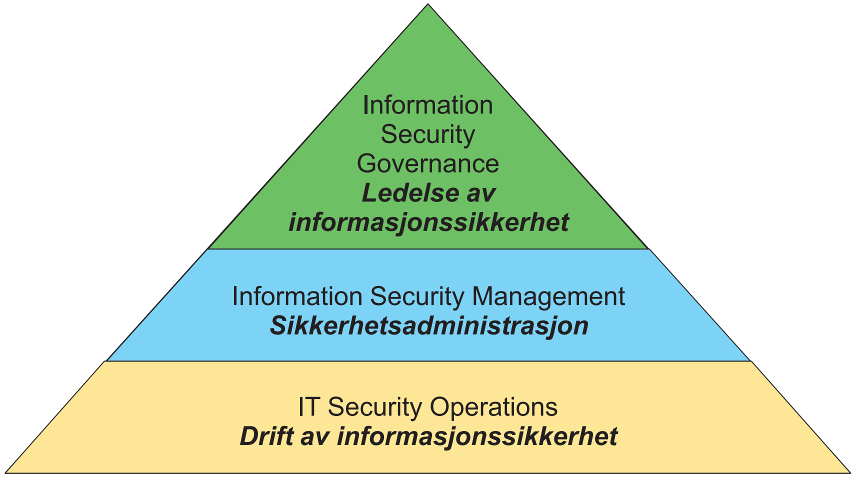
INF3510 Information Security

Lecture 02:
- Information Security Management
- Human Factors for Information Security

University of Oslo, spring 2014

IT Security Management concepts



Information Security Governance
Ledelse av informasjonssikkerhet

Information Security Management
Sikkerhetsadministrasjon

IT Security Operations
Drift av informasjonssikkerhet

GRC – Governance, Risk & Compliance

- GRC encompasses the activities of
  1. corporate governance,
  2. enterprise risk management (ERM)
  3. corporate compliance with applicable laws and regulations
- GRC is the umbrella term covering an organization's approach across these three areas.
- Being closely related concerns, GRC activities are increasingly being integrated and aligned in order to remove overlaps and gaps, an to avoid conflicts.
- IS governance is an essential part of GRC

Defining Information Security Governance

IS governance is a subset of GRC.

IS governance provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme.

- IT Governance Institute

COBIT
Control Objectives for Information and Related Technology

- COBIT is a framework for IT management and IT governance. It is a set of controls and processes aimed at bridging the gap between control requirements, technical issues and business risks.
- The framework defines each process together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.
- COBIT describes processes for IS management
- COBIT is published and maintained by ISACA, the **Information Systems Audit and Control Association**
- ISACA first released COBIT in 1996;
- The current COBIT 5 was released in 2012.

Goals of information security governance as defined by COBIT and ISACA

1. Strategic alignment of security program
2. Risk management
3. Value delivery
4. Resource management
5. Performance measurement
6. Assurance process integration

http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf

ISACA - Mål for IT sikkerhetsledelse

1. Strategisk tilpasning av sikkerhetsprogrammet
   - IS-aktiviteter skal støtte organisasjonens helhetlige strategi.
2. Risikohåndtering
   - Gjøre nødvendige undersøkelser for å avdekke trusler, sårbarheter og risiko som organisasjonen står overfor, og bruke adekvate virkemidler for å redusere risiko til et akseptabelt nivå.
3. Verdiskapning
   - Søk optimal balanse mellom reduksjon av risiko og tap, og kostnader forbundet med sikkerhetsvirkemidler.
4. Ressursbruk
   - Arbeidet med informasjonssikkerhet skal gjøres effektivt
5. Målbarhet
   - Effekten av sikkerhetsarbeidet skal måles
6. Integrering av sikkerhetsområder
   - Separate områder relatert til sikkerhet (fysisk, finansiell, IT etc) skal i størst mulig grad integreres

What is information security management?

Includes:

- Risk management,
- Security policies (creation and maintenance)
  - Documented goals, rules and practice for IS
- Plan and organisation for managing the security activities
  - Information Security Management System (ISMS)
- Information classification
- Definition of security procedures, standards & guidelines
- Deployment and maintenance of security controls
- Security education and training
- Disaster recovery and business continuity planning

Who is responsible for ISM?

