

Keele University

Risk management

? Keele 2002. All rights reserved.

The copyright in this document is vested in Keele University. The document must not be reproduced by any means, in whole or in part, or used for manufacturing purposes, except with the prior written permission of Keele University and then only on condition that this notice is included in any such reproduction.

Information contained in this document is believed to be accurate at the time of publication, but no liability whatsoever can be accepted by Keele University arising out of any use made of this information.

Under the Copyright, Designs and Patents Act 1988, Stephen Bostock and Stephen Linkman assert the moral right to be identified as authors of this work.

Overview

- † risk, loss and probability
- † risk identification
- † risk analysis,
 - annual loss exposure
- † risk handling
 - retain, avoid, reduce, transfer
- † contingency plans

Risk Management

- † management constraints: risks, resources, quality, time
- † risks need managing, especially in
 - IS acquisition
 - System development projects
 - IS security
- † there is a structure and process for undertaking risk management
- † there are techniques useful in risk management

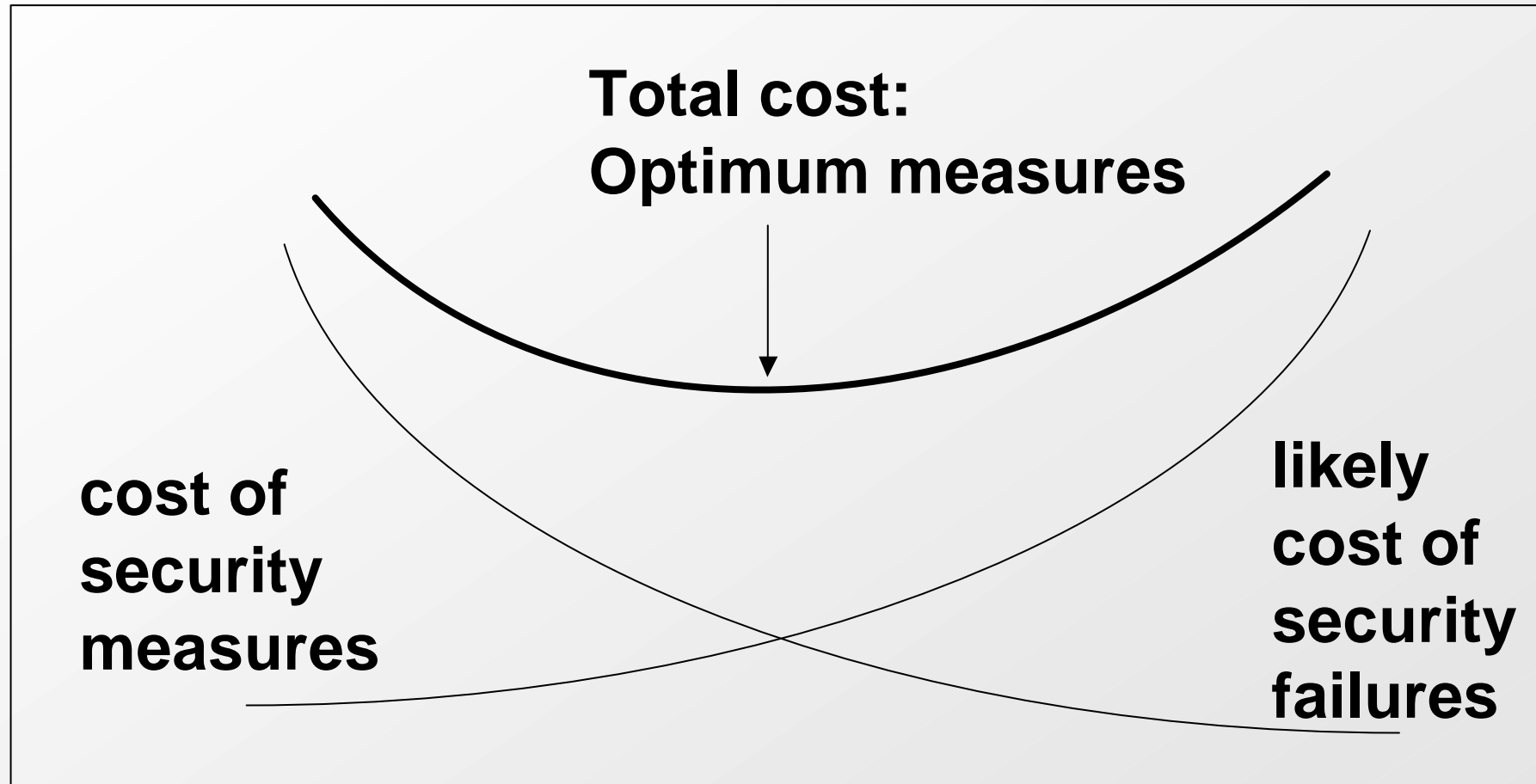
What is risk?

