Information Security and Numbers

QinetiQ

Objectives for Complete Study

- Assessment of current opinions on the nature of ‘information security metrics’
- Definitions of terms relating to ‘information security metrics’
- Particular attention to:
  - Measures of effectiveness
  - Resilience metrics
- Communication of ‘information security metrics’ to management decision-makers
- Candidate directions for future study

Literature Search Findings

- There are no agreed definitions for metrics-related concepts.
- Current terminology does not readily differentiate between:
  - Objective and subjective;
  - Simple and aggregate;
  - Past and future.
- ‘Resilience metrics’ is not an established security term.
- ‘Return on (security) investment’ is an extension of risk concepts and terms.
- Opinions vary on the relationship between a ‘metric’ and the use made of that metric.

Security valuation terms encountered:

- Measures
- Metrics
- Return on (security) investment
- Measures of effectiveness
- Resilience metrics

Generic term chosen for this study: *Valuations*

Security requirements with numbers:

- Government security accreditation (yes/no – binary value)
- BS7799 Certification (yes/no – binary value)
- Crypto-sync time not exceeding x milliseconds
- A firewall evaluated to EAL4
- Security mechanism x with a Residual Risk Indicator no greater than 10.5
- 99.75% system availability
- Recruitment of 3 information security staff

Some numbers for security achieved:

- Accreditation or BS7799 granted/denied
- Crypto-sync period of x milliseconds
- Risk assessment carried out (yes/no)
- Policy written (yes/no)
- EAL 4 product installed (yes/no)
- CRAMM or Residual Risk Indicator results
- Cost of Common Criteria evaluation
- Time taken to achieve accreditation

Some more numbers for security achieved:

- Average time taken to achieve accreditations
- Amount of overtime paid to accreditation staff in month x
- Average residual risk carried
- Number of security breaches in month x
- Information security officer's annual appraisal grade
- UK Government 2004 breaches survey: % of small organisations suffering virus infection
- Return on investment made or planned (risk managed)
- Return on investment made or planned (opportunity taken)

Concepts: Objective and Subjective

Objective valuations - examples

- Crypto-sync time achieved
- Number of security breaches in month x
- Number of information security staff to be recruited
- Return on planned investment (opportunity)

Subjective valuations – examples

- Information security officer annual appraisal grade
- CRAMM risk result
- Return on planned investment (risk)
- Average residual risk carried

Concepts: Past and Future

Past valuations - examples

- Crypto-sync time achieved
- Information security officer annual appraisal grade
- Average residual risk carried
- Average time taken to achieve accreditations

Future valuations – examples

- Crypto-sync time requirement
- Return on planned investment (risk)
- Threat level consequent upon some proposed action
- System availability target

Concepts: Simple and Aggregate

Simple valuations - examples

- Crypto-sync time requirement
- Information security officer annual appraisal grade
- Time taken to achieve a particular accreditation
- Threat level consequent upon some proposed action

Aggregate valuations – examples

- Return on investment made (opportunity or risk)
- Breaches survey result
- System availability target
- Average time taken to achieve accreditations

A Proposed Structure (with examples)

	OBJECTIVE	SUBJECTIVE & RISK	FUTURE OBJECTIVE	FUTURE SUBJECTIVE
SIMPLE	Crypto-sync time	CRAMM result	Number of staff to be recruited	Threat level consequent on proposed action
AGGREGATE	Breaches survey result	Return on investment made (risk)	System availability target	Return on investment planned (risk)

Two Perspectives on Valuations and Their Use

1. A valuation's use is part of the valuation – if it isn't used it isn't a valuation.

2. Any one type of valuation may have zero or more uses. These uses may be created, removed or amended without changing the nature of the valuation.

This study adopts the second approach.

Conclusions

- There is an underpinning structure for information security valuations which recognises and defines their varying characteristics.
- This structure is analogous to existing structures such as Data, Information, Knowledge.
- The selection of valuations is inextricably linked with requirements capture, and future work on information security valuations should start with that process, and with how requirements are recorded and tested.

Future Work

- Relationship between information security valuations and security requirements capture approaches – use on real projects
- Evaluation of Balanced Scorecard for identifying, presenting and using security valuations on real projects
- Relationship between security ‘measures of effectiveness’ and broader C2 ‘measures of merit’
- Use of valuations in respect of BS7799/ISO17799, SSE-CMM, Common Criteria, government accreditations, project management approaches

Contact Details

Michael Stubbings
QinetiQ
Woodward Building
Malvern Technology Centre
St Andrews Road
Malvern
Worcestershire
WR14 3PS
United Kingdom

Tel: +44 (0) 1684 895845

Email: mstubbings@QinetiQ.com

QinetiQ