Security Policy Development for Health Information Systems

Dimitris Gritzalis

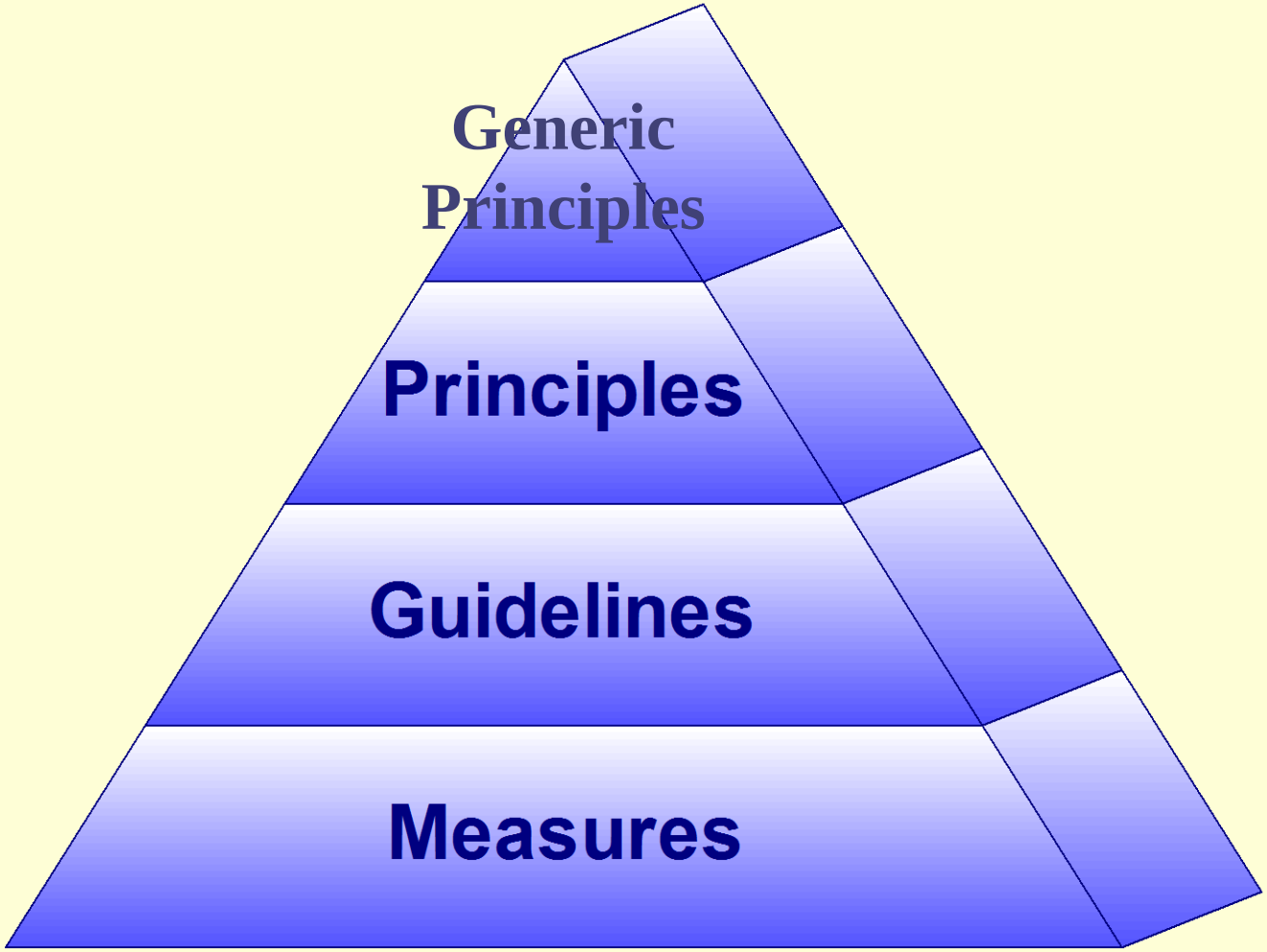
Developing HIS Security Policies

Developing a HIS Security Policy (SP) is a challenge

- HIS entail strict security requirements
- Healthcare institutions have unique organizational characteristics
- Social and human factors play very important role

Aim:
To develop *effective* SP in the social, organizational, and technical context of Health Information Systems.

HIS-SP structure



HIS-SP content

- **Generic principles** govern security and privacy in HIS; society and culture-dependent.
- **Principles** result when generic principles are considered within a specific national environment; state-dependent.
- **Guidelines** are specific organizational steps to be followed; technology-dependent.
- **Measures** result when guidelines are considered under a specific installation environment; installation-dependent.