- Management
  - CEO, CSO, CIO
  - Allocate resources, endorse and abide security policies
- IT Security staff
- General security staff, i.e. guards, janitors etc.
  - Important for physical security
- IT staff
- Users
- Third parties
  - Outsourced information security management
  - Customers, suppliers, business partners

Compliance: Following law and regulation

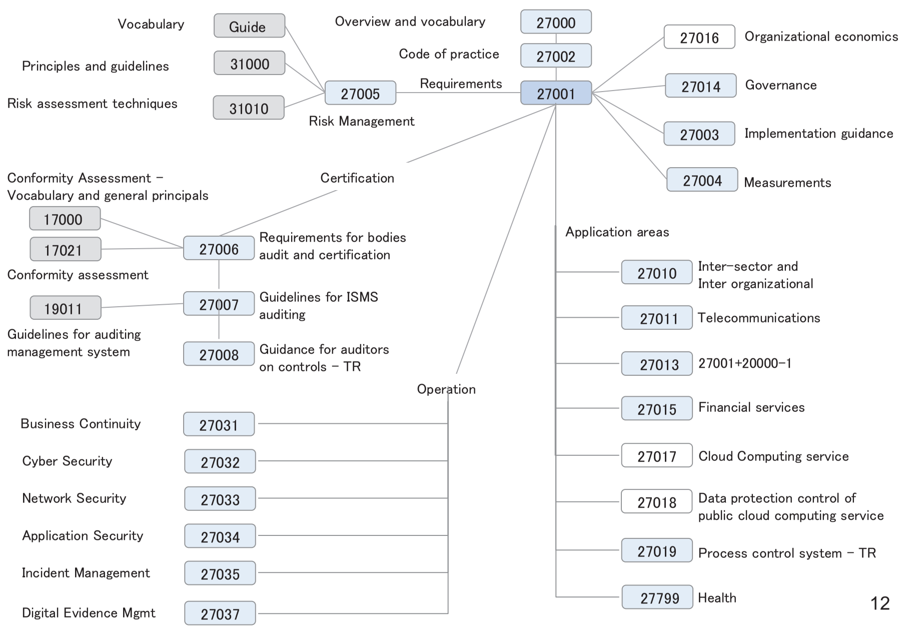
- Law and regulation, e.g.
  - EU Data Protection Directive 1995, mandates privacy regulation in EU member countries
  - Norwegian "personopplysningsloven" (personal data law) (2000) mandates principles for collecting and processing personal data
  - It is mandatory to follow laws and regulation,
  - Breach of compliance is sanctioned by authority
- Explicit company policy
  - Defines who is authorized to do what
  - Defines appropriate use
  - It is good practice to follow company policy,
  - Breach of compliance is sanctioned by company
  - Can lead to liability if incidents result from breach of policy

IS Management Standards

- ISO/IEC 27K security standards:
  - ISO: International Standards Organization
  - IEC: International Electro-technical Committee
  - ISO/IEC is correct, but people mostly refer to the standards as ISO…
  - ISO 2700:1 Information Security Management System (ISMS)
  - ISO 27002: Code of practice for information security management
  - + many more
  - ISO/IEC standards cost money
- USA
  - NIST (National Institute for Standards and Technology) Special Publications, including SP800-12, SP800-14, SP800-18, SP800-26 and SP800-30, SP800-64
  - + many more
  - NIST standards are free

ISO/IEC 27000 family of standards and related standards

as of Oct. 2013



ISO/IEC 27002– What is it?

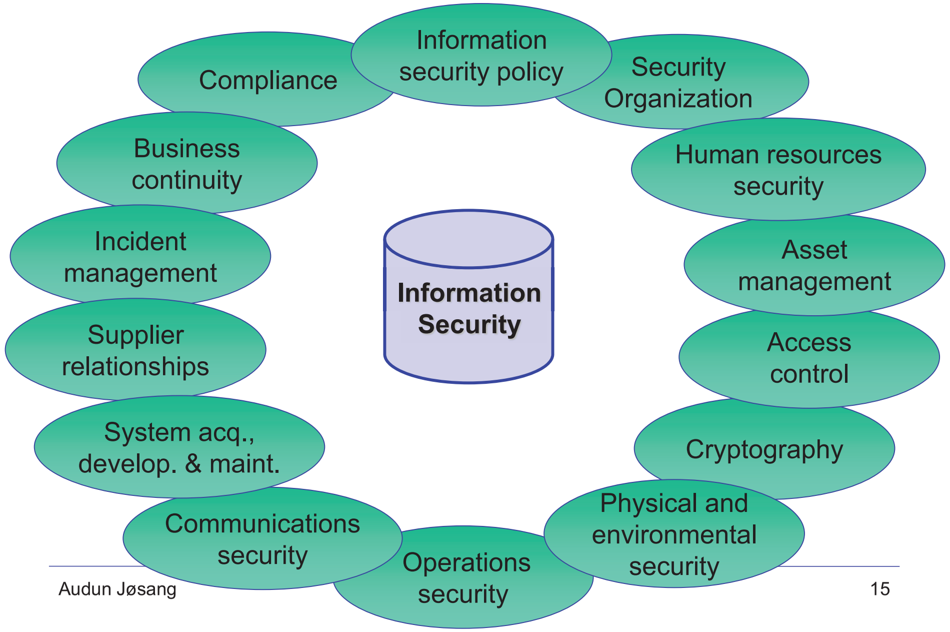
Code of practice for information security management

