The State of Risk Assessment Practices in Information Security: An Exploratory Investigation

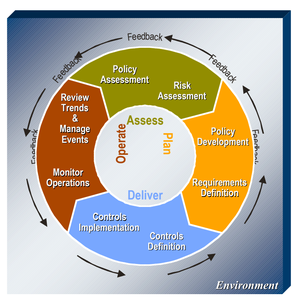
Jackie Rees and Jonathan P. Allen

Risk and Information Security

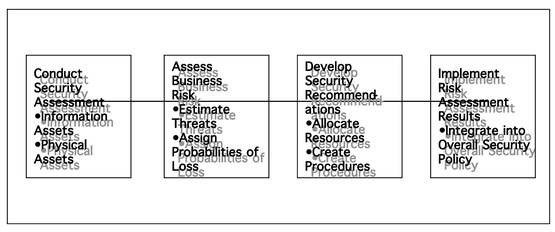
- Security policy:
  - High-level technology-neutral set of procedures concerning the specific risks faced by an organization
  - Sets tone and direction for how various risks are to be mitigated
  - Provides penalties and counter-measures for non-compliance

Risk and Information Security

- Analysis often occurs at Risk Assessment phase of Information Security Lifecycle (Rees, Spafford and Bandyopadhay, 2003)

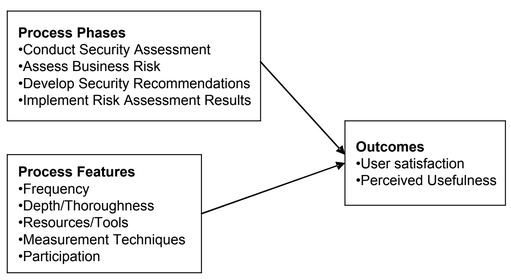


Risk Assessment Process



A Sample Risk Assessment Process (CERIAS and Accenture, 2000)

Conceptual Model



Research Questions

- What are the current risk assessment practices for information security policy management?
- What are the current attitudes expressed by respondents in terms of
  - Difficulty of various process features
  - Satisfaction with various process features
  - Perceived usefulness of various process features

Study Methodology

- Works from information security, user satisfaction and usefulness
  - (Straub, 1990; Straub & Welke, 1998; DeLone & McLean, 1992; Seddon, 1997;Rai, Lang & Welker, 2002)
- Established instruments for user satisfaction and perceived usefulness
  - (DeLone & McLean, 1992; Seddon, 1997; Rai, Lang & Welker, 2002)

Study Methodology

- Generated questionnaire with 43 structured items and 1 general open-ended question
  - Multiple choice
  - Yes/no/don't know/do not wish to disclose
  - Seven-item Likert-type response scale
- 1000 anonymous questionnaires administered
  - Hoovers Company Profiles database
  - CIO/CTO of US-based firms
  - 1250 to 15,000 employees
  - $12.5M to $1.5B in annual sales

Results - Resources

- Has your organization implemented an information security policy or plan?
  - Yes (92%)
  - No (8%)
- When creating and/or updating information security policy or plan, which resources were used?
  - External consulting firms – 37%
  - Guidelines issued by gov't agencies – 51%
  - Guidelines issued by professional orgs. – 70%
  - Other guidelines (text books, white papers) – 60%
  - Sample policy from other organization – 66%

Frequency

- Was a risk assessment conducted as part of designing the information security policy?
  - Yes (64%)
  - No (32%)
  - Don't Know (4%)
- If yes, how frequently are risk assessments conducted?
  - Only at creation (16%)
  - On a fixed schedule (29%)
  - Only after a loss (5%)
  - Periodically (45%)
  - Other (5%)
- If on a fixed schedule, how often?
  - Annually (40%)
  - All others except weekly (16% each)

Frequency

Item	Mean	
Satisfaction with frequency with which RA's are conducted (1 – Very Dissatisfied to 7 – Very Satisfied)	4.1	1.7
Perceived usefulness of frequency with which RA's are conducted (1 – Not Very Useful to 7 – Very Useful)	4.3	1.7

