Datasäkerhet och integritet

Chapter 2

• Planning and Policy
  – Introduction & Terminology
  – Compliance Laws and Regulations
  – Organization
  – Risk Analysis
  – Technical Security Architecture
  – Policy-Driven Implementation
  – Governance Frameworks
Planning and Policy Orientation

• The first intro lecture focused on threats
• The rest of the lectures focuses on defense
• In this lecture, we will see that defensive thinking is built around the plan-protect-respond cycle
• In this lecture, we will focus on planning
Management is the Hard Part

• Technology Is Concrete
  – Can visualize devices and transmission lines
  – Can understand device and software operation

• Management Is Abstract

• Management Is More Important
  – Security is a process, not a product
    (Bruce Schneier)

The Need for Comprehensive Security

Defenders must close off all possible avenues of attack.
This is called comprehensive security.

An attacker only needs one unprotected avenue of attack to succeed.
Weakest Link Failure

A failure in any component will lead to failure for the entire system

1. Firewall administrator creates filtering rules
2. Firewall examines all incoming packets
3. Firewall stores information about each dropped packet in a log file
4. Firewall administrator reads log file looking for problems

FIGURE 2-4  Weakest Link Failure (Study Figure)
Security Management Is a Disciplined Process

- **Complex**
  - Cannot be managed informally

- **Need Formal Processes**
  - Planned series of actions in security management
  - Annual planning
  - Processes for planning and developing individual countermeasures

- **A Continuous Process**
  - Fail if let up

- **Compliance Regulations**
  - Add to the need to adopt disciplined security management processes
Security Management and Systems Life Cycle

The systems life cycle goes beyond the SDLC, to include operational use. SLC thinking is critical in security.

The Plan-Protect-Respond Cycle for Security Management Dominates security management thinking.

FIGURE 2-6 The Plan-Protect-Respond Cycle for Security Management

FIGURE 2-7 Systems Life Cycle
Vision 1

• Vision
  – Your understanding about your role with respect to your company, its employees, and the outside world drives everything else

• Security as an Enabler
  – Security is often thought of as a preventer
  – But security is also an enabler
  – A company with good security can do things otherwise impossible
    • Engage in interorganizational systems with other firms
    • Can use SNMP SET commands to manage systems remotely
  – Must get in early on projects to reduce inconvenience
Vision 2

• Positive Vision of Users
  – Must not view users as malicious or stupid
  – Stupid means poorly trained, and that is security’s fault
  – Must have zero tolerance for negative views of users

• Should Not View Security as Police or Military Force
  – Creates a negative view of users
  – Police merely punish, they do not prevent crime; security must prevent attacks
  – Military can use fatal force; security cannot even punish (HR does that)

• Need New Vision
  – Mother nurturing inexperienced offspring

• Cannot Be Effective Unless Users Work with You
  – Consultation, consultation, consultation
Strategic IT Security Planning

- Identify Current IT Security Gaps
- Identify Driving Forces
  - The threat environment
  - Compliance laws and regulations
  - Corporate structure changes, such as mergers
- Identify Corporate Resources Needing Protection
  - Enumerate all resources
  - Rate each by sensitivity
- Develop Remediation Plans
  - Develop a remediation plan for all security gaps
  - Develop a remediation plan for every resource unless it is well protected
- Develop an Investment Portfolio
  - You cannot close all gaps immediately
  - Choose projects that will provide the largest returns
  - Implement these
Legal Driving Forces 1

• Compliance Laws and Regulations
  – Compliance laws and regulations create requirements for corporate security
    • Documentation requirements are strong
    • Identity management requirements tend to be strong
  – Compliance can be expensive
  – There are many compliance laws and regulations, and the number is increasing rapidly

• Sarbanes - Oxley Act of 2002
  – Massive corporate financial frauds in 2002
  – Act requires firm to report material deficiencies in financial reporting processes
  – Companies that report material deficiencies typically find that their stock loses value, and the chief financial officer may lose his or her job
Legal Driving Forces 2

