Introduction

Systems failure, from whatever cause, needs to be addressed in a structured manner. Such failures need to be managed using incident response and crisis management guidelines. Incident management is not confined to dealing with systems failure. It provides a framework for recovery for all kinds of unwanted events. Causes of systems failure include:

- Fire
- Flood
- Power supply problems
- Industrial action
- Sabotage
- User error

The best preventative measure against systems failure is called Business Continuity Management. Please refer to the PDF entitled ‘Understanding Business Continuity Management’ for further information.

This factsheet is for: any business that wants to know how to guard against and recover quickly from systems failure.

It covers: risk, recovery, prevention and a case study about power failure in London.

Systems Failure – Risk

The risks surrounding systems failure range from minor inconvenience to fatalities, largely depending on the type of system.

An information website being unavailable for a day may just be annoying; the failure of a computerised life-support system would be disastrous.

A true understanding of risk requires risk management if it is to be formally addressed.
QUESTION YOUR RISK
Answer the following questions for an indication of whether you should be taking steps to protect your systems, or use the Health Check tool for a more detailed analysis. See Further Help and Advice section.

1. Are you dependent on any single thing (computer, person, building, telephone line, ISP, supplier, shipping agent, haulage firm, etc)?

If YES, you could be putting all your eggs into one basket. Wherever there is a single point of failure, you run the risk of your entire enterprise depending on that element.

Try to reduce the number of single points. Better still, eliminate them by establishing alternative sources of service and supply.

2. Have you ever analysed your business processes in the context of “What happens if this fails, goes wrong, or simply isn’t there?”

You may benefit from good housekeeping advice.

3. Do you understand the threats your business is facing?

You may, for example, be working near an industrial plant that is inherently dangerous, or near an office under terrorist threat, such as a Government building.

Many threats come from unexpected quarters. About half the organisations that have not prepared incident management or crisis management plans and then suffer an incident fail to survive more than a year.

4. How would you reconstruct your company information should it be lost or corrupted? How long would this take, and how long could you survive in the meantime?

If you don't know, or haven't prepared any contingency, you run the risk of catastrophic failure, as most businesses are totally dependent on their information.

5. Do your staff know who to call if there is a major incident? Do you know the home and mobile telephone numbers of all your key people?

Remember that if you keep your contact details in the office, these become useless if a fire affects your premises.
Systems Failure – Recovery

The key to recovery from a systems failure is preparation. If you have already taken steps towards prevention, or (ideally) looked at Business Continuity Management, you will be in a much stronger position to handle the unexpected.

If you can determine which of your business processes are critical, and which are not, you will be able to provide some priority for recovery.

It is unusual for even the most prepared companies to restore all services immediately after a traumatic event. It can even take time to recover from minor ones.

Criticality is normally determined by how long you can survive without a service. Some need immediate recovery, such as a bank’s online payment system. Others can wait – you can manage without a lot temporarily.

Recovery from a systems failure, or indeed any form of information security breach, is based on the following principles of incident management or, in the worst case, crisis management:

- Qualification
- Containment
- Assessment
- Countermeasures

**QUALIFICATION**
Determine the size of the incident and what effects are likely. The best way to do this is to assemble a response team (often referred to as an Incident Response Team or IRT). Members should include:
- Operational managers within the areas affected
- HR
- Facilities (if buildings and utilities are affected)
- PR or corporate communications (if you have these)

Team members should be able to make decisions for their own area. There’s little point in using someone who needs to seek permission or authority before proceeding; time is often of the essence in recovery situations.

**CONTAINMENT**
Make sure there is no further damage. Consider isolating affected systems and premises if the incident is ongoing. Report the incident to relevant internal and/or external bodies.

**ASSESSMENT**
- Establish the extent of damage and obtain whatever records (electronic or otherwise) of the event that you can, including eyewitness statements.
- If you think there may be some malicious intent behind the event, consider forensics procedures.
If the event is highly technical, contact the most articulate, technically capable person known to help analyse and describe the important issues. Remember that the best technical person is not always the most senior person.

**COUNTERMEASURES**

- If possible, a collective decision should be made on countermeasures, although this is not always possible, due to time constraints or disagreements. Sometimes you just have to bite the bullet.
- Apply countermeasures in risk priority order. Keep monitoring to make sure the countermeasures don’t make anything worse.
- A parallel initiative should be communicating information on the event to whoever needs to know. This can range from members of your family and staff to multi-national news corporations.
- Those who need to know should be told in a timely manner, through the appropriate channels. Larger organisations should consider using their PR facilities.

**Systems Failure – Prevention**

Steps needed to help prevent systems failure are the same, no matter the size and scale of the company involved.