- ISO 27002 provides a checklist of general security controls to be considered implemented/used in organizations
  - Contains 14 categories (control objectives) of security controls
  - Each category contains a set of security controls
  - In total, the standard describes 113 generic security controls
- Not all controls are relevant to every organisation
- Objective of ISO 27002:
- "… gives guidelines for […] information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)."

ISO/IEC 27002 Code of Practice for ISM, History

- In early 1990's, recognized need for a practical guide for information security management
  - Group of leading companies in the UK combined to develop *"Code of Practice for Information Security Management"*
  - Published in the UK as BS7799 (British Standard) version 1 in Feb. 1995
  - New version adopted as ISO/IEC 17799:2001
  - Updated to ISO/IEC 27002:2005.
  - Last version ISO/IEC 27002:2013.

The 14 Control Objectives of ISO/IEC 27002:2013



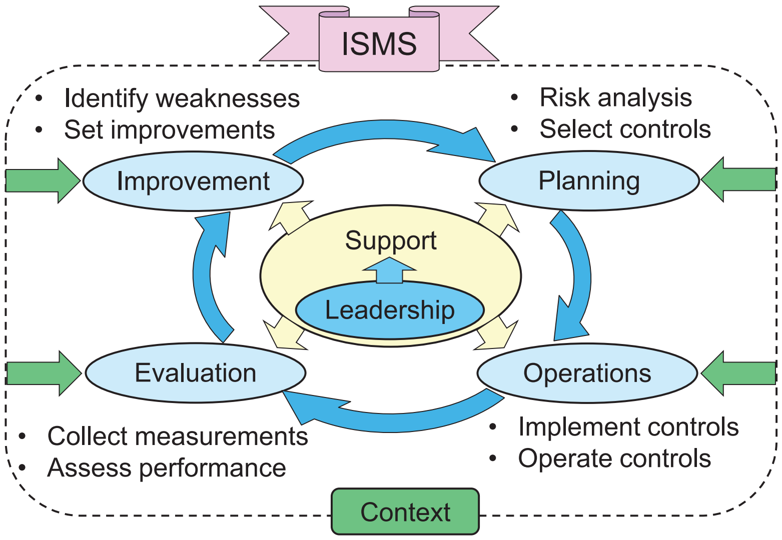
ISO/IEC 27001:2013- What is it?

- ISO 27001 specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization.
- ISMS is a holistic approach to IS management
  - … not an IT system
- While the ISO 27002 (code of practice) defines a set of security goals and controls, ISO 27001 (ISMS) defines how to manage the implementation of security controls.
- Organizations can be certified against ISO 27001
  - … but not against ISO 27002
- ISO 27001 is to be used in conjunction with ISO 27002