- † where a potential for damage exists, and the damage is not certain (probability between 0 and 1)
- † when it has happened it is a problem, not a risk (probability = 1)
- † ‘risk’ is a composite value (product) of probability that damage will occur \times loss suffered if the damage materializes
- † risk management minimizes the probability or minimizes the loss (the effect)

Why manage risk?

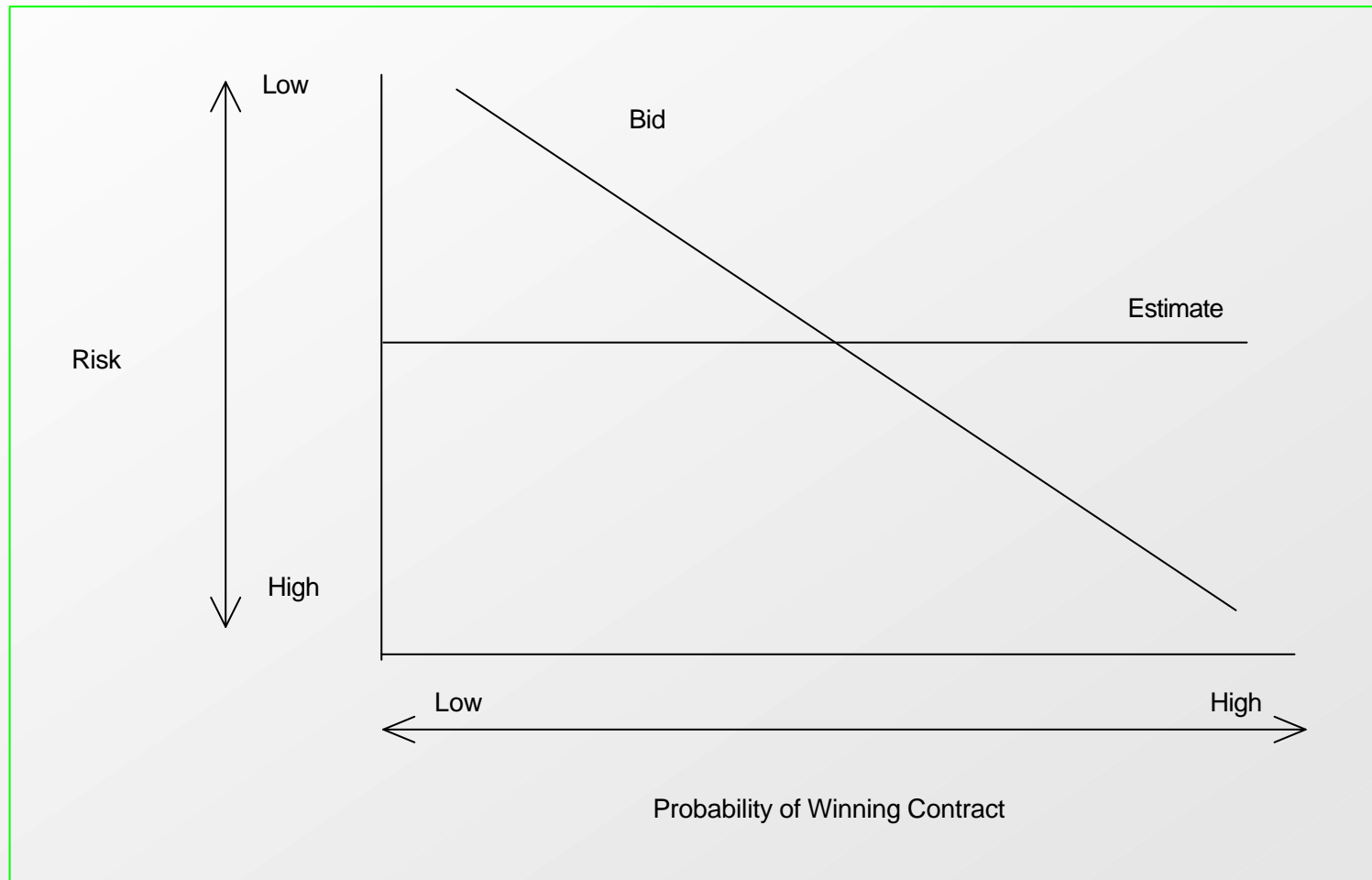
- † as IT is more important to a business, its loss means business death
- † new risks for businesses dependent on IT
 - automatic transactions
 - familiar cues from manual systems gone
 - uncertain legal obligations
 - new types of errors, sources of threats
 - responsibilities in organization divided
- † so it is a balancing act of the cost of for example having security and the expected cost of not having it