• Privacy Protection Laws
  – Many other nations have strong commercial data privacy laws
  – The U.S. Gramm–Leach–Bliley Act (GLBA)
  – The U.S. Health Insurance Portability and Accountability Act (HIPAA) for
    private data in health care organizations

• Data Breach Notification Laws
  – California’s SB 1386
  – Requires notification of any California citizen whose private information is
    exposed
  – Companies cannot hide data breaches anymore

• Federal Trade Commission (FTC)
  – Can punish companies that fail to protect private information
  – Fines and required external auditing for several years
Legal Driving Forces 3

• Industry Accreditation
  – For hospitals, etc.
  – Often have to security requirements

• PCS-DSS
  – Payment Card Industry–Data Security Standards
  – Applies to all firms that accept credit cards
  – Has 12 general requirements, each with specific subrequirements

• FISMA
  – Processes for all information systems used or operated by a U.S. government federal agencies
  – Also by any contractor or other organization on behalf of a U.S. government agency
  – Certification, followed by accreditation
  – Continuous monitoring
  – Criticized for focusing on documentation instead of protection
Organizational Issues 1

• Chief Security Officer (CSO)
  - Also called chief information security officer (CISO)

• Where to Locate IT Security?
  - Within IT
    • Compatible technical skills
    • CIO will be responsible for security
  - Outside of IT
    • Gives independence
      - Hard to blow the whistle on IT and the CIO
    • This is the most commonly advised choice
  - Hybrid
    • Place planning, policy making, and auditing outside of IT
    • Place operational aspects such as firewall operation within IT
Organizational Issues 2

• Top Management Support
  – Budget
  – Support in conflicts
  – Setting personal examples

• Relationships with Other Departments
  – Special relationships
    • Ethics, compliance, and privacy officers
    • Human resources (training, hiring, terminations, sanction violators)
    • Legal department
    • Auditing departments
      – IT auditing, internal auditing, financial auditing
      – Might place security auditing under one of these
      – This would give independence from the security function
Organizational Issues 3

• Relationships with Other Departments cont.
  – Special relationships cont.
    • Facilities (buildings) management
    • Uniformed security
  – All corporate departments
    • Cannot merely toss policies over the wall
  – Business partners
    • Must link IT corporate systems together
    • Before doing so, must exercise due diligence in assessing their security

• Outsourcing IT Security
  – Only e-mail or webservice
  – Managed Security Service Providers (MSSPs)
    • Outsource most IT security functions to the MSSP
    • But usually not policy
E-Mail Outsourcing
Managed Security Service Provider (MSSP)

1. Logged events
2. Encrypted and compressed log data
3. Analysis
4. Small number of alerts
5. Vulnerability test

Corporate site

MSSP has practice-based experience. MSSP has independence to accuse security staff members. Contracts must carefully state log reading requirements.

Managed security service provider

Security manager

Log file

MSSP logging server

FIGURE 2-12 Managed Security Service Provider (MSSP)
Risk Analysis 1

• Realities
  – Can never eliminate risk
  – “Information assurance” is impossible

• Risk Analysis
  – Goal is reasonable risk
  – Risk analysis weighs the probable cost of compromises against the costs of countermeasures
  – Also, security has negative side effects that must be weighed
Risk Analysis 2

- **Asset Value (AV)**
- **X Exposure Factor (EF)**
  - Percentage loss in asset value if a compromise occurs
- **= Single Loss Expectancy (SLE)**
  - Expected loss in case of a compromise

- **SLE**
- **X Annualized Rate of Occurrence (ARO)**
  - Annual probability of a compromise
- **= Annualized Loss Expectancy (ALE)**
  - Expected loss per year from this type of compromise

