Novel security risk assessment for personal health data

Nicole Hazelhoff Roelfzema

Information Security Consultant
Research Student

Healthcare in the information society

- Surveillance studies
  - Privacy discussions
- Innovative technologies
  - Security and reliability, trust
  - Standardisation of data collection
  - Integration of solutions and sharing information
- Professional changes
  - Ethical issues
  - Changes in relationship with patient
- Policy changes
  - Compliance and legislation issues: is current legislation fit for purpose?
- Citizen/patient as stakeholder
  - Data ownership, trust, mobility, accessibility, participation and consent

Research project

- Security risk model for personal health data
  - What are trying to protect and why is it important?
  - What do we know about the security risks and data breaches?
  - Are best practises still fit for purpose looking at current trends?
  - Mapping of risks to standards, best practises and legislation; are they sufficient?

Health care governance codes

Risk management standards

Process:

1. Get stakeholders
2. Define scope
3. Evaluate risks
4. Decide
5. Repeat

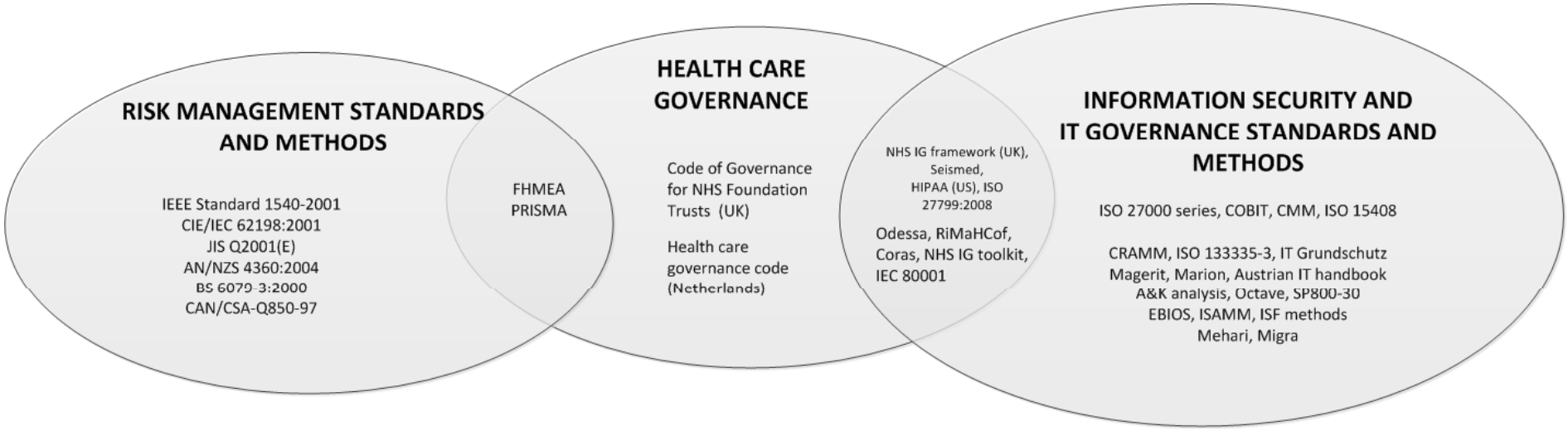
Risks:
Financial, reputational, market, credit, operational

Information security risks?

Baseline approach

RA tools and methods

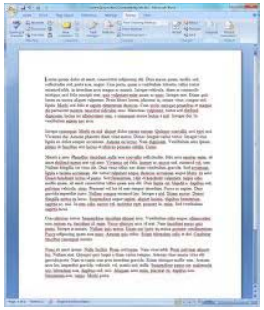
Current best practise approaches

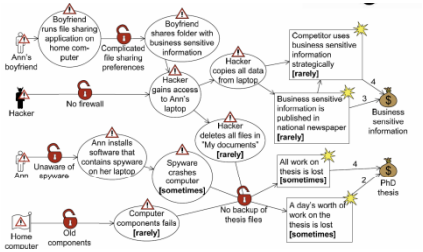


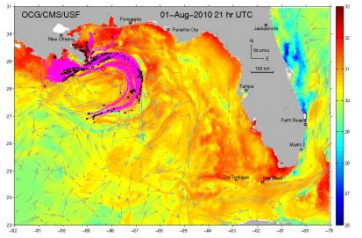
Limitations:
Scope, Taxonomy, Human Factors, Learning from incidents, Presentation

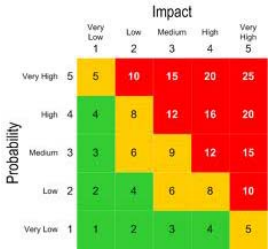
Edinburgh Napier UNIVERSITY

Understanding risks: presentation

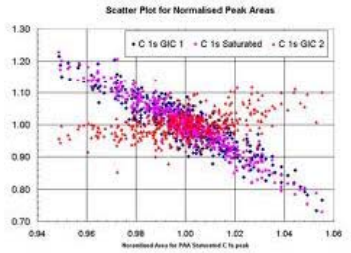


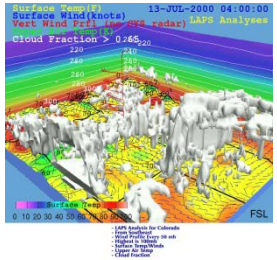


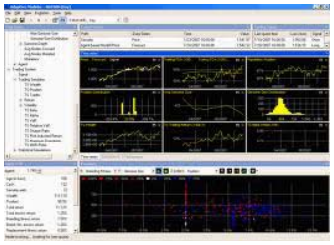


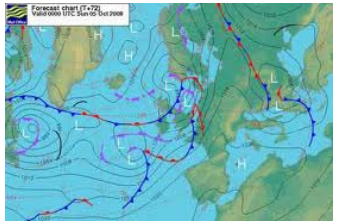


$$AvgWin\ \% = Risk\ \% \times WinLossRatio$$
$$AvgLoss\ \% = Risk\ \%$$
$$E = Expected\ mean\ return\ per\ trade$$
$$E = ProbWin \times AvgWin\ \% - (1 - ProbWin) \times AvgLoss\ \%$$
$$E2 = ProbWin \times (AvgWin\ \%)^2 - (1 - ProbWin) \times (AvgLoss\ \%)^2$$
$$P = 0.5 + \frac{E}{\left(2 \times \sqrt{E2}\right)}$$
$$R = Risk\ of\ Ruin$$
$$R = \left(\frac{1 - P}{P}\right)^{\left(RuinLevel \times \sqrt{E2}\right)}$$









Understanding risk: expertise in other areas

- Quality management
- Environmental risk assessments
- Aviation safety
- Criminal profiling
- Health and safety
- Financial forecasting

Future potential

- Balancing multi-faceted input from many stakeholders with different values and objectives
- Process: not once a year, but continuous (automated) monitoring
- Integration of human factor risks (criminal profiling & psychology)
- Taxonomy and presentation
- Mapping risks to legislation and standards to find gaps
- Learning from incidents and near misses
- Adaptive management based on statistics and controls monitoring
- Knowledge sharing through ongoing benchmarking/aggregation

Thank you

n.hazelhoffroelfzema@napier.ac.uk