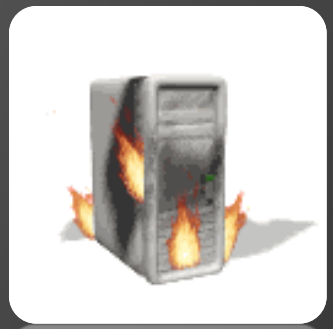
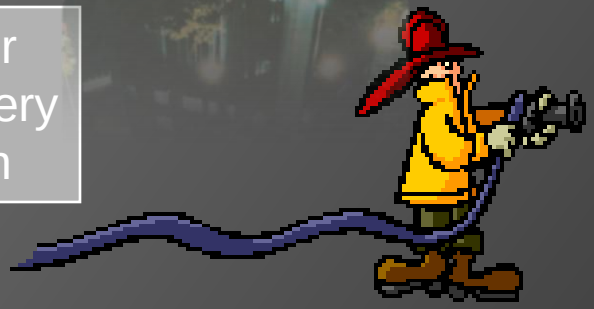
OOPS!
No water



**Business must rise from the ashes**

Poor recovery plan



# CHAPTER 9

## DISASTER RECOVERY MANAGEMENT

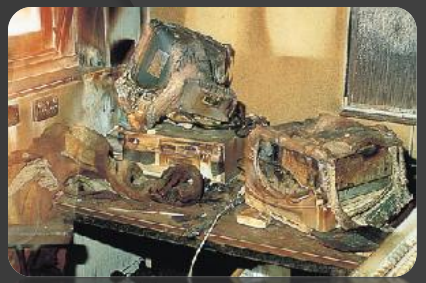
## 13.6 Disaster Recovery Management

# Legal Aspects - the syllabus says:

## Disaster recovery management

- Describe the various potential threats to information systems, e.g. physical security; document security; personnel security; hardware security; communications security; software security.
- Understand the concept of risk analysis. Understand the commercial need to ensure that an information system is protected from threat.
- Describe a range of contingency plans to recover from disasters and relate these to identified threats.
- Describe the criteria used to select a contingency plan appropriate to the scale of an organisation and installation.

# The Corporate Consequences of System Failure



Any company that loses its computer data, even temporarily, will face serious financial losses.

- A EFTPOS is critical to a business where many customer transactions take place every hour. Customers cannot purchase goods, even manually with cash!! Why?
- If customer orders are lost then a company will gain a bad reputation when goods are not dispatched.

If company data is lost permanently then the chances of the company surviving are small.

A well tested contingency plan (disaster recovery plan) is needed to recover data quickly after a disaster.

# Potential threats to an IS

- Communication breach – hacking and altering data
- Hardware failure – disk head crash corrupts H/W,S/W & data
- Physical failure – fire, flood, earthquake, terrorist attack, split coffee on a stand alone.. corrupts H/W,S/W & data
- Personnel – accidental overwrite of data
- Unexpected invalid data causes software program to crash or corrupt files
- Power surge or power loss corrupts H/W,S/W & data
- Virus – such as Trojan horse corrupts S/W & data

CHPPPV

## Disaster Avoidance or Counter Measures CHPPPV

- Communication breach
  - Allow 3 password attempts before disabling user id, firewalls to prevent unauthorised external access, encryption of data doesn't prevent corruption but prevents viewing..all lessen chance of data being seen/corrupted
- Hardware failure
  - have duplicate system or hot site set up so can transfer backup discs quickly causing minimum down time.
- Physical failure
  - backup of data and software kept off site/fireproof safe/above flood line causing minimum down time.

## Disaster Avoidance or Counter Measures CHPPPV

- Personnel
  - training in ICT good practice procedures so less likely to make mistakes
- Unexpected invalid data
  - should be caught with validation/verification checks on data entry and test with every type of data.
- Power surge/loss
  - should have a power surge protector device and a back up generator in place so can save files before power loss.
- Virus
  - run up-to-date anti-virus software on all machines to detect viruses before they can cause damage.

# The Contents of a Contingency Plan

- Who is responsible for different activities (eg who they are and their role)
- Timetable of events in case of disaster to enable recovery of the system
- Alternative computer hardware – eg reciprocal site or specialist company
- Backup location/frequency etc (max 2 marks for discussion re backup)
- Insurance/warranty arrangements for ICT/buildings

# What is Risk Analysis?

| Likelihood | Consequences | | | | |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Severe |
| Almost certain | M | H | H | E | E |
| Likely | M | M | H | H | E |
| Possible | L | M | M | H | E |
| Unlikely | L | M | M | M | H |
| Rare | L | L | M | M | H |

- identify each element of an information system
- place a value to the business on that element
- identify any potential threats to that element
- consider the likelihood of the threat occurring
- calculate an overall **Risk Figure** based on the value and likelihood of the potential threat
- make contingency/disaster recovery plan based on the various risk figure results

