Risk Management in Education And Research

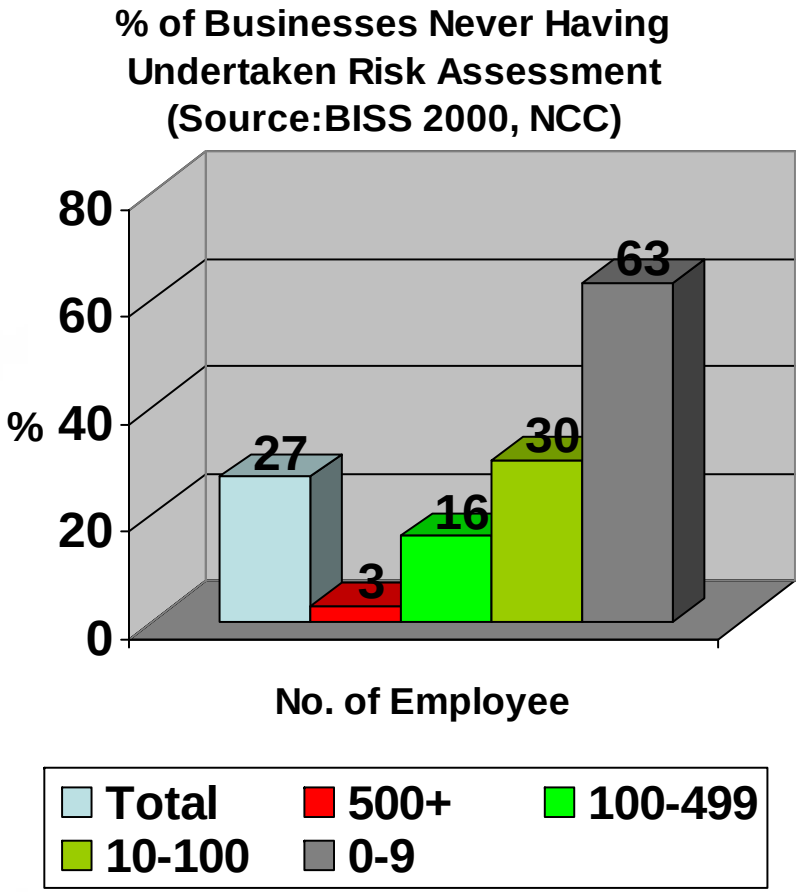
Jeremy Hilton
Cardiff University

Sun Tzu: The Art of War

- "So it is said that if you know others and know yourself, you will not be imperilled in a hundred battles;
- "If you do not know others but know yourself, you win one and lose one;
- "If you do not know others and do not know yourself, you will be imperilled in every single battle"

Problem

- In the UK, one third of the business have never performed risk assessment
- Most of them are from SMEs
- Academic institutions are no different
  - Control of students
  - Want information sharing, but with attribution



Danger is real, but risk is socially constructed[1]

- Risk Assessment is inherently subjective and represents a blending of science and judgement with important social, cultural, and political factors
- Whoever controls the definition of risk, controls the rational solution to the problem at hand

[1] Paul Slovic, Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield, 1999, Society for Risk Analysis

Danger is real, but risk is socially constructed[1] [2]

- If risk is defined one way, then one option will rise to the top as the most cost effective or the safest or the best
- Defining risk is thus an exercise in power
- The public is not irrational and should be involved more in risk assessment and risk decision making

[1] Paul Slovic, Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield, 1999, Society for Risk Analysis

Research Funding

- Risk Assessment is essentially a review of bids by fund holders as to whether they will provide funding or not
- Employs peer review of 3 or so researchers with related knowledge
- Assesses subject of research, method, researcher's experience etc. to test likelihood of success and if it is a worthwhile investment

Forensic Psychologists[3]

- "Most adult-based studies are unabashedly one-sided; they emphazise risk factors to the partial or total exclusion of protective factors"
- "Risk-only evaluations are inherently inaccurate"
- "Risk-only assessments in risk-averse mental health systems may produce lop-sided assessments and resource allocations