A cost balancing act - e.g. security risks

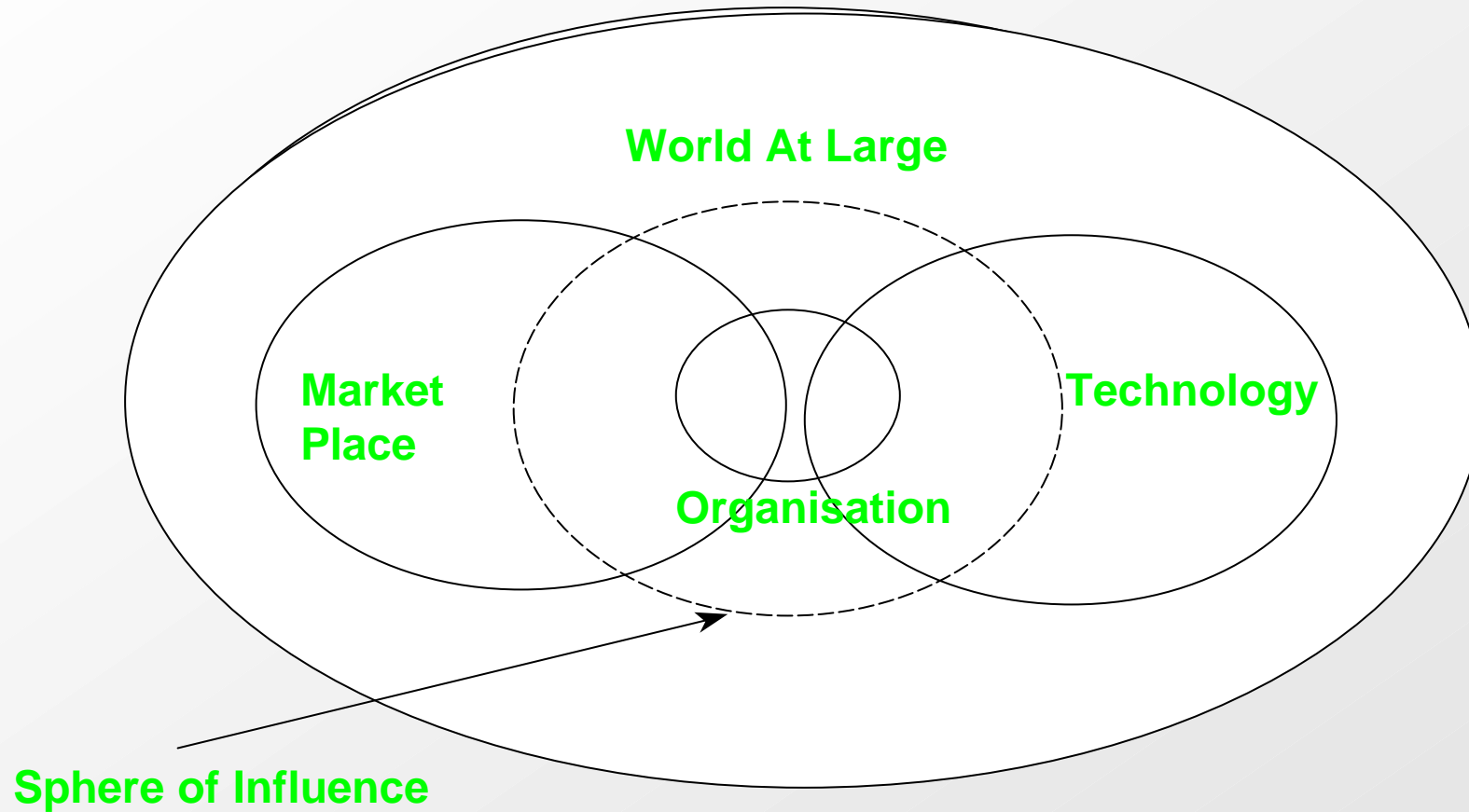


Increasing security measures →

The Situation



The Project World



Systematic risk management

1 risk identification

- identify all the potential threats

2 risk analysis

- quantify the probability and severity of threats

3 risk handling

- select the counter-measures to optimize cost

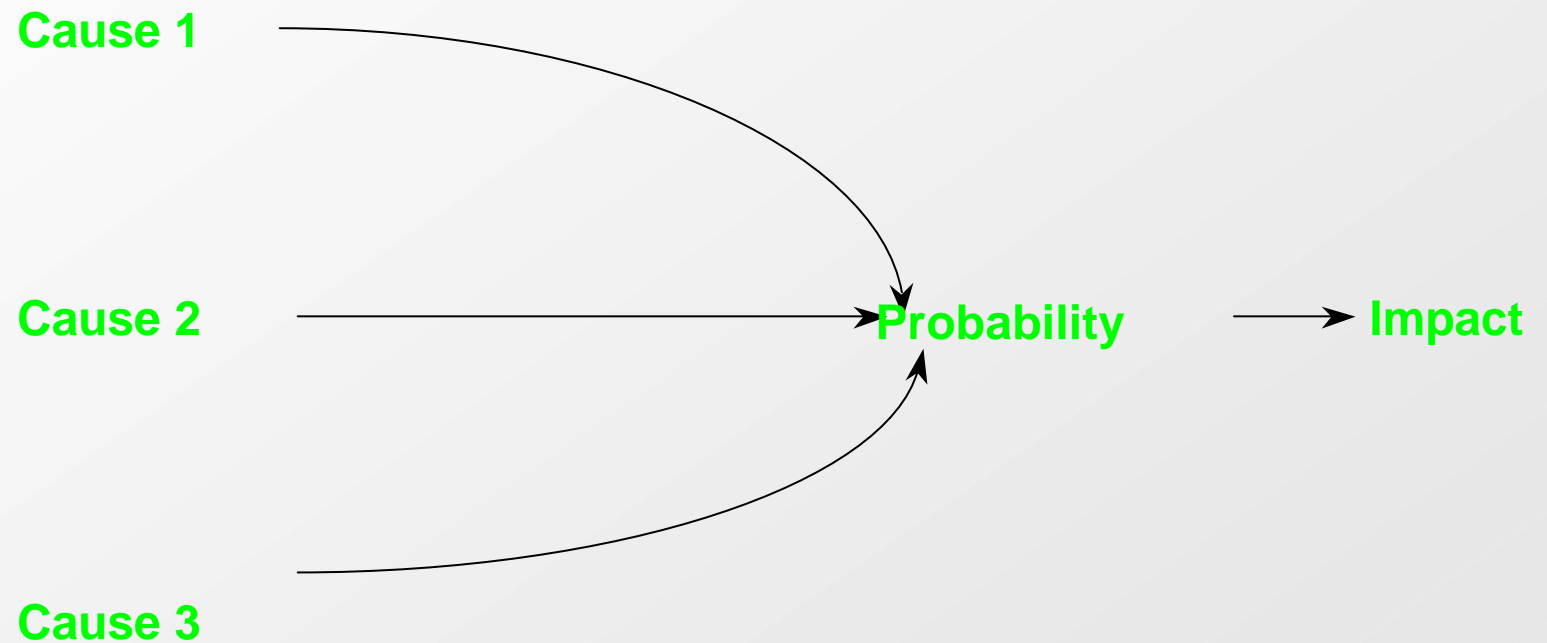
4 disaster recovery

- contingency plans for threats that do occur despite the counter-measures taken

1. Risk identification

- † identify 'all' the threats
by internal staff with detailed knowledge,
and external consultants with wider knowledge
- † weak spots are
 - sources of threats
how vulnerable are we to this type of threat?
 - vulnerable assets
what can happen to each asset?
 - locations of risk
what could happen here?