**Single Loss Expectancy (SLE)**

**Annualized Loss Expectancy (ALE)**
## Classic Risk Analysis Calculation 1

<table>
<thead>
<tr>
<th></th>
<th>Base Case</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Value (AV)</strong></td>
<td>$100,000</td>
<td>$100,000</td>
</tr>
<tr>
<td><strong>Exposure Factor (EF)</strong></td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td><strong>Single Loss Expectancy (SLE): = AV*EF</strong></td>
<td>$80,000</td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>Annualized Rate of Occurrence (ARO)</strong></td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td><strong>Annualized Loss Expectancy (ALE): = SLE*ARO</strong></td>
<td>$40,000</td>
<td>$10,000</td>
</tr>
<tr>
<td><strong>ALE Reduction for Countermeasure</strong></td>
<td>NA</td>
<td>$30,000</td>
</tr>
<tr>
<td><strong>Annualized Countermeasure Cost</strong></td>
<td>NA</td>
<td>$17,000</td>
</tr>
<tr>
<td><strong>Annualized Net Countermeasure Value</strong></td>
<td>NA</td>
<td>$13,000</td>
</tr>
</tbody>
</table>

Countermeasure A should reduce the exposure factor by 75%
## Classic Risk Analysis Calculation 2

<table>
<thead>
<tr>
<th></th>
<th>Base Case</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Value (AV)</strong></td>
<td>$100,000</td>
<td>$100,000</td>
</tr>
<tr>
<td><strong>Exposure Factor (EF)</strong></td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td><strong>Single Loss Expectancy (SLE): = AV*EF</strong></td>
<td>$80,000</td>
<td>$80,000</td>
</tr>
<tr>
<td><strong>Annualized Rate of Occurrence (ARO)</strong></td>
<td>50%</td>
<td>25%</td>
</tr>
<tr>
<td><strong>Annualized Loss Expectancy (ALE): = SLE*ARO</strong></td>
<td></td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>ALE Reduction</strong></td>
<td>NA</td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>Annualized Countermeasure Cost</strong></td>
<td>NA</td>
<td>$4,000</td>
</tr>
<tr>
<td><strong>Annualized Net Countermeasure Value</strong></td>
<td>NA</td>
<td>$16,000</td>
</tr>
</tbody>
</table>

Countermeasure B should cut the frequency of compromises in half
## Classic Risk Analysis Calculation 3

<table>
<thead>
<tr>
<th></th>
<th>Base Case</th>
<th>Countermeasure A</th>
<th>Countermeasure B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Value (AV)</strong></td>
<td>$100,000</td>
<td>$100,000</td>
<td>$100,000</td>
</tr>
<tr>
<td><strong>Exposure Factor (EF)</strong></td>
<td>80%</td>
<td>20%</td>
<td>80%</td>
</tr>
<tr>
<td><strong>Single Loss Expectancy (SLE): AV*EF</strong></td>
<td>$80,000</td>
<td>$20,000</td>
<td>$80,000</td>
</tr>
<tr>
<td><strong>Annualized Rate of Occurrence (ARO)</strong></td>
<td>50%</td>
<td>50%</td>
<td>25%</td>
</tr>
<tr>
<td><strong>Annualized Loss Expectancy (ALE): SLE*ARO</strong></td>
<td>$40,000</td>
<td>$10,000</td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>ALE Reduction for Countermeasure</strong></td>
<td>NA</td>
<td>$30,000</td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>Annualized Countermeasure Cost</strong></td>
<td>NA</td>
<td>$17,000</td>
<td>$4,000</td>
</tr>
<tr>
<td><strong>Annualized Net Countermeasure Value</strong></td>
<td>NA</td>
<td>$13,000</td>
<td>$16,000</td>
</tr>
</tbody>
</table>

Although Countermeasure A reduces the ALE more, Countermeasure B is much less expensive. The annualized net countermeasure value for B is larger. The company should select Countermeasure B.
Problems with Classic Risk Analysis Calculations 1

• Uneven Multiyear Cash Flows
  – For both attack costs and defense costs
  – Must compute the return on investment (ROI) using discounted cash flows
  – Net present value (NPV) or internal rate of return (ROI)

• Total Cost of Incident (TCI)
  – Exposure factor in classic risk analysis assumes that a percentage of the asset is lost
  – In most cases, damage does not come from asset loss
  – For instance, if personally identifiable information is stolen, the cost is enormous but the asset remains
  – Must compute the total cost of incident (TCI)
  – Include the cost of repairs, lawsuits, and many other factors
Problems with Classic Risk Analysis Calculations 2