Finance.xls [Compatibility Mode] - Microsoft Excel

Home Insert Page Layout Formulas Data Review View Developer Add-Ins @RISK

Define Distributions | Add Output | Define Correlations | Distribution Fitting | Model Window — Model
Iterations 1000 | Simulations 1 | Start Simulation | Advanced Analyses — Simulation
Browse Results | Summary | Define Filters — Results
Excel Reports | Swap Functions | Library | Utilities | Help — Tools

C10 =RiskOutput()

## Financial Forecasting

This model demonstrates the analysis of uncertain
whether to launch a new product line. A simplifie
look as shown below. Since most of the elements
they all involve uncertainty. The values in cells in
formulas. The cells in red, the NPV value in cell C
marked as @RISK outputs so a detailed analysis
@RISK distributions to your financial models, you
analysis that can lead to bad business decisions.

| | |
|---|---|
| NPV (10%) | $363,248.03 |

| Year | 2008 |
|---|---|
| Cash Flow | |
| Total Revenue | $ - |
| Cost of Goods Sold | $ - |

@RISK - Results Summary

Inputs | Outputs

Simulation Results For Outputs: Inputs= 22, Outputs= 11

| Name | Cell | Graph | Min | Mean | Max | 5% | 95% | Errors |
|---|---|---|---|---|---|---|---|---|
| Net Income / 2015 | J22 | -0.2m 1.2m | -166581 | 246469.3 | 999854.9 | 29213.44 | 653548.6 | 0 |
| Net Income / 2016 | K22 | -0.2m 1.0m | -113779.1 | 247584 | 990937.9 | 30810.19 | 676444.9 | 0 |
| Net Income / 2017 | L22 | -0.2m 1.2m | -91443.77 | 254076.3 | 1040976 | 30617.88 | 706371.3 | 0 |
| Range: <none> | | | | | | | | |
| NPV (10%) | C10 | -0.2m 1.4m | -102415.5 | 441709.9 | 1381116 | 26967.12 | 956709.4 | 0 |

Close

@RISK - Output: C10

NPV (10%)

0.027 0.957
5.0% 90.0% 5.0%

Values x 10^-6
1.6 1.4 1.2 1.0 0.8 0.6 0.4 0.2 0.0
-0.2 0.0 0.2 0.4 0.6 0.8 1.0 1.2 1.4
Values in Millions

NPV (10%)
Minimum -102415.4743
Maximum 1381115.8076
Mean 441709.9264
Std Dev 302530.5024
Values 1000

Close

| | | | | |
|---|---|---|---|---|
| 84,043.75 | $ 141,787.50 | $ 186,876.09 | $ 295,421.10 | $ 415,064.54 |
| 30,000.00 | $ 20,000.00 | $ 20,000.00 | $ 20,000.00 | $ 25,000.00 |
| 54,043.75 | $ 121,787.50 | $ 166,876.09 | $ 275,421.10 | $ 390,064.54 |
| (126,331.25) | $ (4,543.75) | $ 162,332.34 | $ 275,421.10 | $ 390,064.54 |
| - | $ - | $ 74,672.88 | $ 126,693.70 | $ 179,429.69 |
| 54,043.75 | $ 121,787.50 | $ 92,203.22 | $ 148,727.39 | $ 210,634.85 |
| 1 | 1 | 1 | 1 | 1 |
| $24.41 | $25.63 | $26.91 | $28.26 | $29.67 |
| 5% | 5% | 5% | 5% | 5% |
| 46% | 46% | 46% | 46% | 46% |
| $58.03 | $61.08 | $64.29 | $67.65 | $71.18 |
| 2500 | 4000 | 5000 | 7500 | 10000 |
| - | $ - | $ - | $ - | $ - |
| 10,000.00 | $ - | $ - | $ - | $ - |
| 20,000.00 | $ 20,000.00 | $ 20,000.00 | $ 20,000.00 | $ 25,000.00 |
| 30,000.00 | $ 20,000.00 | $ 20,000.00 | $ 20,000.00 | $ 25,000.00 |

Sheet1

Ready 100%

# Most Recent Exam Question

***6** Disaster Recovery **(Jun 07)***

*All organisations are advised to have a contingency plan to guide them in case a disaster strikes their computerised operations.*

*(a) State **three** of the criteria that should be considered when drawing up a contingency plan for recovery after a disaster. (3 marks)*

*(b) Discuss what should be included in the plan. (6 marks)*

(a) Any 3 x 1

- Scale of the organisation & its ICT systems/Volume of data/Size of the system
- Nature of the operation
- The importance of data held
- Timescale until the system is up and running
- Costs of recovery options relative to the value of the information system
- Perceived **likelihood** of disaster happening, based on risk analysis