Causes, Impacts and Probability



Techniques for Hazard Analysis

- † Standard Checklists

 - † Organisational

 - † Local

- † Scenario Analysis

 - † Decision drivers

 - † Assumption analysis

 - † Other techniques

2. Risk analysis

- † move from qualitative listing of threats to quantitative assessment of expected loss
- † expected loss

$$\begin{aligned} \textit{expected loss} \\ = \\ \textit{potential loss} \\ \times \\ \textit{probability} \end{aligned}$$

- † also called ‘annual loss exposure’
- † loss is monetary or other numerical value

Quantifying potential losses

- † hardware
 - replacement cost + procurement cost
- † data, information
 - most serious and difficult to estimate
- † software
 - replacement + costs of processing down time
- † processing capability
 - depends on length of disruption and criticality
- † staff
 - loss of knowledge and skills
- † funds
 - money value

Categories of loss - CIA

† Confidentiality

lost exclusive ownership

† Integrity

lost confidence in data of uncertain accuracy

† Availability

lost access to data

Primary consequences of loss

- † total business losses are
 - primary (direct) losses and
 - secondary losses due to business disruption
- † primary consequences of lost security follow directly and immediately, for example
 - interruption of processing
 - destruction of data storage media
 - disclosure of sensitive information
 - removal of equipment
 - corruption of data records

Secondary consequences of loss

secondary consequences are due to lost or damaged systems, causing business disruption with its costs, for example

- † lost production
- † delayed delivery
- † cash flow problems
- † lost customer goodwill
- † inaccurate management information
- † penalties from breaching legal requirements

Probability

- † probability = frequency over the period as a proportion or percentage
- † under-reporting makes estimates unreliable, so use relative measures such as
 - very high (0.9), medium (0.5), low (0.2)
 - inverse of mean time between events
 - frequency scale (1 to 5)

Probability values

Probability is likelihood based on frequency.

It can be estimated from

- † actuary tables,
- † empirical evidence (but under-reporting)
- † reasoned estimates

Estimating probability

To estimate probability, break it down into rates of attack (attempted break-in) and of successful attack

probability = attack rate x success rate
(per year)

† hacking

attack 0.2 x success 0.5 = 0.1 probability

† incorrect data input

'attack' 0.9 x success 0.5 = 0.45 probability

† fire

'attack' 0.5 x success 0.7 = 0.35 probability

Summary - threat severity matrix

		probability (frequency) rating				
		1	2	3	4	5
severity of loss rating	1			virus		input error
	2			theft	comms error	power break
	3			storm		
	4		fire			
	5	earth quake				

Annual Loss Exposure reckoner

probability as time between events

loss	300 yr	3 yr	10days	1 day	1/10th day
£10			£300	3000	30000
£100			3000	30000	300000
£1000		300	30000	300000	3M
£10000		3000	300000	3M	30M
£1M	3000	300000	30M		

Annual Loss Exposure

- † Annual Loss Exposure shows expected cost of severe infrequent threats the same as mild frequent threats
- † both types of risks have to be handled
 - severe infrequent threats close the business, may insure against them
 - mild frequent threats - counter measures have a high net return
- † risk analysis (threat identification), and loss estimating not difficult, but probability is

3. Risk handling

having estimated the annual loss exposure we select strategies before implementing cost effective counter measures appropriate to risks

- a. risk retention
- b. risk avoidance
- c. risk reduction
- d. risk transfer

a. Risk retention

- † accept the risk
 - 'grin and bear it'
 - for small losses that can be born
- † for low direct losses and minor secondary consequences
- † however, be careful that the accumulated costs of frequent small losses do not give a high total exposure
 - for example, coffee spilt on keyboards

b. Risk avoidance

- † take steps to totally avoid the risk
- † for high Annual Loss Exposure and high consequential losses
 - for example
 - move an installation to a safe place
 - alter methods of working to create facility controls
 - not decentralizing IT controls, backing up

c. Risk reduction

- † commonest strategy - not possible to avoid many risks entirely and inappropriate to ignore
- † so introduce controls and counter-measures
- † must reduce the annual loss exposure *more* than its costs
- † what is total cost of countermeasures?
 - costs will be in development, operation, maintenance and flexibility of systems
- † what is the reduction in risk, and therefore in the annual loss exposure?