• Many-to-Many Relationships between Countermeasures and Resources
  – Classic risk analysis assumes that one countermeasure protects one resource
  – Single countermeasures, such as a firewall, often protect many resources
  – Single resources, such as data on a server, are often protected by multiple countermeasures
  – Extending classic risk analysis is difficult

• Impossibility of Knowing the Annualized Rate of Occurrence
  – There simply is no way to estimate this
  – This is the worst problem with classic risk analysis
  – As a consequence, firms too often merely rate their resources by risk level
Problems with Classic Risk Analysis

Calculations 3

• Impossibility of Knowing the Annualized Rate of Occurrence
  – There simply is no way to estimate this
  – This is the worst problem with classic risk analysis
  – As a consequence, firms too often merely rate their resources by risk level

• Problems with “Hard-Headed Thinking”
  – Security benefits are difficult to quantify
  – If only support “hard numbers,” may underinvest in security

• Perspective
  – Impossible to do perfectly
  – Must be done as well as possible
  – Identifies key considerations
  – Works if countermeasure value is very large or very negative
  – But never take classic risk analysis seriously
Responding to Risk 1

• Risk Reduction
  – The approach most people consider
  – Install countermeasures to reduce harm
  – Makes sense only if risk analysis justifies the countermeasure

• Risk Acceptance
  – If protecting against a loss would be too expensive, accept losses when they occur
  – Good for small unlikely losses
  – Good for large but rare losses

• Risk Transference
  – Buy insurance against security-related losses
  – Especially good for rare but extremely damaging attacks
Responding to Risk 2

- **Risk Transference cont.**
  - Does not mean a company can avoid working on IT security
  - If bad security, will not be insurable
  - With better security, will pay lower premiums

- **Risk Avoidance**
  - Not to take a risky action
  - Lose the benefits of the action
  - May cause anger against IT security

- **Recap: Four Choices When You Face Risk**
  - Risk reduction
  - Risk acceptance
  - Risk transference
  - Risk avoidance
Corporate Technical Security Architecture 1

- Technical Security Architectures
  - Definition
    - All of a company’s technical countermeasures
    - How these countermeasures are organized
    - Into a complete system of protection
  - Architectural decisions
    - Based on the big picture
    - Must be well planned to provide strong security with few weaknesses
  - Dealing with legacy technologies
    - Legacy technologies are technologies put in place previously
    - Too expensive to upgrade all legacy technologies immediately
    - Must upgrade if seriously impairs security
    - Upgrades must justify their costs
Corporate Technical Security Architecture 2

- **Principles**
  - Defense in depth
    - Resource is guarded by several countermeasures in series
    - Attacker must breach them all, in series, to succeed
    - If one countermeasure fails, the resource remains safe
  - Defense in depth versus weakest links
    - Defense in depth: multiple independent countermeasures that must be defeated in series
    - Weakest link: a single countermeasure with multiple interdependent components that must all succeed for the countermeasure to succeed
  - Avoiding single points of vulnerability
    - Failure at a single point can have drastic consequences
    - DNS servers, central security management servers, etc.
Corporate Technical Security Architecture 3

• Principles cont.
  – Minimizing security burdens
  – Realistic goals
    • Cannot change a company’s protection level overnight
    • Mature as quickly as possible

• Elements of a Technical Security Architecture
  – Border management
  – Internal site management
  – Management of remote connections
  – Interorganizational systems with other firms
  – Centralized security management
    • Increases the speed of actions
    • Reduces the cost of actions
Policies 1

• Policies
  – Statements of what is to be done
  – Provide clarity and direction
  – Does not specify in detail how the policy is to be implemented in specific circumstances
  – Allows the best possible implementation at any time
  – Vary widely in length

• Tiers of Security Policies
  – Brief corporate security policy to drive everything
  – Major policies
    • E-mail
    • Hiring and firing
    • Personally identifiable information
    • ...