(b) An answer encompassing some of the following ideas, to a maximum 6 marks - *1 mark per **well explained** point*

- Who is responsible for different activities (eg who they are and their role)
- Timetable of events in case of disaster
- Options for recovery (e.g. reciprocal site)
- Backup location/frequency etc (max 2 marks for discussion re backup)
- Insurance/warranty arrangements for ICT/buildings

*13.6* ***Disaster Recovery Management***

*A medical practice, in an area prone to flooding, has carried out a risk analysis and is now preparing its disaster recovery plan. The main elements of its ICT system are the patient records and prescription systems, and the network used to access and maintain them.*

*(a) Explain what is meant by risk analysis.(3)*

*(b) State **two** different potential threats to **this** ICT system, and describe a countermeasure for each one.(6)*

*(c) Name **three** criteria that the medical practice should consider when choosing a suitable disaster recovery plan. (3)*

(a) Any 3x1

- To identify each element of a successful information system, (1)
- place a value to the business on that element (1)
- and identify any potential threats to that element (1)
- with the likelihood of the threat occurring. (1)
- Use an algorithm to calculate an overall risk figure (1)
- that will indicate a degree of severity. (1)

(c) Any 3 x 1

- Scale of the organisation and its ICT systems/Volume of data/Size of the system
- Nature of the operation / The importance of data held
- Timescale until the system is up and running
- Costs of recovery options relative to .value. of systems
- Perceived **likelihood** of disaster happening, based on risk analysis

***NOT****: Any of the contents of the recovery plan (eg how to set up, reciprocal site, who does what or anything to do with back-ups)*

# (b) Answer

(b) 1 for threat(**t**), 1 for counter-measure(**c**), 1 for description of why/how it would counteract threat(**e**). Any 2x (3,2,1,0) *Don't need to have threat to get the other two marks; however, if valid threat is offered, then no credit to non-matching (c) and (e).Two countermeasures for one threat can gain both (c) and (e) marks*

| Threat | **Counter measure** *(examples)* | **Example/expansion** *(examples)* |
|---|---|---|
| Natural disaster– e.g. flood, earthquake | backup kept off-site;<br><br>hardware kept above<br><br>flood-line; | so that a safe copy is held and system can be reloaded; |
| Electrical surge/power loss | UPS/ RAID/ off-site duplication/ Mirror | as above |
| Physical – e.g. theft | use locks etc | prevent easy entry |
| Personnel – e.g. accidental overwrite | have procedures | trained staff less likely to make mistakes |
| Hardware – e.g. disk crash | have duplicate system/ hot site arrangment | so that system can be up and running a.s.a.p |
| Communications breach – e.g. hacking in | firewalls, encryption, passwords | to lessen ability to see/steal/tamper with data |
| Virus – e.g. Trojan | anti-virus software | to stop files getting infected |
| Data errors, inaccurate data in system | verification and validation | pick up data errors before they get into the system |

# The 20 marker exam question

*Syllabus 13.6 13.9*

*Q. Protecting its Information systems and the data that they contain is a major concern for an organisation. Discuss the aspects of system security and data security that an organisation needs to consider, paying particular attention to the following:*

- *risk analysis;* • *security policy;* • *audit requirements;* • *disaster recovery management.*

*(The quality of written communication will be assessed in your answer (20 marks))*

Continuous prose is expected. *Discuss* means each point made must be full, not just a single phrase. Mark as **R**,**S, A** or **D** for four bullets. A full explanation gets extension mark (**Re**, **Se, Ae** or **De**) *Max 16 m*

**R** .**risk analysis**
- identify each element of a successful information system
- place a value to the business on that element
- identify any potential threats to that element
- the likelihood of the threat occurring
- use an algorithm to calculate an overall risk figure
- that will indicate a degree of severity

**S** . **security policy**
- Prevention of misuse
- Physical security procedures
- Logical (software) security procedures
- Detection of misuse
- Investigation of misuse
- Staff responsibilities
- Disciplinary procedures
- Code of Practice
- Adherence/Compliance with legislation

**A** . **auditing**
- Network auditing • Financial systems auditing
- Application systems auditing • Impact of auditing
- Audit tools • Audit trails

**D** . **disaster recovery**
- Threats to systems . e.g. physical, document, personnel, hardware, communications (network), software
- Contingency plans . e.g. People involved, steps to be taken, types ( RAID, cold site recovery, reciprocal agreements) etc
- Criteria for selecting contingency plan . e.g. scale, location, likelihood, recovery costs , type of systems etc

(1m in total if listed, but 1m for each explained – 3 bullets above)
- Why protect - commercial need
- Backup (must talk about a feature or reason to get the first mark e.g. thinking about where to keep backup or frequency etc)
- Recovery (ditto)