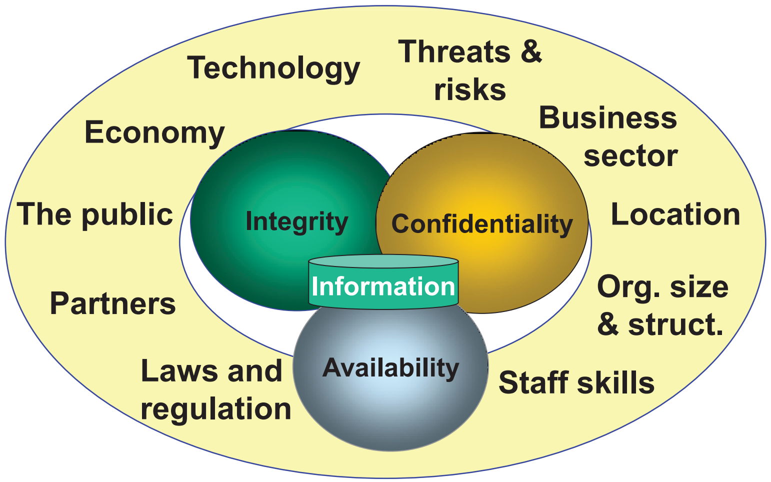
ISO/IEC 27001- ISMS
History

- The need to establish a certification scheme for information security management emerged late 1990s
- A general approach to security management was needed for certification purposes, not just the “code of practice”
- BS 7799-2:1999 was created to define a comprehensive **ISMS (Information Security Management System)** against which certification was possible.
- Led to the dramatic conclusion that **ISMS is perhaps of far greater and fundamental importance than the original Code of Practice**.
- ISMS which originally was a “part 2” of BS7799 became ISO 27001:2005, the main standard in the ISO 27K series
- Updated to ISO/IEC 27001:2013

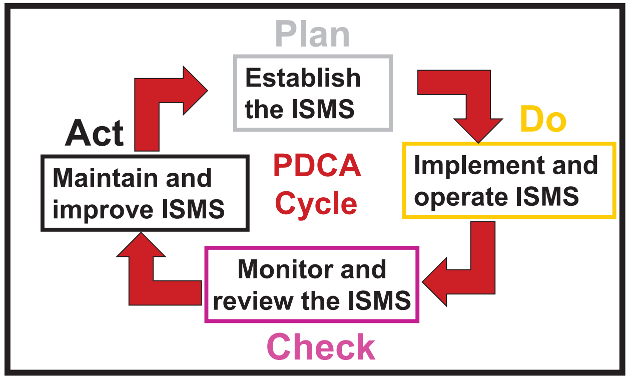
ISO 27001:2013 - ISMS Elements



Context for IS Management



PDCA model in previous ISO27001:2005

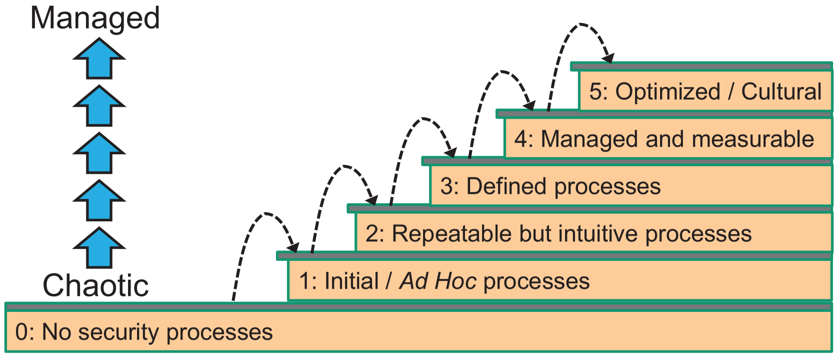

Plan
Establish the ISMS
Do
Implement and operate ISMS
Check
Monitor and review the ISMS
Act
Maintain and improve ISMS
PDCA Cycle

- Based on Deming’s PDCA quality control model.
- PDCA no longer used for ISMS

W. Edwards Deming (1900-1993)

COBIT ISM CMM
Capability Maturity Model for IS Management

Considerable effort and time is required to reach each next level in the maturity model.


Managed
Chaotic
5: Optimized / Cultural
4: Managed and measurable
3: Defined processes
2: Repeatable but intuitive processes
1: Initial / *Ad Hoc* processes
0: No security processes

CMM levels 1 - 3

1. Initial / Ad Hoc
   - + Processes are ad-hoc and disorganised.
   - + Risks are considered on an ad hoc basis, but no formal processes exist.
2. Repeatable but intuitive
   - + Processes follow a regular pattern.
   - + Emerging understanding of risk and the need for security
3. Defined process
   - + Processes are documented and communicated.
   - + Company-wide risk management.’
   - + Awareness of security and security policy

CMM levels 4 - 5

4. Managed and measurable
   - + Processes are monitored and measured.
   - + Risks assessment standard procedures
   - + Roles and responsibilities are assigned
   - + Policies and standards are in place
5. Optimized
   - + Security culture permeates organisation
   - + Organisation-wide security processes are implemented, monitored and followed