Policies 2

• Tiers of Security Policies cont.
  – Acceptable use policy
    • Summarizes key points of special importance for users
    • Typically, must be signed by users
  – Policies for specific countermeasures
    • Again, separates security goals from implementation

• Writing Policies
  – For important policies, IT security cannot act alone
  – There should be policy-writing teams for each policy
  – For broad policies, teams must include IT security, management in affected departments, the legal department, and so forth
  – The team approach gives authority to policies
  – It also prevents mistakes because of IT security’s limited viewpoint
Policies, Implementation, and Oversight

FIGURE 2.19 Policies, Implementation, and Oversight
Implementation Guidance 1

• Implementation Guidance
  − Limits the discretion of implementers in order to simplify implementation decisions and avoid bad choices in interpreting policies

• None
  − Implementer is only guided by the policy itself

• Standards versus Guidelines
  − Standards are mandatory directives
  − Guidelines are not mandatory but must be considered

• Types of Implementation Guidance
  − Procedures: detailed specifications for how something should be done
    • Can be either standards or guidelines
Implementation Guidance 2

• Types of Implementation Guidance cont.
  – Procedures cont.
    • Segregation of duties: two people are required to complete sensitive tasks
      – In movie theaters, one sells tickets and the other takes tickets
      – No individual can do damage
    • Request/authorization control
      – Limit the number of people who may make requests on sensitive matters
      – Allow even fewer to be able to authorize requests
      – Authorizer must never be the requester
    • Mandatory vacations to uncover schemes that require constant maintenance
    • Job rotation to uncover schemes that require constant maintenance
Implementation Guidance 3

- Types of Implementation Guidance cont.
  - Processes: less detailed specifications of what actions should be taken
    - Necessary in managerial and professional business function
  - Baselines: checklists of what should be done but not the process or procedures for doing them
  - Best practices: most appropriate actions in other companies
  - Recommended practices: normative guidance
  - Accountability
    - Owner of resource is accountable
    - Implementing the policy can be delegated to a trustee, but accountability cannot be delegated
  - Codes of ethics
Ethics 1

• Ethics
  – A person’s system of values
  – Needed in complex situations
  – Different people may make different decisions in the same situation
  – Companies create codes of ethics to give guidance in ethical decisions

• Code of Ethics: Typical Contents (Partial List)
  – Important for having a good workplace and to avoid damaging a firm’s reputation
  – Applies to everybody
    • Senior managers usually have additional requirements
  – Improper ethics can result in sanctions, up to and including termination
  – An employee must report observed unethical behavior
Ethics 2

- Code of Ethics: Typical Contents (Partial List) cont.
  - An employee must involve conflicts of interest
    - Never exploit one’s position for personal gain
    - No preferential treatment of relatives
    - No investing in competitors
    - No competing with the company while still employed by the firm
  - No bribes or kickbacks
    - Bribes are given by outside parties to get preferential treatment
    - Kickbacks are given by sellers when they place an order to secure this or future orders
  - Employees must use business assets for business uses only, not personal use
  - An employee may never divulge
    - Confidential information
    - Private information
    - Trade secrets
Exception Handling

- Exceptions Are Always Required
  - But they must be managed
- Limiting Exceptions
  - Only some people should be allowed to request exceptions
  - Fewer people should be allowed to authorize exceptions
  - The person who requests an exception must never be authorizer
- Exception Must be Carefully Documented
  - Specifically what was done and who did each action
- Special Attention Should be Given to Exceptions in Periodic Auditing
- Exceptions Above a Particular Danger Level
  - Should be brought to the attention of the IT security department and the authorizer’s direct manager
Oversight 1

- **Oversight**
  - Oversight is a group of tools for policy enforcement
  - Policy drives oversight, just as it drives implementation

- **Promulgation**
  - Communicate vision
  - Training
  - Stinging employees?

