is represented in Upper Management
- Without the Security Functional Unit
 - the Security Head does not take part in Strategic Planning
 - i.e. s/he is not a SIRO in the government sense.

Could the Head of General IT take the role as SIRO?

Communication with your Organisation

- The organisation is a fine machinery
 - each part must know its role
 - all the parts must be co-ordinated to work together
- Management is responsible for co-ordination and consistency
 - has the overview
- Everyone must do his/her own part
 - good communication is **key** to co-ordination
- Policies, standards, and other documents are essential communication tools

Warning

- Documents do not exist for their own sake
- Documents are not security features
- Each document has a purpose
 - otherwise it is not worth writing
- Each document has a target audience
 - and must be written specifically for that audience
 - different audiences have different needs and abilities
- Don't write documents that no one will read
 - don't make the document longer than what will be read

If you do not know why you write a particular document, it is bound to be a bad one.

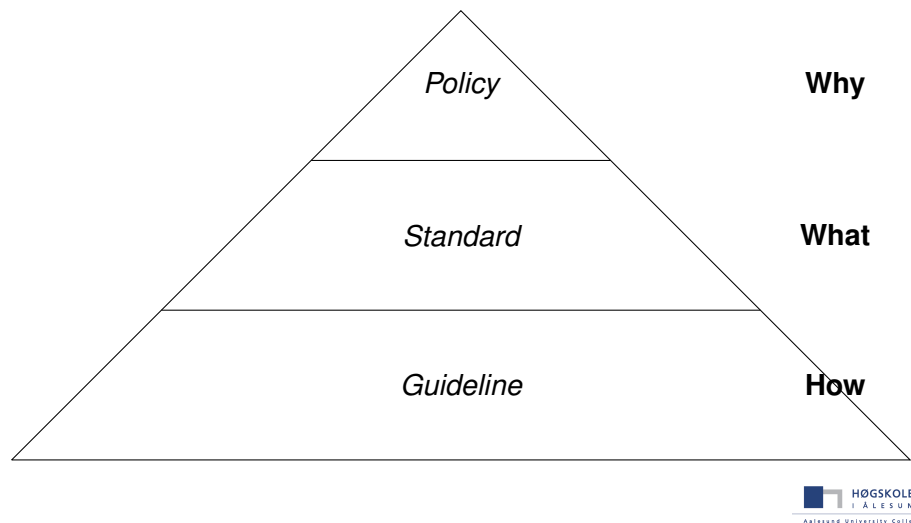
Do not cut and paste

- For instance: BP's Gulf Oil Spill Response Plan
<http://www.csmonitor.com/From-the-news-wires/2010/0609/BP-s-gulf-oil-spill-response-plan-lists-the-walrus-as-a-loc-Louisiana-Gov.-Bobby-Jindal-is-furious>
- Addresses species which do not even exist

Don't proliferate

- How do staff find information?
- Probably google
- Old documents on the web is a serious threat
- Hard to tell which document is accurate

Documents



Security Policy

Definition (Organisational Security Policy)

The laws, rules, and practices regulating how an **organisation** manages, protects, and distributes resources to achieve specified security policy objectives.

Definition (Automated Security Policy)

Set of restrictions and properties that specify how a **computing system** prevents information and computing resources from being used to violate an organisational security policy.

Scope of the Security Policy

- The organisational security policy
 - aims to secure the resources of the organisation
 - not limited to software and hardware
 - the users are part of the system
- The automated security policy
 - one of the means to implement the organisational security policy
 - limited to software and hardware
- Organisation and management
 - contributes to security
 - privileges must be assigned intelligently
 - privileged users must use their rights correctly.

Policies and Other Documents

Policy defines the priorities and focus on the why of security. Responsibilities are assigned, and security requirements may be defined.

Standard defines mandatory rules of conduct, aiming to implement the policy.

Guidelines is a set of *best practice* and advice to help units and individuals to implement the policies and the standards. They are not mandatory.