NIST: http://csrc.nist.gov/ Computer Security Resource Center

Library of freely available SP800-X publications

-100: Information Security Handbook: A Guide for Managers
-53: Recommended Security Controls for Federal Info Systems
-35: Guide to Information Technology Security Services
-39: Managing Information Security Risk
-30: Guide for Conducting Risk Assessment
-27: Engineering Principles for Information Technology Security
-18: Guide for Developing Security Plans for Federal Info Systems
-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
-12: An Introduction to Computer Security: The NIST Handbook
-26: Security Self-Assessment Guide for Information Technology Systems

Evaluation of the ISMS through Security Measurements

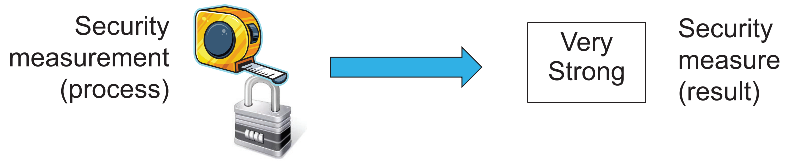
- What is the effectiveness of a security control ?
  - You have to measure it to know it.
- Security measurements provide
  - info about how well security controls work
  - basis for comparing effect of controls on risks
  - benchmark for assessing security investments

Why do we care: Example

- **The CEO asks**, *"Is our network perimeter secure?"*
- **Without metrics:**
  "Well, we installed a firewall, so it must be."
- **With metrics:**
  "Yes, our evidence tells us that we are. Look at our risk score before we implemented that firewall project. It's down 10 points. We are definitely more secure today than we were before."

What is a security measure ?

- Variable to which is assigned the result of a security measurement
- Security measurement is the process of obtaining information about the effectiveness of ISMS and controls using a measurement method
- Although standard security measures exist, security measures should ideally be adjusted and tuned to fit a specific organization's needs.



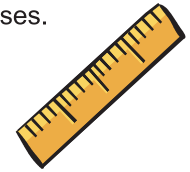
Security measurement (process)

Very Strong

Security measure (result)

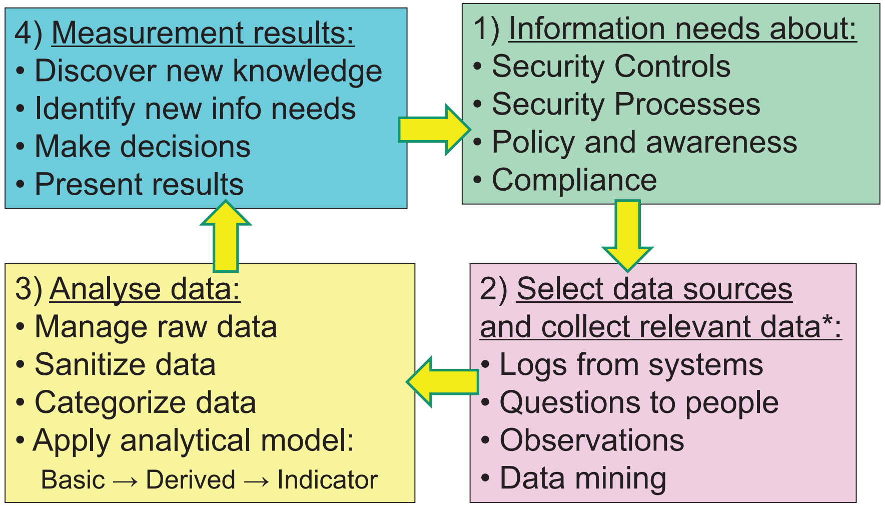
Data types

- Quantitative data
  - Nominal labels: A, B, C, etc.; IP ports and addresses.
  - Ordinal data: Rank 1,2,3, etc.; Memory addresses
  - Interval data: Distance, Range
  - Quantity data: How much, or how many
  - Proportion data: quantity / reference quantity



- Qualitative data
  - Text
  - Statements
  - Categories
  - Multimedia

IS Measurement Model (ISO 27004)



4) Measurement results:
- Discover new knowledge
- Identify new info needs
- Make decisions
- Present results

1) Information needs about:
- Security Controls
- Security Processes
- Policy and awareness
- Compliance

