Security Organization: Spotlights and Rants

GI FG SecMgt, 14.10.2004

Peter Berlich

„This is security‘s job“

- „Manage Security“
- Governance
- Risk Management
- Operations security
- Compliance
- Incident Management
- User, Management, Technical Staff Awareness
- Support for business functions and product developers
- Intelligence
- Controls management

- Create a budget for other people
- Cost justification („We understand RoSI doesn‘t work, all we need is an idea of what we save through security“)
- Scape goat
- Police, State attorney and jury in one person
- Auditor – and defense against the audit department
- ... But please leave us alone, we don‘t need you right now.

Content

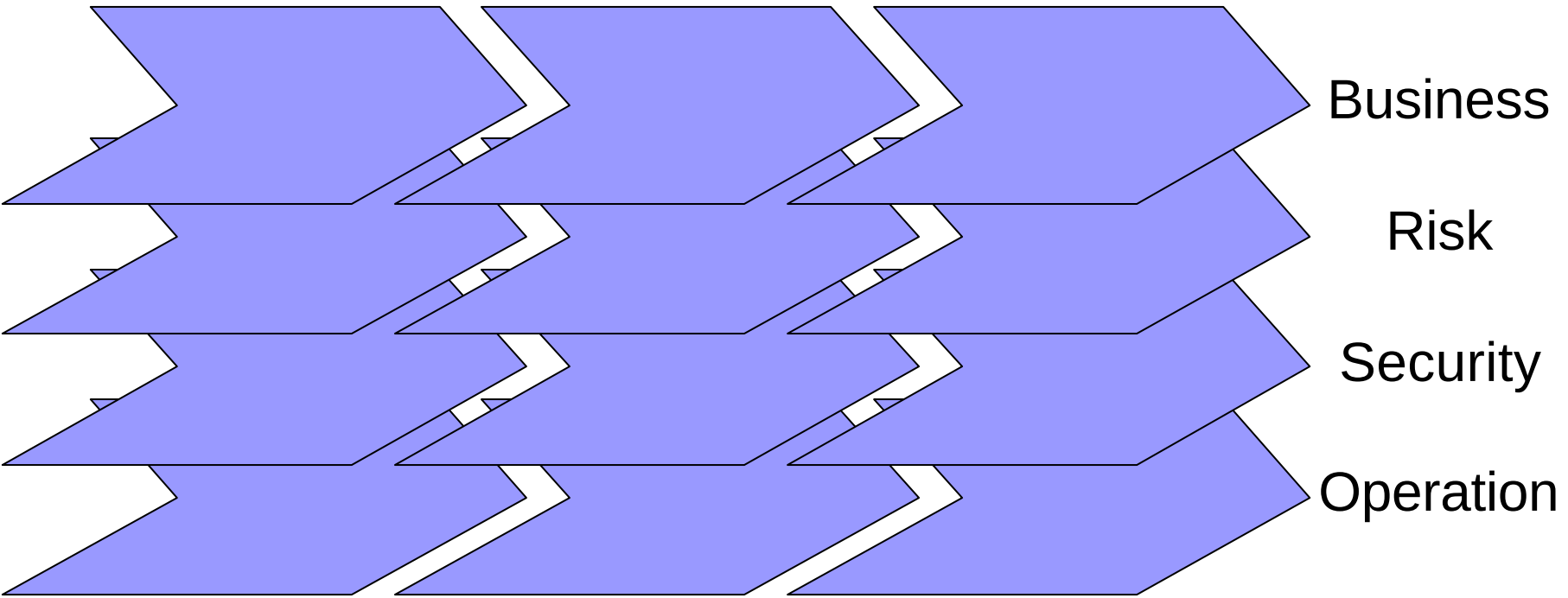
- Tasks of a security organization
  - Layers of responsibility
  - The Role of the External Service Provider
- Roles & Responsibilities within a security organization
  - Elements of a Security Organization
  - Organizational funding and finance
  - Management system
  - Practical problems

Layers of responsibility

Require-
ment

Manage-
ment

Result



The Role of the Service Provider

- Internal Service Providers
  - The key in internal service provision security is governance
  - As security, especially security operation is maturing, more and more technical process are being operationalized.
- External Service Providers
  - The key in outsourcing security is governance
  - Helps establish, define and declare roles and responsibilities
  - The provider will provide security measures but not risk management.
  - It will provide internal but not external governance

Elements of a security organization

- Information Security Function – in the CFO domain and in business domains
- IT Security Function – in the CIO domain
- IT Security Operations – within IT Operations
- IT Security Compliance – within CIO domain and Audit domain

Organizational funding and finance

- Security is a cost center
  - It should be accrued at the highest level of the organization it is meant to overlook
  - By definition, thereby security will always be perceived as (organizational and financial) „overhead“
  - There is no „fair“ way of charging out security
- The fallacy of RoSI by ALE
  - Security investment is a business decision
  - RoSI – tougher than ROI?
  - Get your statistics straight
- Ambiguity of KPIs, metrics for Security
  - How would we measure our Service Level?

Management System

- A good management system enables accountability and gives predictability
- The management system has to work
  - From bottom to top
  - On a regular basis
  - Involving all stakeholders
- A management system can be used to make gaps and conflicts of interest visible

Practical problems

- Security is dispersed
  - Process phases (Plan/Do/Check/Act)
  - Geographies
  - Lines of business and business units
  - Central vs local
  - ... And anyone who can afford one.
- „The Business „doesn‘t listen“ or understand“
  - **We** need to listen – not the business.

References

- **Survey der Schweizer Informatikergesellschaft**
  - **http://www.fgsec.ch/ag/sfs.html**
  - **http://www.fgsec.ch/events/ft2001.07/**
- **Information Security Forum Congress 2002**
  - **IT Security Organization: The Jekyll and Hyde approach**