The Audience

The Organisational Security Policy

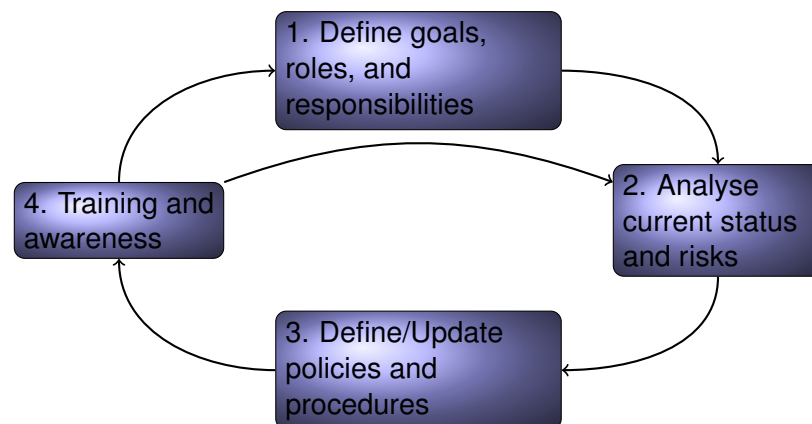
- Different audiences
 - Users
 - Owners
 - System Administrators
 - Customers (and other beneficiaries)
 - Developers (system designers and programmers)
- Each group needs
 - 1 Assurance
 - their security needs are taken care of
 - 2 Awareness of their responsibility
 - they know to act correctly, maintaining security

Structure of the Policy

- No set format for policies
 - you write what the application requires
 - different organisations — different needs
- It depends on other documents
 - Some things are necessary, but could go in a policy document or elsewhere
 - Catalogue of Assets, Threat Descriptions, Risk Analysis
- Literature tends to focus on large corporations
 - rarely explicit or specific
 - but tend to assume a dozen people in the information security department...
- Very little literature on policies for SMEs
 - Ilona Ilvonen (ECIW 2009)
- Bottom line — there is no cookbook for this
 - you will help to think, and look at what the problem requires
- Policies must be managed over time
 - We will return to this

Information Security Management Life Cycle

Ilona Ilvonen 2009



Security Policy in Context

Systems Design

- Working as a system designer
 - what is the role of the security policy?
- Requirements gathering
 - many requirements are stated in the policy
 - many requirements follow from the policy

The Enron/Andersen Scandal

- The Enron Energy Corporation (USA)
 - Criminal investigation for fraud (a few years ago)
- Arthur Andersen Consulting
 - World renowned accounting company
- Andersen was implicated when they destroyed client files
 - ... relating to Enron

Security Policy

or Obstruction of Justice

- Andersen staff charged with obstruction of justice
 - shredding documents relevant for the investigation
- Claimed to be following policy
 - Anderson should not keep client files longer than necessary
- Who's right? Should client files be destroyed?

A question of timing

- When policy contradicts law
 - the law is right
 - the policy is illegal
- However, that was not the problem
- Inconsistent implementation of the policy
 - Shredded started **after** the investigation
- Consistent and timely shredding according to policy
 - one could get away with that
- Timely shredding according to policy **before** the investigation is known
 - That's OK.

Setting Security Targets

- Who decides what is **good enough**?

Standards

- Industry standards
- Legal requirements
- Following the standards is an insurance
 - generally considered 'good enough'
- Criticism
 - reduced to **minimum standards**
 - no incentive to do better than the standard
- No responsibility when the standard is insufficient
 - People stop thinking – the standard does it for them
- Standards are slow to update to new circumstances

Liability and Accountability

- Liability is the **opposite** of standards
- Responsibility to **avoid damage**
 - not necessarily to follow standards
- Focus on results, and not method
- Liability applies both to organisations and individuals
 - organisations may be liable for damage to client assets
 - managers may be liable for their decisions
- Advantage in economic terms
 - security is internalised in the business' economic model
 - intelligent decisions based on local knowledge
- Possibly hard to enforce
 - what constitutes negligence and what is reasonable care
 - liability under criminal or civil law?

Accountability versus Liability

- Accountability is a weaker form of responsibility than liability
- accountable [...] required or expected to give an explanation for one's action, etc; responsible*
Oxford Advanced Learner's Dictionary
- liable [...] responsible by law*
Oxford Advanced Learner's Dictionary

Accountability in Information Security

- Accountability usually refers to an obligation to follow policy
- In information security it motivates audit logs monitoring the actions of users
 - who must answer for their actions
- It is usually not related to an expectation to achieve (or avoid) particular results
- However, **managers** are different from users
 - their accountability has to be different

Summary

- Security Awareness and Decisions are required at all levels of management
 - Strategic management
 - Functional management
 - Operational management
- Good communications is essential to implement decisions in the *organisation*
- Management and Development require continuous learning and improvement
 - Lifecycles is a common and useful model
 - Evaluation and Reflection is key to the cycle