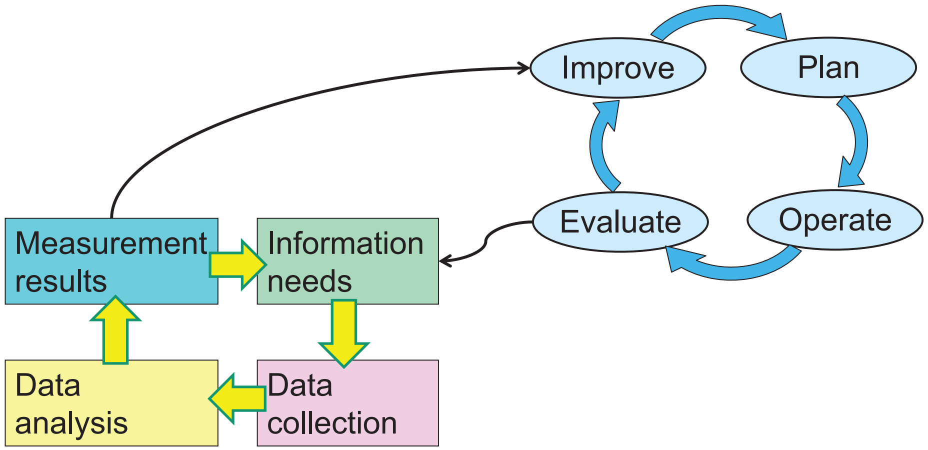
3) Analyse data:
- Manage raw data
- Sanitize data
- Categorize data
- Apply analytical model:

Basic → Derived → Indicator

2) Select data sources and collect relevant data*:
- Logs from systems
- Questions to people
- Observations
- Data mining

*) Called Objects of measurement in ISO 27004

Measurement – ISMS integration



The human factor in information security

- ❖ Personnel integrity
  - ❖ Making sure personnel do not become attackers
- ❖ Personnel as defence
  - ❖ Making sure personnel do not fall victim to social engineering attacks
- ❖ Security usability
  - ❖ Making sure users operate security correctly

Personnel Integrity
Preventing employees from becoming attackers

- Consider:
  - – Employees
  - – Executives
  - – Customers
  - – Visitors
  - – Contractors & Consultants
- All these groups obtain some form of access privileges
- How to make sure privileges are not abused?

Personnel crime statistics

- Organisations report that large proportion of computer crimes originate from inside
- US Statistics (CSI/FBI) 2005
  - http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
  - 71% had inside (65% had external) computer crime attacks
- Australian Statistics (AusCERT) 2006
  - http://www.auscert.org.au/images/ACCSS2006.pdf
  - 30% had inside (82% had external) electronic attacks
- Norway: Mørketallsundersøkelsen 2012
  - http://www.nsr-org.no/moerketall/
  - Approx. 50% of attackers are either staff or consultants.

Strengthening employee integrity

- Difficult to determine long term integrity at hiring
  - Integrity can change, influenced by events
- All personnel should follow security awareness training
- Reminders about security policy and warnings about consequences of intentional breach of policy
  - Will strengthen power of judgment
- Personnel in highly trusted positions must be supported, trained and monitored
- Support and monitor employees in particular situations
  - Conflict, loss or change of job, personal problems
  - Try to stay on good terms with staff leaving the company

Personnel Departure

- Different reasons for departure
  - Voluntary
  - Redundancy
  - Termination
- Different types of actions
  - Former employee may keep some privileges
  - Revoke all privileges
  - Escort to the exit.
- During exit interview, terms of original employment agreement reviewed (i.e. non-compete, wrongful disclosure, etc.

Social engineering attacks

Where people are the defence

Social Engineering Attacks

- According to Kevin Mitnick:
  - “The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you.”
  - “What I found personally to be true was that it’s easier to manipulate people rather than technology. Most of the time, organisations overlook that human element”.

From “How to hack people”, BBC NewsOnline, 14 Oct 2002

SE Tactics: Develop Trust

- People are naturally helpful and trusting
- Ask during seemingly innocent conversations
- Slowly ask for increasingly important information
- Learn company lingo, names of key personnel, names of servers and applications
- Cause a problem and subsequently offer your help to fix it (aka. reverse social engineering)
- Talk negatively about common enemy
- Talk positively about common hero

SE Tactics: Induce strong affect

- Heightened emotional state makes victim
  - Less alert
  - Less likely to analyse deceptive arguments
- Triggered by attacker by creating
  - Excitement (“you have won a price”)
  - Fear (“you will lose your job”)
  - Confusion (contradictory statements)