Most respondents thought Annually was optimal frequency (31%) followed by Quarterly (25%) and Bi-Annually (18%)

External Consultants

- Use external consultants?
  - Yes (53%)
  - No (41%)
  - Don't Know (4%)
  - DNWTD (2%)

External Consultants

Item	Mean	
Satisfaction with external consultants used in conducting RA	4.9	1.3
Perceived usefulness of external consultants used in conducting RA	5.1	1.2

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center

The State of Risk Assessment Practices in Information Security: An Exploratory Investigation

Jackie Rees and Jonathan P. Allen

Software

- Is risk assessment/management software used?
  - Yes (37%)
  - No (57%)
  - Don't Know (4%)
  - DNWTD (2%)
- If yes, how acquired?
  - Purchased off-the-shelf (60%)
  - Purchased & customized, developed in-house, part of consulting contract (10 % each), don't know, open source (5% each)

Software

Item	Mean	
satisfaction with software used in conducting RA	4.8	1.4
perceived usefulness of software used in conducting RA	4.8	1.3

Additional Resources

- Which additional resources were used for risk assessment?
  - Guidelines issued by gov't agencies – 20%
  - Guidelines issued by professional orgs. – 34%
  - Other guidelines – 25%
  - Sample risk assessment process from other organization – 15%
  - Don't Know – 3%
  - Other (common sense, wisdom of employees, internal audit info) – 3%

Depth

- Data/Informational assets
  - Every identified asset/vulnerability examined (10%)
  - Only select assets/vulnerabilities examined (69%)
  - Both (18%)
  - Don't know (4%)
- Physical assets
  - Every identified asset/vulnerability examined (12%)
  - Only select assets/vulnerabilities examined (76%)
  - Both (8%)
  - Don't know (4%)

Depth

Item	Mean	
difficulty of inventorying various assets for RA	3.2	1.3
confidence in results of asset inventory for RA	4.2	1.2
satisfaction with level of thoroughness in conducting RA	4.2	1.5
perceived usefulness of level of thoroughness in conducting RA	4.6	1.4

Who & Where

- Organizational level
  - Unit/departmental (29%)
  - Enterprise (41%)
  - All (27%)
  - Don't know (2%)
- Who performs?
  - External consultants (17%)
  - IT group (28%)
  - Information security team (20%)
  - Financial risk management group (13%)
  - Physical security group (5%)
  - Inter departmental committee (6%)
  - Don't Know (1%)
  - Other (9%)

Threat ID

Item	Mean	
difficulty of identifying threats	3.7	1.1
confidence in results of threat identification techniques	4.2	1.3
satisfaction with techniques used for identifying threats	4.2	1.3
perceived usefulness of techniques used for identifying threats	4.3	1.4

Measurement

- Measures of the likelihood of loss
  - Probabilities/likelihood (ALE) (27%)
  - Certainty Factors (12%)
  - Measures of Belief (12%)
  - Risk levels (39%)
  - Don't Know (10%)

Measurement

Item	Mean	
difficulty of estimating likelihood of loss	2.8	1.0
confidence in results of estimation of loss	3.6	1.2
satisfaction with techniques used to estimate likelihood of loss	3.8	1.3
perceived usefulness of techniques used to estimate likelihood of loss	3.8	1.3

Outcomes of RA Process

Item	Mean	
satisfaction with security recommendations resulting from RA activities	4.5	1.2
perceived usefulness of security recommendations resulting from RA activities	4.7	1.4
satisfaction with implementation of results from RA	4.2	1.4
perceived usefulness of implementation of results from RA	4.7	1.4

Preliminary Results - Overall

Item	Mean	
confidence in current RA practices	4.2	1.4
satisfaction with current RA practices	3.9	1.4
perceived usefulness of current RA practices	4.2	1.5
satisfaction with current information security policy	4.5	1.5
perceived usefulness of current information security policy	4.6	1.3

Conclusions

- IS researchers need to further examine RA process for Information Security
- Apparent need for improved techniques for estimating risk and overall process
- Assistance appears available from many sources
- Limited study and limited data mean very limited conclusions

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center