d. Risk transfer

- † pass on the exposure to a third party
 - for example
 - insurance, fixed price maintenance contracts, standby arrangements for a retainer
- † the excess payment in insurance, or the terms of maintenance contract, retain some risk, so it may still be worth avoiding it
- † insurers will require risk reduction before underwriting it
 - for example, insurance is 1% of price per annum if equipment is maintained, or 6% if not

Risk Transfer - Time

- † Move the point in time when a hazard occurs
- † Example
 - † High level of requirements change
- † Strategy
 - † Incremental development and strong change control

Risk Transfer - Space

- † Move the problem to a point where the impact is removed
- † Example
 - † Automation of a particularly complex credit agreement
- † Strategy
 - † Put in a trap and let the bank staff handle the problem
- † Also termed “Transfer outside system boundary”

Risk management

- † a risk management portfolio
- † a mixed set of the four risk handling strategies addressing
- † a list of risks prioritized by their annual loss exposure
- † risk avoidance and transfer for most serious risks
- † risk reduction and risk transfer for others
- † risk retention for low losses unless avoidance is cheap and does not impair flexibility

A security policy

- † documents the risk identification and analysis
- † prioritizes risks by annual loss exposure
- † describes risk handling strategies addressing them in a risk register
- † describes contingency plans for disaster recovery

Risk handling table (risk register)

Risk	Loss	Probability	Strategy
computer room fire £30K	processing of production, payroll, orders	low	/measures backups, standby system insure, fire precautions

4. Contingency plan for disaster recovery

- † total risk avoidance is impossible or too costly so there must be a plan to cope with security breakdowns - prepare for the worst
- † need not be an act of God or Nature - machine failures can lead to the same business consequences
- † contingency planning is part of strategic planning
- † we are planning for business continuity so having safe, reliable backups is essential

Do companies have plans?

- † most UK companies have no, or only inadequate, disaster plans (1993)
 - 43% have no plan, only 22% with viable plan
 - half had not tested it for 6 months or more
- † when tested, 80% contingency plans fail because they ignore the secondary consequences - dependencies internally and externally
- † traditionally mainframe accidents are planned for, but office systems are not
 - in one survey 84% have a plan for mainframes but only 64% have an plan for offices (1992)

Contingency planning

- † make a 'timetable of importance'
 - prioritize applications by *how quickly* they are needed for business processes to continue
- † two categories of applications:
 - standby element - business critical systems
 - recovery element - all aspects of IS use
- † difficult to stay up to date with the business changes
- † difficult to stay up to date with new disaster types

Disaster plans

- essential elements

- † first line physical defenses and documentation
- † off-site backup for data, software and documentation
- † standby hardware
- † thorough maintenance contracts
- † rules for software development and acceptance
- † good personnel procedures

A framework for a disaster plan - 1

1. *Introduction* and index

- versions, use, ownership, summary

2. *Definition* of a disaster

- and description of the levels of disasters, with different recovery strategies, from local to major disasters

3. *Assumptions*

- for example, all key personnel will be available

4. *Exclusions* large disasters not included

- for example, nuclear war

5. *Inventories*

- list equipment covered by the plan

A framework - 2

6. *Emergency budgets*

- a source of cash and special budgets, with an audit trail for claiming from insurance later

7. *Invocation*

- how the alarm is raised and the plan invoked, the disaster management team

8. *Logistics*

- details of what should happen

9. *Maintenance and testing of the plan*

- change control documentation

10. *Appendices*

- insurance policies, contracts, agreements, results of risk analysis

Post-Project Review Meetings

- † Ensure all interested parties invited
- † Provide summary of relevant information
- † Use project log
 - † Source of detailed information
 - † Source of summary information
- † Identify lessons learnt
- † Prepare summaries for risk database

Summary

- † risk, loss and probability
- † risk identification
- † risk analysis,
 - annual loss exposure
- † risk handling
 - retain, avoid, reduce, transfer
- † contingency plans