SE Tactics: Information overload

- Reduced the target’s ability to scrutinize arguments proposed by the attacker
- Triggered by
  - Providing large amounts of information to produce sensory overload
  - Providing arguments from an unexpected angle, which forces the victim to analyse the situation from new perspective, which requires additional mental processing

SE Tactics: Reciprocation

- Exploits our tendency to return a favour
  - Even if the first favour was not requested
  - Even if the return favour is more valuable
- Double disagreement
  - If the attacker creates a double disagreement, and gives in on one, the victim will have a tendency to give in on the other
- Expectation
  - If the victim is requested to give the first favour, he will believe that the attacker becomes a future ally

SE Tactics: Diffusion of responsibility and moral duty

- Make the target feel the he or she will not be held responsible for actions
- Make the target feel that satisfying attacker's request is a moral duty

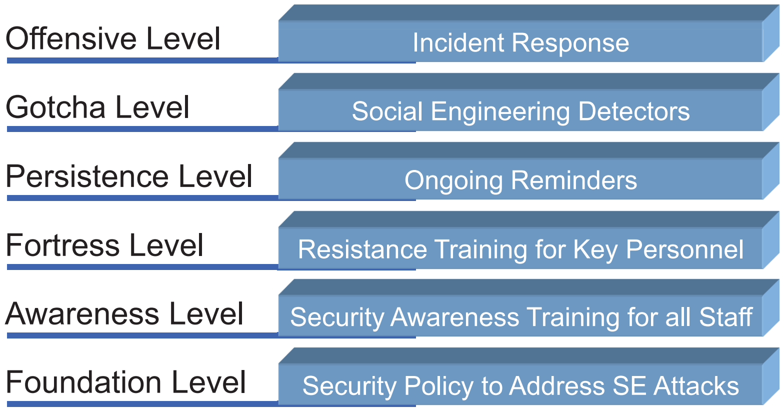
SE Tactics: Authority

- People are conditioned to obey authority
  - Milgram and other experiments
  - Considered rude to even challenge the veracity of authority claim
- Triggered by
  - Faking credentials
  - Faking to be a director or superior
  - Skilful acting (con artist)

SE Tactics: Commitment creep

- People have a tendency to follow commitments, even when recognising that it might be unwise.
- It's often a matter of showing personal consistency and integrity
- Triggered e.g. by creating a situation where one commitment naturally or logically follows another.
  - First request is harmless
  - Second request causes the damage

Multi-Level Defence against Social Engineering Attacks



Offensive Level – Incident Response

Gotcha Level – Social Engineering Detectors

Persistence Level – Ongoing Reminders

Fortress Level – Resistance Training for Key Personnel

Awareness Level – Security Awareness Training for all Staff

Foundation Level – Security Policy to Address SE Attacks

Source: David Gragg: http://www.sans.org/rr/whitepapers/engineering/

SE Defence: Foundation

- The security policy must address SE attacks
  - Policy is always the foundation of information security
    - Address e.g.: Shredding, Escorting, Authority obedience
- Ban practice that is similar to social attack patterns
  - Asking for passwords over phone is a typical SE attack method
    → Therefore never provide passwords over the phone
  - Calling a user and pretending to represent IT department is a typical SE attack
    → Therefore never call user, or make it possible/mandatory for user to authenticate the IT Department
  - Calling IT dep. and pretending to be user is a typical SE attack
    → Therefore make it possible/mandatory for IT department to authenticate the user

SE Defence: Awareness

- Security awareness training for all staff
  - Understanding SE tactics
  - Learn to recognise SE attacks
  - Know when to say “no”
  - Know what is sensitive
  - Understand their responsibility
  - Understand the danger of casual conversation
  - Friends are not always friends
  - Passwords are personal
  - Uniforms are cheap
- Awareness of policy shall make personnel feel that the only choice is to resist SE attempts

SE Defence: Fortress

- Resistance training for key personnel
  - Consider: Reception, Help desk, Sys.Admin., Customer service,
- Fortress training techniques
  - Inoculation
    - Expose to SE arguments, and learn counterarguments
  - Forewarming
    - of content and intent
  - Reality check:
    - Realising own vulnerability,

SE Defence: Persistence

- Ongoing reminders
  - – SE resistance will quickly diminish after a training session
  - – Repeated training
  - – Reminding staff of SE dangers
    - Posters
    - Messages
    - Tests