[3] R Rogers, The Uncritical Acceptance of Risk Assessment in Forensic Practice, Law and Human Behaviour, Vol 24, No. 5, 2000

Critique of Risk Assessment[3]

- "Risk assessments are not inherently inaccurate"
- "However, two broad questions appear fundamental:
  - Is the risk assessment fair and balanced?
  - Is the risk assessment based on relevant and well-established base rates

[3] R Rogers, The Uncritical Acceptance of Risk Assessment in Forensic Practice, Law and Human Behaviour, Vol 24, No. 5, 2000

Procedures for Health Risk Assessment in Europe[4]

- Risk Assessment involves an evaluation of hazards associated with exposure to chemicals,
  - an understanding of relationships between dose and adverse effect,
  - extrapolation of effects from high experimental doses to low doses associated with actual exposure, and
  - extrapolation from effects observed in animals to effects in humans
- Several elements of the risk assessment can affect the outcome:
  - Choice of study on which to base the critical effect
  - Procedures for extrapolation

[4] MR Seeley, LE Tonner-Navarro, BD Beck, R Deskin, Procedures for Health Risk Assessment in Europe - Regulatory Toxicology and Pharmacology, 2001

Risk Assessment in Academia

- Controls in place for most common risks:
  - Student activities
  - Back-ups of servers
  - Virus & anti-spam
- Best practice, not risk assessment-based – does this constitute base factors?
- Philosophy of information sharing, but with attribution
- Some informed individuals

Information Assurance

- Generally not covered in Computer Science syllabi
- Included in Cardiff Computer Science and Information Systems BSc and MSc courses
- Put in context of spectrum of risk
- Avoids complex tools
- No base data available, as it cannot be scientifically determined
- Therefore subjective and experience/knowledge-based

Using Abuse Case Models for Security Requirements Analysis[2]

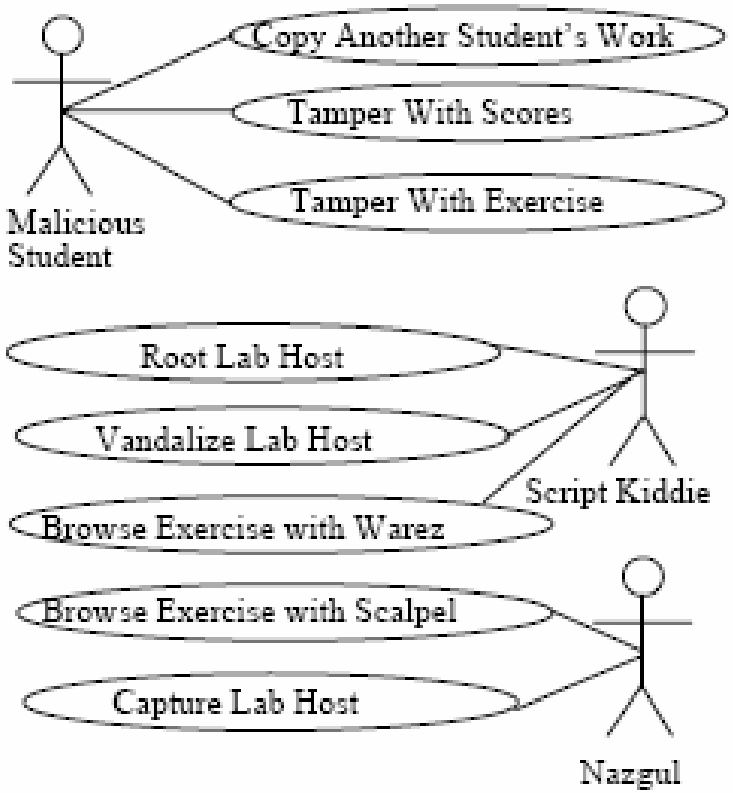


Figure 3. Abuse Case Diagram for an Internet-Based Information Security Laboratory

[2] J McDermott, C Fox - Computer Security Applications Conference, 1999.(ACSAC'99)

Final Note …

New methods/models are needed

"If you always do what you've always done, you'll always get what you've always got"

jeremy.hilton@cs.cf.ac.uk