- **Electronic Monitoring**
  - Electronically-collected information on behavior
  - Widely done in firms and used to terminate employees
  - Warn subjects and explain the reasons for monitoring
Oversight 2

- **Security Metrics**
  - Indicators of compliance that are measured periodically
  - Percentage of passwords on a server that are crackable, etc.
  - Periodic measurement indicates progress in implementing a policy

- **Auditing**
  - Samples information to develop an opinion about the adequacy of controls
  - Database information in log files and prose documentation
  - Extensive recording is required in most performance regimes
  - Avoidance of compliance is a particularly important finding
  - Internal and external auditing may be done
  - Periodic auditing gives trends
  - Unscheduled audits trip up people who plan their actions around periodic audits
Oversight 3

• Anonymous Protected Hotline
  – Employees are often the first to detect a serious problem
  – A hotline allows them to call it in
  – Must be anonymous and guarantee protection against reprisals
  – Offer incentives for heavily damaging activities such as fraud?

• Behavioral Awareness
  – Misbehavior often occurs before serious security breaches
  – The fraud triangle indicates motive.

FIGURE 2-24  Fraud and Abuse Triangle
Oversight 4

• Vulnerability Tests
  – Attack your own systems to find vulnerabilities
  – Free and commercial software
  – Never test without a contract specifying the exact tests, signed by your superior
  – The contract should hold you blameless in case of damage
  – External vulnerability testing firms have expertise and experience
  – They should have insurance against accidental harm and employee misbehavior
  – They should not hire hackers or former hackers
  – Should end with a list of recommended fixes
  – Follow-up should be done on whether these fixes occurred

• Sanctions
  – If people are not punished when they are caught, nothing else matters
Governance Frameworks

FIGURE 2-25  Governance Frameworks
COSO 1

• Origins
  – Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org)
  – Ad hoc group to provide guidance on financial controls

• Focus
  – Corporate operations, financial controls, and compliance
  – Effectively required for Sarbanes–Oxley compliance
  – Goal is reasonable assurance that goals will be met

• Components
  – Control Environment
  – General security culture
  – Includes “tone at the top”
COSO 2

• Components cont.
  – If strong, weak specific controls may be effective
  – If weak, strong controls may fail
  – Major insight of COSO
  – Risk assessment
    • Ongoing preoccupation
  – Control activities
    • General policy plus specific procedures
  – Monitoring
    • Both human vigilance and technology
  – Information and communication
    • Must ensure that the company has the right information for controls
    • Must ensure communication across all levels in the corporation
CobiT 1

• CobiT
  – Control Objectives for Information and Related Technologies
  – CIO-level guidance on IT governance
  – Offers many documents that help organizations understand how to implement the framework

• The CobiT Framework
  – Four major domains
  – 34 high-level control objectives
    • Planning and organization (10)
    • Acquisition and implementation (7)
    • Delivery and support (13)
    • Monitoring (4)
  – More than 300 detailed control objectives
• Dominance in the United States
  – Created by the IT governance institute
  – Part of the Information Systems Audit and Control Association (ISACA)
  – ISACA is the main professional accrediting body of IT auditing
  – Certified information systems auditor (CISA) certification

The CobiT Framework
Four major domains

FIGURE 2-28  CobiT
The ISO/IEC 27000 Family of Security Standards 1

• ISO/IEC 27000
  – Family of IT security standards with several individual standards
  – From the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

• ISO/IEC 27002
  – Originally called ISO/IEC 17799
  – Recommendations in 11 broad areas of security management

• ISO/IEC 27001
  – Created in 2005, long after ISO/IEC 27002
  – Specifies certification by a third party
    • COSO and CobiT permit only self-certification
    • Business partners prefer third-party certification

• Other 27000 Standards
  – Many more 27000 standards documents are under preparation
### The ISO/IEC 27000 Family of Security Standards 2

- ISO/IEC 27002: Eleven Broad Areas

<table>
<thead>
<tr>
<th>Security policy</th>
<th>Access control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization of information security</td>
<td>Information systems acquisition, development and maintenance</td>
</tr>
<tr>
<td>Asset management</td>
<td>Information security incident management</td>
</tr>
<tr>
<td>Human resources security</td>
<td>Business continuity management</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>Compliance</td>
</tr>
<tr>
<td>Communications and operations management</td>
<td></td>
</tr>
</tbody>
</table>