SE Defence: Gotcha

- Social Engineering Detectors
  - – Filters and traps designed to expose SE attackers
- Consider:
  - – The justified Know-it-all
    - Person who knows everybody
  - – Centralised log of suspicious events
    - Can help discover SE patterns
  - – Call backs mandatory by policy
  - – Key questions, e.g. personal details
  - – “Please hold” mandatory by policy
    - Time to think and log event
  - – Deception
    - Bogus question
    - Login + password of “alarm account” on yellow sticker

SE Defence: Offensive

- Incident response
  - – Well defined process for reporting and reacting to
    - Possible SE attack events,
    - Cases of successful SE attacks
- Reaction should be vigilant and aggressive
  - – Go after SE attacker
  - – Proactively warn other potential victims

Security awareness training

- Back up and protection of work related information
- Passwords
- Email and web hygiene and acceptable use
- Recognising social engineers
- Recognising and reporting security incidents
- Responsibilities and duties for security
- Consequences of negligence or misbehaviour
- Security principles for system and business processes

Security Usability

Kerckhoffs - 1883
The father of security usability

- Auguste Kerckhoffs. La cryptographie militaire.
  Journal des sciences militaires, IX(38):5-38, 1883.
- Most famous for *“avoid security by obscurity”*
- Also defined security usability principles

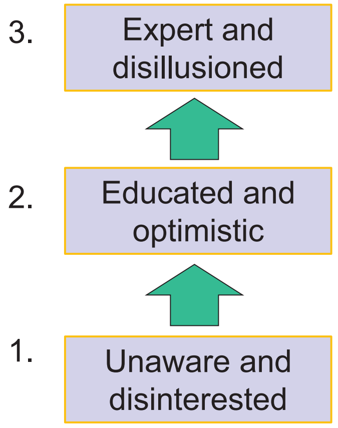
It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants.

Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Security Learning

- Good metaphors are important for learning
- Many security concepts do not have intuitive metaphors
- Better avoid metaphors than use bad ones
- Define new security concepts
  - and give them semantic content
- Security learning design
  - Design systems to facilitate good security learning
  - Largely unexplored field

Stages of security learning
Revealing a deeper problem

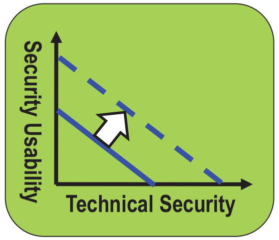


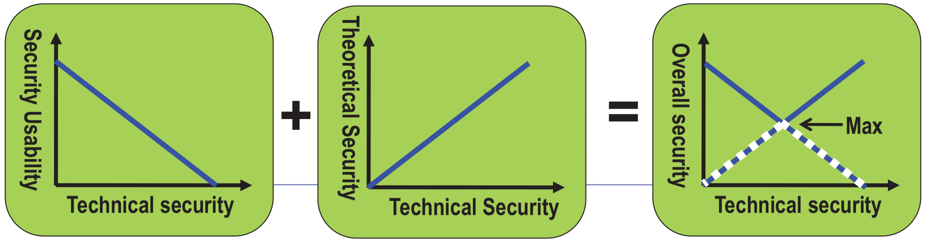
3. Expert and disillusioned
2. Educated and optimistic
1. Unaware and disinterested

- *This is far more complex than I first thought. I actually don’t think this can ever be made secure.*
- *I understand it now, it’s simple, and I know how to operate it*
- *I don’t understand it, and I don’t want to know about it. Why can’t security simply be transparent?*

Security/Usability trade-off

1. Trade-off between technical security and usability.
2. Goal is to increase both usability and technical security.
3. Find the right amount of technical security to maximize overall security





Security usability vulnerabilities

Security usability vulnerabilities exist when:

- users don't know or understand which security decisions or actions are required,
- systems do not provide the user with sufficient information for deriving a security conclusion,
- an intolerable mental or manual load results from deriving the required security conclusion,
- an intolerable mental or manual load results from deriving security concl. for any practical # of instances.

A.Jøsang *et al.*. (ACSAC'07)
Security Usability Principles for Vulnerability Analysis and Risk Assessment

Remarks on security usability

- Security usability is difficult to get right
  - Not the same as IT usability
- Security can never be 100% transparent
  - Security learning is a challenge
- Little information for making security decision
  - Security decision support is a possible solution
- Knowledge about security usability exists
  - User-friendly security can be designed

End of lecture