Role of standards and evaluation criteria & non-technical topics – risk analysis, security manager, etc.

PV018

Vašek Matyáš

Broader scope of standards related to information security

- Audit standards
  - Financial audit – IS/IT audit
- IT security standards
- (Other) IT standards

IT security standards

- Basic standards – OSI security architecture, entity authentication mechanisms
- Functional standards – how to use basic standards
- Evaluation criteria
- Industrial standards and methodologies
- Interpretative documentation – dictionaries, guidelines, etc.

Classification of standards

- By publisher
  - Worldwide – ISO, ISO/IEC, CCITT/ITU
  - US – ANSI, NIST
  - EU – CEN, CENELEC, ECMA
  - Groups – IETF-RFC, IEEE
  - Industrial – RSA – PKCS
- By content/cover

Basic cryptography standards

- Symmetric crypto – DES, AES
- Asymmetric crypto – encryption, signatures, key exchange and transfer
  - IEEE P1363 – Factoring-based, Discrete log based, Elliptic curve
  - NIST FIPS 186-3 – Digital Signature Standard
- Hash functions – SHA-1, RIPEMD, (MD5), SHA-512

Cryptographic algorithms

- Crucial to most systems
- National (self-)interests
- Decades of intentional avoidance of this topic for international standardization
- Crucial to DES importance – indirect support by missing a widely accepted better standards
- Therefore high expectations of AES

Applied/Functional cryptography standards

- Digital certificates – X.509,
- PKCS – RSA, D-H, Certificate, Message, Private-Key, Attributes, Certificate Request, Crypto Token Interface & Information, ECC
- Security/Crypto protocols
  - Low level – basic standards (entity auth.)
  - ISO/IEC – Key Management 11770, Non-rep. 13888
  - IETF – PKIX, IPSEC, S/MIME

Cryptonessie

- *New European Schemes for Signatures, Integrity, and Encryption* – EU, start 2000, closed recently
- Block ciphers, stream ciphers
- Message authentication codes
- Hash functions
- Pseudorandom functions
- Asymmetric schemes for
  - Encryption
  - Signatures
  - Identification
- All two levels – standard/high; *http://cryptonessie.org*

Other areas in ISO/IEC

- OSI security – subcommittee 6, 21
- Smartcards – SC17
- Message Handling Services – SC18
- Security mechanisms – SC 27
  - Group 1 – General documents – Requirements, Security Services, Guidelines
  - Group 2 – Majority of the (technical) work – Techniques and Mechanisms
  - Group 3 – Security evaluation criteria

Application areas

- Banking security
  - Standards of ISO TC68
  - ANSI X9 – authentication, key management, public-key cryptography
- Cryptographic modules – FIPS 140-1 (2)
- Trusted Third Parties
- Electronic payments

Evaluation criteria

- USA – late 60s and 70s – need to minimize costs for individual evaluations
- 1985 – Trusted Computer System Evaluation Criteria – “Orange Book”
  - D class – no security
  - A1 – highest security (mathematical formalism)

Development of criteria

- Europe – ITSEC – separation of functionality and assurance
- Canada – CTCPEC – functionality separated into confidentiality, integrity, accountability, and availability
- US – Federal Criteria – development halted
- Common Criteria – worldwide standard
  - ISO/IEC 15408

Common Criteria

- Interests of users, manufacturers, evaluators
- Target of evaluation (TOE) – what is (to be) evaluated
- Protection profile (smartcards, biometrics, etc.)
  - Catalogued as a self-standing evaluation document
- Security target (ST) – theoretical concept/aim
- Evaluation of TOE – is the reality corresponding to theory (ST)?
- Functional and Assurance requirements

Importance of criteria

- Eases application and use of secure systems – easier comparison and choice-to-fit
- Eases specification of requirements
- Easier design and development

BS7799

- Code of Practice for Information Security Management – 1995
- Specification for Information Security Management Systems – 1998
- Update of both in 1999
- ISO/IEC standard 17799

Information dominance

1. Aim: Reaching own information dominance: having the right information at the right place in the right time.

2. Aim (offensive): Limit the other party in reaching full information dominance.

One step after another…

1. Risk analysis
2. Specification of security policy and security architecture
3. Design and implementation of security mechanisms
4. Support, maintenance, control, re-evaluation (back to 1…)

Risk

- **Risk –** The probability that a particular threat will exploit a particular vulnerability of the system.
- **Risk analysis –** The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk analysis

- Often rather risk assessment – less formal and rigorous process
- Quantitative vs. qualitative
- Quantitative
  - Easy to understand the results
  - Results usually in $$$ (risk exposure)
- Qualitative
  - Discrete scale (not $$$)
  - Easy to automate, not that easy to understand the results

Analysis of IS in general

- Often based on BS7799
- Comparison of risks and controls
  - Use of defined scale
  - Does not value assets
- Asset-based evaluation
  - For companies critically dependant on IT and those with a bit more complicated structure. A one-man shop can do things rather informally, comparing risks and controls.