Social and organizational context of Health Information Systems

- **Stakeholders interests and concerns**

  Medical personnel, data subjects, government, medical associations, pharmaceutical companies, insurance etc.

- **Organizational structure**

  Medical personnel takes active role in decision making.

- **Structures of domination and power**

  Several groups (e.g. doctors, managers, unions etc.) co-operate and antagonize.

- **Social and ethical values**

  Affect all aspects of HIS operation.

SP development methodologies

1. **Checklists and Generic Security Policies**
   - Guidelines proposed by key actors (e.g. BSI), Policy Cookbooks (e.g. *Security Policies Made Easy*, C. Cresson-Wood), etc.
   - MEDSEC Generic Security Policy.
   - BMA, SMA, Associations' policies and guidelines.
2. **Profiles**
   - CEN/ENV12924: Security categorization and protection for healthcare information systems

SP development methodologies

3. **Standard security management guidelines**
   - ISO/IEC 17799: Code of practice for information security management.
4. **Risk analysis and management**
   - Dozens of different methods and tools.
5. **Socio-technical methodologies**
   - SIM-ETHICS (Warren, 1996).
   - Virtual methodology (Hitchings, 1996).
   - Structures of responsibilities (Backhouse & Dhillon, 1996).

Overview of SP development methodologies (1/5)

1. Checklists and Generic Security Policies

- **Social context:** General, static, social context.
- **Organizational context:** Only general organizational considerations.
- **Technical context:** Considered, without installation-focused analysis.
- **Policy content:** Lists of *principles* and *guidelines*.

Overview of SP development methodologies (2/5)

2. Security profiles

- **Social context:** General, static, social context.
- **Organizational context:** Categorization of organizations.
- **Technical context:** HIS categorization according to technical characteristics.
- **Policy content:** Extensive lists of principles and guidelines. A separate list for each profile.

Overview of SP development methodologies (3/5)

3. Standard security management guidelines

- **Social context:** Social factors taken into account; national particularities are ignored.
- **Organizational context:** It is largely ignored.
- **Technical context:** General technological environment; Risk analysis is recommended for the analysis of the technical context.
- **Policy content:** Comprehensive list of principles and guidelines.

Overview of SP development methodologies (4/5)

4. Risk analysis and management

- **Social context:** Mostly neglected; only considered as source of threats.
- **Organizational context:** Not analyzed; considered as source of threats.
- **Technical context:** Analyzed in detail.
- **Policy content:** Guidelines and measures selected according to level of risk. Large repositories of measures are often provided.

Overview of SP development methodologies (5/5)

5. Socio-technical methodologies

- **Social context:** Its analysis plays central role.
- **Organizational context:** Emphasis on it is given.
- **Technical context:** No special emphasis on technical issues.
- **Policy content:** No specific lists of guidelines or measures are offered.

Concluding remarks

- HIS-SP not taking into serious account the social and organizational context are *ineffective*.
- Developing an *effective* HIS-SP requires:
  - Analysis of the **specific** social and organizational context
  - **Technical** analysis of the relevant HIS.
- HIS-SP developers need to combine *elements from different methodologies*.

References

1. Gritzalis D., “A digital seal solution for deploying trust on commercial transactions”, *Information Management & Computer Security*, Vol. 9, No. 2, pp. 71-79, March 2001.
2. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
3. Gritzalis D., “A baseline security policy for distributed healthcare information systems”, *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
4. Gritzalis D., Kantzavelou I., Katsikas S., Patel A., "*A classification of health information systems security flaws*", Proc. of the 11th International Information Security Conference, pp. 453-464, Chapman & Hall, South Africa 1995.
5. Iliadis J., Gritzalis D., Spinellis D., Preneel B., Katsikas S., “Evaluating certificate status information mechanisms”, *Proc. of the 7th ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, Greece, October 2000.
6. Katsikas S., Gritzalis D., Spirakis P., “Attack Modeling in Open Network Environments”, *Proc. of the 2nd Communications and Multimedia Security Confe*rence, pp. 268-277, Chapman & Hall, Germany 1996.
7. Katsikas S., Spyrou T., Gritzalis D., Darzentas J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
8. Pangalos G., Gritzalis D., Khair M., Bozios L., "Improving Medical Database System Security", *Proc. of the 11th International Information Security Conference*, pp. 11-25, Chapman & Hall, South Africa 1995.