The following points provide a high level guide to preventing (or at least, reducing the likelihood of) systems failure:

- Perform a risk analysis. This can be a sophisticated and extensive exercise, but it is essential to:
  - Establish the importance of each system or system element
  - Work out what could stop them operating
  - Implement appropriate controls to minimise the disruption caused by any untoward event
- Take regular backups of information and store them away from the system. Establish how long your company can tolerate a system failing (a day, a week?) and make sure your backups allow you to recover before that time elapses.
- If you hold sensitive information, remember to apply appropriate security to your backup media.
- Make sure you have access to alternative machines to run your systems and hold your data should you lose premises through a catastrophic event, such as a flood or a fire.
- Consider making a mutual support agreement with another organisation, preferably one that is unlikely to suffer from the same event as yours (i.e. they aren’t next door, they use a different power supply, and they won’t be flooded by the same river).
- Make arrangements with hardware suppliers for rapid installation if you are running a time-sensitive operation. Some companies specialise in providing support premises and equipment, normally on an annual charge basis (a bit like an insurance policy).
Establish sound fire prevention and detection systems. You should also consider looking at water detection systems, especially if you operate in a high-risk flood area.

Environmental risk should form part of your initial risk analysis. Environmental issues should include:

- Investigating neighbouring industrial concerns, to see if they carry a high-risk (for example, a chemical works)
- Investigating neighbouring companies to see if they might be the targets of civil unrest (for example, animal testing, nuclear power, etc)
- Checking local conditions by contacting the local authority, who normally have information on environmental risks and often make a local emergency plan available

Look for single points of failure. These can be telephone exchanges, power supplies and road transport links. If you are dependent on a single supplier for key goods or services, make sure you know who they are.

Having identified single points of failure, look for alternative suppliers, or seek insurance against them failing.

Consider a UPS (Uninterruptible Power Supply), as these not only reduce the impact of a real event, but also protect your computer systems against voltage spikes that can corrupt data even if they don't take your system down.

Be aware of the details of any software support contracts. If you need specialist help at 4am on a Saturday, you may find yourself in trouble if you haven't made provision for it.

Make sure you have appropriate licences and support agreements in place for all hardware and software. Try to avoid invalidating any warranty agreements, as this can severely hamper support.

Make sure all staff know what to do in an emergency and that they have the means to contact you if getting to the office is made difficult or hazardous.

Case Study - London Power Failure

THE ORGANISATION
A range of businesses, covering multinationals to one-person companies, based in Central London.

WHAT HAPPENED
A London power company was experiencing severe problems in providing a stable supply. Voltages kept “spiking” and there was intermittent total loss of supply. None of these events was predictable (other than in its unpredictability).

This event went on for several weeks until the service was stabilised.

IMPACT
Large companies which were affected had provided themselves with powerful generators to provide a second source of supply. They coupled these with sophisticated Uninterrupted Power Supply (UPS) facilities.
The smaller companies affected did not have the capacity to deal with the event in this way, as UPS and generators are expensive and outside their financial reach.

These companies suffered constant losses of processing and normal service to clients was disrupted. There were multiple cases of data corruption, as power-down sequences were not carried out and systems crashed as they lost power.

Companies had to rework input, clean corrupted data and pacify disgruntled customers. Many lost work, had increased operating costs and lost client goodwill. It is possible that some companies went out of business due to these increased overheads.

**LESSONS**

- Back up your data. Never rely on a single store of information.
- If your data stores are large, prioritise what is essential and make sure this is backed up in a structured manner that makes rebuilding priority systems and applications as quick and easy as possible.
- Consider a small-scale UPS. It may not allow you to keep your systems running, but it will allow you to perform a controlled power down. It will also reduce the impact of voltage ‘spikes’ and other variations in current.

**Checklist – How to guard against Systems Failure**

**RISK**

- Are you dependent on any single thing (computer, person, building, telephone line, ISP, supplier, shipping agent, haulage firm, etc)?
- Have you ever analysed your business processes in the context of “What happens if this fails, goes wrong, or simply isn’t there?”
- Do you understand the threats your business is facing?
- How would you reconstruct your company information should it be lost or corrupted? How long would this take, and how long could you survive in the meantime?
- Do your staff know who to call if there is a major incident? Do you know the home and mobile telephone numbers of all your key people?

**RECOVERY**

- Qualify the incident – determine the size of the incident and what effects are likely
- Contain the incident – ensure there is no further damage and report the incident to relevant internal and/or external bodies
- Assess the incident – establish the extent of the damage and seek technical advice where necessary
- Apply countermeasures (but ensure these don’t make things worse) and ensure that anyone who needs to know is informed in a timely manner
**PREVENTION**
- Perform your own risk analysis
- Ensure that important information is backed up on a regular basis
- Ensure that sensitive information is maintained in a secure environment
- Plan for ‘worst case scenarios’ such as fire or flood
- Ensure that hardware and systems maintenance contracts are sufficient for your business needs
- Avoid single points of failure
- Make sure all staff know what to do in an emergency

**Further Help and Advice**

<table>
<thead>
<tr>
<th>General</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check Tool</td>
<td><a href="http://healthcheck/">healthcheck/</a></td>
</tr>
<tr>
<td>publications</td>
<td></td>
</tr>
<tr>
<td>DTI Information Security</td>
<td><a href="http://www.dti.gov.uk/bestpractice/infosec">www.dti.gov.uk/bestpractice/infosec</a></td>
</tr>
<tr>
<td>business advice pages</td>
<td></td>
</tr>
</tbody>
</table>

For more further help and advice, please open the pdf titled Information Security: Further help.