Risk analysis – ALE method

- Annual Loss Expectancy (sometimes called Estimated Annual Cost – EAC)

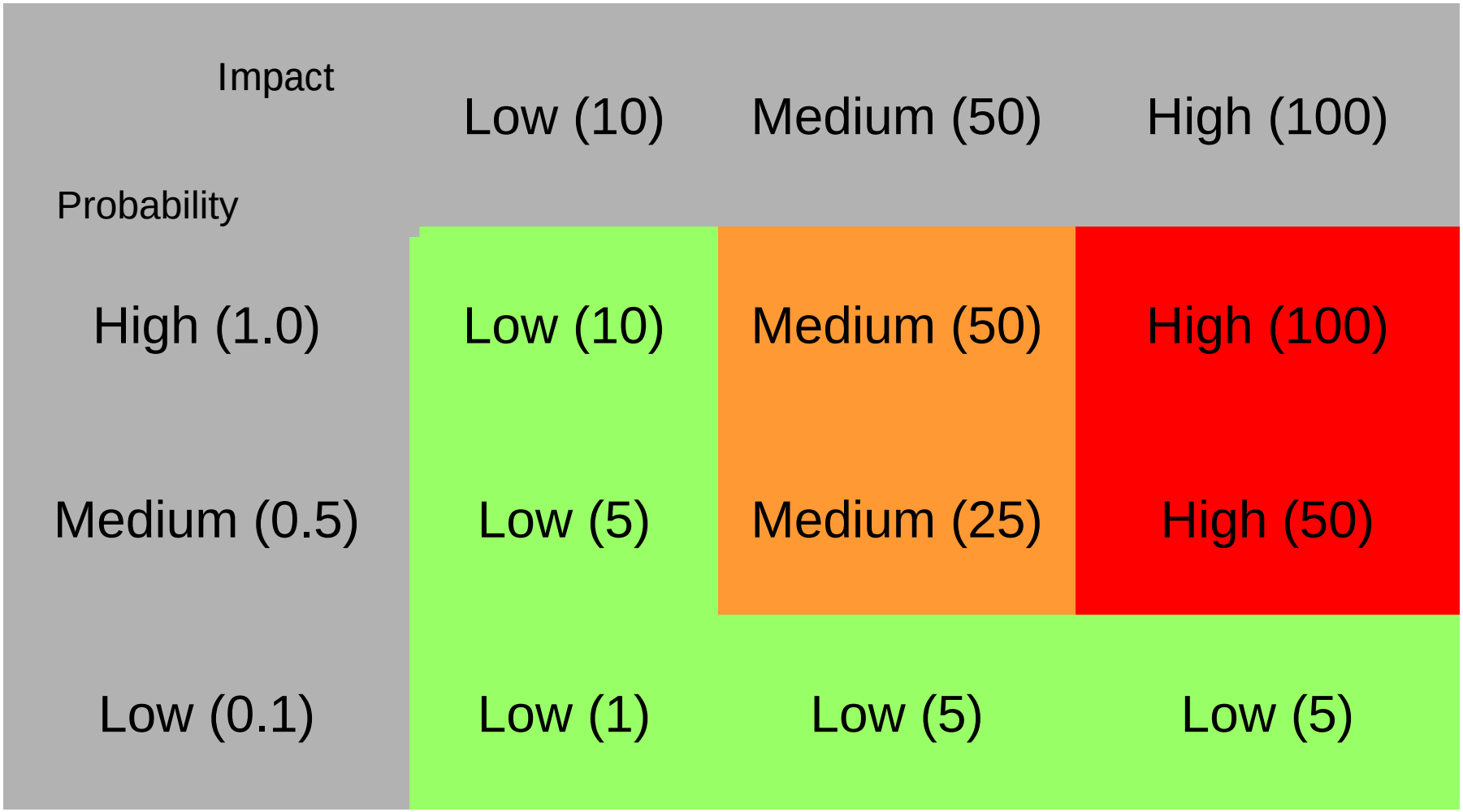
- ALE = SLE x ARO

- SLE – Single Loss Exposure
- ARO – Annualized Rate of Occurrence

Problems of quantitative risk analysis

- Unreliability and inaccuracy of the data used.
- Probability is hardly precise.
- Expectations based on data from the past can lead to ungrounded complacency.
- Countermeasures and controls can address some events that are inter-related.

Principle of qualitative risk analysis



Risk analysis – BPA

- Business Process Analysis
- Broader view of risks, not just IT
- Some IT risks might not be identified if they do possibly not impact a business process
- Outputs
  - map of processes and their descriptions
  - Table of risks (qualitative) and controls
  - Recommendations

CRAMM

- 1985 – UK Government Risk Analysis and Management Method
- Structured three-stage approach
  - Identify and value assets
  - Assess the threats and vulnerabilities to the assets
  - Select appropriate recommended countermeasures
- Very complex analysis (need for time and trained specialists, use of special software).

Risk analysis – notes

- Information collection – questionnaires, interviews
- Control of completeness – formal checks, experience of the evaluator (!!!)
- Processing of inputs (semi-automated)
- Report with suggestions for risk reduction or even elimination

Incidents caused by

- Errors (not intended to happen): 50-70%
- Natural/utility influence: 10-15%
- Malicious software: 5-10%
- Intentional sabotage/attack/corruption by own/past employees/members: 10-20%
- External attackers: 1-5%

Impact of incidents is yet another issue!

Role of IT security manager

- Experience with IT security very important
- Art of persuasion critical!
- Experience: 60% management skills, 40% security expert skills
- Very demanding and challenging position
  - Criticized for incidents
  - Criticized for obstructions to “normal” processes
  - Can be appreciated for “nothing happening”? ☺

Security is not just prevention

1. Prevention (protection)
2. Detection
3. Reaction

Security policy

- VERY IMPORTANT for improving the (IT) security in any company
- Company *business goals* → IT goals → IT security goals
- Helps with
  - Setting priorities (for IT, security departments)
    - Long-term goals vs. short-term goals
    - Improvement of services (vs.) company survival(!)
  - Getting management support and assuming direct responsibilities

Security policy and company culture

- The best security mechanisms are useless without effective support of all parties involved
- End-users must be trained and interested
- Management must be involved (or better lead!)
- Security is a process, not a product

Recommended reading this week

- Paper "*Trends in Government Endorsed Security Product Evaluations*", RE Smith

`http://csrc.nist.gov/nissc/2000/proceedings/papers/032.pdf`